ISSN (Online) : 0975-1432
ISSN (Print) : 0975-153X
DOI: 10.18311/gjeis

Vol 2 | Issue 1 | Jan-June 2010

global Journal of ENTERPRISE INFORMATION SYSTEM

GJEIS

Dr. Subodh Kesharwani
Editor-In-Chief

www.gjeis.com

Co-Published

Scholastic Seed Inc.
e-Publishing Aggregator & Periodical Mentor

Karam Society

Global Journal of Enterprise Information System

Published since 2009

Global Journal of Enterprise Information System (GJEIS) is being published as a co-published peer-reviewed journal by KARAM Society and Scholastic Seed Inc. The subjects covered by the journal are IT linkages in business, finance, marketing, management, organizational behaviour, buyer behaviour and other relevant fields. It also covers many aspects in Information System and related areas. The journal provides an international forum for the exchange of ideas, principles and processes concerning the application of diverse topics of EIS to organizations, institutions and the world at large. GJEIS considers research submissions in several categories but revolves around three buzzwords Enterprise Information and System.

Editor-In-Chief : Dr. Subodh Kesharwani

Online ISSN	:	0975-1432
Print ISSN	:	0975-153X
Frequency	:	Quarterly
Publishers	:	Scholastic Seed Inc. & Karam Society

Subscription rate for the year 2019

Online Only (Single Volume) :-	INR 4,000 | $300	Single Issue Online :-	INR 2,000 | $150
Print Only (Single Volume) :-	INR 12,400 | $320	Single Issue Print (Coloured) :-	INR 5,100 | $180
Print+Online (Single Volume) :-	INR 13,000 | $470	Single Issue (Print+Online) :-	INR 6,000 | $200

Pay Per Article (Online) :- INR 250 | $20

Contact: Scholastic Seed Inc., 6, M G Road, New Delhi 110 030, India

Tel: +91-8929-03-7575 | Email: scholastic.seed@gmail.com | Web: www.scholasticseed.in

Kedar Amar Research and Academic Management Society known for it's acronym KARAM Society has been established in the year 2009 keeping in dream the empowerment and comprehensive expansion needs of society. The society has been established as a "Not for Profit" Company under the societies registration act, 1860 with a Registration no. S/65067/2009. In the present state -of-affairs, the KARAM Society engaged in the advancement of medical knowledge and provision of assistance to medical students and professionals.

The mandate behind KARAMS is to make certain transparency, accountability and adherence to corporate governance norms. Recently KARAM Society had put it's ware bouts in an online publishing and collaborated with Open Magazine Inc. and Publishes two hard core empirical research magazine on information systems (www.gjeis.org) and in medical science (www.agems.in). Both the Research magazines are now available in a Brick-&-Mortar mode also with an ISSN and eISSN Numbers respectively. The rationale of the KARAM Society is to promote empowerment and inclusive development with an emphasis on social, digital and financial inclusion; strengthening of delivery systems and participatory democracy for bringing about a systemic change to help meet development objectives better. During the past two decades founder members of KARAM Society have travelled transversely the country to learn critique and encourage social, digital, medical and financial inclusion. In the process, knowledge repositories have been created on what works-the most excellent practices-actively engaging all stakeholders from policy makers and civil society to ordinary citizens. The KARAM will allocate this knowledge for progression and nation-building all the way through e-learning modules and virtual platform for practitioners and publishing video documentaries on our portals. Recently it had started new portal http://open-journal.com which is backed by the gamut of great academician from different part of the world.

In the last few years KARAM Society conducted numerous health camps in a charitable mode in a various districts of Haryan, Rajasthan, Utta.rpradesh, New Delhi, etc. which are organized with support from corporate, civic bodies, the government, NGOs and individual volunteers. KARAMS has conducted over 75 general health camps till date and has benefitted more than 25,000 people directly. In line with the policy to provide healthcare services to the community around our facilities, KARAM Society has started a Mobile Medical launched Mobile Medicare Unit (MMU hereafter) to address the health concerns of older persons living in urban slums. Technical aids are provided to the poor elderly that could improve their quality of life and make them independent. Eye camps are organized every year now and then to screen beneficiaries for cataract. Awareness about diseases and healthy living is an important component and constant effort byKARAM Society is being made in this direction. The team of KARAM SOCIETY India consists of a medical doctor, a community health mobilizer, a pharmacist and a social protection officer. The team will not only provide curative medical services but will also raise public awareness on preventive and promotive aspects through awareness generation andmultidisciplinary medical camps, etc.

KARAM Society best practices have been documented as information cards, video case studies, policy and white papers that are consistently shared with group of people at great, so that it can become a wider learning process. Having done all the above driven by individual enthusiasm and excitement, the members now felt the need to create an institutional Mework that not only takes this work forward and emerges as a key expansion institution but also helps in facilitating implementation mechanisms such that the benefits of wide-ranging development are actually received by society.

6. M. G. Road,
Opposite Bhartiya International Ltd. (E-52)
New Delhi- 110030, India
Phone: +91-11-41431051
Mobile: 8929-03-7575
Email: karamsociety@gmail.com

Online Digital Era of EIS

Message from the Editor-in-Chief's Desk

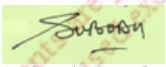
It's my privilege to welcome you all once again to celebrate the first Anniversary of GJEIS after publishing two vital issues in a year 2009. The theme dedicated to this issue itself is "Online Digital Era of EIS". This is a first issue of 2010 valid from January-June 2010.

Assortment expansion is a fundamental process in creating and building AN ARCHIVE, be it in an Institution, college, school or a public library. It is a well planned movement for which a well defined policy is essential. Online Digital is a step in this direction.

Making articles pertain to Digital and online theme explicitly answers some exceptionally imperative questions: how to make your enterprise an edge above competitors', Thinking out-of-box so to do the right thing at a right time. We have got a hard core empirical paper and a theme based conceptual papers SoA, Information Security, CAD Facilitating aesthetic design, Role of XML in Securing e-commerce, Flexible Manufacturing System, etc..

I, therefore, respectfully ask that you consider preparing a submission for our Journal. Because submissions are peer-reviewed and blindly evaluated. I recommend that you prefer on-line submission rather than mailing on gjeis.ejournal@gmail.com

I wish to see GJEIS develop into an information based journal with the balance changing toward research communication rather than remain a bulletin. The success of this enterprise depends on your response. I would appreciate your feedback. Once again grateful for developing a faith in a GJEIS.



Dr. Subodh Kesharwani Editor-In-Chief [GJEIS]

gjeis.ejournal@gmail.com http://www.ejournal.co.in/gjeis

30th June 2010

Insight of Online Shopping Trend: *An Empirical Study with relevance to Bahrain*

Dr. Akram Jalal

Chair of MIS Department, College of Business and Finance, Ahlia University, Kingdom of Bahrain

ajalal@ahliauniversity.edu.bh

Mazen Al-Maskati

College of Business and Finance, Ahlia University, Kingdom of Bahrain

contactmzn@gmail.com

ABSTRACT

Online Shopping is growing globally. However, there may be notable differences in the way people engage the online marketplace based on such factors as age, gender, and educational background (among others). This research focuses on the expanding trend of electronic retail (e-tail) in Bahrain. It examines various factors such as availability, knowledge, awareness, security and customer service which are expected to have an impact on online shopping popularity among different age groups and their educational background. The study challenges the growth of e-tail in Bahrain's heterogeneous market and highlights that the main dependencies that affect it can be either related to technology availability or lifestyle perspective of Internet users. The study hypothesizes that the highest online shopping activity is not sustained within a specific age group.

The research also discusses the advancement of online shopping in a country like Bahrain and how the business trend can be transforming from retail to e-tail. In conclusion it attempts to forecast the move towards e-tail and highlights the underlying factors such as product variety, cost, security and customer service. Another area that is moderately explored is online banking usage which is an area that is closely related to e-tail as it requires similar mechanisms.

KEYWORD

Online, E-commerce, E-tail, Customer, Technology, Bahrain, Credit Cards, Internet

Preface

Before the 1990s, consumers had to go to great lengths to acquire things that made their life better. As time went by retailers and marketers continuously tried to come up with inventive ways in order to get their customers what they want. Along the way various technological advances helped guide the way to e-commerce. Newspapers, magazines, radio and television all helped pave the way for eager consumers to look for what they wanted to purchase and where they wanted to purchase it. Various mediums such as paper catalogues, telephones and postal services combined to allow the public to shop at the comfort and tranquility of their own homes. But the ultimate shopping experience was yet to come. It wasn't until the mid 1990s that businesses found the most ideal way to serve their valued customers. It took the combination of the pioneering technologies at that time: the personal computer and the Internet, to launch the true future of the electronic retail marketing. From that bubble burst started a whole revolution of technological advancements towards the shopping experience for both retailers and customers.

The fundamental concept behind Electronic commerce (e-commerce) constitutes the use of Information Communication Technology (ICT) to exchange of products and services between businesses, groups and individuals while facilitating and maintaining their external activities and relationships. This view has been supported in the work of **[Davies[i], 2004]** and [**Louis[ii] Et. Al, 2005].**

Online shopping (also known as online retail or (e-tail) which extends from e-commerce can be summarized in the act of buying or selling goods, items, products or services through the Internet while using many different media forms. Online shopping has indeed evolved mutually with technology. Thus, Marketing Charts on Nielsen Research (2008) and Celent Report Figures published by Celent.net (2006) have both shown that it has become so popular that more than 85% of the world's online population has used the internet to make a purchase according to the latest Nielsen Global Online Survey on internet shopping habits. "When The Nielsen Company conducted its first global survey into internet shopping trends in 2007, approximately 10% of the world's population (627 million) had shopped online," said Bruce Paul, VP, Customized Research, Nielsen US. "Within two years, this number has increased by approximately 40% (to 875 million)." As technology is further expanding worldwide it is allowing people to access the Internet and thus engage in online shopping. One must only have an Internet connection and a method of paying online perhaps through a debt or credit card. With online banking further facilitating bank account accessibility to customers the e-tail concept is growing more efficient than traditional retail. While credit cards seem to be the most popular means of paying for online goods and services there is in fact many different ways such as postal money order, SMS billing, cash on delivery or even various types of electronic money such as PayPal. Celent Research claimed that alternative online payments accounted for almost 26% of e-commerce in 2009 and will remain to grow in the future.

In the context of this research online shopping, electronic retail (e-tail), e-commerce and e-buying will all refer to the former description.

The significance of this research can impose a great deal of help to the government of Bahrain and business entrepreneurs by exposing the scale and scope of the required approach to the e-business marketplace. When you understand who the people that are adopting online shopping and for what reasons they are using it instead of traditional retail can lead us to visualize a target in the market and assist in overcoming implementation challenges. The outcome could also suggest further research for global web vendors and website designers.
In the following section we will look at the advancement of Bahrain becoming a future e-business hub. Later in the Literature review section we attempt to compare similar researches conducted in a global scale that identified the age group brackets and educational level of online shoppers. We take a closer look at key examples to set a comparative discussion between the traditional retail market in Bahrain and the move towards the pure e-tail in Bahrain market as we look into some live examples.

The research will attempt to hypothesize and measure the adoption growth of online shopping trend in Bahrain through an empirical quantitative measure and attempt to identify which age groups and educational background as factors that stimulate it. A complete analysis of the results will be given under the findings and analysis section.

Finally a conclusion and recommendation will be provided for further studies in this discipline.

Background

In a business world increasingly defined by global markets, connected consumers and volumes of digital information, The GCC (Gulf Cooperation Council) – despite being from the third world nations - stands as one of the most imperative yet eccentric global economical role players in the world. In particular, the consumer expenditure is prominent to be one of the highest when compared to all other countries in the Middle East. Consumer expenditure is marked as a multi-billion size industry in this region.

In a 2006 a study conducted by Abu Dhabi-based Arab Monetary Fund (AMF), Bahrain alone emerged as the fourth largest spender in the Middle East despite its relatively low oil wealth, with private consumption standing at $5.6 billion or average of $7,587 per person. Based on Business Monitor International (BMI) the traditional retail sales in the Middle East countries in 2009 amounted to an estimated US$412.28bn while the total consumer spending for the region amounted to US$704.94bn. In 2009 Bahrain's market share stood at 0.6% compared to the Middle East and is expected to increase to 0.8% by 2014. (Bahrain Retail Report Q2, 2010).

In 2005, 71.2% of the Bahraini population was described by the UN as economically active, with 40.7% in the 20-44 age range crucial for retail sales. By 2010, 72.7% of the population is expected to be economically active but the proportion of those in the 20-44 age band is forecast to fall to 39.9%. A very high level of urbanization is contributing to a vibrant retail sector. In 2005, more than 90% of the population was classified by the UN as urban, and this is forecast to increase to 91% by 2010. About 89% of the population lives in the two principal cities of Manama and Muharraq. (Bahrain Retail Report Q2, 2010).

Exploiting aggressive advertisement and competitive marketing campaigns retail businesses in the region magnetize the average Middle Eastern countryman into spending. Money is spent on shopping, entertainment, luxury, telecommunication, transportation and many other obligations from main household goods and products to ongoing contracted services. With all this in perspective local and global businesses started to redesign their vision to extend their ventures and start looking into alternatives to further expand and grow in a challenging market such as the one in Bahrain. Thus, even with the credit crunch augmenting worries over average consumer expenditure and unemployment rates drastically increasing, it has become essential to overlook such issues by looking into alternatives when it comes to consumer expenditure on retail.

Many banks, financial institutions and businesses understand that their customers continuously demand more satisfaction. They expand their customer services to cover more ground and provide extended exposure to facilitate their reach to services and products. Hence, online banking solutions such as the ones provided from various Bahrain based banks such as Bank of Bahrain & Kuwait (BBK), HSBC or Ahli United Bank (AUB) has opened a whole range of new customer service possibilities.

Why Bahrain?

Bahrain is considered to be an emerging nation, which has recently entered into a significant period of development, growth and transition. This has led Bahrain to a market revolution in which it is marking its intentions in becoming the new Middle East hub for the global financial sector. Even with the recent conditions in the global financial market, interest to establishing a presence in Bahrain on the part of international institutions remains strong. Central Bank of Bahrain has licensed over 400 banks and financial institutions (as of 30 April 2010) which reflects the confidence of these companies in Bahrain's potential as a leading financial center. With ongoing attractive infrastructure development, the instigation of strong government laws that protect overseas investors together with the establishment of regulatory firms such as the TRA (Telecommunication Regulatory Authority), LMRA (Labor Market Regulatory Authority) and the e-GA (e-Government Authority), Bahrain is indeed confirming its strong desire to lead the region into a new business revolution. CEO of the e-Government Authority Mr. Mohammed Al Qaed agrees that well-developed comprehensive electronic national portals are a significant factor in the progress of nations when it comes to simplifying processes, increasing

efficiency across society, and facilitating and developing business and commerce. Today the UN e-Government Readiness Report ranks Bahrain as the first in the Middle East, third in Asia and 13th internationally in e-Government. (AMEINFO, Gulf e-Commerce Forum 2010)

The emergence of the Internet in Bahrain to the public since 1994 has played a major role in exploiting new opportunities and markets for many businesses. Today the Internet is considered to be an essential part of every business infrastructure and with the help of web technologies infinite advancement they are able to provide customer satisfaction easily and efficiently through a multitude of techniques.

World Economic Forum (2009-2010) showed that today the Kingdom ranks 29th out of 133 studied countries and second in the GCC in technological competitiveness, according to a 2010 Global Information Technology Report. As of September 2009, almost 55 percent of the Kingdom's population was using the Internet, the International Telecommunication Union (ITU) reports. To further overcome the difficulties that enterprises are facing when developing their e-business initiatives the e-GA is slowly yet confidently providing the appropriate policies and laws. Despite that, the lack of awareness and Internet business development remains to be a key issue that waits to be resolved in order to adopt e-business approach. Bahrain Internet Society (BIS) chairman, Ahmed Albalooshi describes that the biggest issue for e-business in Bahrain lies in the business-class connectivity, its quality and affordability. The average Internet speed in Bahrain is 1.56 MB/sec (TRA) as against the Asian average of 4.12 MB/sec and the world average of 5.37 MB/sec. In a BIS survey, 71 percent of respondents said that they weren't satisfied with the overall quality of Internet service. The majority was disgruntled with the threshold limit of their Internet package and thought the quality of service needs to improve. Nevertheless, Bahrain remains to have an adequate business environment and there is a lot of potential from the government to help support and facilitate local e-businesses to emerge. Ahmed Al Balooshi (2009)

Currently, there are no statistics for Bahrain when it comes to e-tail. According to Nielsen, the global e-commerce sales will contribute to 13 percent of overall sales by end of 2010. Eric Schonfeld (2010) indicated that e-commerce sales in the U.S. will keep growing at a 10 percent compound annual growth rate and 11 percent in Europe through to 2014. There is a lot of room for improvement in tempting consumers to cross over between e-tail and retail. A lot of businesses in Bahrain adopt a Western style retailing, hence, try to imitate and copy those market trends in the US and EU. Still most business owners, retailers and even customers remain on brick-and-mortar approach when it comes to shopping. Despite that with the growth we see from the western market towards online retails, it is still safe to say that e-business is bound to materialize eventually in Bahrain. The researcher will attempt to prove this by showing the influential factors of online shoppers in the Hypothesis number 3 from the next section. From the results we can perhaps deduce that there is no dearth of e-buyers currently shopping online from international e-business sites in Bahrain.

Hypotheses

The researcher has set out to measure the validity of three hypotheses. The attempt is to identify that the highest online shopping activity is not sustained within a specific age group and in which educational qualifications has no significant affect. In general we might look into the main constraints that make people engage in online shopping, but in a country such as Bahrain there are perhaps additional influential factors that differentiate it from comparing it to the rest of the world. In particular is the adoption of online shopping focused on specific age groups. The hypotheses can be described as follows:

H1: There is an acceptable degree of willingness among the general public of Bahrain to adopt online shopping

H2: Age is not a factor affecting the adoption of online shopping in Bahrain

Literature Review

There has been a lot of research done on online shopping most of it focuses on technical or psychological factors. Yet, there is still a need for closer assessment on e-commerce in specific countries. Swinyard & S.Smith (2003) agree that academic literature for Internet shopping has not reached mature development. Most of the literature reviewed had no focus on Bahrain online shoppers which indicates that Bahrain market has no

major global significance towards online shopping trends. The most comprehensive related researches found were conducted for US, EU and some Southeast Asian nations due to the fact that the greatest percentages of online shoppers seem to come from such nations. Nielsen found that among internet users, the highest percentage shopping online is in South Korea, where 99% of those with internet access have used it to shop, followed by the UK (97%), Germany (97%), Japan (97%); the US is eighth, at 94%. In South Korea, 79% of these internet users have shopped in the past month, followed by the UK (76%) and Switzerland (67%); the US is at 57%. (Marketing Charts on Nielsen Research, 2008)

Today with the recent global financial crisis, many of the leading e-commerce countries are now facing a shifting trend as luring expectations of introducing additional costs from registration and taxation on online retailing are coming their way. Beijing Bureau of Industry and Commerce announced back in August 2008 that web stores hosted in China will have to comply with tax policy but this has yet to be enforced as no web store has been registered yet until February 2010. (People Daily News, 2010)

In a similar case, the US congress has been attempting to file a policy which will privilege all states to tax online shops since 2007. Executive Director of Shop.org, Scott Silverman highlighted that introducing such costs will hinder the growth of e-tail as it compromises the advantage it has over brick-and-mortar traditional approach in retail.
In the other hand, Bahrain seems to be on a different level (even though it has also been hit by the global financial crisis) however would prove to appeal as an ideal location for such research to be conducted revealing much more accurate results due to the following facts:

- Dynamic business development & high level government support
- Small yet diverse Population (people share a lot of commonalities and are easily reachable e.g. Bahrain 2010 census will be conducted in a very short time)
- Location & land size (affecting the ease of delivery and meeting customer satisfaction)
- Lifestyle (consumer expenditure is high and has a rising potential)
- Market and consumer needs (conducting business is open, safe and protected, competitive and challenging)

An interesting research which recognizes some statistics of online shoppers in the Middle East was conducted by Pew, Nielsen and Forrester; in their global online shopping survey they calculated that 35% of the Middle East online shopping community had made purchases online within the last month (December 2009).

Formerly when we talk about online shopping one would assume that online shoppers would be high capacity internet users and possess higher education levels such that they are more aware and more knowledgeable. In the context of this research the focus mainly revolves around the aspect that Bahrain online shoppers do not lie in a certain age group or having a certain level of educational background.

Looking at relevant researches we notice that the few who involve age groups as a factor to the willingness and adoption of online shopping. Swinyard and S. Smith suggest that online shoppers are younger, wealthier, better educated, have higher computer literacy, spend more time on their computer, spend more time on the internet, find online shopping to be easier and more entertaining and are more fearful of financial loss from online shopping. Though their study seems comprehensible, yet within their studied sample the average age was approximately 49 years and that three-quarters of all their respondents were household owners and are married.

Pew Research Center surveyed (results for December 2009) the US online marketplace and found that 65 percent of Americans who shop online come from the age bracket 30-49 and 70% are with at least a college education. A similar survey conducted on a global scale found that 56% of online shoppers are females and the average age of online shoppers is 42. Their research also concludes that the highest percentage of internet users that shop online are between the age of 33 and 44. There could be many reasons behind these figures. Online shoppers would appear to be more mature, more financially stable, and knowledgeable in some level just as Swinyard and S. Smith suggested. Parallel to that, Bigne (2005) claims that if we look closely at the demographic characteristics of the in-home shopper, in general, the higher the level of education, income, and occupation of

the head of the household, the more favorable the perception of non-store shopping. This can be applied to online shopping perception too.
Still one could argue that age as a factor cannot be taken as a dependency in correlation to online shopping adoption. This is because countries around the world have different population growth and age group structure. For example Bahrain population pyramid indicates that the highest percentage of the population is to those of age group between 35 to 39 years where as in the US it is between 40 to 44 years. This differs from country to another and hence a consensus study needs to be conducted on each country separately.

Moving from Retail to e-tail

To indicate that there is actually an increasing growth in Bahrain population in adopting online shopping there are few examples we can focus on. First of all, (Business Monitor International) BMI's Q210 Bahrain Retail Report forecasts that the country's retail sales will grow from an estimated US$2.66bn in 2009 to US$5.26bn by 2014. Key factors behind the forecast growth in Bahrain's retail sales are a favorable long-term economic outlook as mentioned earlier and the growing interest in Western styles of retailing and a steady rise in disposable income and consumer expenditure. Bahrain's nominal GDP in 2009 was US$15.13bn, with that year's decline of 0.1% expected to turn into growth of 1.3% in 2010 as the economy begins to recover. Average annual GDP growth of 1.95% is predicted by BMI between 2009 and 2014. With the population forecast to increase from 1.01mn in 2009 to 1.09mn by 2014, GDP per capita is predicted to rise to US$26,547. (Business Monitor International, 2010)

E-tail vs Traditional

There are various reasons both for customers to either choose traditional over electronic retail or vise-versa. Some may argue that shopping online is more transparent while others insist that traditional retail gives a customer the full experience of shopping. Yet, by understanding what Beynon-Davies, Falk, Louis K.; Sockel, Hy; Chen, Kuanchin, we know that the common factor for e-commerce to remain successful a business reputation needs to be maintained.
In Bahrain the e-tail market is still in its infant stage. It would take time for concepts of e-tailing to be adopted by e-businesses here. To understand where it stands the researcher compares the brick and mortar approach with few real life examples of e-businesses in Bahrain:

Brick & Mortar

Bahrain market is different to others within the GCC. It is much more competitive and challenging when it comes to retail. There are many factors that play a role in this, perhaps it is the size of the country or the population density and diversity. The mall-to-human ratio in Bahrain surely challenges even the most shopaholic of nations. The mall concept has been developed such that it provides a satisfaction pleasure to customers and ensures a successful experience to retailers. Retail sub-sectors that are predicted to show strong growth over the forecast period include automotives, with sales forecast to rise by more than 20% during the forecast period, from US$0.86bn in 2009 to US$1.03bn by 2014. Sales of consumer electronics are predicted to increase from US$0.44bn in 2009 to US$0.55bn by the end of the forecast period, a rise of 25%. Over the counter (OTC) pharmaceutical sales are expected to increase by almost 20%, from US$0.013bn in 2009 to US$0.015bn by 2014. Bahrain's retail sector is booming and is expected to contribute largely to the kingdom's gross domestic product in the future. (Business Monitor International, 2010)

Moving towards online shopping

There are many challenges facing the adoption of online shopping in Bahrain. E-businesses are not very fond and comfortable with adaptation of the available payment systems provided from financial institutions and banks in Bahrain. Yet, the government has taken the initiative to impose it and use it publicly. People in Bahrain are aware of transaction facilities offered by available credit cards. But they remain a bit dubious with using credit cards comfortably for online payment systems. Hence, different payment options are made available. Perhaps cash on delivery and online banking can give a lot of assurances. From that perspective we tend to see many people using international online financial services such as PayPal which can also be adapted as a form of payment in a localized e-tail shop. One interesting e-business currently functioning in Bahrainis is Communication Channels (com-

channels.com) which sells computer peripheral, network equipment and photography gear. Their service is slowly yet efficiently providing customers the experience of online shopping. Perhaps their web site is still in a premature state compared with global e-business enterprises such as amazon.com, but the fact that Communication Channels provides a localized online shopping experience to its customers gives some hope. Since its launch in October 2009, its Bahraini founder Ammar Al Haiky is still working hard to establish the security gateways with BBK's CrediMax Online Payment Services. Today Communication Channels sells to customers from all around the GCC with most of its customers coming from Saudi Arabia.

From another perspective Bahrain e-government portal (Bahrain.bh) has opened a new channel of facilitation to the citizens of Bahrain. The portal provides over 120 services including the electricity of water bill payment service, payment of traffic violations and renewing vehicle registrations. Since its inception (May 2007), the e-Government Portal has registered over 21 million visits (April 2010), processed over 180,000 financial transactions at a total value of BD 11,926,067. To further expand and facilitate the e-government services for all citizens (customers), the government has established a network of kiosk gateways all over the island. It has fully standardized its web site policies and processes while continuously running auditing and security checks to assure citizens that using the e-government is safe and secure. Of course citizens can still go through traditional channels, but the portal provides a unique and comprehensive experience that is less time consuming and very efficient.

In another case, due to the global downturn a lot of businesses have defaulted. Many had to close their businesses to pay off expenses and loans. Conducted a quick survey on DVD rental shops around Bahrain revealed how comprehensive this issue has reached as many of them had to close in a very short time during 2009. Worst, it has become a pastime trend to Bahrain lifestyle to go to rental shops. In spite of that an e-business called (Film2Go.net) which uses the Internet to provide DVD rentals at ease in Bahrain still stands. This is a good example of online shopping for Bahrainis, thus, Film2Go seems to be in the business of convenience. Hasan Haidar, one of the key founders agrees that the key advantage of the service is the delivery system at its heart. It is much easier to search for a movie title online rather than digging through hundreds while looking at DVD cases. Hasan believes that there is a significant opportunity in providing convenient, easy to use and great value service using the internet as the primary medium for interaction here in Bahrain. A lot of Bahrainis already use online service heavily such as Amazon, eBay and Google, and it should be even more convenient for them to use a locally based service. Our region is significantly behind the rest of the world in the development of locally based e-commerce services for consumers. We are hoping that this is just the first step in a greater leap towards harnessing the capabilities of the online world for our region. Bahrain has the skills and ambition to lead the rest of the region in the development of locally based online services.

Research Method

The research uses a quantitative approach in which a digital online form was created using Google Documents in a questionnaire style. The link was then shared and publicized to Bahraini's through email channels targeting different working sectors as well as posting it on discussion forms and different society groups. Once a subject would answer the questionnaire the raw data will automatically be logged in a spreadsheet which can be only accessed and downloaded by the researcher. Since the questionnaire form was to be submitted online it guaranteed two things. First of all it targeted people who have internet access even though they are not necessarily considered online shoppers. Secondly, the collection of data will be done automatically, efficiently and that there won't be any loss of data as all questions need to be answered before submitting.

The first part of the questionnaire was related to demographic details while making sure to include a breakdown for the age groups and a break down for the education background. The second part of the questionnaire was designed to measure the subject's willingness to adopt online shopping. Eight questions resembled eight willingness factors and can be summarized from the diagram below:

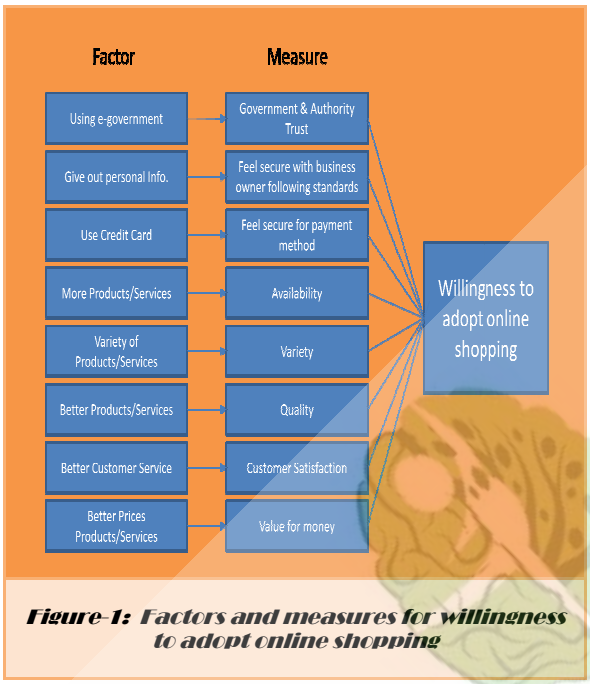


Figure-1: Factors and measures for willingness to adopt online shopping

Willingness will be combined into a hypothesis (W1) or H1 in this case.

The questionnaire yielded 97 responses in total during a one week collection period.

Results

The population demographics indicate that the majority of the sample (56.7%) is male. Most of the sample came from either Banking & Finance (21.6%) or Information Technology (18.6%) sectors. This is perhaps why it is noticed that (68%) of the sample actually use online banking and that more than (80%) are comfortable in using a credit card for shopping online with a trusted website. When asked how much they use the internet the majority (67%) indicated that they use it more than 3 hours a day. The main purpose of the internet usage goes to reading emails (40.2%) while only (3.1%) indicated that they use the internet mainly for online shopping.

Most of the sample (61.9%) came from the age group (20 to 29 years). The age breakdown was compressed to four groups as the highest group (50 or above) only had two records, therefore it was combined with (40 to 49) and renames (40 or above).

Based on the methodology a new computer value is calculated to indicate the willingness variable. This is done by combining the results for the last eight questions.

Table 1 shows a cross tabulation for the breakdown of Age based on gender:

Table1: Age & Sex Cross Tabulation

			Sex		Total
			Male	Female	
Age	20 or below	Count	4	3	7
		% of Total	4.1%	3.1%	7.2%
	21 to 29	Count	28	32	60
		% of Total	28.9%	33.0%	61.9%
	30 to 39	Count	16	6	22
		% of Total	16.5%	6.2%	22.7%
	40 or above	Count	7	1	8
		% of Total	7.2%	1.0%	8.2%
Total		Count	55	42	97
		% of Total	56.7%	43.3%	100.0%

Analysis

To investigate the willingness of the sample in adopting online shopping we had to combine the results of the last eight questions in to a hypothesis H1. We use a One Sample T-Test analysis to get the statistics in Table 2:

Table 2: One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
W1	97	3.8595	0.53316	0.05413

We can see from Table 2 that H1 was supported as the data indicate from the T-test analysis that there is a high degree of acceptance and willingness from people to adopt online shopping. This is shown clearly by the

mean=3.85 which is greater than 3 and the standard deviation=0.5332

Table 3: One-Sample Test

	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
W1	15.878	96	0.000	0.85954	0.7521	0.9670

From Table 3 we identify that t-test value is (15.878) is greater than the t-table value (3.177) at degree of freedom 96. Also Sig. value is (0.000) hence we conclude that H1 is acceptable.

To investigate the relationship between age and willingness purchase online, the last two age groups were collapsed because of the small number of individuals in these groups. The willingness variable was obtained by adding up scores on the eight relevant questions. One-way ANOVA was used to compare the means of the four age groups on the willingness variable. Table 4 shows the mean and standard deviation of the four groups on this variable.

Table 4: The mean and standard deviation of the willingness variable according to age

	N	Mean	Std. Deviation
20 or below	7	32.29	5.99
21 to 29	60	30.68	4.14
30 to 39	22	31.05	4.50
40 to 49	8	30.63	3.29
Total	97	30.88	4.27

According to this table the means of the groups were fairly close. The largest mean difference was 1.66, which is not large when compared with the standard deviation of the last group whose mean was the smallest. The ANOVA results were consistent with the above results.

Table 5: ANOVA for Willingness mean differences as per the Age

	Sum of Squares	df	Mean Square	F	Sig.
B/W Groups	17.274	3	5.758	.310	.818
Within Groups	1729.241	93	18.594		
Total	1746.515	96			

As table 5 indicates, the mean differences were not statistically significant. It can thus be concluded that H2 is acceptable as the age groups were not different with regard to willingness to make online purchases.

Discussion and Conclusion

Based on the results and analysis of the questionnaire it is safe to conclude that there is actually a high growth of online shopping adopted in Bahrain. Most of the people are in fact utilizing online banking facilities. Furthermore, with the examples mentioned of Bahrain government promoting e-tail as well as several online businesses starting in personal and small businesses there is no doubt that a large sum of the population of Bahrain would gradually start considering more of online shopping.

There is no doubt that brick & mortar retail will still be the favorable approach in Bahrain. Regardless of that on a more personal level, people in Bahrain are high capacity internet users in average as this can be concluded from the research results and the results from ITU (People Daily News, 2010). Even when it comes to traditional retail the study from BMI stated that the age range crucial for traditional retail sales is between 20 and 44 even though it mentioned that this is falling. This would indicate that even with retail there is no specific age group is in the lead. The main argument here is due to the fact that there will always be a specific age group which tends to be the highest

online shoppers in a specific country due to how the population demographics are made.

In conclusion the results provide an optimistic overview on the growth of online shopping adoption trend in Bahrain. A lot of the individuals are already using online banking. Even more are optimistic and willing to use an e-government portal to pay for bills and services. This shows that people in general are comfortable to adopt e-commerce when it is supported and protected by government. Also in contradiction to international studies [12] with age groups adopting online shopping, age groups in Bahrain are almost identical in their approach towards using e-commerce.

Reference

[i] Beynon-Davies P. (2004). *"E-Business"*. Palgrave Macmillan in Houndmills, Basingstoke, Hampshire, New York.

[ii] Falk, Louis K., Sockel, Hy, Chen, Kuanchin. (2005). *"E-Commerce and Consumer's Expectations: What Makes a Website Work"*. Journal of Website Promotion. Vol. 1(1) PP. 65-75.

i. Marketing Charts on Nielsen Research (29 January, 2008). Over 875 Million Consumers Have Shopped Online - The Number of Internet Shoppers Up 40% in Two Years. [Online] Available: http://www.marketingcharts.com/direct/875mm-consumers-have-shopped-online-up-40-in-two-years-3225/ (July 17, 2010)

I. Celent Report: Figures published by Celent.net (2006). [Online] Available: http://reports.celent.com/PressReleases/20060525/OnlinePayments.htm (July 11, 2010)

II. Amy Glass. (2008). UAE tops Arab consumer spending. [Online] Available: http://www.arabianbusiness.com/507709-uae-tops-consumer-spending-study (August 12, 2010)

III. Business Monitor International (BMI). Bahrain Retail Report Q2 2010, (March 2010), Page: 55. [Online] Available: http://www.researchandmarkets.com/research/913386/bahrain_retail_rep (August 13, 2010)

IV. AMEINFO, Gulf e-Commerce Forum 2010 PRESS RELEASE, (Tuesday, January 12 – 2010) "Bahrain is ranked in first position for Arab Gulf countries, third for Asia, and thirteenth at the world level for e-government". Bahrain. [Online] Available: http://www.ameinfo.com/220874.html (August 13, 2010)

V. World Economic Forum (2009-2010). The Global Information Technology Report. [Online] Available: http://www.weforum.org/pdf/GITR10/TheNetworkedReadinessIndexRankings.pdf (August 13, 2010)

VI. Ahmed Al Balooshi, Bahrain Internet Society Chairman, (2009). Bahrain Internet Speed Ranking. [Online] Available: http://internetbh.wordpress.com/2009/07/09/bahrain-internet-speed-ranking/ (August 13, 2010)

VII. Eric Schonfeld. (2010). Forrester Forecast: Online Retail Sales Will Grow To $250 Billion by 2014. [Online] Available: http://techcrunch.com/2010/03/08/forrester-forecast-online-retail-sales-will-grow-to-250-billion-by-2014/ (August 13, 2010)

VIII. [12] Swinyard, William, Smith, Scott, (2003). Why People (Don't) Shop Online: A Lifestyle Study of the Internet Consumer. Research Group, Brigham Young University, United States. [Online] Available: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=10146453&site=ehost-live (August 15, 2010)

IX. People Daily News, China. Online shops facing registration, taxation. (2010). [Online] Available: http://english.peopledaily.com.cn/90001/90778/90860/6883574.html (July 13, 2010)

X. Ryan Gibson on Scott Silverman, Executive Director of Shop.org, (May 2008). Eight Important Online Retail (and Marketing) Policy Issues. [Online] Available: http://www.rimmkaufman.com/rkgblog/2008/05/28/online-policy-issues/ (August 10, 2010)

XI. Bigne, Enrique.(2005) The Impact of Internet User Shopping Patterns and Demographics on Consumer Mobile Buying Behaviour. Journal of Electronic Commerce Research. Vol.6, PP. 3.

Analytical Resarch on Indian Online Banking and Users' Privacy

Dr. Abha Chandra

Reader (Statistics), Meerut College
Ch. Charan Singh University, Meerut
abhachandra09@rediffmail.com

Mrs. Vinita Sharma

Assistant Professor (IT), New Delhi Institute of Management, New Delhi
vinitasharma75@rediffmail.com

ABSTRACT

Privacy preserved e-society consists of three intangible factors firstly applications, which have data to share with authorized clients; secondly clients who want data that contains in the applications and finally the privacy control factor which is required to maintain records about the purposes. People now a day are more concerned about their personal information, which is supposed to be leaked out from the organizations to which they are trading online. There are many types of banks in India, which provide net banking or online banking service to the consumers through Internet. The significant point to be noted with respect to these banks is to make their personal and financial information totally secure so that no unauthorized person or organization should acquire their data to mistreat over the Internet. An empirical study is conducted to evaluate the existence and format of privacy policies of different banks of India in conducting online banking through their websites. The endeavor of this paper is to throw more light on the study, methodology, modus operandi and its results.

KEYWORD

Bank	World Wide Web
Online banking	Data
Phishing	Cookies
Net banking	Privacy Policy

Empirical Article

Preface

a) What is Privacy Policy

Privacy is defined as a state or condition of limited access to a person [Li & Hung[i], 2004]. Privacy Policy describes the practices and policies followed by E-Commerce [G. Karjoth and M. Schunter[ii], 2002]. Privacy Policy represents the way of collecting data, what is the purpose of utilization of data, whether the enterprise provides access to the data, who are the data recipients (beyond the enterprise), how long the data will be retained, and who will be informed in what cases[Directory of Bank websites of India[iii]]. In simple words, Privacy Policy is the document which is supposed to be attached or linked with the website while collecting the personal or non-personal or both the information of the user of that site at that juncture. The major points that a privacy policy generally accommodates may be listed down as follows-

- Presence of Privacy Seal in the document.
- What type of data is collected from the user/customer?
- How the data is collected from the user i.e. through which link/source of the website, the data is collected.
- How will the data collected be used?
- Use of cookies.
- Data collected is shared with the third parties or not.
- Use of web beacons or links of third parties on the website.
- Security techniques used to make the user's data secure.
- Children's privacy.
- P3P Reference File and Privacy Policy.

b) What we are going to study

In this paper, we will first study the privacy policies of various Indian Nationalized Banks. This paper presents the results of the privacy policies survey of websites of Indian banks, conducted during April and May of 2008. This survey is done to determine the extent to which bank's website posted privacy policy and information practice statements. The survey gives answer to the following questions:

- What proportion of websites posts privacy disclosures, and what do these disclosures say?
- What proportion of websites collects personal information and what types of information are collected?

The purpose of the survey was to obtain an indication of the state of the Nationalised and Private Banks in India with respect to on-line privacy disclosures, data collection and interactivity. The report addresses only the disclosures posted on the websites and does not consider institutions' adherence to these policies and heir actual practices.

The website survey results are based on an analysis of 55 websites selected from the Directory of Bank Websites in India [4].

This survey identified characteristics of the Indian banks and included questions related to the types of services theses banks offer on-line.

2) Methodology

To precede this research work, we collected the list of Indian Banks and URLs of their websites from the Directory of Bank Websites in India [Adkinson F. William And Et Al[iv], 2001]. This list of websites contains different categories of banks like:

Indian Banks and URLs
Websites of Public Sector/Nationalized Banks
Websites of State Bank Group
Websites of Other Public sector Bank
Websites of Old Private Banks
Websites of New Private Banks
Websites of Foreign Banks

1. First of all, the websites of the above mentioned banks were checked for the presence of privacy policy. Secondly, if included, it is observed that what information practice statements are offered to the customers through those privacy policies. These privacy policies were also analysed with respect to their format, content and characteristics on the basis of a self-made questionnaire. [Interagency Financial

Institution Web Site Privacy Survey Report[v], 1999] [Tan, Koon[vi], 2006].

a) Data Collection

A list of 55 different Indian Banks, containing their website addresses (URLs), was collected from the "Directory of Bank Websites in India" [Adkinson F. William, et al, 2001].

Out of these, 19 are public sector/nationalised banks, 8 are making group of state banks, 1 bank is other public sector bank, 11 are old private banks, 8 are new private banks and 8 are foreign banks.

A Questionnaire was prepared to analyse Privacy Policies of different banks. There are 27 different questions in the questionnaire which cover the following points –

a) Existence of Privacy Policy.
b) Personal and demographic information taken from the web sites from the customers.
c) Data sharing and selling to the third party.
d) Options/Choices given by the websites to the customers.
e) Online Security of the customer's information.
f) Cookies
g) P3P Reference File, P3P Privacy Policy

The survey examined the extent to which websites collected personal or demographic information of the consumers. Personal information is information that can be linked to a specific individual, for example, a name or a mobile number. Demographic information is personal information, such as income or gender, which does not identify a specific individual.

Websites were classified as interactive if a consumer could access an account or transfer funds, open a new account, apply for a credit card, or apply for a loan. [Tan, Koon, 2006]

3) Analysis

In this section, the analysis part of the paper begins.

a) Existence of Privacy Policies

First of all, it is analyzed that only 93% websites of banks are accessible out of the list used in this survey and out of those only **43% have posted privacy policy on their websites.**

Table:1

Websites URL Accessible	Percentage
Yes	93%
No	7%

Table:2

Existence of Privacy Policy	Percentage
Yes	43%
No	57%

Amongst these banks -

- 36% are Public Sector/Nationalized Banks
- 15% are State Bank Group
- 20% are Old Private Banks
- 15% are New Private Banks
- 15% Foreign Banks

Table:3

Types of bank	Percentage
Govt. banks	36%
SBI Group	15%
New Private	15%
Old Private	20%
Foreign banks	15%

Chart-1

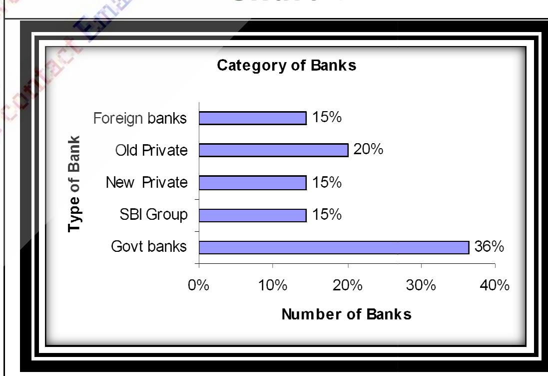
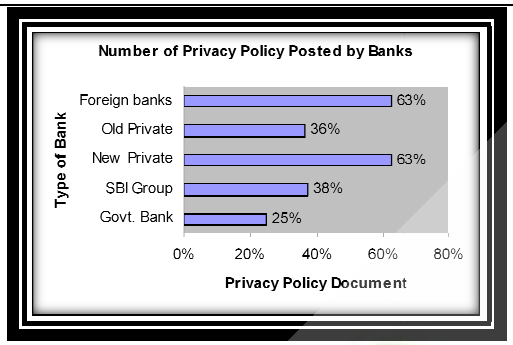


Chart:2



The above two charts show that maximum number of banks in the list are from public sector (36%, Chart 1) while these banks have posted least number of privacy policies (25%, Chart 2).

Foreign banks and new private sector banks have posted maximum number of Privacy Policies (63%, Chart 2).

b) Existence of Net banking service, Phishing Information or Security Alerts

In computing, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Online banks are common targets. Phishing is typically carried out by e-mail or instant messaging, [Skoudis, Ed[vii], 2006] and often directs users to enter details at a website, although phone contact has also been used. [W3C Recommendation[viii], 2002] Phishing is an example of social engineering techniques used to fool users.

Table:4

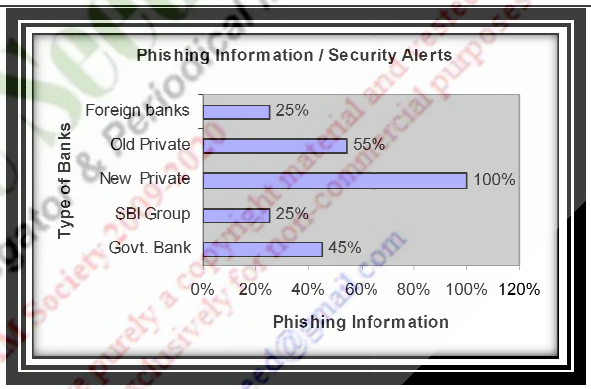
Existence of Phishing Information / Security Alerts on websites	Percentage
Yes	53%
No	47%

Table:5

Bank provides facility of Net banking / online banking	Percentage
Yes	90%
No	10%

Phishing is very important information which is supposed to be provided by every bank while providing the facility of Net banking/ Online banking. This survey finds that almost 90% banks provide net banking facility whereas only 53% banks provide net banking service. All new private banks provide either phishing information or security alerts. The link of Phishing information or security alerts appears as soon as the consumer chooses the option for net banking and sometimes on home page too. Chart 3 gives clear picture of phishing information provided by different banks.

Chart : 3



c) Place of Privacy Policy Link on Website

Table 6: Link of Privacy Policies placed on websites

Place of Privacy Policy on website	Percentage of Privacy Policies Posted
Linked at home page	69%
At top of the page	8%
At bottom of the page	92%
Linked from Information collection	31%

As table 6 shows, of the 43% of websites surveyed that posted a privacy policy, 69% had a link to the privacy policy from their home page. For 8% of the sites with home page links, the link was located at the top of the home

page, while for 92% of these sites the surfer had to scroll down the visible portion of the page to locate the link. 31% of the websites posted privacy policy link at the place from where the consumer's information was collected.

d) Existence of Privacy Seal

Table:7 Privacy Seal

Privacy Seal	Percentage
Yes	10%
No	90%

The presence of Privacy Seal in privacy policy makes the user feel more relaxed for the safety of his/her personal or demographic information. But this survey finds that only 10% policies have privacy seal. In this survey, it is observed that in most of the websites privacy seal is not placed in the privacy policy whereas it appears wherever the link of privacy policy is placed on the website. Also, almost all the privacy seals were of "Verisign", specifically for SSL certification. The consumer could also get more information regarding the seal, wherever it was placed on the site.

e) Content of Privacy Disclosures by information collection

We evaluated the content of privacy disclosures by answering questions concerning the extent to which the disclosures addressed certain principles of fair information practice. For purposes of this survey and ease of presentation, the principles were defined as follows:

i) **Notice**

It included statements informing the consumer about what information was collected, how the collected information would be used and whether the site said anything about the use of "cookies". A "cookie" is a piece of information that a Web site stores on a visitor's Web browser that is retrieved when the visitor logs onto the site again.

Table 8 : Notice

Notice	Percentage
Privacy Policy says anything about what specific personal information is collected on domain from consumer	8%
Privacy Policy says anything about regarding how the information collected about consumer will be used	77%
Privacy Policy says anything about the use of "cookies"	23%
At least one of the above	55%
All of the above	14%
Privacy Policy informs consumers of any opportunity to exercise choice about whether they want to be contacted by bank for marketing or other purposes (Opt Out/Opt In/Choice)	9% (choice)

Notice was the most frequently addressed principle. 77% of sites that posted privacy disclosures contained language about how the information collected from consumers would be used. 8%contained language about what information they collected. 23% contained language about their use of cookies.

Overall, for sites with a privacy disclosure 55% provided a statement addressing at least one of the questions concerning notice and 14% provided statements addressing all three questions.

No Opt out or Opt in choice is given to the consumer in the website, but 9% privacy policies agree that some choice is provided to the consumer without disclosing the type of choice whether it is opt out or opt in.

ii) Choice (Disclosure to Third Parties)

It included statements that informed consumers of any opportunity to exercise choice about whether they wanted to be contacted by the bank or whether consumers could exercise choice about the disclosure of information to third parties.

Table 9: Choice

Choice	Percentage
Privacy Policy says that the bank may use the personal information collected about consumers to contact them for marketing or other purpose	**82%**
Privacy Policy says that the information collected about consumers may be disclosed to third parties	**86%**
Privacy Policy says that consumers may exercise choice about whether collected information will be shared with third parties (Opt Out/Opt In/ Choice)	**18% (Choice)**

The survey contained two questions concerning choice. These questions asked whether the privacy policy informed consumers about any opportunity of being contacted by bank for marketing or other purposes ("internal opt out") or the sharing of their information with a third party ("external opt out").

82% of the sites with disclosures offered an internal opt out. 86% provided an external opt out.

No Opt out or Opt in choice is given to the consumer in the website, but 18% privacy policies agree that some choice is provided to the consumer, about whether collected information will be shared with third parties, without disclosing the type of choice whether it is opt out or opt in.

iii) Online Security of Consumers' Information

Security included statements informing consumers about the steps taken to provide security for information during on-line transmission and while stored by bank.

This could include statements related to the use of a secure server (SSL). A logo of "Verisign (SSL Certified)" is pasted on almost every site which is asking for information to the consumer.

Table10: Security

Security	Percentage
Privacy Policy says anything about the steps taken to provide security for information	77%
Privacy Policy says anything about the steps taken to provide security for information during online transmission between the consumer and bank	36%
Privacy Policy says anything about the steps taken to provide security for information while stored by bank	59%
At least one of the above	18%
All of the above	36%

The survey contained three questions concerning security. These questions asked whether the policy says anything about the steps taken to provide security for information, site provided a statement informing consumers about the steps taken to secure information during on-line transmission and while in storage.

77% privacy policies say something about the steps taken to provide security for information. 36% of sites with a privacy disclosure provided a statement addressing the security of data being transferred on-line and 59% addressed the security of information in storage.

18% of sites with a privacy disclosure provided a statement addressing at least one question concerning security and 36% provided statements addressing all questions.

iv) Existence of P3P Reference File and Privacy Policy

The Platform for Privacy Preferences Project (P3P) enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.

Although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information, it does not provide a technical mechanism for making sure sites act according to their policies. Products implementing this

specification may provide some assistance in that regard, but that is up to specific implementations and outside the scope of this specification. However, P3P is complementary to laws and self-regulatory programs that can provide enforcement mechanisms. In addition, P3P does not include mechanisms for transferring data or for securing personal data in transit or storage. P3P may be built into tools designed to facilitate data transfer. These tools should include appropriate security safeguards. [Tom Young[ix], 2007]

Table10: P3P

Security	Percentage
domain has a P3P Reference File	0%
Does the domain has a P3P Privacy Policy	0%

The survey contained two questions concerning P3P. These questions asked whether the policy says whether the website contains P3P reference file and P3P privacy policy. Unfortunately, no bank has these files associated with its website.

4) Discussion

This paper has shown that only 43% of the banks have posted their privacy policies on their web sites. However, as privacy policies are becoming increasingly expected on commercial web sites around the world, Indian banks are beginning to post those. Also, the banks which had privacy policies posted did not express completely the necessary information for the consumers.

The items collected most often by the sites were the consumer's name, e-mail address, and postal address and bank account number. Most of the sites have Registration Forms for different services provided by different banks on their websites, but in most of the cases, these forms are in PDF format. Therefore, these sites are not supposed to be interactive sites as the consumer can not interact with bank directly (online). Purpose of net banking can be solved only when the sites are interactive.

Privacy policies include some positive and some negative points which somewhat makes the consumer confused towards the safety of their personal information.

The presence of Privacy Seal in privacy policy makes the users feel more secure for their personal information but it is a finding here that very few websites have privacy seal.

a) Shortcomings of Privacy Policies posted on websites

Amongst all, we found that 9% banks have either same copy of privacy policies or same URL to access their websites while the names of the banks are entirely different.

It is observed that in some cases, like PNB, privacy policy is exceptionally small and does not include even minimum number of points which are essential to make a privacy policy. These types of privacy policies should be improved.

9% websites are having inactive link of privacy policy on their home page which is not fair with the consumer.

5) Summary

The authentic implementation of e-Commerce these days is moreover dissimilar from its real-life counterpart, and for the most part it's a "Web page" with listing of items and prices. The social facet such as personalization, collaboration, security, interactivity etc. is lacking. We, for that reason argue to come together the solution with a social place, where customers who participate in should get foolproof security.

As we found that the websites disclose personal information of the users to Third Parties, which may or may not have their own privacy policies, is to be counted as one of the reasons for the same.

This study also finds that no *Universal Standard* format for a Privacy Policy has been designed and declared for banks in India yet.

It will be very helpful for net banking consumers, if there is an authority to monitor and control the proper format and points included in the privacy policy for banks.

There is no general privacy law in India [Privacy and Human Rights, An International Survey of Privacy Laws and Practice, 1998]. India does not have any data protection law equivalent to that in the UK and there have been recent cases of information being leaked from call centers to criminals who have then blackmailed the companies involved. The Data Security Council of India (DSCI) is being set up by Indian IT industry group NASSCOM (June 2007).[Naavi[x], 2002] NASSCOM Information Technology Action Plan said [Skoudis, Ed, 2006] that a National Policy on Information Security, Privacy and Data Protection Act for handling of computerised data shall be framed by the Government within six months. However, a recent study tells that more than 40 countries around the world have passed, or are preparing to pass, laws that protect the privacy and integrity of personal consumer data. *India is not however one amongst them*. Some time back, NASSCOM did take some initiatives to push through a drafting exercise but it appears that the exercise has not been pursued further [Privacy and Human Rights, An International Survey of Privacy Laws and Practice[xi], 1998].

Finally, the results of this study may be pointed out as –

- Maximum number of banks in the list are from public sector, while these banks have posted least number of privacy policies.
- The interactive sites collected more personal information than sites that were not interactive.
- The analysis shows that new private banks and foreign banks have posted maximum number of privacy policies (63%) on their websites.

6) Limitations

There are few limitations of this research which may be discussed as:

There is no standard format of privacy policy. Some policies are too small whereas some of them are too large and difficult to understand. At least few standard points should be made mandatory in a privacy policy that a website should include.

How will we come to know that the user is more than 13 years of age? Suppose a kid enters his age 18 and registers / buys things himself on the site then how can this procedure be stopped i.e. inserting wrong age?

How can we check that the companies are implementing their privacy policies? If they are not implementing the policies after displaying on the net then how can we make them implement?

7) Future work

Significance of privacy seal is still an unclear point in general. Further studies can be done to check the awareness and to get suggestions of people from different backgrounds on this topic. Further work may be done to make a standard format of Privacy Policy for banks which should be universal.

More studies can be done to check the interactivity of banks' websites to solve the purpose of net banking.

More studies can be done to check the interactive capabilities of Indian Banks, like for how many services the bank is supporting interactive facilities, like, Access or transfer funds between accounts, open a new account, apply for a credit card, apply for a loan etc.

Appendix: Survey Questionnaire

Answer the following questions in YES or NO:-

1.	Is URL of the website accessible?
2.	Is Internet banking available on site?
3.	Does privacy policy exist?
4.	Link for phishing information/ security alerts is there on site?
5.	Does Privacy Seal exist?
6.	Does the link for Privacy Policy exist on home page?
7.	Information Practice Statement(s) posted on domain ?
8.	Does domain collect e mail addresses?
9.	Does domain collects Personal Identifying Information other than e mail address?
10.	Does domain collect Non Personal Identifying Information?
11.	Does Privacy Policy declare that domain does not collect any personal information from consumer (If NO, go to Next else go to 16).
12.	Does Privacy Policy say anything about what specific personal information is collected on domain from consumers.
13.	Does Privacy Policy say how the domain may use personal information it collects for internal purposes (If YES go to Next else go to 16).

14.	Does Privacy Policy say that the domain uses personal information to send communications to the consumer (If YES go to next else go to 16).
15.	**Choose any one :**
I.	Does Privacy Policy say that domain provides consumers an opportunity to opt in to receive future communications from the domain
II.	Does Privacy Policy say that domain provides consumers an opportunity to opt out of receiving future communications from the domain
III.	Does Privacy Policy say that domain requires consent or offers a choice with respect to receiving future communications from the domain, but does not make clear for opt in or opt out choice
IV.	Domain does not say anything about offering consumers choice with respect to receiving future communications
16.	Does Privacy Policy say that domain discloses personal information it collects to the third party (If Yes, go to Next, else go to 18)
17.	Choose any one :
I.	Does Privacy Policy say that domain provides consumer an opportunity to opt in to the disclosure of Personal Identifying Information to third parties?
II.	Does Privacy Policy say that domain provides consumers an opportunity to opt out of the disclosure of Personal Identifying Information to third parties?
III.	Does Privacy Policy say that domain requires consent or offers a choice w.r.t. the disclosure of Personal Identifying Information to third parties, but does not make clear for opt in or opt out choices
IV.	Does not say anything about offering consumers choice w.r.t. disclosure of personal identifying information to third parties
18.	Does Privacy Policy say anything about third party advertising/ad services OR Third Party Link on website
19.	Do third-party services may place a cookie on the computer for the purposes of ad tracking and presentation/Advertising
20.	Does Privacy Policy say that the domain takes any steps to provide security (If YES go to next else go to 23)
21.	Does Privacy Policy say that domain takes steps to provide security, for personal information the domain collects, during transmission of the information from the consumer to the domain e.g. SSL
22.	Does Privacy Policy say that domain takes steps to provide security, for personal information the domain has collected, after the domain has received the information (after collection)
23.	Does Privacy Policy say anything whether that domain does or may place cookies
24.	Does Privacy Policy say anything whether THIRD PARTIES may place cookies/ Web Beacons on the domain (If Yes, else go to Next else go to 26)
25.	Is a third party attempting to place a cookie at this domain's home page?
26.	Does domain has a P3P Reference File? (YES if access check step 1-1 indicates that /w3c/p3p.xml can be retrieved (blue fonts) ; Id access check ...can not be retrieved then choose NO and STOP)
27.	Does the domain have a P3P Privacy Policy?

References

[i] Haifei Li, David Ahn, Patrick C. K. Hung, "Algorithms for Automated Negotiations and Their Applications in Information Privacy," cec, pp.255-262, 2004 IEEE International Conference on E-Commerce Technology (CEC'04), 2004

[ii] G. Karjoth and M. Schunter. A Privacy Policy Model for Enterprises. In 15th IEEE Computer Security Foundations Workshop (CSFW) pages 271-281. IEEE Computer Society, 2002

[iii] Directory of Bank Websites in India; http://www.banknetindia.com/banklinks.htm

[iv] Adkinson F. William And Et Al. Privacy Online: A Report On The Information Practices And Policies Of Commercial Websites. World Internet Secure Key, Privacy Policy, WISeKey S.A, E-Commerce PKI CA Privacy Policy - Version 1.0, 1 July 2001, pp. 1-7

[v] Interagency Financial Institution Web Site Privacy Survey Report, November 1999

[vi] Tan, Koon. Phishing and Spamming via IM (SPIM). Internet Storm Center. Retrieved on December 5, 2006.

[vii] Skoudis, Ed. "Phone phishing: The role of VoIP in phishing attacks", searchSecurity, June 13, 2006.

[viii] The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation 16 April 2002 ; http://www.w3.org/TR/P3P/#Introduction

[ix] India to set up data privacy watchdog; Tom Young, Computing 08 Jun 2007 http://www.vnunet.com/computing/news/2191739/india-gets-privacy-watchdog

[x] Data Protection Laws in India; Naavi, May 24, 2002. http://www.naavi.org/cl_editorial/edit_25may_02_1.html

[xi] Privacy And Human Rights, An International Survey of Privacy Laws and Practice http://www.gilc.org/privacy/survey/surveyak.html#India

Performance Evaluation and Design of Flexible Manufacturing System: *A Case Study*

Ajay Singholi
Assistant Professor, Mechanical & Automation Engineering Department, GGS-Indraprastha University, Delhi, India
ajay.igit@gmail.com

Deepti Chhabra
Assistant Professor, Mechanical & Automation Engineering Department, GGS-Indraprastha University, Delhi, India
deepti2226@yahoo.co.in

Sampada Bagai
Research Scholar, Mechanical & Automation Engineering Department, GGS-Indraprastha University, Delhi, India
sampada.bagai@gmail.com

ABSTRACT

This case study reflects results of a detailed simulation study in order to design and analyze a Flexible Manufacturing System. This paper aims at the performance enhancement of manufacturing system in Indian industry. An ample amount of literature review has been done to apprehend various factors affecting the performance of a manufacturing system which includes conceptual study of the machine & resource utilization, reducing time span, reducing in process inventories and improving control etc. The manufacturing company under focus of our research is operating on a traditional manufacturing system. With the intensifying global competition demands increased productivity in order to fulfil market demands for which the company should change to FMS. The research undertakes analysis of manufacturing systems of the gear manufacturing unit and hence attempts to provide solution to its prolonging problems. This research work will benefit other manufacturing industries as well. To conclude, simulation models are developed and the effect of seizing on the performance improvement is studied.

KEYWORD

FMS	Simulation
Machine	Productivity
Modeling	Workstation
System	Software

Preface

The manufacturing industry is the wealth of a country which showcases the prosperity of country. With the aggrandizing competition in global trade, these industries are facing dynamic environment. Such environment is characterized by the large amount of uncertainty caused due to rapid market changes, competitive prices and reduced product life cycles. All these factors have contributed to performance enhancement in automated industry. Traditional manufacturing systems lack the capability of meeting these requirements. These factors, thus, prompt the manufacturing industries to increase flexibility & productivity to stand in tough competition. The introduction of FMS (flexible manufacturing system) helps in improvises a manufacturing system. Flexible Manufacturing System (FMS) is a system which compiles production equipments actually coupled by a central sustainable system and logically structured under a host workstation. As the flexibility of a manufacturing system increases, the profit also increases because of improved quality. Productivity & flexibility have been the two conflicting objectives of production units. FMS tries to provide an optimization between improvising flexibility while maintaining the productivity of a medium scale mass production unit. While designing an FMS the focus should be on increasing the performance. Designing of FMS should always be apropos to the company's current production scenario which should focus on layout design, production capacity, material handling, level of automation, manpower, no of work stations etc. The earlier stages in designing of FMS should focus on deciding these parameters. The FMS hence designed should be able to justify performance improvement by meeting some set goals which include increased machine & resource utilization, reduced in process inventories, reduced time span, improved control etc. Performance is one of the main factors affecting the design, development & configuration of the FMS. Measurements, analytical models, and simulation models are alternative techniques for performance analysis. Analytical models were earlier used for analysing the performance of a manufacturing system. Nowadays, simulation based models are preferred over it so as to obtain accurate results for larger & complex calculations with fewer assumptions. FMS works on complex structure and dynamic character of real manufacturing units, hence using simulation techniques are used to analyse them. The simulation softwares provide an interface which can represent the real world by numbers & can be easily analysed & manipulated.

This case study is on a company which is based on traditional production system. The cutthroat market competition demands this company to convert into FMS in order to increase the productivity & meet market demands. The research attempts at analysing the manufacturing systems of the gear manufacturing unit and hence provides solution to its prolonging problems. Every manufacturing industry benefits from this research work. Performance analysis holds the key for improvement. Organisations adapt to the core concepts of research and

hence benefit from it by following the standards and the goal set forth by modelling. The paper presents study of the existing system followed by designing & analysis of FMS. The paper is divided in the following sections: Section 2- Literature survey overview Section 3- Problem statement & Case Company's details Section 4- Design & analysis of FMS model Section 5- Comparison of results Section 6- Conclusion.

2. Literature Review

The desirable qualities needed in a manufacturing system to have a speedy reaction against today's varying market needs form the basic structure of FMS. Flexible manufacturing system is used for manufacturing of a variety of products of medium sized volume using computer for central control, CNC tools for operation and automated handling of material [Browne et al[i]., 1998]. Better quality, high flexibility and an increase in productivity are its basic features [Womack[ii], 1990]. Flexible Manufacturing System (FMS) is a compilation of production equipments actually coupled by a central sustainable system and logically structured under a host workstation. The most vital element of a production system is Flexible Manufacturing System due to its ability to conform to a change three times as compared to an ordinary job shop. Performance of a system is largely influenced by the loading and control strategies [Stecke[iii], 1983; Solberg[iv], 1981].To implement an FMS, a well planned designing with controlling strategies is required [Gowan Jr., & Mathieu[V], 1996]. Similar NC machines form the main constituents of an FMS, forming a well connected network by a transportation system that is automated in nature. A dedicated computer called FMS cell computer is allotted for each process. A chief impact on operation of an FMS is achieved by the hardware used for transferring of tools to/from the central storage to the tool magazine automatically while the operation is taking place [Edghill, & Davies[vi], 1985; Jaikumar[vii], 1986]. FMS is an emergent technology which is appropriate for mid-variety, mid-volume type of production and comprises of multipurpose NC machines [Sridharan[viii], 2007]. As compared to the traditional manufacturing systems which are used for higher volume and lower part variety, an FMS has the ability of managing a wide variety of products simultaneously in small to medium size lots at a higher efficiency. This system processes any part within the specified capacity belonging to a specific part family according to an encoded plan. It functions in such a way that the change over time is minimum and there is a lesser human intervention [Chan, & Chan[ix], 2004]. Productivity and flexibility are the two conflicting objectives of production Ability to produce a greater number of products distinct in nature in a job shop is referred to as flexibility while high production rate closely resembling an assembly line in its operation, is referred to as Productivity. The two decisions related to FMS operation are categorized as pre-release and post-release. Pre-release decisions are taken before FMS begins its operation and is related to the tools and parts' collection. While the system is in operation, Post-release decisions indicate the sequence of parts and their routing [Stecke[iii], 1983]. Given the current condition in the manufacturing industry, the focus has shifted towards increasing the flexibility with the available resources while

maintaining high utilization of the resources. Flexibility is a system's capability to produce a variety of products with an acceptable excellence while modifying the resources to do so [Sethi, & Sethi[x], 1992].It is the capability of a system to cope up with variation by dynamically exploring the choices [Wadhwa, & Rao[xi], 2000]. Flexibility is of two types-Process and Product flexibility. The property of a company to perform adequately under varied operating conditions is referred to as Process flexibility while product flexibility deals with manufacturing of wide variety of a particular product [Benjaafar, & Ramakrishman[xii], 1996]. To make decision making procedure effective, there are eight types of flexibilities namely routing flexibility, product flexibility, volume flexibility, process flexibility, machine flexibility, operation flexibility, production flexibility and expansion flexibility [Browne et.al[i]., 1984]. Increase in flexibility ensures maximum resource utilization [Shnits et al.[xiii], 2004]. An FMS is said to be effective if it is capable of dealing with any change in the volume, mix, nature or activity timing and this capability is referred to as flexibility [Correa, & Slack[xiv], 1996]. Designing of FMS is related to control and physical aspects. Control aspects deal with defining the rules of scheduling and algorithms defining the way in which a system can function while the physical aspect deals with selection of the types of machines depending upon the time taken for its processing, transportation, material handling, loading unloading etc. As the machinery involved in FMS is quite costly, the layout should be selected bearing in mind the various options of layouts. The layout of machines deals with the problem of arrangement of machinery is in such a way that there is a minimum transfer time taken by materials between them. To evaluate the other layouts in a system, the minimum distance between machines, the transporting path etc are to be considered apart from the other factors like distance and time. The results on the layouts of FMS are evaluated and aspects vital in the designing of an FMS layout are identified [Kouvelis, & Kiran[xv], 1989]. As an experimental inspection of an FMS, the number of completed parts was a measure of system performance. Researchers have been constantly in improving performance of an FMS [Wadhwa, S. et al.[xvi], 2005; Chan, F.T.S.[xvii], 2003]. Deterministic models are also used by some researchers to approximate the performance of an FMS by estimating parameters of the system like utilization of resources; rate of production etc during the initial stages itself. A commonly accepted mathematical model for evaluation of performance parameters was given by [Solberg[iv], 1981; Mejabi[xviii], 1988]. For intricate systems, researchers have proposed the use of Simulation as it provides a simplified method of modelling of complex systems while representing the real world system. Simulation modelling is very useful in problems like scheduling, routing etc, which are faced while functioning of a system. There are two types of difficulties involved with FMS. Design problem is concerned with choosing the appropriate FMS components, while operational problem is concerned with the utilization aspects in an FMS. Both these aspects are considered in this paper. Analyzing the existing FMS using analytical models and an alternative FMS model devised to improve the performance characteristics. A simulation model has been designed which identifies the machine as

blockage point apart from calculating the parameters of performance of the new FMS. As an advice to increase the production rate and to ensure better resource utilization, some strategies for up gradation are also suggested to the company.

3. Problem Statement & Company Details

The company under consideration is located in Uttar Pradesh State of India. It manufactures various kinds of three wheelers. The company is ISO 9001:2000 and ISO 14001 certified and has established its name in international markets. The company integrates departments for design, development, manufacture & sales. The company has a large market in India as well as overseas. The manufacturing division is divided into assembly line, foundry line, machine shop etc. Various parts are manufactured in the machine shop including shafts, cylinders, gears etc. This case study is on manufacturing of gear. The line for gear manufacturing process includes machines like hobbing, turning, gear shaving etc. The company is a progressive company and is willing to invest in R&D. The company's vision of growing into a globally competitive company & meeting the increasing & different needs of customers have created a need to switch on to new type of manufacturing systems from current traditional type. The paper focuses on analysing the current manufacturing setup which is based on cellular technology & propose a new flexible manufacturing system using simulation techniques. This analysis & design will help in performance improvement of the company by studying various parameters on which performance depends.

The study started with the data collection which was done by preparing a questionnaire & distributing it to various people involved in the line for manufacturing of gears. The line is responsible for production of two types of gears Gear 1 & Gear 2. The FMS study is carried out on production of these two gear types & is a standard batch type manufacturing case. The gear manufacturing process is carried out in 10 steps which include chamfering, facing, turning, hobbing, shaving of the initial blank. The manufacturing process of the two gears in detail is given as under:

3.1 Gear-1 processing

The total time taken in production of one piece of gear one is 2279 seconds. The detailed description is given in Table-1

Table 1. Processing description of Gear-1

S. No	OPERATION DESCRIPTION	M/C DESCRIPTION	Cycle Time in Sec.
1.	OD Chamfer, Face, OD Turn, Face, Chamfer etc.	Mini Chucker	330
2.	Turn Second side face and chamfer OD	Mini Chucker	300
3.	Spline Broaching	Broaching	250
4.	Washing	Washing M/c	150
5.	Spline Deburring	Manual	150
5.	Final turning	PTC Lathe	300
6.	Burr Chamfering	Manual	100
7.	Hobbing	Hobbing M/c	149
8.	Teeth Chamfering	Cham. M/c	100
9.	Oil Grooving	Hyd.Press	150
10.	Shaving	Shaving M/c	300
	Total Time		2279

3.2 Gear-2 processing

The total time taken in production of one piece of gear one is 2195 seconds. The detailed description is given in Table-2.

Table 2. Processing description of Gear-2

S. No	OPERATION DESCRIPTION	M/C DESCRIPTION	Cycle Time in Sec.
1.	OD Chamfer, Face, OD Turn, Face, Chamfer etc.	Mini Chucker 1	288
2.	Turn Second side face and chamfer OD	Mini Chucker 2	240
3.	Spline Broaching	Broaching	250
4.	Washing	Washing M/c	150
5.	Spline Deburring	Manual	113
5.	Final turning	PTC Lathe	250
6.	Burr Chamfering	Manual	150
7.	Hobbing (10 Jobs)	Hobbing M/c	149
8.	Teeth Chamfering	Cham. M/c	155
9.	Oil Grooving	Hyd.Press	150
10.	Shaving	Shaving M/c	300
	Total Time		2195

4. Performance Analysis and Modelling of Case system

Profitability and survival of a manufacturing firm depends upon accommodating fluctuating product demands, day-to-day technological advancements, and competition from and among different firms. Flexibility plays a vital role for operation in such a scenario. Modeling and performance analysis of manufacturing systems helps decision makers at higher levels to conduct an economic feasibility analysis for expansion/diversification or modification of the system. Also, this could help in installing a new manufacturing system with a substantial reduction in the number of machines, floor space, inventory level, throughput and lead time and also high quality products, with a greater flexibility to respond to the market needs. To meet the objective, various manufacturing flexibilities need to be measured to evaluate and select a desired flexible manufacturing system. There are various universal mathematical models available to perform deterministic study and therefore may be utilized. It is felt that better study of an existing system would also help in improving performance and in designing operational parameters of a new FMS. Getting the motivation from the earlier studies it was decided to adopt a well recognized mathematical model proposed by [Solberg[iv], 1981] and further modified by [Mejabi[xviii], 1988]. These models have been duly verified and validated in the literature to provide primary estimates of operational parameters such as production rate, workstation load etc. The considered research case involves the assessment and analysis of performance of a flexible manufacturing system at operational level under various parameters. Primary step may be to identify the various such parameters that can affect performance of the system.

4.1 Operational parameters

Average Workload

Various performance parameters are analyzed by calculating the average workload for each work station of FMS which is denoted by *WLi* and is the mean total time spent by a part at a machining station. It is used to identify the bottleneck station in the system if any.

$$WLi.(\min) = \sum_{j}\sum_{k} tijk\ fijk\ Pj$$

WLi = average workload for station *i (Min)*, *tijk* = Processing time for operation *k* in process plan *j* at station

i (Min), *fijk* = operation frequency for operation *k* in part *j* at station *i*, *pj* = part-mix fraction for part *j*. The average workload calculated for various workstations of case FMS is summarized in table 3.

Table 3. Average workload for workstations

S No.	Machine	Average Workload (sec)
1	Mini Chucker 1	309
2	Mini Chucker 2	270
3	Broaching	250
4	Washing M/c	150
5	Manual	131.5
6	PTC Lathe	275
7	Manual	125
8	Hobbing M/c	149
9	Cham. M/c	127.5
10	Hyd.Press	150
11	Shaving M/c	300

Estimation of Bottleneck Station

Bottleneck station refers to the station having the maximum workload per server. For an FMS, it can be found out by finding the ratio of largest workload to the no. of servers.

Bottleneck station = Largest workload to no. of server ratio, i.e. WLi/si

Table 4. Calculation of various parameters

S No.	Machine	Average Workload (sec)	No. of Servers	Bottle neck station? Workload/no. of servers
1	Mini Chucker 1	309	10	30.9
2	Mini Chucker 2	270	9	30
3	Broaching	250	6	41.66667
4	Washing M/c	150	5	30
5	Manual	131.5	5	26.3
6	PTC Lathe	275	6	45.83333
7	Manual	125	7	17.85714
8	Hobbing M/c	149	3	49.66667
9	Cham. M/c	127.5	4	31.875
10	Hyd.Press	150	4	37.5
11	Shaving M/c	300	2	**150**

4.2 FMS Performance Measures

Various performance evaluation studies are mentioned in literature and they have used performance measures like average flow time, [Chan F.T.S.[xvii], 2003], machine utilization, system utilization etc. Here popular performance measures have been used i.e. Production Rate of all parts, Production Rate of each Part Type, Average Utilization of Workstations, manufacturing lead time and mean waiting time experienced by a part at the stations.

Maximum Production Rate of all Parts

The bottleneck station restricts the maximum production rate for all parts and it can be calculated by finding the ratio of s* (No. of servers at bottleneck station) to WL* (Workload at Bottleneck Station).

$$Rp * (Pc./Min) = \frac{s*}{WL*}$$

Correspondingly, part production rate for the separate stations (of part type j) can be found out by multiplying R*p and the corresponding part mix ratios (Pj).

$$Rpj *= pj(Rp *) = pj\frac{s*}{WL*}$$

By using the above formula, maximum production rate for all parts is calculated to be 0.00666667 Pc. /hr. for our case.

Utilization of each Workstation

The mean utilization of each workstation is the time for which the servers are working at the station(excluding the ideal time). The utilization will be 100% for the bottleneck station (at *R*p)*.Mean utilization *Ui* is given as the product of the ratio of workload per server and the maximum production rate(*R*p)*

$$Ui = \frac{WLi}{si}(Rp*) = \frac{WLi}{si}\frac{s*}{WL*}$$

Average station utilization (*Uav*) can also be calculated by finding the average utilization value for all the stations. The transport system value also needs to be taken into consideration.

$$\mathbf{Uav} = \frac{\sum_{i=1}^{n+1}\mathbf{Ui}}{\mathbf{n+1}}$$

Table 5. Station utilizations

Machine	Station Utilization	
	NUM	%
Mini Chucker 1	0.206	20.6
Mini Chucker 2	0.2	20
Broaching	0.277778	27.7778
Washing M/c	0.2	20
Manual	0.175333	17.5333
PTC Lathe	0.305556	30.5556
Manual	0.119048	11.9048
Hobbing M/c	0.331111	33.1111
Cham. M/c	0.2125	21.25
Hyd.Press	0.25	25
Shaving M/c	1	100

Overall FMS utilization

This is a vital measure for performance measurement and can be computed by taking into account the average number of servers for each station (*n*) and not considering the transport system. The overall FMS utilization in this case has been calculated as 24.44809%.

$$Uoverall = \frac{\sum_{i=1}^{n} siUi}{\sum_{i=1}^{n} si}$$

4.3 Proposed FMS: Sizing and Other Issues

The analysis of the existing system in the company has been done in the previous section 4 on the data collected. Using the mathematical models, various performance parameters have been calculated. The results showed that the performance of current system is not at the optimum level. The competition in global market coerced the management of company to invest in achieving a better & productive system and was willing to see our designs. A new FMS was designed by following normal procedure based on the inputs received. The sizing of FMS, layout selection etc was done using a mathematical models from the literature. After the calculation, the performance of proposed system is assessed by the simulation models. The simulation models have been developed in SIMAN based software package ARENA version 12.0 and results verified.

Sizing of proposed FMS

With the help of the mathematical models suggested by [Mejabi[xviii], 1988; Solberg[iv], 1981], we can calculate the number of servers required & realize a specified production rate. Such estimations done in the initial stages of FMS design helps to decide the size of the system. The part mix, process sequence, and process times, the

number of servers at each station *i* can be calculated as given in table 6.

Table 6. No. of Servers in Proposed FMS Workstations

Workstations (Description)	No. of Servers (Proposed)
Mini Chucker 1	2
Mini Chucker 2	2
Broaching	2
Washing M/C	1
Manual	1
Ptc Lathe	2
Manual	1
Hobbing M/C	1
Cham. M/C	1
Hyd.Press	1
Shaving M/C	2

4.4 Calculation of Performance Measures of proposed FMS

On the lines of initial sizing calculations, done in the previous section we can estimate the performance measures for the new FMS. The mathematical model described in section 4 can be used to calculate important performance parameters like increased station utilization, overall system utilization, maximum production rate etc. Various performance parameters of proposed FMS and increased utilizations are shown in Table 7 and 8.

Table 7. Performance Parameters of proposed FMS

S.No.	Performance Parameters	Estimated Value
1	Maximum Production Rate (Pcs./Hr)	23.30097
2	Most Utilized Station	100
3	New Bottleneck Station	MINI CHUCKER 1
4	Overall Utilization of System (%)	90.4935

Table 8. Increased Station Utilization in proposed FMS

Stations Utilization	(%)
Mini Chucker 1	100
Mini Chucker 2	87.37864
Broaching	80.90614887
Washing M/c	97.0873786
Manual	85.11327
PTC Lathe	88.99676
Manual	80.90615
Hobbing M/c	96.44013
Cham. M/c	82.52427
Hyd.Press	97.08738
Shaving M/c	97.08738

5. Software model development: simulation modelling of proposed FMS

Simulation modeling is a prototype used to attain a simplified depiction of an intricate system while generating performance parameters of the system. Various simulation software used are Arena, Pro-Model etc but the simulators incorporating system information is advantageous over the others. It is beneficial and less time consuming to use simulation modeling in place of the mathematical models particularly in cases where compound problems are involved. This will aid in determining and substantiate the key performance parameters. For performance of complex systems, ARENA has found a large application in the literature, therefore ARENA 11.0 professional was used for modeling. For the proposed FMS, a model was prepared and simulated to achieve the performance parameters and system's response in real life situations. The simulation results when compared for different parameters with the results obtained from the deterministic model varied between 5-7%.

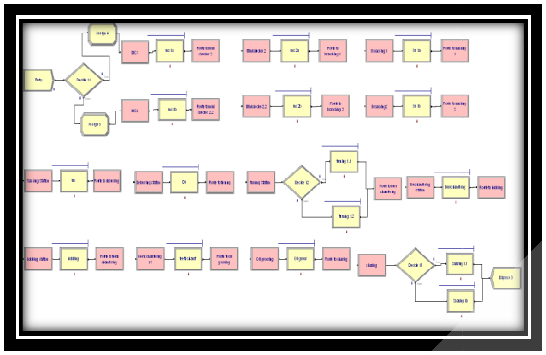


Figure 1. Arena model window

6. Results & Discussions

In the previous section we have presented the performance analysis of existing system and proposed system. Case calculations (Average workload, system utilizations, bottleneck, number of servers etc) are presented in table 3,4,5,6,7 and 8. Initially maximum workload on each workstation has been taken out and it is found that the average workload on shaving station is 300(min) with the total number of servers 2, on this basis the ratio of average workload to server comes out to be 150 (maximum in all stations) which clearly indicates that the shaving station is creating a bottleneck in the processing of gears. To improve the performance it is required either to shift the bottleneck to any other station or neutralize the effect of the bottleneck. So, a new system has been proposed and the bottleneck has been shifted to mini chucker1station with the sufficient number of servers to meet the workload requirement. The mean utilization of the workstations is also another important performance measure. The utilization of each station for the existing system has been calculated and is summarized in table 5. It is observed that most of the stations are underutilized (like mini chucker1, mini chucker 2, washing m/c, manual) whereas some are highly loaded (100% utilized like shaving) and because of this only the overall performance of the system is very less. To overcome this problem the seizing of the proposed system is done. For the optimum number of servers for each workstation have been done and presented in table 6. Comparison between the old and proposed system's station utilization and the number of servers is shown.

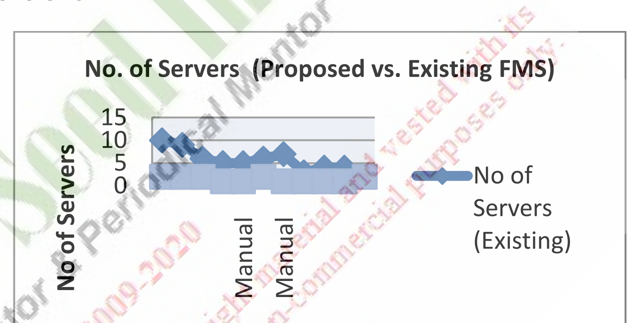


Figure 2. No. of servers (existing vs proposed)

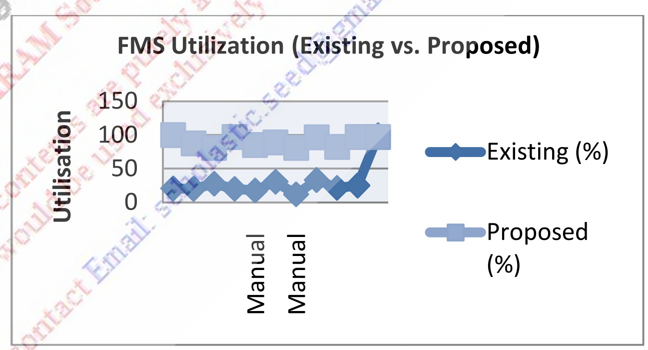


Figure 3. FMS utilization (Existing Vs Proposed)

A comparison chart of all the parameters (station utilization, maximum production rate, bottleneck etc) showing performance improvement (verified with simulation) is presented in table 9.

Table 9. Comparison Chart of Performance Parameters of FMS (Proposed vs. Existing)

S No.	Performance Parameters	Proposed	Existing
1	Maximum Production Rate (Pcs./Hr)	23.30097	24
2	Most Utilized Station	100	100
3	New Bottleneck Station	MINI CHUCKER 1	Shaving Machine
4	Overall Utilization of System (%)	90.4935	24.4481

Conclusion

The evaluation of performance parameters in this case study is based on a universally accepted mathematical model given by [Solberg[iv], (1981); Mejabi[xviii], (1988)]. The performance parameters of the manufacturing firm's present conventional manufacturing system were calculated analytically. A new FMS model is then proposed by reducing the number of servers to an optimum number. The new FMS model shows an improved machine utilization and reduced workload per machine. In the present system, Shaving, a very important gear manufacturing operation, was the bottleneck station. It had the maximum workload per server and 100% machine utilization amongst all the operations. The aim of the new designed FMS was thus to reduce the workload on Shaving machine & shift the bottleneck station to a less significant station. According to the new model, Mini chucker was classified as the new bottleneck station. In order to have a better machine utilization, the workload has been redistributed in the proposed FMS. Machine utilization, witnessed a significant increase from 11 to 30% to 80 to 100% in the proposed model.

Reference

[i]Browne, J., Dobois, D., Rathmill, K., Sethi, S.P., and Stecke, K., (1984),*"Classification of flexible manufacturing systems"*, The FMS Magazine 2, pp. 114-117.

[ii]Womack, J. P., Jones, D. T., Roos, D., (1990), *"The Machine that Changed the World"*,New York: Rawson Associates, pp.11–15.

[iii]Stecke, K., (1983), *"Formulation and solution of non-linear integer production planning problem for flexible manufacturing systems"*, Management Science 29 ,pp. 272-285.

[iv]Solberg, J. J.,(1981), *"Capacity Planning with a stochastic work flow model"*, AIIE Transaction, Vol.13, No.2, pp.116-122.

[v]Gowan, Jr. J.A, Mathieu R.G., (1996), *"Critical factors in information system development for a flexible manufacturing system"*, Computers in Industry, v.28 n.3, pp.173-183.

[vi]Edghill, J.S., and Davies, A., (1985), *"Flexible manufacturing systems - The myth and reality"*, International Journal of Advanced Manufacturing Technology, Vol-1,pp. 37-54.

[vii]Jaikumar, R., (1986), *"Postindustrial manufacturing"*, Harvard Business Review 64 ,pp. 69-7.

[viii]Kumar, S., Sridharan, R., (2007), *"Simulation modeling and analysis of tool sharing and part scheduling decisions in single-stage multi-machine flexible manufacturing systems"*, Robotics and Computer-Integrated Manufacturing, Vol-23, pp. 361–370

[ix]Chan, F.T.S., Chan, H.K. (2004), "*Analysis of dynamic control strategies of an FMS under different scenarios"*, Robotics & Computer-Integrated Manufacturing Vol 20(I5), pp.423-437

[x]Sethi, A. and Sethi, S., (1992), *"Flexibility in Manufacturing: A survey"*, International Journal of Operations and Production Management, pp. 35-45

[xi]Wadhwa, S., Rao, K.S. (2000), "*Flexibility: an emerging meta-competence for managing high technology"*, International Journal of Technology Management, Vol. 19, Nos. 7/8.

[xii]Benjaafar, S. and Ramakrishman, R., (1996), *"Modeling, measurement and evaluation of sequencing flexibility in manufacturing systems"*, International Journal of Production Research, Vol. 34, pp. 1195-1220

[xiii]Shnits, B., Rubinovittz, J., Sinreich, D., (2004), *"Multi-criteria dynamic scheduling methodology for controlling a FMS"*, Int. J. Prod. Res., Vol. 42, pp. 3457–3472.

[xiv]Correa, H. L., Slack, N., (1996), *"Framework to analyze flexibility and unplanned change in mfg systems"*, Comput.-Integr. Manuf. Sys., Vol. 9, pp.57–64.

[xv]Kouvelis, P., and Kiran, A.S. (1989), *"Layout problem in flexible manufacturing systems: Recent research results and further research directions"*, in: Proceedings of the Third ORSA/TIMS Conference on Flexible Manufacturing Systems-Operations Research Models and Applications ,pp. 147-152.

[xvi]Wadhwa, S., Rao, K. S., Chan, F. T. S., (2005), *"Flexibility-Enabled Lead-Time Reduction in Flexible Sys"*, Int. J. of Prod Research, Vol.43(15), pp.3131-3163.

[xvii]Chan, F.T.S., (2003) *"Effects of Dispatching and Routing Decisions on the Performance of a Flexible Mfg Systems"*, Int. J. Mfg Tech., Vol.-21, pp. 328-338

[xviii]Mejabi, O., (1988), *"Modeling in Flexible Manufacturing Systems Design"*, Ph.D. Dissertation, Lehigh University, Bethlehem, Pennsylvania, USA.

XML Secure Documents for a Secure e-Commerce Architecture

Rupesh Kumar
Department of Management Studies, I.I.T. Roorkee, India.
rk584ddm@iitr.ernet.in

Mario Muñoz Organero
Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid, Spain.
mario.munoz@uc3m.es

Rajat Agrawal
Department of Management Studies, I.I.T. Roorkee, India.
dr.rajat07@gmail.com

ABSTRACT

Security is one of the main issues that must be taken into consideration before implementing e-Commerce architecture. The architecture can be developed by using some security factors namely confidentiality, integrity, authentication, and non-repudiation for XML web services. This paper has examined these factors for implementing the secured system by using suitable security services like XML Encryption, XML Decryption, XML Signatures, and XML Validations. Various algorithms, implementations, and coding have been developed for security services and web services for creating the secured system. The most important part of the system is the gateway or web service which is implemented with suitable technologies for passing only the XML file throughout the whole system. This study shows how only XML files pass from client side to the server side through a central gateway with the help of web service applications. The result indicates that the XML file is delivered securely to its destination in the secured e-Commerce architecture which is mandatory for organizations like banking, insurance etc.

KEYWORD

Security	XML Signatures
e-Commerce	XML Validation
XML Encryption	Web Service Security
XML Decryption	Cryptography

Empirical Article

Preface

In the early 90's, the advent of internet technologies has opened a new phase to globalization. Many of the companies like SME's or organizations are today using such technologies i.e. World Wide Web (WWW) for doing their businesses online. This gives an opportunity to reach large number of peoples to get involved in the business where the proper development of web applications is applied. These technologies are very much useful for the organizations like medicine, education, banking, e-Commerce,[i] etc to share their information electronically. But the main issue for performing such activity is the security. Security is the primary concern that must need proper attention to overcome in exposing sensitive data. The security has four important factors such as confidentiality, integrity, authentication, and non repudiation. Due to adoption of these factors, any e-Commerce architecture can be designed securely. This study shows that how the e-Commerce architecture is designed securely with the help of these security factors that depends on some security services like encryption, decryption, signatures, and validations. The purpose of using these services is to establish a smooth flow of XML document throughout the designed system. This study shows the designed system is passing only XML file from intranet to the internet via gateway. Gateway is also called as web service which is a java application and has direct access to the database. The interaction between intranet, internet and gateway is very much effective to pass the secured XML file in the system. The basic design of the system is shown in Figure-1,

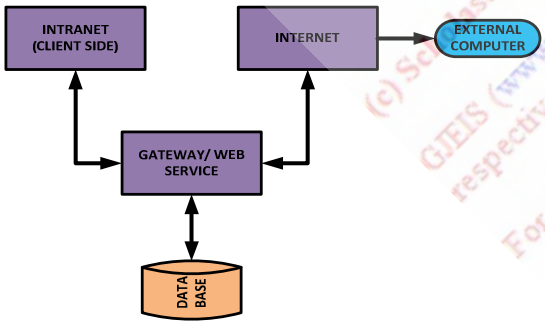


Figure 1: Basic Design of the System

During the past few years, Web services, a collection of technological standards that are using by many organizations in an effective manner. For example: almost every major software companies like Sun, Microsoft, IBM, TCS, etc are working with it. Web services are used to enhance many web applications by using suitable technologies that helps to maintain the system security level. The implementation of the web service is the most important part to give an effective output for designing the system. Web service is defined as a service that sent messages by using standard hypertext transfer protocol (HTTP) protocol[ii]. Others protocol like internet protocol i.e. Simple Mail Transfer Protocol (SMTP) is used for sending e-mail in this designed system. This study explained the necessities of using web service. The proper integration of the web service will work in an effective manner with the use of certain technologies. Web service technology is used for exchanging data securely among the peoples. For example, searching information over internet based on security factors. XML is a text based format which is highly supportable by the web services.

XML has no wire security[iii] that can exchange standard documents by means of e-Commerce applications. World Wide Web Consortium (W3C) is working with two specifications for securing the XML documents namely, XML Signatures and XML Encryption standards[iv,v]. These specifications are very useful for signing and encrypting the XML file. These standards are the integrated technologies of the web service security with cryptographic requirements[vi]. Both these standards are applied for Key-Info element which includes the child of Signed-Info, Encrypted-key element, and provide some key materials used for validating the signed XML file or decrypt the encrypted XML file[vii]. XML Signatures must be used only when validation takes place whereas, XML Encryption is used only when decryption takes place. In this way, these four security standards are interlinked to each other in a proper sequence to create effective and secured system. This study shows the use of such security standards while implementing this e-Commerce architecture by using some predefined application programming interface (API's) with suitable visual tools.

Now summarizing the main objectives of this paper are,

- to sending and/or receiving only XML document in a secured way from client to receiver end via gateway using Java programming language
- to study various security services like XML Encryption, XML Decryption, XML Signatures, and XML Validations with the help of respective algorithms

- to configure the gateway with web service applications for developing the secured system using one of the API method

Literature Review

E-Commerce

With the advent of e-Commerce application brings revolutionary for the companies. Many companies get benefit from e-Commerce usage. E-Commerce has also brought drastic changes among the peoples view. By using this concept, the relationships among the sellers-buyers have improved and fulfill the customer needs very quickly. In early 1980, this application has client-server architecture which is used for improving e-Commerce factors like usability, flexibility, interoperability, and scalability[viii]. With the improvement of such factors will reduce the operating cost, and give support to customers and trading partners. But the main disadvantage to the e-Commerce architecture is the security. If an e-commerce system is not secure then no one will have the confidence to use it for carrying out high level business transactions. For example, internet is an unsecured network for sharing the information between two parties. But the information can be accessed freely through an open source[ix]. The insecurity level can be fulfilled by using certain security technologies as used for designing this system. Due to insecurity reasons, electronic businesses will not take place unless the accuracy and the authenticity of signatures are confirmed.

Concept of XML

The extensible Markup Language (XML)[x] is a collection of data which describes the structure of the data. XML format is platform independent which is used for representing the data. For example, Microsoft products such as Word, Excel, and Visio allow the documents to get stored in XML format[vi]. The concept of XML document is the element which further divided into two tags i.e. placed at the beginning of the element and another at the end of the element. XML is a sort of database management system (DBMS) which includes storing XML documents, Document Type Definition (DTD) schemas, parser methods, etc. XML access the data very slowly due to use of parser methods and while converting the text. This study has used Simple Application Programming Interface for XML (SAX) parser for loading the element in the XML document. The designed system is created with this parsing method such that the XML document passes inside the system as a string form. This must be overcome by using suitable parser for implementing the web service is developed using Java programming.

Concept of WS-Security

Web services is a web based application that provide services over the internet in form of data. The data can be exchanged by using transport protocol with the use of web services. These services are developed using predefined API's and tools and technologies by an integrated Web Services Stack. The web service plays an important role while transactions in the whole process of the system.
Web Service Security provides message level security with security factors like confidentiality, authentication, and integrity by using XML Encryption and XML Signatures for web services. WS- Security is defined as a web based application that provides security to web services. It is a communication protocol which contains certain specifications to show how security factors are enforced on messaging. In April 2002, some companies like IBM, Microsoft have proposed certain specifications which address few issues for web service security like WS-Policy, WS-Trust, WS-Privacy, etc[xi]. WS-Security is controlled by using these policy files of the target web service. With the use of WS-Security, the data is encrypted securely before it reaches the target web service.

Concept of Cryptography

Cryptographic techniques are used for building a secure e-Commerce system[viii]. The secured system depends on the concept of XML Encryption and XML Signatures technologies which fulfills the system security[xii]. Cryptography is defined as "to keep messages secret". This can be done by using some common elements like public keys, private keys, algorithms, key pair generators, key factories, and key stores[iii]. Cryptography is generally classified into two pair of keys are symmetric and asymmetric keys. This concept is generally applied throughout the banks or companies for sending any confidential and private information or data. This technique is used with the help of certain security factors through which only authorized person get privilege for accessing

the information. By considering these factors, XML document can be send easily to various banks, large corporations, IT companies, small businesses etc with universally accepted standards. Figure-2 shows all four security factors are interlinked with each other through security services.

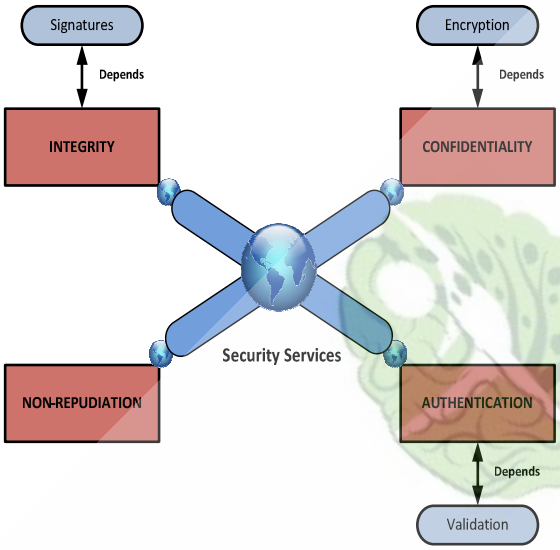


Figure 2: Security Factors

The following are the main security factors of the designed system as follows,

	Main security factors of the designed system
Confidentiality	It is used to keep the information secret so that only intended recipient can read. Data confidentiality is accomplished by using security services i.e. encryption. With the help of encryption method, the data can be accessed only to the authorized parties.
Integrity	It is used only when the information is not tampered so that the recipient can detect it. Data integrity is accomplished by using digital signatures. With the help of digital signatures, nothing is added nor taken from the information in an unauthorized way.
Authentication	It is used to establish or validate the identity throughout the system. Authentication is accomplished by using validation method. With the use of validation, one can access the secured system with username and/or password in an open e-Commerce system.
Non-repudiation	If integrity and authentication can be ensured, then the non-repudiation requirement can also be satisfied. This means that while transaction, sender or receiver has to prove to a third party that their counterpart must take an action to achieve the desired necessities.

Concept of XML Security

In open e-Commerce architecture, security is the key issue for doing businesses through WWW. The security is integrated with certain XML technologies like protocols to provide XML solutions[xiii]. The main aim of XML security is to implement the security standards using XML. These security standards can be placed at different levels i.e. XML Signature, Secure Socket Layer (SSL), S-HTTP etc[ii]. There are many security technologies and cryptographic techniques that help to provide practical solutions to fulfill the security requirements. In this way, the XML security comes in position to provide security to the parts of the XML document. XML provide granularity and their security services are much portable in using some standards of XML. Thus, XML Security reduces some barriers by defining minimum security standards to obtain better results. The first XML specifications were published in the year 2000 for defining the trust services. The older security technologies had created a platform for algorithms and technologies to define trust by using XML Security services. The Organization for the Advancement of Structured Information Standards (OASIS)[xiv] is responsible for XML security services which produce some specific standards.

XML Encryption

It is defined as W3C XML Encryption[xv] used for encrypting the XML elements. The purpose is to maintain the confidentiality of information during the encryption process with the help of Secure Socket Layer (SSL) or Transport Layer Security (TLS) or Virtual Private Network (VPN). The encryption process is controlled by encryption key. In simple terms, XML Encryption provides end-to-end security[xvi] and used to encrypt the XML document which further represents the encrypted data in XML documents. This is possible only when proper use of algorithms and technologies are defined. The reliability of the encryption algorithm depends on the size of the key or number of bits[viii]. If the encryption key is not reliable then the output will vary accordingly. The designed system is using XML encryption to encrypt the whole XML elements using suitable algorithms like (AES, DES) and technologies that are associated with it. Derek Smyth has identified "XML encryption is used for encoding the XML documents by scrambling them into a jumbled numerical sequence"[xvi]. This means that XML Encryption is used for the conversion of original message i.e. plaintext to the ciphertext (scrambled message, for example-123@98@ndnsk3c9kf) with the help of encryption key as shown in Figure-3.

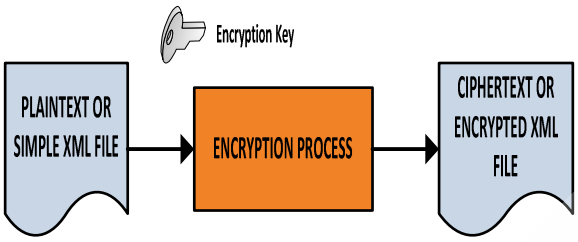


Figure 3: XML Encryption

For this, the following encryption function shown,

- E [plaintext | encrypt_key] = ciphertext

where, E is the encryption, plaintext is the XML file, ciphertext is the encrypted XML file i.e. secret message, encrypt_key is the encryptin key.

XML Decryption

It is defined as a W3C XML Decryption[xvii] used for decrypting the encrypted XML file. In simple terms, XML Decryption is used for the conversion of ciphertext i.e. encrypted XML file to the original message i.e. plain text[xvii]. This means that it is the reverse process of the XML encryption. During the process, the conversion of messages take place by using decryption key as shown in Figure-4. This is possible only when developed with suitable algorithms (RSA) and techniques as in the designed system. The correct decryption key only gives result to obtain back the original message or file. The following decryption function shows a general example,

- D [ciphertext | decrypt_key] = D [E [plaintext | encrypt_key] | decrypt_key]

Or,

- D [ciphertext | decrypt_key] = plaintext

where, D is the decryption, decrypt_key is the decryption key.

Figure 4: XML Decryption

XML Signatures

XML Signatures also called as XMLDsig, XML-DSig, and XML-Sig which is defined as a W3C XML Signatures[xv] used for signing the digital content and verifying the digital signatures. This method is used to provide data integrity that no one can tamper with the information. W3C defines XML syntax for digital signatures which is used to sign the XML file using PKC#7[xviii]. XML Signatures are designed for secure transactions in form of XML format. There are certain technologies and suitable algorithms i.e. DSS used for XML signatures in the designed system. The digital signatures can be read on any computer because of the same message digest and hash algorithm which is used for signing the XML file. [xix]OASIS explains that the digital signatures are used to sign just parts of the XML document by an authorized user only. For example: a form where user needs to fill it with their personal data. The designed system shows that XML Signatures is used only when encryption process takes place for encrypting the XML file with suitable key[viii,xx]. The basic steps for generating the digital signatures are shown in Figure-5.

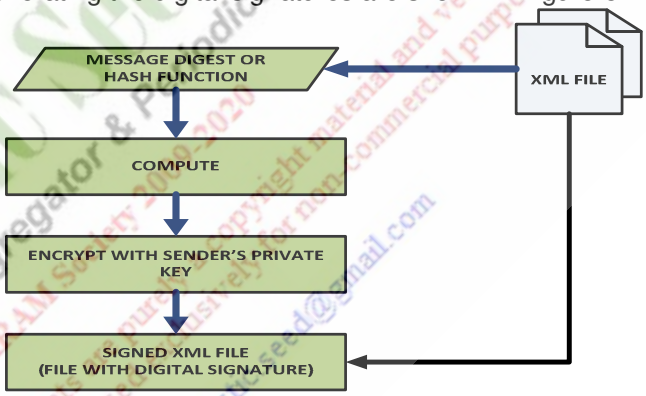


Figure 5: Steps for generating XML Signatures

XML Validation

It is defined from the W3C recommendation[xv] which is used for verifying the digital signatures. XML Validation is used to validate the decrypted XML file which satisfies the authentication and data integrity. The output of this always performs in true/false statement or in binary form i.e. 0's or 1's. In the designed system, XML Validation is operating on the gateway i.e. internally which verify the signed information to generate the original message or XML file. It is possible with algorithms like DSS and RSA which are used for performing the validation method in this system. [xxi]Bradley W. Hill has proposed that the signatures can be verified with the help of same hash algorithm as used by the sender and signer's public signature key. If it does not, then the signature will not be verified which gives unsatisfactory result in terms of error or false statement.

Problem Definition

1. The sending and/or receiving only XML document (modern web service technology) on the internet is the real problem for sharing the information in an effective manner. Thus, the number of ciphers exists in the system to give more or less satisfactory result. To overcome this problem, the proper pairing of secret keys must be required as the whole system security depends on these keys. With the advent of commercial data networks, the system security is important because there should be proper communication between the parties with the help of cryptography technology.
2. With the use of security services like XML Encryption, XML Decryption, XML Signatures, and XML Validations is useful for providing solutions to the SME's, or less affluent businesses. But there are certain problems exist that must be taken into consideration before employing private key encryption method in an open e-Commerce system. These are,
   - This method uses the same key for the encrypting and decrypting the XML documents which is a problem. To overcome this problem, the establishment of different secret keys with each receiver is needed.
   - The key distribution methods may not work well in an open e-commerce system because both the sender and receiver do not know each other previously or may be in different locations in the world. This problem can be only solved if both sender and receiver know each other but it does not matter whether they are located in different part of the world[viii].
   - The passing of secret keys between the parties in a secured way is very important because the private key encryption method relies on keeping the private key secret otherwise the whole method becomes useless.
   - The classical way of distributing secret keys to each user(s) pair becomes very expensive.
3. The most important and complicated part of the system is the gateway/web service which is a java application that helps in developing the secured system. Due to which, various methods are implemented securely with the help of predefined API's and tools & technologies. With the use of these tools, the system requires extensive professional services for solving the programming problems. Thus, the proper implementation is also extended which delays system deployment and consequently anticipated revenue and profitability gains. This study shows the system is designed for passing only the XML document with the security services. Thus, some complications must be taken care likewise,
   - There should be proper format of methods require for implementing the gateway
   - The algorithms used for these applications must be supportable individually
   - The databases used for the system also warrant a business to employ additional resources for licensing, maintenance, and administration

Hypothesis

- **The gateway/ web service is implemented using some security services like XML Encryption, XML Decryption, XML Signatures, and XML Validations.**
- Only XML document can able to pass throughout the designed system without any information leakage.
- The designed system is completely secured.

Research Design

The aim of this study is to send and/ or receive the secured XML document from intranet (client side) to the external computer (receiver end) through a gateway with web services applications using Java. To achieve this aim, the objectives of the study are divided into three main parts. These parts comprises of theoretical investigation and practical implementation of the gateway or web services. The middleware or logical part i.e. the gateway is the most important and complicated part because of configuring the gateway in such a way that the XML document must pass throughout the system securely.

The design of the research is divided into three stages are as follows,

- At the primary stage, the study requires to understand the concept of using suitable algorithms for generating

the appropriate pairing of keys with security services/ methods in implementing the gateway. This stage also requires the use of appropriate tools for developing the designed system.

- At the secondary stage, the designed system is passing only the XML documents via gateway, so that, the study needs to know the type of parser methods used to support XML document.
- At the tertiary stage, the study requires the description of security services/ methods namely XML Encryption, XML Decryption, XML Signatures, and XML Validations of the designed system, and to find out the sequential order for implementing these methods to provide successful secured system. This stage also describes the four security factors that are associated with these methods of the designed system.

Research Methodology

The method for performing this study, the information is collected through WWW by observing the suitable techniques, and using predefined application programming interfaces (API's). These techniques are the security services and the suitable algorithms. For integrating the designed system with these techniques, only the visual tools like Net beans or Eclipse can be used. In this, we have used Net beans 6.0 version and proper Java Development Kit (JDK) version for implementing the system. The Java programming language is used to implement the web service applications, and MySQL database is used for storing the critical information of the users and the XML documents in the system.

System Logic Structure

The logic behind the designed system is to pass the XML document or file from sender end to the receiver end without any complications. For this, the structure of the system is shown in form of flowchart [see Figure-6] which divide into two parts namely sender part, and receiver part as discussed below,

1. **Sender Part of the designed system:** This part is also known as encryption client window through which the security services like encryption and signature processes are performed for signing and encrypting the .xml file. One can select any of the .xml file and choose email-id from the list of stored users in the encryption client window for performing the security services. Due to this, the whole element of the XML file is encrypted successfully after signing the file and an automatically email is generated to the respective users email-id with the notification in form of message in this client window. The encrypted file will finally get stored in the database on the server side with the help of proper use of supporting symmetric algorithms i.e. AES and DES. This encrypted file will be accessed later on by the user(s) to whom the document is sent to their email-id. For sending the email, Simple Mail Transfer Protocol (SMTP) protocol is used to show the message in text format. The text of the email will show like **"THIS IS AN AUTOMATIC GENERATED E-MAIL. PLEASE CHECK YOUR DATABASE FOR GETTING THE ENCRYPTED FILE".** Finally the output of the sender part comes in the form of signed and encrypted XML file that is waiting for the receiver or user end to access it.
2. **Receiver Part of the designed system:** This part is also known as decryption client window through which the remaining two security services like decryption and validation processes are involved for decrypting the encrypted XML file and then validating it. This part is operated by the user or receiver for accessing the decrypted XML file by entering their decryption-id or user-id and also selecting the path for saving the decrypted file to their respective computer. The decryption-id is already known to the respective user(s) which is generated automatically according to the latest date and time in the database. The database can be access only after receiving the email confirmation to the user end for getting the encrypted file from the server to perform decryption and validation process. These security services are performing with the help of proper use of supporting asymmetric algorithm i.e. RSA and hash algorithm i.e. DSS which helps in decrypting the encrypted file after validating the signatures and finally stores the decrypted file or original XML file to the personal computer at the user end.

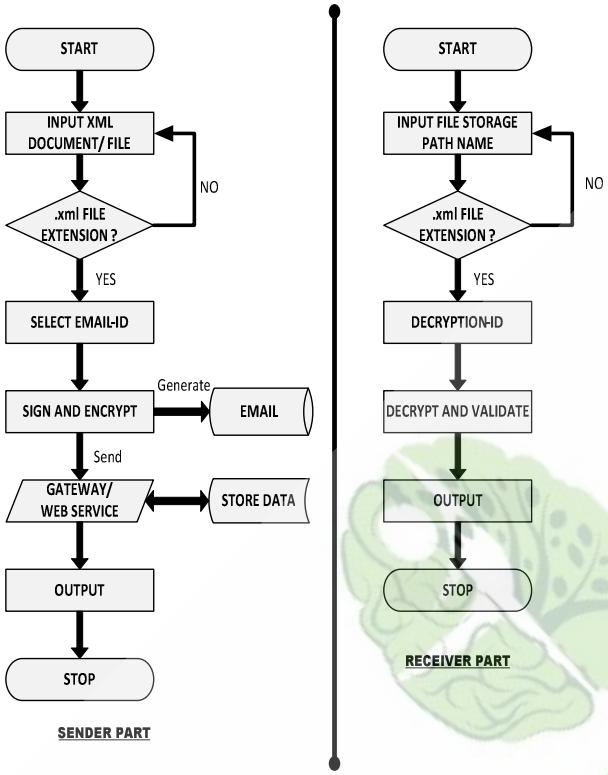


Figure 6: Flowchart of the System

The complete system is designed by using these four security services in a sequential order so that the system works effectively. These services perform in the following stepwise [Figure-7],

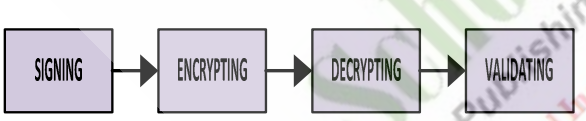


Figure 7: Steps for performing Security Services

Finally the outline design of the developed system is further discussed with the output in the following section and shown in Figure-8.

Results and Discussion

The designed system is a three tier architecture which comprises of intranet, gateway, and internet. These tiers have physical and logical parts for developing the architecture of the system. The most important part in the designed system is gateway/ web service (middleware part) which has some logic behind it for implementing the system. The logic is to pass only the XML file throughout the whole system. This is possible only when the gateway is implemented by applying security services namely, XML Encryption, XML Decryption, XML Signatures, and XML Validations using predefined API's. The designed system shown in Figure-8, gateway performs the four main security services. In this way our first hypothesis is satisfied. The system is also designed in such a way that only XML file passes so that the whole elements of the XML file must be encrypted by the sender and then sent to the receiver for decrypting the whole elements of the XML file with suitable parser. In this way, the information in the XML file (textual data format) remains confidential and can be easily accessed by the authorized party. Thus, we accept our second hypothesis. The architecture of the designed system also shows the security level of the system that up to what extent the system is completely secured. For this, we have used certain symmetric, asymmetric, and hash algorithms with predefined API's using Java Programming language to develop the designed system. Due to proper integration of gateway using these techniques, the system is very much useful in open e-Commerce architecture. This states that our designed system is fully secured which satisfied our third hypothesis.

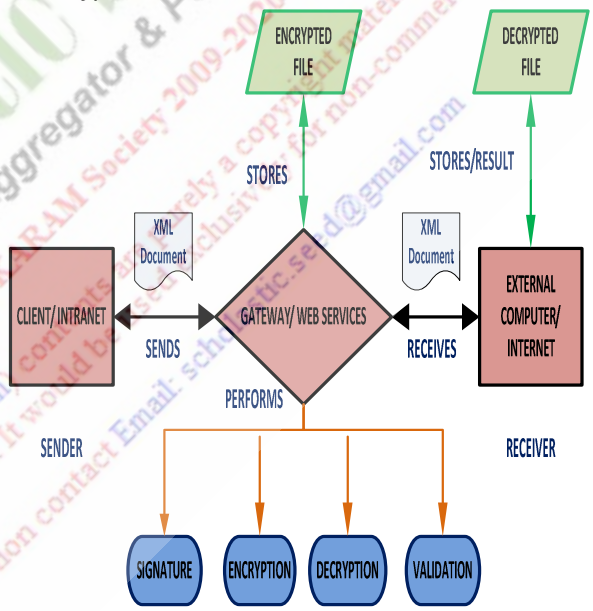


Figure 8: Outline Design of the Software

At the middle tier of the designed system shown in Figure-8, gateway or web service which is a java application finds the place. This tier is intermediary between the intranet

and internet in the designed system. This tier is the most important among others and faces many complications while integrating it with some predefined logics. This layer is responsible for any data manipulation or processing the XML file securely, if the proper integration takes place. The middleware part has direct access to the databases and keeps the encrypted XML file safe on the server side. All these data access objects help to retrieve, update, and delete data from relational databases or XML files. This will be happen only when suitable techniques are applied as this system does. The real implementation of the system especially gateway depends on the company requirements or in business processes. For example, when someone in the company wants to send a secured XML document then it executed the appropriate method in the gateway using the web service interface. In result, when someone in other company receives a secured XML document it does the opposite which involves the corresponding operation in the gateway using the web service. This makes the system very beneficial for the future as involving the security services. Hence, the system is designed in such a way to provide solution for less affluent, small and medium sized businesses. The security services like XML Digital Signatures include signing and validating the XML file are computationally expensive which takes more CPU time to perform the cryptographic operations. For resolving this problem, appropriate tools must be used for the system.

The architecture is generated and implemented to give advantage to the web based business applications like banking or insurance etc. The designed system shows that all the three layers are fully separated and play an individual role during implementation. The first layer or presentation layer i.e. client side is designed to pick only XML files for signing and encrypting it. This is a simple application and is responsible for displaying the user interface with the gateway i.e. a web service. Thus, both client side and gateway can easily communicate with each other for sending the XML file. The middle layer i.e. gateway use all the four securities services and makes the system fully secured to pass the XML file without any barrier. This is the complicated part of the designed system. The third layer or the last phase i.e. receiver end is to decrypt the encrypted XML file by validating the signatures. This is also a simple application and designed in such a way to communicate easily with the gateway. The interaction between the gateway and the internet is used for sending request and getting response with in each other. The third layer is also used for finally storing the original XML file i.e. also known as decrypted XML file. These three layers are distributed to take advantage of the complete designed dimensions or techniques of the system. Internally, there are some securities factors are involved for performing the operation. These factors are confidentiality, integrity, authentication, and non-repudiation. For secure transactions over internet, these factors are must be taken into consideration to deliver the data successfully. This brings the peoples to take participation in such activities like e-transactions. Hence, the designed system involves these four factors with security services to develop the secured system.

Conclusion

The e-Commerce architecture reveals that all the three layers are interconnected to each other so that the proper communication between them exists. The demand for this architecture is very high in the market. The complicated and highly secured system is creating a fast growing market demand by the buyers. The designed system reveals that the middle tier i.e. gateway act as a most important part which drives the whole system security level. The system may not be secured, if the gateway is not implemented with suitable security services. The secured system is possible only by using suitable security services in a proper sequence and supporting algorithms to these services with the help of visual tool i.e. Net beans 6.0 version with Sun Java Application System Server 9 with supportable JDK version. The security services are the core building blocks of the system which was implemented in huge applications and libraries. Due to security standards, the web service or gateway is implemented successfully by using predefined API's. These standards help to do online businesses as XML technology adopts web services. Now a day, XML is used very frequently for exchanging the information among certain applications across multiple platforms. This system is designed to pass only the XML file with the help of suitable parser methods. Thus, the secured XML messages passes in the system which is more trustable to do the business transactions.

At last we conclude that, the project work have some results i.e. encrypting the XML file, encrypting all elements, auto-generation of email with SMTP protocol, signing and validating operations takes place internally, decrypting the encrypted XML file format, and successfully storing data's in the database. The use of Java API is well performed so that the pairing of keys used for the system are generated and encrypted properly. In this way, the quality of the work is completely satisfying the system needs.

Limitations and Future Work

The study is limited to small enterprises only because the system works internally in the company. As the XML file can be sent and received by only to the limited number of employers those email-ids exist in the company database. Either the company has their different branches in different part of the country or has their branches in the same country or regions. But the database should be same and must be restricted to those employers only whose email-id or information is stored in the database. Only, this restriction makes happen to work successfully with this designed system.

The system can be developed in such a way so that there will be more options for choosing an algorithm from the list while encrypting and decrypting the XML file. This makes the client to select any one of the algorithm two or may be more for encrypting the XML file and in reverse, the receiver also do the same for decrypting it. This will provide more appropriate results by performing such operation with different algorithms. This system is encrypting the whole elements of the XML file but in future, the elements of the XML file can be encrypted separately for making it more secure. The output of the designed system i.e. the decrypted file or original file must come in proper format that needs to be taken care. This format can be developed by using different encoder and decoder code.

Reference

[i] R. Bhatti, E. Bertino, A. Ghafoor (2004) "XML-Based Specification for Web Services Document Security", IEEE Computer Society, pp. 41-49.

[ii] A. Selkrik (2001) *"Using XML security mechanisms"*, BT Technology Journal, Vol. 19, No.3, pp. 35-43.

[iii] J. Hanson (2005) *"Managing XML Encryption with Java"*, Devx Website - http://www.devx.com/xml/Article/28701/1763

[iv] M. Bartel, J. Boyer, B, Fox, B. LaMacchia, E. Simon (2008) *"XML-Signature Syntax and Processing (Second Edition)"*, W3C Recommendation, 10 June 2008 - http://www.w3.org/TR/xmldsig-core

[v] XML Security Suite (AlphaWorks) - http://www.alphaWorks.com/tech/xmlsecuritysuite

[vi] Java XML Digital Signatures (Sun Developer Network, development by the Sun Technology) – http://java.sun.com/developer/technicalArticles/xml/dig_signatures/

[vii] XML Security: Signature, Encryption and Key Management (W3C note) - http://www.w3.org/2004/Talks/0520-hhxmlsec/

[viii] C. Chester; Wiley (2001) *"E-commerce: fundamentals and applications"*, [Henry Chanet al.], pp. 203-217.

[ix] J. Eddington (2006) *"How to build an e-commerce Architecture"*, Free Article:: Tutorial, published on Web Site – http://www.e-articles.info/e/a/title/How-to-Build-an-E-Commerce-Architecture/

[x] Extensible Markup Language (XML Version 1.0) (W3C note) - http://www.w3.org/TR/REC-xml

[xi] Web Services, IBM Web Site – http://www.ibm.com/developerworks/library/specification/ws-secmap/

[xii] Tools for securing your XML documents (Builderau: by developers for the developers) – http://www.builderau.com.au/program/development/soa/Tools-for-securing-your-XMLdocuments/

[xiii] Welcome to XML Security (The Apache XML Project) (Apache XML Security) - http://santuario.apache.org/

[xiv] OASIS Website - http://www.oasis-open.org/

[xv] M. Bartel, J. Boyer, B, Fox, B. LaMacchia, E. Simon (2002) *"XML-Signature Syntax and Processing"*, W3C Recommendation, 12 February 2002 – http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[xvi] XML Encryption (Dotnetslackers Web Site) - http://www.dotnetslackers.com/articles/xml/XMLEncryption.aspx

[xvii] T. Imamura, B. Dillaway, E. Simon, D. Eastlake, J. Reagle (2002) *"XML Encryption Syntax and Processing"*, W3C Recommendation – http://www.w3.org/TR/2002/CR-xmlenc-core-20020802

[xviii] E. Simon, P. Madsen, C. Adams (2001) *"An Introduction to XML Digital Signatures"*, O'REILLY Publication XML.com, XML from the inside out -

http://www.xml.com/pub/a/2001/08/08/xmldsig.html

[xix] XML Digital Signatures (Cover Pages hosted by OASIS) (Technology Reports) - http://xml.coverpages.org/xmlSig.html

[xx] XML Signature Features (W3C Recommendation) - http://www.w3.org/2004/Talks/0520-hh-xmlsec/slide6-0.html

[xxi] Command Injections in XML Signatures and Validations (Information Security Partners Web Site) – http://www.isecpartners.com/files/XMLDSIG_Command_Injection.pdf

http://www.karamsociety.org

COMPUTER AIDED DESIGN TOOLS AS APPLIED TO AESTHETIC DESIGNS

Navneet Kumar Pandey

Asst Prof, Mechanical Engineering Department, Vishveshwarya Institute of Engineering &Technology, GB Nagar, India

pandeynavneet1@rediffmail.com

Ram Kumar Tyagi

Asst Prof, Mechanical Engineering Department, Amity University, Noida, U.P. India

tyagi_rk1@rediffmail.com

ABSTRACT

Computers have now found applications in almost every field of engineering now, the same applies to mechanical engineering also with computers been used in the field of design and analysis of components. In this paper we have attempted to explain the utility of computers in the field of aesthetic design of components or system as a whole. Aesthetics are the components of design, which affect the visual importance of the component hence we have tried to explain the application of curves with different continuities to elaborate and make the design procedure better and more pleasing. The various tasks involved in the aesthetic design procedure have also been discussed and their inherent advantages and disadvantages have also been discussed.

KEYWORD

Mechanical Engineering	Computer
Design	CAD
Quality	Loop
Virtual	Surface

Preface

In this article, we are concerned with computer-aided design tasks in which the final evaluation is mostly based on aesthetic criteria. While most engineers accept the fact that one needs to use computers to design jet engines, computer chips, or large institutional buildings, it is less clear whether computers are also useful in the design of artifacts that are judged mostly by their looks. In a traditional CAD setting, the computer primarily serves as a precise drafting and visualization tool, permitting the designer to view the emerging geometry from different angles and in different projections. A digital representation also makes it possible to carry out some analytical tasks such as determining volume or surface area of a part.

Creating maximally satisfactory forms for mathematical models or for geometric sculptures poses quite different requirements and constraints for any CAD tool than developing an optimized airplane wing or designing the most powerful computer chip. Real-time interactivity becomes a crucial factor, when a designer's eye is the key evaluation instrument in the design loop.

This article overview starts by looking at some generic tasks in curve and surface design, in particular, ongoing efforts for defining a beauty functional for procedurally optimizing shapes that are only partially constrained by the designer. It then discusses some research aimed at finding efficient implementations and approximations of such optimization functionals, so that they can be used at interactive design speeds. Next, we look at a parameterized design paradigm that allows an artist to rapidly explore and compare many alternative versions of a geometrical shape. Finally, we make the point that a CAD tool that is well matched to the task at hand is much more than just a 'drafting assistant' and can indeed become an amplifier for one's creative spark.

Smooth surfaces play an important role in engineering and are a main application for many industrial CAD tools. Some surfaces are defined almost entirely by their functions; examples are ship hulls and airplane wings. Other surfaces combine a mixture of functional and aesthetic concerns, e.g. Car bodies, coffee cups, flower vases, etc. Finally, for some cases, aesthetics dominates the designer's concern, for instance in abstract geometric sculpture.

For either situation, it can be argued that an ideal surface design system should allow a designer to specify all the boundary conditions and constraints and then provide the 'best' surface under these circumstances. Best in the context of this article would mean an optimization with respect to some intrinsic surface quality related to its aesthetic appeal. To be usable in a CAD tool, that quality has to be expressible in a functional or procedural form. Commonly, the characteristics associated with 'beautiful' or 'fair' surfaces imply smoothness at least tangent-plane (G^1-) continuity, but often also curvature (G^2-) continuity. If the surface is covered with some textural pattern, then we have to demand more than just geometric continuity and also require smoothness of the parameterization, i.e. C^1- or C2-continuity, respectively. Additional characteristics often cited in the definition of aesthetic shapes are symmetry and simplicity. The first implies that symmetrical constraints should result in symmetrical solutions; and the second implies avoidance of unnecessary undulations or ripples.

All these properties are exhibited by minimal surfaces, i.e. By the shapes assumed by thin soap membranes spanning some given boundary (as long as the air pressure on both sides is the same). Experimentally, such shapes can be generated by dipping a warped wire loop into a soap solution. The lateral molecular membrane-forces will try to minimize overall surface area and thereby implicitly create a minimal saddle surface in which the mean curvature at every point of the surface assumes the value zero. Now, a decade later, what are the prospects for evaluating such functionals at the desired, almost instantaneous and truly interactive rate?

- First, of course, computer power has increased by one to two orders of magnitude over the last decade, thus bringing us closer to our goal of full interactivity, even without any further innovations.

- Second, and most importantly, subdivision surfaces have become mature and popular. They allow us to obtain surfaces with a reasonable degree of built-in continuity by their inherent construction, thus avoiding the very costly inner optimization loops that were used originally to guarantee smoothness at the

seams.

- Third, the inherently hierarchical organization of sub- division surfaces gives us the possibility to optimize the gross shape of the surface at a relatively coarse level, where only a small number of control points have to be adjusted. Then as we gradually refine the surface by increasing the level of subdivision, the number of degrees of freedom grows at a quadratic rate; but since the surface is already relatively close to the desired shape, the optimization procedure need not run for many iteration to achieve convergence

- Fourth, at the research frontier, experiments are now under way to find means to avoid the expensive numerical integration steps in the inner loop of the optimization. The aim is to find a discretized approximation of the salient surface characteristics, to obtain directly an estimate of the behavior of the cost functional that is good enough to guide the gradient descent optimization in the right direction

As our basic framework, we use subdivision surfaces to represent the shapes to be optimized. Using finite differences based on incremental movements of the control vertices, a gradient vector for the chosen cost/energy functional is obtained and then used to evolve the surface iteratively towards a local cost minimum. After obtaining the minimum energy surface for a given mesh resolution, the mesh is subdivided to produce new vertices and therefore new parameters for optimization. In this general approach, we can vary the methods for calculating the actual optimization moves, trading off accuracy for speed.

As a baseline for comparing the various methods, we use exact evaluation of the subdivision surface sampling the limit surface to obtain its geometric properties. Using differential geometry and numerical integration by Gauss-Legendre quadrature, we can compute it with high accuracy a cost functional such as the bending energy. Using this energy computation in the above framework, we can obtain robust results that agree with the theoretically known energy minima for some highly symmetrical smooth surfaces, such as spheres, torus, or the known energy minimizes of higher genus. Since numerical integration and gradient calculations are computationally expensive, this method may take a few hours for surfaces however, it serves as an excellent benchmark for evaluating more approximate methods.

A first simplification calculates an approximate cost functional directly from the discrete mesh of control points of the subdivision surface, as is done, for instance, in. We are exploring vertex-based as well as edge-based functional that express the surface energy as a summation over the local energy at all the vertices or edges. These local energies are calculated with a discredited approximation, using polynomial expressions of vertex coordinates and/or dihedral angles along the edges. These simpler functional are adequate to guide the gradient descent process in the same direction as a more exact functional evaluation would, but do so at significantly reduced cost and thus with higher speed

Interactive CAD applications

With this speedup resulting from the use of discrete functional and/or direct vertex-move calculations, we can envision a CAD system in the not-too-distant future, where the designer specifies boundary conditions and constraints for a surface panel and then picks a suitable cost functional for a quick optimization of the surface. The designer may compare and contrast the results of using two or three different aesthetic functional and choose the one that is most appropriate for the given application domain. The designer further can adjust some of the original constraints or add new ones to force the surface to meet functional as well as aesthetic expectations. The role of the chosen functional is to take care of the details of the surface shape, e.g. to avoid geometric discontinuities or unneeded wrinkles and slope changes

A second key CAD problem is the embedding of beautiful or fair curves onto the kind of optimized surface discussed above. For instance, one may need to draw a fair connecting line between two points on a smooth surface.

The most direct such connection is a geodesic line,

which exhibits no gratuitous lateral curvature. While it is easy to trace a directional geodesic ray on a smooth surface or on a finely tessellated polyhedral approximation thereof, it is a well-known hard problem to connect two points with the shortest geodesic path on a surface that exhibits many areas of positive and negative mean curvature.

Sometimes the geodesic line segment is too restrictive for design purposes; it offers no degrees of freedom or adjustable parameters to the designer. This limitation is particularly detrimental when multiple lines must radiate from the same point. In this situation, a designer would like to have some control over the initial tangent directions of these lines, perhaps to distribute them at equal angles around the point from which they emerge.

The question arises, whether a commercial CAD tool, such as AutoCAD, SolidWorks, or Pro Engineer, would have been adequate to model Collins' sculptures. Indeed, with enough care, spline surface patches and sweeps could be assembled into a geometrical shape that would match one of Collins' creations. But this approach would be lacking the built-in implicit understanding of the constructive logic behind these pieces, which we wanted to generalize and enhance in order to produce many more sculptures of the same basic type. For that we need stronger and more convenient procedural capabilities than those that commercial CAD tools had to offer.

Capturing a sculpture as a program, forces us to understand its generating paradigm. In return, it offers precise geometry exploiting all inherent symmetries, as well as parametric adjustments of many aspects of the final shape. The latter turns out to be the crux of a powerful sculpture generator. If we build too few adjustable parameters into my program, then its impressibility is too limited to create many interesting sculptures. If there are too many parameters, then it becomes tedious to adjust them all to produce good-looking geometrical forms. Figuring out successful dependencies between the many different parameters in these sculptures and binding them to only a few adjustable sliders is the intriguing and creative challenge.

In practice it turned out that almost every sculpture family that we tackled, required a new program to be written. These programs become virtual constructivist 'sculpt- sculpting tools'. Once a new program starts to generate an envisioned group of geometrical shapes, it often will take on a life of its own. In a playful interaction with various sliders that control the different shape parameters, and by occasional program extensions, new shapes are discovered that were not among the originally envisioned geometries. In this process the original paradigm may be extended or even redefined, and the computer thus becomes an active partner in the creative process of discovering and inventing novel aesthetic shapes

Reference

i. Mehrdad Hejazi, (2005) "Geometry in nature and Persian architecture, Building and Environment", Volume 40, Issue 10, October, 2005, Pages 1413-1427.

ii. Karl T. Ulrich and Warren P. Seering, "Function sharing in mechanical design", Design Studies, Volume 11, Issue 4, October 1990, Pages 223-234.

iii. Mike Ashby and Kara Johnson, "Chapter 2 - What Influences Product Design?" Materials and Design (Second Edition) , The Art and Science of Material Selection in Product Design , 2010, Pages 8-27.

iv. Hans Hansen, Arja Ropo and Erika Sauer, "Aesthetic leadership", The Leadership Quarterly, Volume 18, Issue 6, December 2007, Pages 544-560, The Leadership Quarterly Yearly Review of Leadership.

v. Fumihiko Kimura, "Issues in Styling and Engineering Design", CIRP Annals - Manufacturing Technology, Volume 46, Issue 2, 1997, Pages 527-534.

vi. Nathan Crilly, James Moultrie and P. John Clarkson, "Shaping things: intended consumer response and the other determinants of product form", CIRP Annals - Manufacturing Technology, Volume 39, Issue 1, 1990, Pages 111-116.

vii. Hoda A. ElMaraghy Prof. and Shuejun Chen, "A General Model for Mechanical Design", CIRP Annals - Manufacturing Technology, Volume 39, Issue 1, 1990, Pages 111-116.

viii. A. Rashid, B.J. Mac Donald and M.S.J. Hashmi., "Evaluation of the aesthetics of products and integration of the findings in a proposed intelligent design system", Journal of Materials Processing Technology, Volumes 153-154, 10 November 2004, Pages 380-385, Proceedings of the International Conference in Advances in Materials and Processing Technologies.

ix. Yoram Reich, "A model of aesthetic judgment in design", Artificial Intelligence in Engineering, Volume 8, Issue 2, 1993, Pages 141-153.

Enterprise Resource Planning for Financial Analysts

Amit Gautam
Associate Professor,
School of Management Sciences,
Varanasi-221011
vishal_rsmt@yahoo.co.in

ABSTRACT

In the present business environment, role of a financial analyst is considered to be very important and inevitable. Financial analyst as managers, consultants, advisors or auditors plays an important role in controlling, managing, and supporting the business. As the business needs are very complex in nature, the implementation of an ERP package needs financial analyst with functional skills for evaluation, Business Process Reengineering (BPR), Mapping of Business requirements, Report designing, ensuring Business controls, customization of the package for the specific requirements, Documentation etc., Sooner or later a financial analyst without the knowledge of ERP may feel as if he is a fish out of the bowl. By this article it is attempted to highlight various aspects of ERP and specific areas of ERP that are relevant for financial analysts.

KEYWORD

ERP	**Finance**
Organization	**Enterprise**
Planning	**BPR**
Design	**Implementation**

Preface

Enterprise Resource Planning is the latest high-end solution information technology has lent to business application. The ERP solutions seek to streamline and integrate operation processes and information flows in the company to synergize the resources of an organization namely men, material, money and machine through information. Initially implementation of an ERP package was possible only for very large Multi National Companies and Infrastructure Companies due to high cost involved. Today many companies in India have gone in for implementation of ERP and it is expected in the near future that 60% of the companies will be implementing one or the other ERP packages since this will become a must for gaining competitive advantage.

Evolution of ERP

In the ever-growing business environment the following demands are placed on the industry:

- Aggressive Cost control initiatives
- Need to analyze costs / revenues on a product or customer basis
- Flexibility to respond to changing business requirements
- More informed management decision making
- Changes in ways of doing business

Difficulty in getting accurate data, timely information and improper interface of the complex natured business functions has been identified as the hurdles in the growth of any business. Time and again depending upon the velocity of the growing business needs, one or the other applications and planning systems have been introduced into the business world for crossing these hurdles and for achieving the required growth. They are:

- Management Information Systems (MIS)
- Integrated Information Systems (IIS)
- Executive Information Systems (EIS)
- Corporate Information Systems (CIS)
- Enterprise Wide Systems (EWS)
- Material Resource Planning (MRP)
- Manufacturing Resource Planning (MRP II)
- Money Resource Planning (MRP III)

The latest planning tool added to the above list is Enterprise Resource Planning.

Need for ERP

Most organizations across the world have realized that in a rapidly changing environment, it is impossible to create and maintain a custom designed software package, which will cater to all their requirements and also be completely up-to-date. Realizing the requirement of user organizations some of the leading software companies have designed Enterprise Resource Planning software which will offer an integrated software solution to all the functions of an organization.

Features of ERP

Some of the major features of ERP and what ERP can do for the business system are as below [Antweiler Werner and Trefler Daniel, 2002]:

- ERP facilitates company-wide Integrated Information System covering all functional areas like Manufacturing, Selling and distribution, Payables, Receivables, Inventory, Accounts, Human resources, Purchases etc.,
- ERP performs core corporate activities and increases customer service and thereby augmenting the Corporate Image.
- ERP bridges the information gap across the organization.
- ERP provides for complete integration of Systems not only across the departments in a company but also across the companies under the same management.
- ERP is the only solution for better Project Management.
- ERP allows automatic introduction of latest technologies like Electronic Fund Transfer (EFT), Electronic Data

Interchange (EDI), Internet, Intranet, Video conferencing, E-Commerce etc.

- ERP eliminates the most of the business problems like Material shortages, Productivity enhancements, Customer service, Cash Management, Inventory problems, Quality problems, Prompt delivery etc.,
- ERP not only addresses the current requirements of the company but also provides the opportunity of continually improving and refining business processes.
- ERP provides business intelligence tools like Decision Support Systems (DSS), Executive Information System (EIS), Reporting, Data Mining and Early Warning Systems (Robots) for enabling people to make better decisions and thus improve their business processes. [Gupta, Anil & Govindarajan, V, 2002]

Components of ERP

To enable the easy handling of the system the ERP has been divided into the following Core subsystems:

- **Sales and Marketing**
- Master Scheduling
- Material Requirement Planning
- Capacity Requirement Planning
- Bill of Materials
- Purchasing
- Shop floor control
- Accounts Payable/Receivable
- Logistics
- Asset Management
- Financial Accounting

Suppliers of ERP

There are many numbers of ERP suppliers who are very active in the market. Some of the companies offering renowned international ERP products include:

- Baan
- CODA
- D&B
- IBM
- JD Edwards
- Marcarn
- Oracle
- Peoplesoft
- Platinum
- Ramco
- SAP
- SMI
- Software 2000

BPR and ERP

Business Process Reengineering is a pre-requisite for going ahead with a powerful planning tool, ERP. An in depth BPR study has to be done before taking up ERP. Business Process Reengineering brings out deficiencies of the existing system and attempts to maximize productivity through restructuring and re-organizing the human resources as well as divisions and departments in the organization. [Sahay S, Walsham G, 2002]

Business Process Engineering evolves the following Steps:

- Study the current system
- Design and develop new systems
- Define Process, organization structure and procedure
- Develop customize the software
- Train people
- Implement new system

The principle followed for BRP may be defined as USA principle (Understand, Simplify Automate) i.e., Understanding the existing practices, Simplifying the Processes and Automate the Process. Various tools used for this principle are charted below:

- ***Understand Simplify Automate***
- **Diagramming Eliminating EDI**

- **Story-boarding Combining ERP**
- **Brain storming Rearranging**

Change and BPR

BPR is inevitable not only for ERP but as far as any business process is concerned. BPR becomes the first step in the process of ERP implementation. Business process reengineering is taken to conduct feasibility study and other restructuring exercises. Nothing can be done to prevent change. The best way to manage change is to adopt it. Time and again it has been proved that imposing change of any magnitude all on a sudden is not the proper way. There needs to be a proper method to bring about it. Business process reengineering is one scientific study that helps organizations largely to analyse the viability of not only ERP but any other dynamic change. BPR ERP is interrelated. [Verma, S, 1998]

BPR does not necessarily stop with the process of identifying the possibility. It also suggests a series of steps that needs to be executed, for ERP to find a place in the organization. BPR is the first step that comes prior to ERP implementation. The reason is simple. Many parameters are taken while preparing ERP. This includes the assumption of Predefined functions. Hence ERP software will be preconceived to perform those set of functions. On the other hand companies expect ERP to function in such a way that it coincides with the regular business process. BPR ERP can be the biggest challenge for the vendor and the company as such. BPR ERP forms an important part of ERP study.

Solving BPR-ERP Clash

There are two alternatives that will help the companies to combat this menace. The company can either restructure the business process itself or customize the ERP system so that it suits the business process. Deciding this is paramount to ERP implementation. BPRERP has lot of conflicts. The pros and cons of each of them are explained in the following paragraphs:

Implementing ERP Software to Suit Business Needs

When the company demands particular ERP software they have to make compromises on the budget because reworking modules and supplying an ERP Software would definitely be a costly affair. This is because of the complications involved in doing the same. Apart from finance this also calls for persons with greater working knowledge to design the systems. This means the process is not going to be unambiguous. The process will also require frequent updations. This is going to be difficult taking into account the several changes that has already been inflicted on the system to make it business friendly.

Restructuring the business process to be ERP Friendly:

This method also requires lots of monetary outlay because of the major change in business process. The customers will not be receptive to changes in business process. It is possible to train the employees but whereas in the case of customers they cannot be expected to stay in tune in tune with the whims and fancies of the organization. It is possible to train the employees. The likelihood of them to adapting to the change at the immediate outset is very much limited. This will cast a spell on the revenue of the business and unless ERP does not make it good in the later days the voluminous investment cannot be justified. [Christie W, 2001]

Selection of ERP

Once the BPR is completed the next task is to evaluate and select a suitable package for implementation. Evaluation of the right ERP package is considered as more crucial step. Evaluation and selection involves:

- checking whether all functional aspects of the Business are duly covered
- checking whether all the business functions and processes are fully integrated
- checking whether all the latest IT trends are covered
- checking whether the vendor has customizing and implementing capabilities
- checking whether the business can absorb the cost
- checking whether the ROI is optimum

Implementation of ERP

Implementing an ERP package has to be done on a phased manner. Step by step method of implementing will yield a better result than big-bang introduction. The total time required for successfully implementing an ERP package will be anything between 18 and 24 months. [Chase, Richard B., and Nicholus J. Aquilano, 2006]

The normal steps involved in implementation of an ERP are as below:

- Project Planning
- Business & Operational analysis including Gap analysis
- Business Process Reengineering
- Installation and configuration
- Project team training
- Business Requirement mapping
- Module configuration
- System interfaces
- Data conversion
- Custom Documentation
- End user training
- Acceptance testing
- Post implementation/Audit support

The above steps are grouped and sub-divided into four major phases namely

1) Detailed discussions,

2) Design & Customization,

3) Implementation and

4) Production

Benefits of ERP

The benefits accruing to any business enterprise on account of implementing are unlimited. According to the companies like NIKE, DHL, Tektronix, Fujitsu, Millipore, Sun Microsystems, following are some of the benefits they achieved by implementing ERP packages:

- **Gives Accounts Payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.**
- Reduce paper documents by providing on-line formats for quickly entering and retrieving information.
- Improves timeliness of information by permitting, posting daily instead of monthly.
- Greater accuracy of information with detailed content, better presentation, fully satisfactory for the Auditors.
- Improved Cost Control
- Faster response and follow up on customers
- More efficient cash collection, say, material reduction in delay in payments by customers.
- Better monitoring and quicker resolution of queries.
- Enables quick response to change in business operations and market conditions.
- Helps to achieve competitive advantage by improving its business process.
- Improves supply-demand linkage with remote locations and branches in different countries.
- Provides a unified customer database usable by all applications.
- Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improves information access and management throughout the enterprise.
- Provides solution for problems like Y2K and Single Monitory Unit (SMU) or Euro Currency

.

Significance of ERP Implementation

Companies have to clearly know what enterprise resource is planning before thinking of implementing them. The catch word of ERP implementation is speed. The faster it is implemented the quicker and better are the advantages and delivery in terms of results. This early process has another hold. The returns are sought at a shorter period. This deviation from the conventional practice has become the order of the day as far as many companies are concerned. Formerly Business process reengineering played a vital role with respect to implementation. It is important to know the components of Enterprise resource planning .Merely defining enterprise resource planning will not help in this.

This naturally paved way to development of gaps between the actual results and the one derived during the process of foreseeing. Tuning ERP as per the whims and fancies of the practices followed in the company became a routine affair. This led to slogging and dragging beyond the time limits permitted. It was monetarily pinching and played havoc in the customer's trust. It is also necessary to understand that mere ERP planning does not guarantee the benefit of ERP. It has to be implemented as planned after understanding the components of enterprise resource planning.

In spite of having improved the implementation issues what remains static and unfettered is the manner in which companies go ahead with ERP implementation. In fact they don't even check the desirability of going into ERP. Some issues that an organization has to address after defining enterprise resource planning are:

- **Popular information systems**
- **Likelihood of fluctuations in the choice of technology**
- **The ability of market players to stay in tune with it**
- **The ways and means to implement a business applications like ERP**
- **To benefit from the same so as to gain a competitive edge**
- **Their usage and services**
- **The necessity for innovating software applications**

If an organization is able to answer these questions without any ambiguity and substantiate the results then it can be said that it has a path or up focus in taking ERP. The questions mentioned above are crucial and will even decide the business model of the company. ERP implementation is a vital in the whole process of ERP. They can take place only if one understands "What is enterprise resource Planning" and defining enterprise resource planning in their organization. [Bruce, Harry J, 2005]

Current Approach

It is essential to have an overview of the current approach. The current approach is claimed to be relatively successful. The current approach more popularly referred to as "baan" has two underlying principles:

The idea which concentrates on molding the business: This category is prominent when the organizational unit calls for a radical restructuring process by all means. This process will be carried in all aspects of the business .Some of them include strategic maneuver, operation of trade and the circumstances that call for change and adaptability. Defining enterprise resource planning in context to the concerned organization will help to decide on this issue.

The plan which lays more emphasis on technical parameters: Here business takes the back seat. The thrust lies on technical dimensions. This does not ignore the commercial viability as such but they occupy seat only in the due course of time more so when operations are triggered in full stream and not at the initial stage itself. The advantage with this type is that it does not call for an immediate modification of the business structure. However it is essential to know the components of enterprise resource planning.

ERP Implementation Life Cycle

The process of ERP implementation is referred as d as "ERP Implementation Life Cycle". The following are the steps involved in completing the lifecycle.

Shortlist on the basis of observation

Selecting an ERP package for the company can nevertheless be compared with the process of "Selecting the right Person for the Right Job". This exercise will involve choosing few applications suitable for the company from the whole many.

Assessing the chosen packages
A team of Experts with specialized knowledge in their respective field will be asked to make the study on the basis of various parameters. Each expert will not only test and certify if the package is apt for the range of application in their field but also confirm the level of coordination that the software will help to achieve in working with other departments. In simple terms they will verify if the synergy of the various departments due to the advent of ERP will lead to an increased output. A choice is to be made from ERP implementation models. [Greene, James H, 2005]

Preparing for the venture
This stage is aimed at defining the implementation of ERP in all measures. It will lay down the stipulations and criteria have to be met. A team of officers will take care of this, who will report to the person of the highest hierarchy in the organization.

Gap Analysis
This stage helps the company to identify the gaps that has to be bridged, so that the company's practice becomes akin to ERP environment. This has been reported as an expensive procedure but it is inevitable. The conglomerate will decide to restructure the business or make any other alterations as suggested by GAP analysis in order to make ERP user friendly. A choice is to be made from ERP implementation models. [Jetter, Otto, 2006]

Designing the System
This step requires lot of meticulous planning and deliberate action. This step helps to decide and conclude the areas where restructuring have to be carried on. A choice is to be made from ERP implementation models.

In-house Guidance
This is regarded as a very important step in ERP implementation. The employees in the company are trained to face crisis and make minor corrections as well because the company can neither be at liberty nor afford the bounty to avail the services of an ERP vendor at all times.

Checking
This stage observes and tests the authenticity of the use. The system is subjected to the wildest tests possible so that it ensures proper usage and justifies the costs incurred. This is seen as a test for ERP implementation.

The real test
At this stage the replacement takes place viz the new mechanism of operation and administration takes over the older one.

Preparing the employees to use ERP
The employees in the organization will be taught to make use of the system in the day to day and regular basis so as to make sure that it becomes a part of the system in the organization.

Post Implementation

The process of implementation will find meaning only when there is regular follow up and proper instruction flow thereafter and through the lifetime of ERP. This will include all efforts and steps taken to update and attain better benefits once the system is implemented. Hence an organization has to perform ERP implementation safely and correctly.

Financial Analyst (FA) and ERP

A pertinent question one financial analyst may ask is "How does an ERP matter for me?". As mentioned earlier the role of a financial analyst in any business either as a Consultant, Auditor, Advisor or Manager is inevitable.

FA as a Consultant:

Implementation of ERP solutions is one of the largest drivers of growth in the consultancy business. The introduction of such a large and complex software like ERP, which enables an organization to integrate their manufacturing, finance and marketing operations at all levels, is in itself a challenge, since it calls for technical and functional skills and a change in user mindsets. And therein comes a role of a consultant. CA as a Consultant will play a major role in implementation of an ERP solution. [Zipkin, Paul H, 2006]

FA as an auditor:

Assuming a situation where the client has implemented an ERP solution. If the auditor is aware of ERP he can make use of the features of ERP and thereby:

- **Ensures that the internal controls and checks are consistently maintained.**
- **Ensures that the provisions of Income tax or other fiscal laws are not ignored e.g., one can control the payment of cash in excess of Rs.10000 for expenses or Rs.20000 as loans and advances, The TDS deductions and payments are automated etc.,**
- **Ensures that the Accounting Standards are consistently followed across the company.**
- **Improves the quality of the reporting.**

FA as an Advisor:

As an advisor to a company a financial analyst can participate in various stages of ERP implementation. It goes without saying that advising without the knowledge of the current trends and modern management techniques will prove to be a wrong advice and may have a negative impact on the growth of the client.

FA as a Manager:

By now one should know that the ERP is a high end sophisticated software solution that reduces the pressure and work load of the Managers and provides accurate, timely information for taking appropriate business decisions. Financial analyst as managers with knowledge of ERP will be able to achieve their targets and goals by proper implementation of ERP system in their organization. In fact Managers are expected to translate the business rules and requirements for mapping them into ERP software. Managers as representatives of the Organization have to coordinate with Vendors, Consultants, Auditors etc., for a proper implementation of ERP package.

Conclusion

The growing information needs of an enterprise make it imperative to improve or replace old systems. Especially under the present Indian business environment, where the globalization has been initiated, full convertibility is coined, Infrastructure Projects are nearing completion, and it is expected that the whole business system will undergo a major shift. Thus by being a proficient ERP consultant, financial analyst will prove their commitment to the business world and modern management.

Reference

i. Antweiler Werner and Trefler Daniel: ERP: A view from trade, The American Economic Review, March 2002.

ii. Gupta, Anil with Govindarajan, V., "Building Global Presence Through Enterprise Resource Planning," The Financial Times, January 30, 2002.

iii. Sahay S, Walsham G, 'Information Technology in Companies: A Need for Theory Building' Business Standard, 14 Oct. 2002

iv. Verma, S , "Room for ERP", Business India, 12 January, 1998.

v. Christie W, 'Concept Behind ERP', Economist, November 2001.

vi. Chase, Richard B., and Nicholus J. Aquilano. ERP & Its Implementation, 6th ed. Prentice Hall, 2006

vii. Bruce, Harry J. ERP Handbook, Tata McGraw Hill, 2005.

viii. Greene, James H. Enterprise resource palling, 3rd ed., New York, McGraw Hill, 2005.

ix. Jetter, Otto, ERP and BPR, Upper saddle River, NJ, Prentice Hall, 2006.

x. Zipkin, Paul H. Foundations of ERP Management, New York, Mc Graw Hill, 2006.

Virus: A Menace for Information Security

Arun Bakshi
Assistant Professor(Sr) (IT),
Gitarattan International Business School, Rohini, Delhi,
lakshayabakshi@gmail.com

Vikas Dixit
Head Online Division Educosoft International India Pvt. Ltd.
urvikas@gmail.com

Kaushal Mehta
Assistant Professor, Bhai Parmanand Institute of Business Studies, Delhi,
kpu_713@yahoo.com

ABSTRACT

Computer virus is a program that copy itself to harm the computer without the knowledge of user. A virus can spread from one computer to another through some executable code. The user can sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Its chances of spreading from one computer to other increases by infecting files on a network file system or a file system that is accessed by another computer.

KEYWORD

Virus	Security
Information System	Computer
Worm	Linux
Unix	Compact Disc

Preface

The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs. The correct term that should be used is “Malware”. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crime ware, and other malicious and unwanted software), including true viruses. . A worm can exploit security vulnerabilities to spread itself to other computers without needing to be transferred as part of a host, and a Trojan horse is a program that appears harmless but has a hidden agenda.

Now-a-days, almost all computers are connected to the Internet which increases the chance of spreading malicious code. Viruses may also take advantage of network services such as the World Wide Web, e-mail, Instant Messaging, and file sharing systems to spread.

HISTORY

Creeper was the first virus detected on ARPANET in early 1970s. It was a self-replicating progam written by Bob Thomas at BBN in 1971. It copied itself to the remote system and displays a message, "I'm the creeper, catch me if you can!” It used ARPANET to infect DEC PDP-10 computers running the TENEX operating system. The Reaper program was created to delete Creeper.

“Rother J” was the first computer virus that appears “in the wild” means can spread outside the computer or lab where it was written. It was created by Richard Skrenta in 1981 as a practical joke when he was in high school. This program attached itself to the Apple DOS 3.3 operating system and spread via floppy disk. On its 50th use the Elk Cloner virus would be activated, infecting the computer and displaying a short poem beginning "Elk Cloner: The program with a personality."

A boot sector virus named “Brain” created by Farooq Alvi Brothers in 1986. It was operated out of Lahore, Pakistan, reportedly to detect piracy of the software they had written. A variant of Brain named “Ashar” has predated Brain on the basis of code within the virus.

In early days, users use floppy disks to exchange informat5ion and programs. PCs of the era would attempt to boot first from a floppy. Therefore, most viruses spread using floppy disks and other removable media. Some viruses spread by infecting programs stored on these disks, while others installed themselves into the disk boot sector, ensuring that they would be run when the user booted the computer from the disk, usually inadvertently. Until floppy disks fell out of use, this was the most successful infection strategy and boot sector viruses were the most common in the wild for many years.

Traditional computer viruses emerged in the 1980s, driven by the spread of personal computers and the resultant increase in BBS, modem use, and software sharing. Bulletin board-driven software sharing contributed directly to the spread of Trojan horse programs, and viruses were written to infect popularly traded software. Shareware and bootleg software were equally common vectors for viruses on BBS's. Within the "pirate scene" of hobbyists trading

illicit copies of retail software, traders in a hurry to obtain the latest applications were easy targets for viruses.

Macro viruses were introduced in the mid-1990s. Most of these viruses are written in scripting languages to infect Microsoft programs such as Word and Excel. Since Word and Excel were also available for Mac OS, most could also spread to Macintosh computers. Some old versions of Microsoft Word allow macros to replicate themselves with additional blank lines. If two macro viruses simultaneously infect a document, the combination of the two, if also self-replicating, can appear as a "mating" of the two and would likely be detected as a virus unique from the "parents."

Virus can also be spread though instant message by sending a web address link. If the recipient think that it is from trusted source, he/she will follow the link. The virus hosted at the link can able to infect the computer and continue propagating.

Cross-site scripting viruses emerged recently, and were academically demonstrated in 2005. Since 2005 there have been multiple instances of the cross-site scripting viruses in the wild, exploiting websites such as MySpace and Yahoo.

INFECTION STRATEGIES

Virus must have permission for execution of code and written to memory to replicate itself. Therefore, viruses attached with executable files and if the user executes the infected file, the virus code will execute simultaneously. Viruses can be divided into two types based on their behavior when they are executed.

NONRESIDENT VIRUSES

These viruses search for other hosts or applications to spread infection, infect those target hosts and then transfers control to the application they had infected. It can be seen as the combination of the finder module and the replication module. Finder module finds the target hosts which further calls the replication module to infect that file. For each new executable file, finder module is encountered.

RESIDENT VIRUSES

Rather than searching for new hosts immediately, resident virus loads itself into memory on execution and transfers control to the host program. The virus stays active in the background and infects new hosts as they are accessed.

Resident viruses has replication module similar to the one used by non-resident viruses but does not contain the finder module. As the virus has been executed, it loads the replication module into the memory and called each time a new operation is executed by the operating system.

Resident viruses can be divided into two categories fast infectors and slow infectors.

Fast infectors can infect as many files as possible. For instance, a fast infector can infect every potential host file that is accessed. It might create a problem while using anti-virus software, since the virus scanner will scan all the potential host file while performing system-scan and if the scanner fails to find such virus, the virus can "piggy-back" on the scanner and can infect all the files that are scanned. Infect5ing too much files becomes t5he disadvantage of fast infectors as such infections can detect more easily because of slow performance of computer or any other suspicious action detect by the anti-virus software.

On the other hand, slow infectors infect the hosts infrequently. For instance, slow infectors infect files only when they are copied. Slow infectors are designed to avoid detection by limiting their actions and cannot be easily triggered by the anti-virus software that detects suspicious behavior of the programs. However, this approach does not seem vey successful.

CROSS-PLATFORM VIRUSES

With the popularity of cross-platform applications, cross-platform viruses are identified in 2007. This was brought to the forefront of malware awareness by the distribution of an Openoffice.org virus called *Bad Bunny*.

As per the statement of Stuart Smith of Symantec, "What makes this virus worth mentioning is that it illustrates how easily scripting platforms, extensibility, plug-ins, ActiveX, etc, can be abused. All too often, this is forgotten in the pursuit to match features with another vendor. The ability for malware to survive in a cross-platform, cross-application environment has particular relevance as more and more malware is pushed out via Web sites. How long until someone uses something like this to drop a JavaScript infector on a Web server, regardless of platform?"

ABOUT VECTORS AND HOSTS

Viruses have targeted various types of transmission media or hosts. This list is not exhaustive:

- Binary executable files (such as COM files and EXE files in MS-DOS, Portable Executable files in Microsoft Windows, and ELF files in Linux)
- Volume Boot Records of floppy disks and hard disk partitions
- The master boot record (MBR) of a hard disk
- General-purpose script files (such as batch files in MS-DOS and Microsoft Windows, VBScript files, and shell script files on Unix-like platforms).
- Application-specific script files (such as Telix-scripts)
- System specific autorun script files (such as Autorun.inf file needed to Windows to automatically run software stored on USB Memory Storage Devices).
- Documents that can contain macros (such as Microsoft Word documents, Microsoft Excel spreadsheets, AmiPro documents, and Microsoft Access database files)
- Cross-site scripting vulnerabilities in web applications

- Arbitrary computer files. An exploitable buffer overflow, format string, race condition or other exploitable bug in a program which reads the file could be used to trigger the execution of code hidden within it. Most bugs of this type can be made more difficult to exploit in computer architectures with protection features such as an execute disable bit and/or address space layout randomization.

Malicious code can be embedded in the PDFs or in HTML code. Operating systems use file extensions to determine program association. These extensions may be hidden from the user by default. For example, an executable may be created named "picture.png.exe", in which the user sees only "picture.png" and therefore assumes that this file is an image and most likely is safe.

An additional method is to generate the virus code from parts of existing operating system files by using the CRC16/CRC32 data. The initial code can be quite small (tens of bytes) and unpack a fairly large virus. This is analogous to a biological "prion" in the way it works but is vulnerable to signature based detection.

TRICKS OF VIRUS TO AVOID ITS DETECTION

Many approaches are used to avoid detection of virus by users. One oldest approach is, if the file is infected, "last-modified" date of the host file remains same. This approach is especially used in MS-DOS platform. However, this approach does not fool anti-virus software, especially those which maintains date and Cyclic redundancy checks on file changes.

Another approach to avoid detection is: viruses can infect files without increasing their sizes or damaging the files. This can be done by overwriting unused areas of executable files. These are called cavity viruses. For example the CIH virus, or Chernobyl Virus, infects Portable Executable files. As these files have many empty gaps, the virus, which was 1 KB in length, did not add to the size of the file. Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them.

Old hiding techniques need to be replaced or updated as computers and operating systems are growing and becoming complex. File systems may need detailed and explicit permissions of every kind of file access to prevent the computer against viruses.

AVOIDING BAIT FILES AND OTHER UNDESIRABLE HOSTS

Virus needs to infect the host files to spread further. However, infecting the host files may lead to the detection of virus more easily as much anti-virus software performs an integrity check for their own code. For this reason, some viruses are programmed not to infect programs that are known to be part of anti-virus software.

Another host files that virus needs to avoid are Bait files (or goat files). Bait files are designed by the anti-virus

professionals to be infected by virus which helps to detect the virus.

As Bait files are designed to infect themselves by the virus, these files can be used by the anti-virus professionals to find different samples of virus Professionals use these samples to study the behavior of the virus and evaluate detection methods for them. It is more practical to store and exchange a small, infected bait file, than to exchange a large application program that has been infected by the virus. Bait files are especially useful when the virus is polymorphic. In this case, the virus can be made to infect a large number of bait files. The infected files can be used to test whether a virus scanner detects all versions of the virus.

Some Bait files accessed regularly. If any modification finds in these files, the anti-virus software warns the user that virus may be active on the system. Hence, virus needs to avoid such files. This can be done by avoiding the small program files or programs that contain certain patterns of garbage instructions.

Another strategy to avoid Bait files is sparse infection. Sometimes, sparse infectors do not infect a host file that would be a suitable candidate for infection in other circumstances. For instance, virus may decide whether to infect the file or not, or it may infect the host files on a particular day of week.

STEALTH

STEALTH is a technique used by virus to befool anti-virus software by intercepting the request to the operating system. As anti-virus software requests to read a file, virus intercepts it and receives the request. Thus, the request is passed to the virus rather than to the operating system. The virus will then return the uninfected version of file which seems clean to the anti-virus software. Many techniques are used to avoid stealth but the most reliable technique is to boot from medium which is known to be clean.

SELF-MODIFICATION

Virus can be easily find using virus signatures while scanning programs through anti-virus software. A signature is a characteristic byte-pattern that is part of a certain virus or family of viruses. If the scanner finds such pattern, it notifies the user that the file is infected. Then it is up to the user whether to delete, clean or heal the file. Some virus makes the detection difficult using signatures as they modify their code at each infection. However, the detection of virus through signatures is not the impossible task.

ENCRYPTION WITH A VARIABLE KEY

Virus can also be spread using encryption. For this, virus needs decrypted module and the encrypted module. As the virus is encrypted using different keys for each new file which makes the detection of virus difficult. However, the decryption module remains same through which the indirect detection of virus could be possible. Since these would be symmetric keys, stored on the infected host, it is

in fact entirely possible to decrypt the final virus, but this is probably not required, since self-modifying code is such a rarity that it may be reason for virus scanners to at least flag the file as suspicious.

An old method used for encryption is XORing each byte of the virus program with a constant and the same XOR operation will repeated for decryption. It is suspicious code that modifies itself, so the code to do the encryption/decryption may be part of the signature in many virus definitions.

POLYMORPHIC CODE

Polymorphic code uses the concept of encryption to infect files. However, in encryption, decrypted module remains same whereas in polymorphic code, decryption module is also modified on every new infection. It is a serious threat to virus scanner as there is no identical part between infections which makes the detection of virus too difficult.

Anti-virus software can detect such viruses using an emulator or by statistical pattern analysis of the encrypted virus body. To generate polymorphic code, virus needs to have a polymorphic engine (also called mutating engine or mutation engine) somewhere in its encrypted body

Such slow polymorphic code makes it more difficult for anti-virus professionals to obtain the samples of virus. Polymorphic code makes the detection by virus scanner unreliable and also helps to avoid detection even through Bait files which infect themselves in only one run and contains similar or identical samples of virus.

METAMORPHIC CODE

Polymorphic code can be detected using emulation. To avoid this detection, metamorphic code is used. Using this technique, virus rewrites themselves completely on the infection of any new executable file. To enable metamorphism, a metamorphic engine is needed. A metamorphic virus is usually very large and complex. For example, W32/Simile consisted of over 14000 lines of Assembly language code, 90% of which is part of the metamorphic engine.

LINUX VULNERABILITY

Linux supports multi-user environment where users require privileges to access which is implemented using some access control technique. To cause any serious consequence over Linux, malware needs to have the root access to the system.

Shane Coursen, a senior technical consultant with Kaspersky Lab noted, “The growth in Linux malware is simply due to its increasing popularity, particularly as a desktop operating system. The use of an operating system is directly correlated to the interest by the malware writers to develop malware for that OS.”

SecurityFocus's Scott Granneman stated, some Linux machines definitely need anti-virus software. For instance,

Samba or NFS servers, may store documents in undocumented, vulnerable Microsoft formats, such as Word and Excel which may propagate viruses.

Linux mail servers send mails to other computers which are using different operating systems. Therefore, Linux operating system also needs to run AV software to detect viruses before they show up in the mailboxes of Outlook and Outlook Express users. For example the open source ClamAV "Detects viruses, worms and trojans, including Microsoft Office macro viruses, mobile malware, and other threats." Hence, Linux virus scanners search for all known viruses for all computer platforms.

VULNERABILITY AND COUNTERMEASURES

THE VULNERABILITY OF OPERATING SYSTEMS TO VIRUSES

Just as genetic diversity in a population decreases the chance of a single disease wiping out a population, the diversity of software systems on a network similarly limits the destructive potential of viruses.

This became a particular concern in the 1990s, when Microsoft gained market dominance in desktop operating systems and office suites. The users of Microsoft software (especially networking software such as Microsoft Outlook and Internet Explorer) are especially vulnerable to the spread of viruses.

Microsoft gained market dominance because of its desktop operating system and office suites in 1990s. Hence, the Windows become the most popular OS for virus writers and are often criticized for including many errors and holes for virus writers to exploit. Integrated and non-integrated Microsoft applications (such as Microsoft Office) and applications with scripting languages with access to the file system (for example Visual Basic Script (VBS), and applications with networking features) are also particularly vulnerable.

Windows is the most popular OS among virus writers; however, some viruses also exist for other operating systems. Operating system that allows third-party programs to run over it can affect from virus. Unix-based Operating systems are more secure as they provide the facility to run executable code into its own protected memory space.

Mac OS X (with a Unix-based file system and kernel) is considered better OS than MS-Windows as MAC OS X has relatively few security exploits. One older version of Apple OS named “Mac OS Classic” states that there are only 4 known viruses and independent sources states that t5here are as many as 63 viruses. Virus vulnerability between Macs and Windows is a chief selling point, one that Apple uses in their Get Mac advertising.

As the first virus for Linux named “Bliss” has been released, anti-virus vendors issued a warning that Unix-like systems could fall prey to viruses just like Windows. Bliss needs to run it explicitly and can harm only the files

which the users have access permission to modify. Unlike Windows OS, Linux and UNIX blocks normal users access to make changes to the environment and users do not usually log in as an administrator which can save the OS to get infected.

THE ROLE OF SOFTWARE DEVELOPMENT

Because software is often designed with security features to prevent unauthorized use of system resources, many viruses must exploit software bugs in a system or application to spread. Software development strategies that produce large numbers of bugs will generally also produce potential exploits.

ANTI-VIRUS SOFTWARE AND OTHER PREVENTIVE MEASURES

Anti-virus software's are used to detect and eliminate the known viruses after the computer downloads or runs the executable.

Anti-virus software application uses two common methods to detect viruses. The first common method of virus detection is using a list of virus signature definitions. This can be done by examining the content of the computer's memory (its RAM, and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives), and comparing those files against a database of known virus "signatures".

The disadvantage of this detection method is that users are only protected from viruses that pre-date their last virus definition update. The second method is to use a heuristic algorithm to find viruses based on common behaviors. This method has the ability to detect viruses that anti-virus security firms have yet to create a signature for.

Some anti-virus software's uses "on-access scanning" means scanning is performed as and when the file is opened and even while sending and receiving e-mails. Anti-virus software does not change the underlying capability of host software to transmit viruses. Users must update their software regularly to patch security holes.

Anti-virus software also needs to be regularly updated in order to prevent the latest threats.

Damages caused by viruses could be minimized by taking the regular back-ups of data either on devices which kept unconnected to the system (most of the time), read-only or not accessible for other reasons, such as using different file systems. This way, if data is lost through a virus, one can start again using the backup (which should preferably be recent).

Optical media such as CD/DVD stores data in read-only format. Therefore, the data cannot be affected by virus on such devices. Hence, if the OS becomes unusable, an OS on a bootable CD can be used to start the system.

Backups on removable media must be carefully inspected before restoration. The Gammima virus, for example, propagates via removable flash drives.

RECOVERY METHODS

Once the computer gets infected by virus, it is unsafe to use the infected system without reinstalling the operating system. However, there are number of recovery options available while the actions depend upon the type of virus.

VIRUS REMOVAL

There is a tool available on Windows Me, Windows XP, and Windows Vista named "System Restore" which restores the registry and critical system files to a previous checkpoint. A virus may hang the system and a subsequent hard reboot corrupt the system restores point on the same day. Restore point from previous days works only if the virus is not designed to corrupt restore files.

Some viruses such as CiaDoor disable system restore and other tools such as Task Manager and Command Prompt. Administrators can disable such tools to access it by other users. However, a virus can block all users to access these tools by modifying the registry. When an infected tool activates it gives message "Task Manager has been disabled by your administrator.", even if the user trying to open the program is the administrator.

OPERATING SYSTEM REINSTALLATION

Another approach for virus removal is reinstallation of operating system. This is done by formatting the OS partition and install OS using its original media. This approach is faster than using antivirus software and scans the system multiple times. However, it includes the overhead of reinstallation of all other software and drivers

VIRUSES, WORMS AND OPERATING SYSTEMS

VIRUSES, TROJAN HORSES AND LINUX SYSTEMS

Some viruses may threat to Linux systems. Execution of infected binary may infect the system. However, the infection level depends upon the privileges of user which executes the infected binary. Binary file run under root account may infect the entire system. Privilege escalation vulnerabilities may permit malware running under a limited account to infect the entire system.

Virus generators do not require any special malware writing skills. They can simply add a code snippet to any program and as the user downloads that program, it will download through the modified login server. This additional code run anytime, the user logs in. however, special skill may be needed for tricking the user to run the program in the first place.

Threat of installation of malware can be reduced using software repositories. Software repositories are checked by maintainers to ensure that the software is malware-free. For this purpose, md5 checksums are used. Through this, modified versions are identified that may be introduced by different malware attacks. It limits the scope of attacks by only including the original authors, package and release maintainers and possibly others with suitable administrative access, depending on how the keys and checksums are handled.

If the user executes the code which is not from trusted user, vulnerability of Trojan horses and viruses may cause. It is also the fault of distributers which do not provide the default checking for authenticity of software downloaded.

WORMS AND UNIX-LIKE SYSTEMS

UNIX systems have vulnerability in network daemons such as and WWW servers can be used or attacks. Server takes immediate action against vulnerabilities. There is no guarantee on the installation if attack is on targets which are not publicly known. Servers having weak passwords can also be attacked.

WWW SCRIPTS AND LINUX SERVERS

Rather than attacking the system, Linux servers can also be used by malwares. E.g. WWW content and scripts are restricted as it may be used by malware to attack visitors.

POTENTIAL THREATS

New malwares are introduced and increasing day by day to cause threat to the system Some of them are given as:

TROJANS

Kaiten	**Linux.Backdoor.Kaiten trojan horse**
Rexob	Linux.Backdoor.Rexob trojan

VIRUSES

- ✓ **Alaeda - Virus.Linux.Alaeda**
- ✓ Bad Bunny - Perl.Badbunny
- ✓ Binom - Linux/Binom
- ✓ Bliss
- ✓ Brundle
- ✓ Bukowski
- ✓ Diesel - Virus.Linux.Diesel.962
- ✓ Kagob a - Virus.Linux.Kagob.a
- ✓ Kagob b - Virus.Linux.Kagob.b
- ✓ MetaPHOR (also known as Simile)
- ✓ Nuxbee - Virus.Linux.Nuxbee.1403
- ✓ OSF.8759
- ✓ Podloso - Linux.Podloso (The iPod virus)
- ✓ Rike - Virus.Linux.Rike.1627
- ✓ RST - Virus.Linux.RST.a
- ✓ Satyr - Virus.Linux.Satyr.a
- ✓ Staog
- ✓ Vit - Virus.Linux.Vit.4096
- ✓ Winter - Virus.Linux.Winter.341
- ✓ Winux (also known as Lindose and PEElf)
- ✓ Wit virus
- ✓ ZipWorm - Virus.Linux.ZipWorm

WORMS

- ✓ **Adm - Net-Worm.Linux.Adm**
- ✓ Adore
- ✓ Cheese - Net-Worm.Linux.Cheese
- ✓ Devnull
- ✓ Kork
- ✓ Linux/Lion
- ✓ Mighty - Net-Worm.Linux.Mighty
- ✓ Millen - Linux.Millen.Worm
- ✓ Ramen worm

- ✓ Slapper
- ✓ SSH Bruteforce

SOME ANTI-VIRUS APPLICATIONS

There is a number of anti-virus applications available are including:

- ✓ **Avast! (freeware and commercial versions)**
- ✓ AVG (freeware and commercial versions)
- ✓ Avira (freeware and commercial)
- ✓ Bitdefender (freeware and commercial versions)
- ✓ ClamAV (free open source software)
- ✓ Eset (commercial versions)
- ✓ F-Secure Linux (commercial)
- ✓ Kaspersky Linux Security (commercial)
- ✓ McAfee VirusScan Enterprise for Linux (commercial)
- ✓ Panda Security for Linux (commercial version)
- ✓ Sophos (commercial)
- ✓ Symantec AntiVirus for Linux (commercial)
- ✓ Trend Micro ServerProtect for Linux (commercial)

CONCLUSION

As prevention is better than cure, one should take all the preventive measures to safeguard computer against virus threats. Though viruses are dangerous, but there is no need to panic. The name virus itself seems like they can destroy your computer any moment. But it is not the only truth. One can take security measures to protect computer against malicious code using update antivirus and by knowing about the extent of damage and recovery procedures against viruses. The final word of wisdom will be to avoid access of any untrustworthy sources of data whether CD, Pen Drive or online data, and keep your virus scanner updated always.

REFERENCES

i. http://www.bartleby.com/61/97/C0539700.html 5-Nov-2009
ii. http://www.actlab.utexas.edu/~aviva/compsec/virus/whatis.html 7-Nov-2009
iii. "Virus list". http://www.viruslist.com/en/viruses/encyclopedia?chapter=153310937. Retrieved on 2008-02-07. 11-Nov-2009
iv. Thomas Chen, Jean-Marc Robert (2004). "The Evolution of Viruses and Worms". http://vx.netlux.org/lib/atc01.html. Retrieved on 2009-02-16. 1-Nov-2009
v. See page 86 of *Computer Security Basics* by Deborah Russell and G. T. Gangemi. O'Reilly, 1991. ISBN 0937175714. 4-Nov-2009
vi. Anick Jesdanun. "Prank starts 25 years of security woes". http://news.yahoo.com/s/ap/20070831/ap_on_hi_te/computer_virus_anniversary;_ylt=A9G_R3Ga1NhGH0QBIwZk24cA."The anniversary of a nuisance". http://www.cnn.com/2007/TECH/09/03/computer.virus.ap/. 8-Nov-2009
vii. Boot sector virus repair
viii. Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002, Abstract at http://vx.netlux.org/lib/aas10.html 9-Nov-2009
ix. Vesselin Bontchev. "Macro Virus Identification Problems". *FRISK Software International*. http://www.people.frisk-software.com/~bontchev/papers/macidpro.html.
x. Wade Alcorn. "The Cross-site Scripting Virus". http://www.bindshell.net/papers/xssv/.
xi. http://www.pcsecurityalert.com/pcsecurityalert-articles/what-is-a-computer-virus.htm
xii. http://www.virusbtn.com/resources/glossary/polymorphic_virus.xml 5-Nov-2009
xiii. Perriot, Fredrick; Peter Ferrie and Peter Szor (May 2002). "Striking Similarities" (PDF). http://securityresponse.symantec.com/avcenter/reference/simile.pdf. Retrieved on September 9, 2007. 6-Nov-2009
xiv. http://www.virusbtn.com/resources/glossary/metamorphic_virus.xml. 3-Nov-2009
xv. Need a computer virus?- download now. 2-Nov-2009
xvi. http://blog.didierstevens.com/2007/05/07/is-your-pc-virus-free-get-it-infected-here/
xvii. "Malware Evolution: Mac OS X Vulnerabilities 2005-2006". Kaspersky Lab. 2006-07-24. http://www.viruslist.com/en/analysis?pubid=191968025. Retrieved on August 19, 2006. 4-Nov-2009
xviii. Apple - Get a Mac. 7-Nov-2009

xix. Sutter, John D. (22 April 2009). "Experts: Malicious program targets Macs". *CNN.com*. http://www.cnn.com/2009/TECH/04/22/first.mac.botnet/index.html. Retrieved on 24 April 2009. 9-Nov-2009
xx. McAfee. "McAfee discovers first Linux virus". *news article*. http://math-www.uni-paderborn.de/~axel/bliss/mcafee_press.html. 3-Nov-2009
xxi. Axel Boldt. "Bliss, a Linux "virus"". *news article*. http://math-www.uni-paderborn.de/~axel/bliss/. 2-Nov-2009
xxii. "Symantec Security Summary — W32.Gammima.AG." http://www.symantec.com/security_response/writeup.jsp?docid=2007-082706-1742-99
xxiii. "Yahoo Tech: Viruses! In! Space!" http://tech.yahoo.com/blogs/null/103826
xxiv. "Symantec Security Summary — W32.Gammima.AG and removal details." http://www.symantec.com/security_response/writeup.jsp?docid=2007-082706-1742-99&tabid=3. 2-Nov-2009

Global Journal of Enterprise Information System
January 2010 -June 2010
Volume-2 Issue-1

SOA- the backbone of Modern Business

MANISH SINGH
Allahabad Institute of Engineering & Technology
Gohania, Allahabad
manish.singh076@gmail.com

ABSTRACT

The present study examines about the key features of Service Oriented Architecture (SOA) and its utilization in modern business integration like various processes, employees, information, managers etc. Integration is the biggest challenge which is fulfilled by implementing of SOA in business. It provides more strength to business working as a backbone for various services and connecting the cross-platform application together.

KEYWORD

Service Oriented Architecture	Information Technology,
Application	Web Services
Implementation	Cross-Platform

Preface

Modern Businesses need to integration among processes, people, employee, managers, executives and information within the organization and across organizational boundaries to subsidiaries or trading partners[1]. If a lack of integration among Information Technology (IT) assets—systems, applications and data—makes it difficult for IT to respond quickly and effectively to changing business needs. Due to this inflexibility increases costs, decreases customer responsiveness, hinders compliance, and decreases worker productivity. In short, a lack of integration is the biggest challenge that organizations face in their efforts to remain competitive and grow. Therefore it is required that introduce a new web technology in business by which the integration retain in industries and fill the gap in communication, maintain consistency in data base. The present paper explore the concept to SOA (Service Oriented Architecture) and their benefits which should be utilizes by modern business.

Why Service Oriented Architecture?

Service Oriented Architecture (SOA) is a design approach which helps to organizing existing Information Technology assets such that the heterogeneous (mixed) array of distributed, complex systems and applications can be transformed into a network of integrated, simplified and highly flexible resource(s). A well-executed SOA project aligns IT resource(s) more directly with business goals, helping organizations to build stronger connections with customers and suppliers, providing more accurate and more readily available business intelligence with which to make better decisions, and helping businesses streamline business processes and information sharing for improved employee productivity. The net result is an increase in organization agility.

SOA distinguishes three different roles of services: service provider, service consumer and service registry. It postulates a general protocol for interaction: A service provider registers at the service registry by submitting information about how to interact with its service. The service registry manages such information about all registered service providers and allows a service consumer to find an adequate service provider. Then, the service of the provider and the service of the consumer may bind and start interaction.

A service has two kinds of interfaces: *required* and *provided* interfaces. Required interfaces specify which services are used by the service. In contrast, provided interfaces specify which services are offered by the service. So in terms of the service roles in SOA a service plays the consumer's role at the required interfaces and at the provided interfaces it plays the provider's role.

Apart from these technical paradigms services in SOA are also based on an *economical paradigm*: a service is comparable with a business unit. So it should create *value* for its environment. Therefore the two kinds of interfaces can be seen as the *buy side* and the *sell side* of the service. On the buy side a service behaves as a service consumer or *client* and buys other services. On the sell side a service behaves as the service provider and offers its service to other services. Services are operating as actors on a market place. This means, they offer their services to any consumer who needs it and they buy services from providers with the best value proposition. So both parties publish their needs and offerings at a repository, respectively.

Requirements for SOA

Figure 2-1 shows an example of an information system scenario that could benefit from a migration to SOA. Within one organization, three separate business processes use the same functionality, each encapsulating it within an application. In this scenario, the login function, the ability to change the user name, and the ability to persist it are common tasks implemented redundantly in all three processes. This is a suboptimal situation because the company has paid to implement the same basic functionality three times.

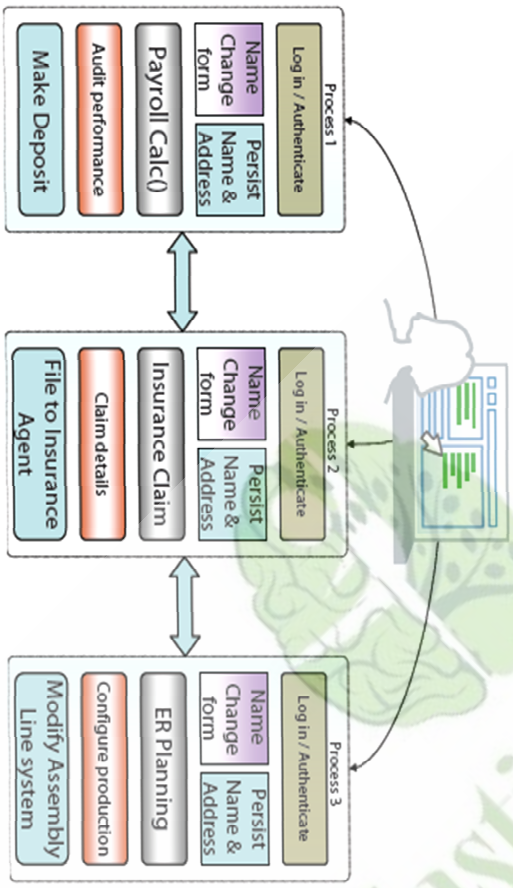


Figure 2.1 – three business processes within one company duplicating functionality

Moreover, such scenarios are highly inefficient and introduce maintenance complexity within IT infrastructures. For example, consider an implementation in which the state of a user is not synchronized across all three processes. In this environment users might have to remember multiple login username/password tokens and manage changes to their profiles in three separate areas. Additionally, if a manager wanted to deny a user access to all three processes, it is likely that three different procedures would be required (one for each of the applications). Corporate IT workers managing such a system would be effectively tripling their work –and spending more for software and hardware systems.

IT Service Management

IT Service Management provides visibility into applications as well as the supporting infrastructure. Service Management services provide reporting and monitoring services.

It supports IT service management through both features core to its BIG-IP platform as well as stand-alone products designed specifically to provide core service management features as well as additional functionality.

Enterprise Manager™ is a stand-alone device designed to aid in the configuration and management of large BIG-IP platform installations. Enterprise Manager provides configuration management services, and can act as an aggregation point for reporting and monitoring services across all BIG-IP platform instances. Additionally, F5's BIG-IP platform contains a number of features that support reporting and monitoring services, as well as the means by which both can be easily tailored to provide better visibility into both the organizational SOA as well as its supporting Service-Oriented Infrastructure.

Infrastructure Services

The core purpose of any SOI should be to support the availability, scalability, and optimization of SOA-based services and applications. These functions are provided through product features such as:

- Load balancing
- Compressing
- Caching
- TCP connection management
- Advanced health monitoring of services

Effectiveness of SOA

While a well planned and executed SOA undertaking can help organizations realize greater responsiveness in a changing marketplace, not all service oriented efforts have been successful. SOA projects have limited success when they are driven from the bottom up by developers; building SOA for

the sake of SOA without reference to the business context is a project without organizing principles and guidance; the result is a chaotic implementation that has no business relevance. On the other hand, taking a **top-down mega-approach** to SOA requires such enormous time investments that by the time the project is complete, the solution no longer maps to business needs.

Web Services and SOA

It is the ability to readily change and optimize business processes is the success key to organizational competitiveness and growth. Organizational agility can be compromised when supporting Information Technology assets cannot respond flexibly to changing business needs. Unlocking IT resources from their application silos and making their functionality broadly available across the organization promotes business process optimization and organizational agility.

Service Oriented Architecture (SOA) is a design approach to organizing existing IT assets such that the heterogeneous array of distributed, complex systems and applications can be transformed into a network of integrated, simplified, and highly flexible resources. A well-executed SOA project aligns IT resources more directly with business goals, helping organizations to build stronger connections with customers and suppliers, providing more accurate and more readily available business intelligence with which to make better decisions, and helping businesses streamline business processes and information sharing for improved employee productivity. The result is the unlocking of IT resources for the increased agility that organizations seek[1].

Service Oriented Architecture provides the design framework to integrate soloed applications so that their functionality can be accessed as services on a network. Most commonly implemented through standards-based, technology-neutral Web Services [3], SOA breaks down monolithic applications into a suite of services, implementing functionality in a modular fashion.

From the business perspective, a service performs a specific task; as such, it can map onto a business process as simple as inputting or outputting a field of data such as 'customer ID' alternatively services can be aggregated into a composite application that provides a higher-order service as complex as 'fill customer order,' a process that end to end spans multiple business applications.

Web services as illustrate by **Figure 1**, are the most common way to implement SOA. Web services are applications that use standard transports, encodings, and protocols to exchange information. It enable computer systems on any platform to communicate, and are used in a range of application integration scenarios, both within the organization and among trading partners.

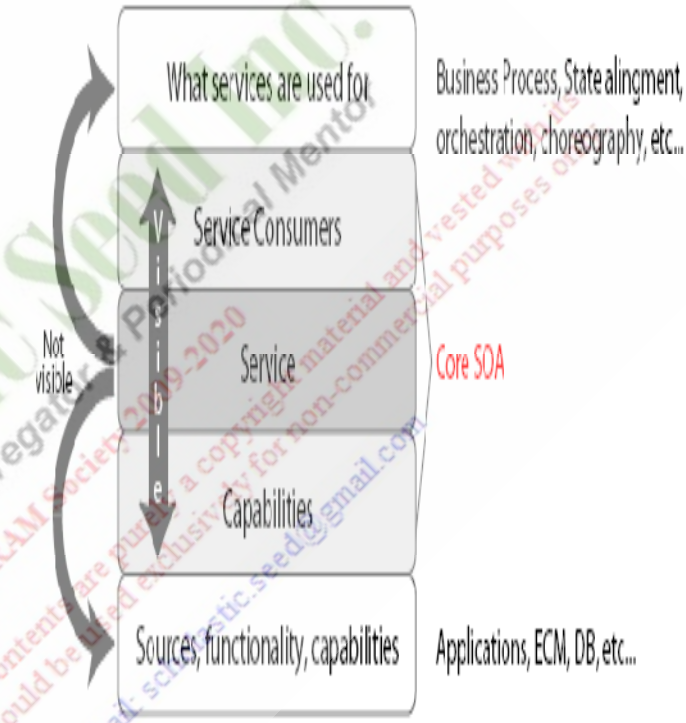


Figure 1: Web services within overall architecture in SOA [3]

The service oriented approach allows the creation of services and composite applications that exist independent of the underlying technologies.

At the beginning with version 1.0 of the .NET Framework, Microsoft investments in tools together with the intrinsic support for Web services in the Windows platform have helped make Service Orientation mainstream. Shortly thereafter, Microsoft worked with IBM to develop the Web services Interoperability Organization (WS-I) which promotes interoperability across platforms, operating systems

and programming languages. Now grown to nearly 150 member companies, WS-I has created Web services that address critical areas such as interoperability, security, and the reliability of messaging.

Microsoft's real world approach has helped organizations of all sizes to optimize their business processes and to realize greater business agility and faster time to value through use of Microsoft's SOA design principles, best practices, tools and technologies.

The concept of **SOA** can be viewed from several perspectives, which help in understanding the underlying architectural requirements of the architecture.

There are three abstract capability layers exposed within a **SOA**.

1. **Expose: focuses on how existing IT investments are exposed as a set of broad, standards-based services, enabling these investments to be available to a broader set of consumers. A Service Implementation Architecture describes how services are developed, deployed and managed.**

2. **Compose** : focuses on combining services into applications or cross-functional business processes. A Service Integration Architecture describes a set of capabilities for composing services and other components into larger constructs such as business processes.

3. **Consume** : focuses on delivering new applications that enable increased productivity and enhanced insight into business performance. A Service Oriented Application Architecture describes how "composed services" are made available for consumption through business processes, new services or new end-user applications.

Focus on the Business Drivers

Before a developer writes a single line of code, it is critical to identify both specific business drivers of the SOA endeavor and the dependencies between the business and the underlying technologies. Two approaches are commonly pursue for implementing SOA:

- Top-down and ,
- Bottom-up.

Both approaches have possible pitfalls that can prevent success. Most of the organizations that have attempted to roll out SOA infrastructure through a top-down approach have discovered that when the infrastructure is finally delivered it is out of sync with the needs of the business. Likewise, a bottom-up approach can fail as well, because it can lead to a chaotic implementation of services created without regard to organizational goals.

The "middle-out" approach is a successful hybrid of the two other approaches. Business drivers and strategic vision are first employed to set clear direction and priorities. Based on these, the organization takes multiple iterative steps to build out slices of end-to-end capabilities, with each iteration delivering a new, dynamic application back to the business that is used to create business return. Company like Microsoft has long advocated this "real-world" approach to leveraging service-oriented architectures: The approach is focused on rapid time-to-value, and it delivers business results through iterative, incremental steps that facilitate close alignment of IT resources with changing business conditions.

Benefits of SOA

SOA benefits accrue for the organization at two different levels, that of the business user and that of the IT organization. From the business point of view, SOA enables development of a new generation of dynamic applications that address a number of top-level business concerns that are central to grow and competitiveness. SOA solutions promote:

1. **Enhanced Business Decision Making -** By aggregating access to business services and information into a set of dynamic, composite business applications, decision makers' gain more accurate and more comprehensive information. People, processes and systems spanning multiple departments can more readily be mapped into a single unified view, enabling organizations to better understand the cost tradeoffs that they are making in daily

business operations. And by providing better information faster, organizations can react more quickly to problems as they arise.

2. **Increases Employee productivity -** By providing streamlined access to systems and information and enabling business process improvement, businesses can drive greater employee productivity. Employees can focus their energies on addressing the important, value-added processes and on collaborative, semi-structured activities, rather than having to conform to the limitations and restrictions of the underlying IT systems. Moreover, since end-users can access information in the form and presentation factor (web, rich client, mobile device) that meets their needs, productivity is enhanced.

3. **Stronger connections with customers and suppliers** -The benefits of SOA extend beyond organizational boundaries. Mergers and acquisitions become more profitable, since it is easier to integrate disparate systems and applications. Integration with trading partners and streamlining of supply chain processes are readily attainable goals. Providing more responsive customer service is enabled, as are new customer initiatives, such as one-stop service portals. By making available dynamic applications and business services to external customers and suppliers, not only is richer collaboration is possible, but customer/partner satisfaction is increased. SOA unlocks critical supply and demand chain processes—such as outsourcing of specific business tasks—from the constraints of underlying IT architectures, thereby enabling better alignment of processes with organizational strategy.

Technical Benefits:

From the IT department's point of view, service orientation provides the framework through which to simplify the creation and management of integrated systems and applications, and a way to align IT assets with the business model and changing business needs.

1. **More productive, more flexible applications.** The service oriented approach enables IT to make existing IT assets—including legacy systems and applications—more productive and more profitable to the business without the need for custom-coded one-off integration solutions. Service orientation also enables the development of a new generation of composite applications that provide cross-functional capabilities to the organization irrespective of the underlying platforms and programming languages. Moreover, since services are uncoupled from their underlying IT infrastructure, there is inherently greater flexibility in solution design.

2. **Faster, more cost-effective application development**. Standards-based service design enables IT to create a repository of reusable services that can be combined into higher level services and composite applications as new business needs arise. This lowers the cost of solution development and testing, reduces redundancy, and speeds time to business value. And the use of a single development model and framework simplifies and standardizes application building, testing and maintenance.

3. **More manageable and secure applications**. Service oriented solutions provide a common infrastructure (and documentation) for developing secure, monitored, and predictable services. As business needs change, SOA makes it easier to add in new services and

capabilities that map onto critical business processes. Because services are accessed rather than the applications themselves, service orientation provides the means for protecting existing IT investments without inhibiting the deployment of new capabilities. And since a strong authentication and authorization model is used for all services—as well as because services exist independently of one another and cannot therefore impact other services—the SOA approach provides greater overall security.

Discussion:

Present study stated that if business introduced the Service Oriented Architecture (SOA) then they take various benefits not only in the application part but also in the integration of person to person upward and downward as well as linear. It provides more flexibility in solution design, cost effective in secure application development and improves the decision making. The productivity of employee no doubt increased. According to my opinion the implementation of SOA makes the smaller business to large because it exploits the business world wide. So I suggest to modern business to implement the SOA and take its cross-platform real benefits.

Reference

i. Enabling "Real World SOA" through the Microsoft Platform, Microsoft Corporation,Published: December 2006.

ii. UFIDA U9 ERP Software: Optimizing the SOA Implementation, White Paper, Published: 08-12-08

iii. Duane Nickull, Service Oriented Architecture (SOA) and Specialized Messaging Patterns, Technical White Paper

iv. Abrial, J.R., Schuman, S.A., Meyer, B.: Specification language. In: On the Construction of Programs. (1980)343{410

v. Jones, C.: Systematic Software Development using VDM. Prentice Hall (1990)

vi. High, R., Kinder, S., Graham, S.: IBM's SOA Foundation { An Architectural Introduction and Overview. Technical Report 1.0, IBM (2005)

vii. Beisiegel, M., Booz, D., Edwards, M., Hurley, O., Ielceanu, S., Karmarkar, A., Malhotra, A., Marino, J., Nally,

viii. M., Newcomer, E., Patil, S., Pavlik, G., Rowley,M., Tam, K., Vorthmann, S., Waterman, L.: Service Component Architecture { Assembly Model Speci¯cation. SCA Version 0.96 draft 1, August 2006, BEA,Cape Clear, IBM, Interface21, IONA, Oracle, Primeton, Progress Software, Red Hat, Rogue Wave, SAP, Software AG., Sybase, TIBCO (2006)

ix. McIlroy, M.D.: Mass Produced Software Components. In Naur, P., Randell, B., eds.: Proceedings of NATO Software Engineering Conference. Volume 1., Garmisch,Germany (1968) 138{150

x. Szyperski, C.: Component Software{Beyond Object-Oriented Programming.Addison-Wesley and ACM Press

xi. (1998)

xii. Messerschmitt, D., Szyperski, C.: Software Ecosystem{Understanding an Indis-pensable Technology and Industry. MIT Press (2003)

xiii. Bass, L., Clements, P., Kazman, R.: Software Architecture in Practice. 2nd edition Wesley Professional (2003)

xiv. Chinnici, R., Moreau, J.J., Ryman, A., Weerawarana, S.: Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language. W3C Candidate Recommendation 27 March 2006, W3C (2006)

xv. White, S.A.: Business Process Modelling Notation Version 1.0. Technical report,Business Process Management

xvi. Initiative (BPMI) (2004)

xvii. Andrews, T., Curbera, F., Dholakia, H., Goland, Y., Klein, J., Leymann, F., Liu, K., Roller, D., Smith, D., Thatte,

xviii. S., Trickovic, I., Weerawarana, S.: Business Process Execution Language for Web Services, Version 1.1.

xix. Specification, BEA Systems, International Business Machines Corporation, Microsoft Corporation (2003)

xx. B.Äorger, E., St.Äark, R.: Abstract State Machines. A Method for High-Level System Design and Analysis.

xxi. Springer-Verlag (2003)

xxii. Abrial, J.R.: The B-Book: Assigning Programs to Meanings. Cambridge University Press (1996)

xxiii. Christensen, E., Curbera, F., Meredith, G., Weeravarana, S.: Web Service Description Language (WSDL) 1.1.

xxiv. C Note 15 March 2001, Ariba, International Business Machines Corporation, Microsoft (2001)

xxv. Object Management Group: UML2.0 Object Constraint Language (OCL) Specification. Specification, Object Management Group (OMG) (2003)

xxvi. Aalst, W.: The application of Petri nets to work°ow management. Journal Circuits, Systems and Computers 8(1) (1998) 21{66}

xxvii. Reisig, W.: Petri Nets. EATCS Monographs on Theoretical Computer Science edn.Springer-Verlag, Berlin, Heidelberg, New York, Tokyo (1985)

xxviii. Billington, J., Christensen, S., Hee, K., Kindler, E., Kummer, O., Petrucci, L., Post, R., Stehno, C.,Weber, M.: The Petri Net Markup Language: Concepts, Technology,and Tools. In Aalst, W., Best, E., eds.: Applications and Theory of Petri Nets 2003, 24th International Conference, ICATPN 2003, Eindhoven, The Netherlands, June 23-27, 2003, Proceedings. Volume 2679 of Lecture Notes in Computer Science.,Springer (2003) 483{505}

xxix. Beatty, J., Blohm, H., Boutard, C., Brodsky, S., Carey, M., Dubray, J.J., Ellersick,R., Ho, M., Karmarkar, A., Kearns, D., Brettevillois, R.L., Nally, M., Preotiuc-Pietro, R., Rowley, M., Smith, S., Yan, H.: Service Data Objects For Java. Specification, Version 2.01, IBM, BEA, Oracle, SAP, Siebel, Xcalia, Sybase (2005)

xxx. White, S.A.: Business Process Modelling Notation Version 1.0. Technical report,Business Process Management Initiative (BPMI) (2004)

xxxi. Andrews, T., Curbera, F., Dholakia, H., Goland, Y., Klein, J., Leymann, F., Liu,K., Roller, D., Smith, D., Thatte,

xxxii. S., Trickovic, I., Weerawarana, S.: Business Process Execution Language for Web Services, Version 1.1. Speci¯cation, BEA Systems, International Business Machines Corporation, Microsoft Corporation (2003)
xxxiii. B.Äorger, E., StÄark, R.: Abstract State Machines. A Method for High-Level System Design and Analysis.
xxxiv. Abrial, J.R.: The B-Book: Assigning Programs to Meanings. Cambridge University Press (1996)
xxxv. Christensen, E., Curbera, F., Meredith, G., Weeravarana, S.: Web Service Description Language (WSDL) 1.1.W3C Note 15 March 2001, Ariba, International Business Machines Corporation, Microsoft (2001)
xxxvi. Object Management Group: UML2.0 Object Constraint Language (OCL) Specification. Specification, Object Management Group (OMG) (2003)
xxxvii. Aalst, W.: The application of Petri nets to work°ow management. Journal of Circuits, Systems and 8(1) (1998) 21{66}.
xxxviii. Reisig, W.: Petri Nets. EATCS Monographs on Theoretical Computer Science Edition. Springer-Verlag, Berlin, Heidelberg, New York, Tokyo (1985).
xxxix. Billington, J., Christensen, S., Hee, K., Kindler, E., Kummer, O., Petrucci, L., Post,R., Stehno, C.,Weber, M.: The Petri Net Markup Language: Concepts, Technology,and Tools. In Aalst, W., Best, E., eds.: Applications and Theory of Petri Nets 2003,24th International Conference, ICATPN 2003, Eindhoven, The Netherlands, June 23-27, 2003, Proceedings. Volume 2679 of Lecture Notes in Computer Science.,Springer (2003) 483{505}.
xl. Beatty, J., Blohm, H., Boutard, C., Brodsky, S., Carey, M., Dubray, J.J., Ellersick, R., Ho, M., Karmarkar, A.,
xli. Kearns, D., Brettevillois, R.L., Nally, M., Preotiuc-Pietro, R., Rowley, M., Smith, S., Yan, H.: Service Data Objects For Java. Specification, Version 2.01, IBM, BEA, Oracle, SAP, Siebel, Xcalia, Sybase (2005)

Global Journal of Enterprise Information System

Jan 2010-June 2010

Volume-2 Issue-1

'DIGITAL SIGNATURE : NATURE SCOPE UNDER THE IT ACT, 2000 - SOME REFLECTIONS'

Dr. Vijaykumar Shrikrushna Chowbe

Head, Department of Law, Sant Gadge Baba Amravati University, Amravati [Maharashtra], India.

vijuchowbe@gmail.com

ABSTRACT

This article has attempted to understand the nat meaning and scope of 'digital signature'. In turn, article has also focused on the mechanism of affixing 'digital signature' to electronic record. Signature sig authentication, verification and non-repudiation, bu electronic environment this mechanism happens altogether different sense as compare to paper-bc world because paper-based and paper-less world different in its context and contents.

The attempt is to understand the effect and impac 'digital signature' in the cyberspace, its techno-le effect and system if issuing, granting and maintaining 'Digital Signature' in India. The limitation of this artic the legal system it focused upon, i.e. Indian Legal syst This article has understand the effect and impact 'digital signature' in general sense, but keeping Information Technology Act, 2000 [Indian piece legislation dealing with Information Technology], t context different to that effect.

KEYWORD

Digital	Signature
IT Act	Legal system
India	IT

Preface

Authentication, repudiation and verification of electronic record is flesh and bone of the electronic transactions. Therefore, unless these objectives have not been achieved, the authentication and secure electronic transaction will merely remain virtual. In order to achieve the authentication and security of electronic record the mechanism of 'digital signature' has been introduced by the Information Technology Act, 2000.

Thus while endeavoring the research on regulatory mechanism of information technology, it is necessitated to focus on the 'digital signature', its functional mechanism, authorities involve and objectives it achieve in electronic environment. The present study title, 'digital signature' has focused its attention on this vary technological aspect which is meant for achieving the goal of authentication, repudiation and verification of electronic record by affixing digital signature.

Meaning of Signature

Signature signifies the legal identity of the person and requires authenticating the documents. The person affixing signature to the document owes legal responsibility oozing out of it. Thus, a signature is not part of the substance of a transaction, but rather of its representation or form. Signing writings serve the following general purposes: [i]

- **Evidence:** A signature authenticates writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the singer.[ii]
- **Ceremony:** The act of signing a document calls to the singer's attention the legal significance of the signer's act, and thereby helps prevent "inconsiderate engagements.[iii]
- **Approval:** In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it has legal effect.[iv]
- **Efficiency and logistics:** A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.[v] Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.[vi]

What is digital signature?

Just the role the 'stamps', 'seal' or 'signature' play in traditional system to create the authentication of paper document, the digital signature plays the role to authenticate the electronic record. It establishes the authenticity of any electronic record which subscriber of digital signature wants to be authenticated the electronic record by affixing his digital signature. Digital signature in facts has two asymmetric pair of private and public key unique to the each subscriber. The private key and public key are corresponds to each other in such a way that the electronic record encrypted with the help of any private key can be decrypted only with the help of corresponding public

key. This digital signature creates digital ID for the subscriber holding digital signature certificate. This certificate is issued by Controller of Certifying Authority after due verification and adopting procedure.

This certificate contains basic information about the person holding it. The information such as, the name, public key, place of working, date of issuance, date of expiry of the certificate and name of the Certification Authority. The certificate is also publicly made available through the directories or public folders on WebPages. The law specifically made it clear that Controller will act as a repository for all Digital Signature Certificates issues under the Act and maintain a computerized data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.[vii]

This is essential because the public key of subscriber should be known to the interested person and should be readily available these information for them to verify the electronic record encrypted by subscriber of digital signature by affixing his digital signature.

Common features of Digital Signature: As stated above the digital signature play the same role as assigned to seal, stamps and signatures in the traditional system. It performs Signer Authentication, Message authentication and Verification.

a. **Signer Authentication: The digital signature must be capable to identify and link the signer with the electronic record which subscriber of digital signature has created. It is also necessary to ensure that the tampering of documents should not be happened after its creation. The private key belongs to subscriber who signs it and incurs legal responsibility out of it.**

b. **Message authentication:** The electronic record transformed by algorithm mapping with hash function by affixing private key of digital signature typically identify the matter to be signed, since verification also reveals any tampering with the message.

c. **Verification:** The ultimate aim of creation of digitally signed document is capability of its verification at latter moment of its creation. Thus the mechanism must be capable to verify the authenticity and non-repudiation to resolve the disputes between originators and recipient and a third party must be able to verify the signature as independent verifying institution.

'Digital Signature' – techno-legal aspects

Due to its varied nature, digital technology has provided faster, easy, accurate and convenient mechanism for creation, storage, transmission and retrieval of data without involving traditional paper-based formalities. This hastens the increasing use of digital technology in everyday life. Distance, transportation, conveyance are withered away between two individuals when they sit in front of their respective terminals sharing common network. They can share information, data, communicate by remaining online without diminishing their efficiency in

executing their work. These characteristic features of digital technology have led the world to go online. It has, in turn, increased the techno-dependency. Increasingly the business dealings, communication, official data and commercial transactions are being carried out in Cyberspace. The transformation of world from paper-based to digital based work culture has shifted the attention of world to find out the consequences of this transformation. Despite the speed, convenience and preciseness of the digital technology, some of the weaknesses of this technology has expressly manifested during the course of time. The most debatable issue in forefront is absence of degree of 'privacy' and 'authentication' of transactions, dealings and communication one can enjoy in traditional paper-based culture.

Privacy is an essence of individual liberty. No one wants to enter into the zone where his privacy would be at stake. If one is unable to feel secure about and does not have confidence for the consequences the digital environment put him for, he would hardly chose such medium for his transactions. Therefore, a sense of privacy and assurance of its respect in the medium play vital role for an individual to chose the medium. It is only because of the danger of being prospective violation of privacy, the net is treated is most dangerous zone where the 'privacy' has involved as a basic issue. It should be noted down that the concept of 'privacy' discussed here is not from point of view of any right to privacy, but is should be understood as a part of all transactions, dealing, communication that is used to be carried out by an individual with a feeling to be maintained by the concept of 'privacy'. It can be simply understood by taking an example of 'E-mails' and 'chat rooms'. Nobody assure that how so far these 'E-mails' and 'chat-rooms' are safe to safeguard the privacy of an individual. The 'privacy' is at stake in digital environment in two different ways.

First, because if one remains connected to the network, he loses control over his data. It may possible that the data may be hijacked by someone else, driven out of the computers, or passes from one server to another server without the knowledge of user. Data in digital environment is in the form of bytes which is capable to move, transfer, copy, distribute, disseminate in number of ways sometime, with the knowledge, sometime without the knowledge of user. It is utmost difficult to check the various routes, channels and paths of data in network.

Secondly, because netizens use network for creation, transfer, distribution, storage or dissemination of their data of personal nature. Today, billions of netizens are using Internet and they use the services provided by the Internet Service Providers [ISP]. The netizens use Internet for creating their E-mail account(s), chatting, surfing, gathering information of government offices & companies, to search job opportunities and even put their personal information on matrimonial sites in search of prospective life partner. Once any private information or communicate in digital environment either uploaded or received, transmitted or stored in mail account, everything is stored in the server of the Internet Service Provider. In this case despite the information, which is of private in nature, does not remain in actual possession of the intended recipient, but stored in the server of Internet Service Provider. In most of the cases it is observed that Internet Service Providers treat either the subscriber of their services or the information they generate, as a commodity for their own business promotion or projecting their Internet Services in to Digital Market.

Bigger the number of subscribers availing services of ISPs, more the advertisement revenue generation for Internet Service Provider. This can be more clearly evident by surfing to the matrimonial sites that uses the photographs, liking and disliking, hobbies, what they are looking for, of their subscribers to put on their home page to attract the other. Even in most of the cases, the netizens can view, share, surf and retrieve the data from these matrimonial sites. Therefore, entering into the digital environment is appeared to be risky now a day. Privacy is an essence of individual liberty which remains at stake in digital environment.

Another, serious problem one can pose in digital environment is lack of degree of 'authentication'. 'Authentication' is a soul essential for transactional solidarity. In absence of 'authentication', there would be difficulties in fixing the responsibilities and liabilities arise out of transactions and dealing. If the respective parties do not have the sense of 'authentication' for their counterparts, the documents coming from them, or if it is difficult to scrutinize whether the originator is the same and documents is not tampered in between the transaction, it is always have gap to air the doubt which lead to complex problem of fixing respective responsibility. Therefore, 'authentication' is one of the important ingredients for any transaction and dealing in any medium.

The traditional medium has set a mechanism to safeguards the interest of parties with entering into transaction and dealing with regards to 'privacy' and 'authentication'. Transactions, communication, information are passes in closed enveloped, stored in a locked cabinet, marked as 'confidential' and places has restricted entry for authorized personnel only. Secrete envelopes are marked to be opened by 'only addressee' or even sometime by using secrete codes in cryptographic languages which is able to decrypt by recipient only. The legislation like 'the Official Secrete Act, 1923' is an example to safeguard the information of public offices. The degree of authentication is met out with the help of 'stamps', 'seals', identity cards, 'logos', 'official emblems', 'signatures', 'encrypted messages' and several times by agreements signed by parties and attested by competent witnesses to protect information of 'confidential nature'. Such agreements are generally known as 'Non-disclosure Agreement'. Thus, the mechanism of authentication of information is neither new, nor uncommon to the legal system and there are several ways to generate sufficient degree of 'privacy' and 'authentication'. The need of 'privacy' and 'authenticity' of transactions, information, data, communication is still not diminished at all, which in contrast was lacking in digital environment. Therefore, it was felt necessary to introduce the technological safeguards which would able to provide the same level of authenticity and privacy the traditional system claimed for. 'Digital signature' has been introduced with the purpose to provide a degree of 'authentication' and 'privacy' to digital content. The present mechanism of affixing 'digital signature' is able to provide 'authentication' and to some extend create a degree of 'privacy' in the digital environment.

General and Technological aspects

This chapter attempted to understand the 'Digital Signature' in two different parts. The part – I has deal with the general & technological aspects of 'Digital Signature' in which various aspects are touched but from the aspect to understand the nature, scope, working phenomenon and modality of execution of

'Digital Signatures'. The other part will deal with the legal aspects of 'Digital Signatures'.

Digital Signature – Necessity and objectives

Digital Signature is created by using cryptographic method. For the purpose of under standing the affixing of 'Digital Signature' by way of cryptographic method, it is essential to bear in mind the purpose of affixing 'Digital Signature'. The basic objectives of affixing of 'Digital Signature' are –

Affixing of 'Digital Signature'

Create authenticity of the originator – so that at any moment after the creation of any digital material, the authenticity of the originator can be verified. It will be possible only if the mechanism is capable to create any impossibility of anybody else to represent himself with the digital material which he has not created. At the same time it is also essential that at any latter moment, the originator will not capable to deny the creation of document by him

Create authenticity of the document - so that any recipient will not be in position to modify, change, alter, or tamper with the document created by originator. The mechanism should also ensure to the originator that no one else than him will be capable to modify, change, alter or tamper with the document

Non-repudiation – so that the entire mechanism will ensure that the document and identify mechanism will not play foul and nobody will be in position at any latter moment to deny the responsibility and liability arising out of the document. For originator, that he will not be in position to repudiate what he had created, for recipient, he will not be in position by any means to modify the content created by originator

The 'Digital Signature' has evolved to achieve these objectives. It can be done with the help of 'Public Key Cryptography'. Therefore first it is essential to have fundamental understanding of the concept and meaning of term 'Cryptography'. It can be represented as:

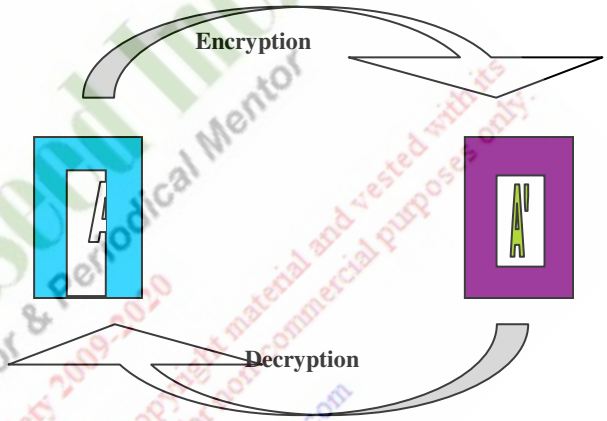


Fig: 2 Encryption/Decryption of an electronic record to convert it from one form to another

'Cryptography' is a way of scrambling of electronic record from one form to another form using hash function which leads to create hash result. Encryption stands for the modifying the electronic record in different form and decryption stands for bring it into the original form.

Normally, it is easier to encrypt any electronic record from one form to another and bring it back to its original form by decrypting it. It is important to note here that both encryption and decryption is easy for those who are aware about the methods used in this process. In this process generally a key is used to encrypt the electronic record and by using the same

key. This keys act as a secret password and generally know to both the parties i.e. originator and recipient. Therefore, if both the parties are aware about the keys required for encryption and decryption they can assure the authenticity of an electronic record.

Mechanism of Digital Signatures

However, recently, the mechanism has been developed to use two different keys. By one key the encryption can be carried out and decryption used to be carried out by different key. Both the public and private keys are different from each other commonly but correspond to each other in such a way that the public key can decrypt the document encrypted by private key. The main purpose of using two keys is very apparent. The first key of the set is 'private key' which is unique and only know to its holder.[viii] It acts as a secrete key of holder and plays very vital role. It helps any holder of this key to encrypt the electronic record. Once the electronic record is encrypted with the help of private key it scrambled the electronic record in such a clever ways so that putting it back to its original form is almost all impossible. Even the holder of private key now cannot put the electronic record into original form. Now only viewing this record is possible with the help of corresponding public key. The mechanism of private key is that it leads every time to the same result for same electronic record. Thus once any electronic record is encrypted with the help of private key the holder of private key cannot deny that it is encrypted with the help of his private key.

The second key in the set is public key which is used to verify electronic record and available and known to the public at large. Anybody who wants to verify the content of the electronic record encrypted with the help of private key, can use corresponding public key to verify the electronic record, however, only verification of electronic record is possible with the help of public key and no alteration, modification, change or tampering is possible furthermore once it is transformed into hash result by applying private key. Both these keys are so related with each other that only the electronic record encrypted by private key can be open by its corresponding public key only. Thus use of this asymmetric pair of keys for encryption and decryption of electronic records serve following purposes:

For Originator

It helps the originator to encrypt the electronic record. Once originator encrypts any electronic record with the help of his private key, nobody [even originator] can modify the content of the electronic record. Thus private wrap the digital content and does not allow modifying, altering, changing or tampering the content of the electronic record. Thus after apply his private keys originator will assure himself that the electronic record cannot be bring to its original format and any change is almost impossible in the electronic record.

Once the electronic record is encrypted it get wrapped, and no further alteration by any means allowed to be made. Therefore originator remains assured that any electronic record he has created is safe. Such electronic record can be decrypted only with the corresponding public key of originator. Thus, if any alteration has been made to electronic record created with the help of originator's private key, the public key of originator will unable to open the electronic record. Therefore, public key of originator will works only in case when the electronic record created by encryption of private key of originator.

For recipient

As the document so created by private key of originator is unique one which can be opened only with the help of public key of originator, recipient can verify and get assured by decrypting the electronic record with public key of originator which is readily available. Once the electronic record is able to decrypt, it is evident that it was encrypted by the private key of originator. If the deception is possible, it is evident that it is not modified after its encryption.

Therefore, if the electronic record is capable to decrypt with the help of public key of originator, the originator cannot deny the authenticity of electronic record. But if electronic record is unable to be verified with the help of public key of originator, it is possible that originator had not created it or it has altered after its creation.

Because technically whenever private keys applies to the electronic record, hash function works upon it to transformed it by algorithm mapping into another electronic record called hash function, this hash function is only able to verify with the help of corresponding public key of the originator. This helps the originator that once he applies his private key to any electronic record, the resulting record [known as hash result] will neither be able to tamper nor any change is possible, and only can be verified with the help of his public key and not otherwise.

For the purpose of legal system

a. This system also helps to create authenticity and accuracy for electronic record. In case of any doubt and denial of authentication either by originator or recipient, the electronic record can be varied. Because hash function is such algorithm mapping system which generate the same hash result every time with same input.

Therefore, if the electronic record is capable to decrypt with the help of public key of originator, the originator cannot deny the authenticity of electronic record. But if electronic record is unable to be verified with the help of public key of originator, it is possible that originator had not created it or it has altered after its creation.

Verification can be made out in following ways. If the recipient has brought any electronic record in question before the court claiming that it is created by originator, and if originator denies its creation, it can be verified by applying public key of the originator. If the document gets decrypted with the public key of originator, the originator would not be in position to deny that he is a creator of the document. Because there is only one set of corresponding public and private key. It is highly impossible to decrypt the electronic record encrypted by one private key using public key of different originator.

This system in short is called affixing of digital signature. As the originator by using his private key create a electronic record in such a way that his private key act as his signature to the electronic record. The necessity of digital signatures is the essence to create authentic transaction, creating non-repudiation and integrity. It can be achieved by this process in following manner –

Authentication: As discussed above, authentication is achieved in the digital environment because this process ensure that no two sets of public and private key pair match with each other. Again the electronic record encrypted by private key of a pair is only decrypted by public key of the same pair. However, the electronic record once created by applying private key, get tampered, altered, modified or change, the public key will not able to decrypt it anyway.

Therefore, the parties, originator and recipient, can authenticate the genuineness and originality of electronic record. The Information Technology Act, 2000 has created a mechanism for affixing digital signature. The office of Controller of Certifying Authority has entrusted the responsibility for issuing, maintaining and taking all steps for safeguarding the digital signature. It issues the digital signature to subscriber, keep record and provide guidelines for its safeguards. Thus, in case of any dispute office of the Controller of Certifying Authority referred. As the record of the digital signature which constitution a key pair[ix] of private and public key is issues and maintained by the Controller of Certifying Authority, the subscriber [holding key pair] is not in position to deny its possession and authenticity.

Non-repudiation: The manner in which digital signature affixed to any electronic record can cerate authenticity of an originator, it also make is disable to repudiate any argument of its non-creation. Thus once the electronic record is created by any private key, the originator cannot deny its creation. He furthermore has to accept all the responsibilities and consequences arise by its creation. His authorship gets fixed to the electronic record and all the right and a liability oozes out automatically lies to the creator. This is important because most of the time, the creator deny the creation of the electronic record to overthrow the legal responsibility. In the eye of law this is called as non-repudiation. It is important to resolve the problems and solve the legal disputes.

Integrity: This is another important objective achieve by the digital signature. By creating a mechanism solidifying authentication and non-repudiation, it develops the sense of integrity of both the parties to the transactions. Once the digital signature are involve, both the parties remain assured, and enter into the transactions, dealing with full sense of assurance that the transactions would capable to fix right and responsibilities oozing out of it. Furthermore, both the parties are having legal alternatives open for them in case of denial or allegations. If the electronic record carries the digital signature, parties are hardly in position to deny creation and participation in the transactions. Again, both parties also remained assured about the so called 'tampering' to the electronic record. If the electronic record gets tampered, it automatically loses its authentication and non-repudiation character and lose it legal genuineness. Thus the digital signature is also capable to achieve the object of 'integrity'.

Technological mechanism of Digital Signatures

It is essential to have brief look at the technological working of a 'digital signature' mechanism. As stated earlier, each user has a pair of private and public key. This can be graphically represented as follows:

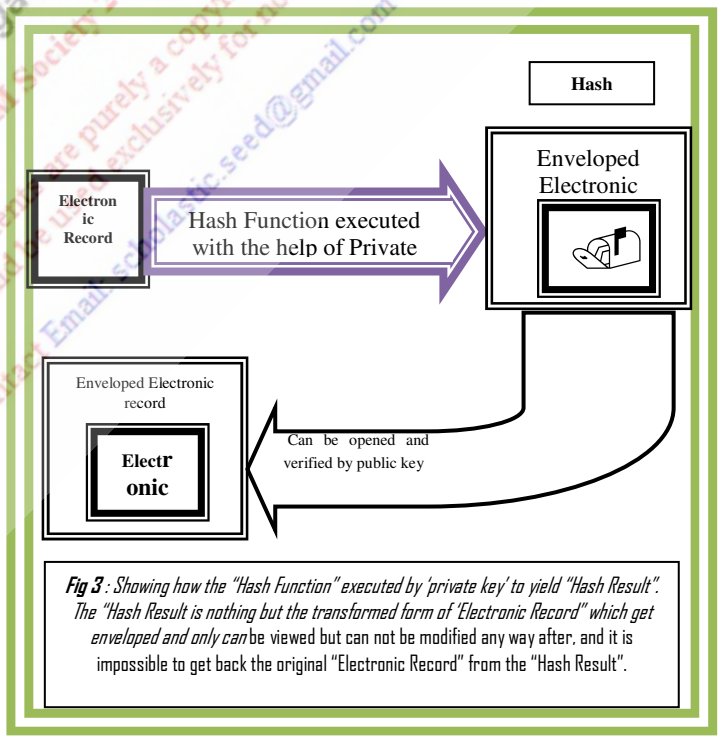


Fig 3 : Showing how the "Hash Function" executed by 'private key' to yield "Hash Result". The "Hash Result is nothing but the transformed form of 'Electronic Record" which get enveloped and only can be viewed but can not be modified any way after, and it is impossible to get back the original "Electronic Record" from the "Hash Result".

The private key remain secrete with the user and nobody is aware about it, while public key is freely distributed for the public which can be used to decrypt and verify the electronic records encrypted by person. While affixing the digital signature to any electronic record, the originator (subscriber of Digital Signature Certificate) applies his private key. When he applies his private key, an asymmetric crypto system and hash function transform the initial electronic record into another electronic record.

The "hash function" stands for an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(i).	**to derive or reconstruct the original electronic record from the hash result produced by the algorithm;**
(ii).	Those two electronic records can produce the same hash result using the algorithm. And

This mechanism also ensure that the set of private key and the public key are unique to the subscriber and constitute a functioning key pair.[x] The keys (also) have the property that it is computationally not feasible to discover one of the key pairs merely by knowing the elements of the other key.[xi]

It can be understood from above that –

- Once the "hash function" works on electronic record, it yield "hash result". This process is such that the hash function yield as hash result each times it works upon.
- "Hash function" is an algorithm which makes it infeasible to derive or reconstruct the original electronic record from the hash result produced by the algorithm.
- The two electronic records cannot produce the same hash result using the algorithm.

Therefore, every mechanism set forth must ensure all these standards. If the algorithm is unable to achieve all or any of the above objectives, the mechanism of digital signature would be futile and unable to ensure authenticity. This criterion is required by S. 3 of the Information Technology Act, 2000 and Controller of Certifying Authority has to ensure that the technological standards are capable to ensure these objectives. However, the different standards can be set forth for government and non-government entity by the Controller of Certifying Authority.[xii]

Jurisprudential and Legal aspects of Digital Signatures

If the preamble of the Information Technology Act, 2000 has given a close look, it is apparent that the act has enacted to provide 'legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication'.[xiii] The act has attempted to legally recognize the process in sum called 'electronic commerce'. The act is in furtherance of the resolution passed by United Nation on 30th January, 1997 to which India was signatory, where UNCITRAL [United Nation Commission on International Trade Law] has proposed a 'Model Law' and recommend to member states to give favourable consideration while bringing any enactments, amendments, or inceptions in the legislation relating to 'Electronic commerce'. In furtherance to promote the 'Electronic commerce' that is inter alia requires reliability of electronic documents,

it is essential to have mechanism that would ensure the trustworthiness of the electronic documents. The concept of 'Digital Signature' has brought into being with the sole purpose to develop mechanism for creating reliability and authenticity of electronic documents.

Legal Recognition of Digital signatures

The Act has set forth the objective to provide legal recognition for transactions carried out by means of electronic data interchange. At the same time, the authentication, integration and non-repudiation of electronic record is equally important. But more important than anything else is to provide a provision that would create a sense of responsible and assurance about the mechanism. The genuineness and of medium is equally important than creation of medium, and the information technology in general and digital signature in particular has attempted to bring authentication in this medium.[xiv]

Therefore, it was important that not only the affixing of 'digital signature' would make important, but it is also necessary to give equal force to the electronic record created by digital signature which in traditional medium has for attested and signed document. S. 5 of the Act fulfill this requirement which runs as under[xv] :

S. 5. Legal recognition of digital signatures.

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation.—For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Thus the plain reading of S. 5 makes it clear that the electronic record to which the 'digital signature' has been affixed has equal binding force which in traditional system the signed document has. It has also expressly made it clear if any law require that any document must bear signature, the requirement will deem to be satisfied if the electronic record is authenticated by affixing digital signature.

The explanation clause clarifies the meaning of "signed" and "signature". The clause explain that as the word "signed" has the meaning and expression attached to it which is generally done by mean of affixing of his hand written signature or any mark on any document, and signature has its meaning, in the same way, the 'affixing of digital signature should be construed accordingly. One very important differentiation should be beard into mind that in India the Act has adopted "Digital Signature" which is created by hash function and pair of public and private key. In contrast, in most of the nation, it speak about "Electronic Signature". The basic different between "Digital Signature" and "Electronic Signature" is, the digital signature is in digital form contain may be alpha-numerical, where electronic signature may also contain sound, signature by digital pen, watermark, thumb impression, eye scan. Comparatively, 'Electronic Signature' provides more security. The proposed amendment in Sept 2005 which is still pending for want of enactment, which will provide the

mechanism for 'Electronic Signature' by replacing 'digital signature', if would take shape of legislation.

Digital Signature – Legal Definition and effectuation

The 'Digital Signature' has been defined by S. 2 (1) (p) of the Information Technology Act, 2000 [the Act] as follows :

> *2 (1) (p)* "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

Thus, what exactly the 'digital signature' stands for has not been defined by the Act. It simply point out that 'digital signature' means authentication of electronic record by subscriber by and in accordance of the procedure laid down by Chapter II, S. 3 of the Act. For reference it is essential to have a look to Section 3 of the Act which runs as under:

> **Section 3. Authentication of electronic records.**
>
> (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
>
> (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.
>
> *Explanation.*—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—
>
> *(a)* to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
>
> *(b)* that two electronic records can produce the same hash result using the algorithm.
>
> (3) Any person by the use of a public key of the subscriber can verify the electronic record.
>
> (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Ss. 3 (1) of the Act explain the category of person who can authenticate the electronic record. It provides that the 'subscriber' can authentication any electronic record by affixing his digital signature to it. This sub section empowers only to the subscriber, *and not any general person*, the capacity to authenticate the electronic record. The Act also defined 'subscriber' vide S. 2 (1) (zg) as :

> "subscriber" means a person in whose name the Digital Signature Certificate is issued;

Thus the person having Digital Signature Certificate is only empowered to authenticate (any) electronic record by affixing his 'digital signature'. The Act does prescribe that subscriber can authenticate electronic record by affixing his 'digital signature'. Therefore it is not required by the Act that subscriber can authenticate only 'his' electronic record. It is clear from the language of the S. 3 (1) that subscriber can authenticate any of the electronic record whether created by himself or by any other person by affixing his 'digital signature'. It is apparently clear that though only the subscriber can authenticate the electronic record by affixing his 'digital signature', but no

limitation has been put on the subscriber to authenticate only his electronic record. He can authenticate the electronic record of other's also, but subject to provision of the Act, and only electronic record bearing valid 'digital signature' is treated reliable and authenticate in the eye of law. The general public using Internet for the purpose of E-mails, Chatting, sharing files, surfing, downloading for educational or any other purpose or even taking information from the WebPages, or government institutions, offices, companies having their Webpage cannot be treated as authenticate electronic record unless the creator of these electronic record has not holding 'digital signature certificate' and even if holding it, he has not authenticated his electronic record by using his 'digital signature'. Therefore, it should be noted down that all those electronic records which exists in digital environment are neither reliable nor authenticated. The authentication process is deliberate attempt by subscriber holding 'digital signature' and an option for him to affix his 'digital signature' to the electronic record. However, once the subscriber opted to authenticate the electronic record, and in this attempt, affix his 'digital signature' to any electronic record, it will be treated authenticate by world at large against the subscriber and subscriber cannot afterward repudiate its authenticity. Anyone can verify the authenticity by applying 'public key' of creator as the mechanism of 'digital signature' is capable to verify[xvi] the authenticity of electronic record created using 'digital signature' and this mechanism is recognized by means provided by law.

The electronic record bearing 'digital signature' thus presumed to be authenticates and can be relied upon for the purpose of commercial and other transactional business. Subject to other provisions of the Act, the electronic record bearing 'digital signature' carries evidential value and can be used against subscriber if denied or alleged to be non-authenticated.

Ss. 3 (2) prescribe the procedure of affixing of 'digital signature' to the electronic record. It stipulates that the authentication of the electronic record shall be effectuated by use of the asymmetric crypto system and hash function. The Asymmetric Crypto System' is a cryptographic process in which two different asymmetric key pair has been used to secure the record. These two key are private key and public key in which private key is used for creating a digital signature and corresponding public key to verify the digital signature.[xvii] S. 3 (4) of the Information Technology Act, 2000 states that the private key and the public key are unique to the subscriber and constitute a functioning key pair.[xviii] These two keys are related and correspond to each other in such a way that the electronic record created by a private key can only verify by public key related and corresponds to it.[xix]

Though traditionally, only one key pair use to encrypt the record and same key pair use to decrypt it. But for securing the record and unable its reversibility, two different key pairs are used in which one key pair modify the record and other key pair can only verify it, but does not able to alter, change its content.

When the private key is used to effectuate the 'digital signature' to the electronic record, hash function which is a kind of algorithm mapping use to envelop and translate one sequence of bits into another work on it to generate "hash result". The hash function is one which whenever works upon the same electronic record yield the same hash result every time.

However, the legal provision prescribe with regard to hash function that –

(i)	**The hash function is one which is used to envelop and transform the electronic record into another electronic record which is called hash result**
(ii)	The hash function is to yield same hash result every time whenever executed with same electronic record as it input
(iii)	This hash function must bear the feature that deriving or reconstruction of original record from hash result shall not be possible
(iv)	No two electronic records yield same hash result with hash function

These four conditions are mandatory to ensure that nobody able to get the original electronic record back from hash result. The first condition will ensure that hash result shall envelop and transform the electronic record into another electronic record. This process blocks the content and wraps it so that the content of the electronic record get block from any change or modification.

The second condition is to safeguard the interest of subscriber. The quality of hash function to yield same hash result every time whenever executed upon the same input will help the subscriber to verify any latter moment tampering or change into the electronic record. Thus if subscriber is doubtful about the authenticity of the electronic record, he can execute hash function to verify that the result is same or not. If the result remains unchanged each time, he can ensure that the document is one which he had created. But if two hash results differ, he can very well take plea that the input is different. The same methodology can be used by forensic lab to verify that whether the same hash result yield second time or not. They can check it with the alleged electronic record by comparison.

The third condition laid down by the Act is due to the reasons that once the digital signature affixed to the electronic record, it get enveloped and wrapped by the hash function. Now it is only possible that one can only verify it but cannot modify. Once the system ensure this feature, it give a legal presumption that once the electronic record bears digital signature, it is neither modified, changed, altered or tampered by anybody. Even the subscriber cannot able to get original record by any means. Therefore, reliability of electronic record can be ensured.

The last condition ensures that no two results from two different inputs shall yield after execution by hash function. This is because if the two hash result will be identical despite the inputs were different, its authenticity will at stake. Thus for different input, different hash result must be yield and no two hash result shall be identical if the input is different. These conditions can ensure and strengthen the reliability of mechanism and chances of creeping up of loopholes.

Creation and maintenance of Digital Signature

The Information Technology Act, 2000 has also set up the mechanism for creation and maintenance of 'Digital Signatures'. The office of the Controller has been created for the purpose. The Controller grants the licences to the 'Certifying Authority' which further issue 'digital signature' to the subscriber. Thus, Controller does not directly issue 'digital signature', but issues licences to the 'Certifying Authority'. The Certifying Authority issues the 'Digital Signature Certificate' to the subscribers. These can be represented graphically in following manner :

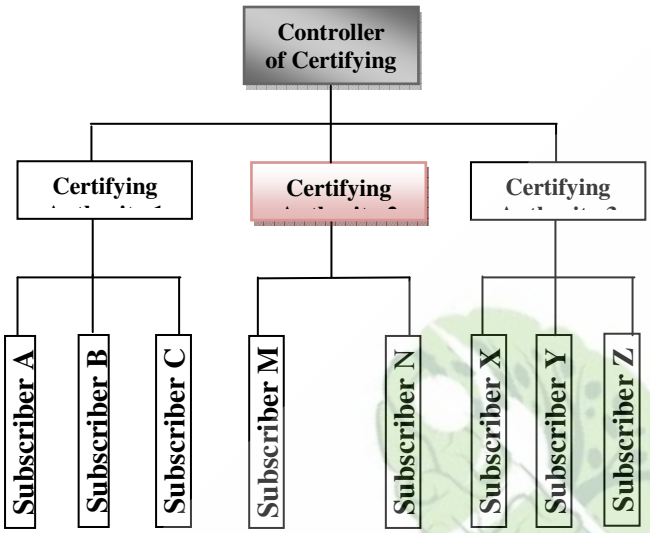


Fig 4 : Showing hierarchical set up of Controller of CA

Note : Subscribers are not the constituent part of the office of CCA

The Controller of Certifying Authority [CCA] is appointed by Central Government by notification in Official Gazette in accordance with S. 17 of the Act. by the Central Government. The Controller shall discharge his functions under the Act subject to the general control and directions of the Central Government.[xx] The functions of the Controller are prescribed by S. 18 of the Act which following major functions:

- exercising supervision over the activities of the Certifying Authorities
- certifying public keys of the Certifying Authorities
- laying down the standards to be maintained by the Certifying Authorities
- specifying the qualifications and experience which employees of the Certifying Authorities should possess
- specifying the conditions subject to which the Certifying Authorities shall conduct their business
- specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key
- specifying the form and content of a Digital Signature Certificate and the key,
- specifying the form and manner in which accounts shall be maintained by the Certifying Authorities
- specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them
- facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems
- specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers
- resolving any conflict of interests between the Certifying Authorities and the subscribers
- laying down the duties of the Certifying Authorities
- Maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.[xxi]

If the above functions of the Controller of Certifying Authority are scrutinized closely, it can be averted that Controller enjoys great control over the Certifying Authority. The Controller exercises greater control with regards to the activities of Certifying Authorities as he supervises activities of Certifying Authorities, laying

down the standards to be maintained by the Certifying Authorities, specify the qualifications and experience of employees of the Certifying Authorities should employ, specify the conditions of business carried by Certifying Authorities, specify the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key, specify the form and content of a Digital Signature Certificate and the key, specify the form and manner in which accounts shall be maintained by the Certifying Authorities, facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems, specify the manner in which the Certifying Authorities shall conduct their dealings with the subscribers, resolve any conflict of interests between the Certifying Authorities and the subscribers, lay down the duties of the Certifying Authorities and maintain a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public. Therefore, even though Controller does not directly play the role of distribution of 'digital signature' to the subscriber, he enjoy almost all the power in which manner the 'digital signature' shall be issued and maintained by 'Certifying Authorities'. In practices, the Controller of Certifying Authority issue licence to Certifying Authorities who in fact give digital signature to the subscriber.[xxii]

The Act has also specified the scope for the recognition of foreign Certifying Authorities. For this purpose, the act has prescribed that Controller may with prior approval of Central Government and subject to such conditions and restrictions as may be specified by regulations, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of the Act. In this case, if the foreign Certifying Authority would given recognition, the 'Digital Signature Certificate' issued by such Certifying Authority either to any citizens having any nationality, any company or institution incorporated in India or any foreign person, company or institution will be treated recognized for the purpose of the Act and will have the same effect and force as if the 'digital signature' is issued by the Certifying Authority having licence by Controller for all purposes laid down by the Act. [xxiii]

Digital Signature – Safeguard and functional mechanism

The Acts prescribe vide various provisions to safeguards and functional mechanism for 'Digital signature'. These safeguards can be put in following ways:

Provisions to safeguard the 'Digital Signature' mechanism

- The Controller acts as the repository of all Digital Signature Certificates and also maintains the computerized data base of all public keys.[xxiv] This ensures the availability of public key to any member of public and verification of data is possible
- The Controller has responsibility to ensure from any intrusion and misuse of any hardware, software and procedures to safeguards 'Digital Signature mechanism' and
- Shall observe such other standards as may be prescribed by the Central Government.[xxv]
- The Controller is empowered to investigate any contravention of any of the provisions of the Act either by himself or through authorized officer[xxvi]

- S. 30 of the Act provide the procedure which Certifying Authority should follow. This section laid down the responsibility on Certifying Authority with regard to hardware, software and procedures that are secure from intrusion and misuse. It also laid down that Certifying Authority should provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions. In addition to it, Certifying Authority should also adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and observe such other standards as may be specified by regulations. This is because to ensure the security measures for 'Digital Signature' and prevents it from any intrusion and misuse.[xxvii]

Provisions with regards to functional aspects of 'Digital Signature'

- The Controller is empowered to issue the licence to issue Digital Signature Certificates any person only after fulfillment of requirement laid down by the Act.[xxviii] The **Terms and conditions of licence to issue Digital Signature Certificate have been provided vide rule 3 of** the Information Technology (Certifying Authority) Regulations, 2001.
- The licence to Certifying Authority is issued only subject to satisfaction of qualification, expertise, manpower, financial resources and infrastructure facilities. This shows that person must comply with the requirement laid down by the Act and corresponding rules from time to time. Therefore, while granting the licence to any Certifying Authority to issue 'Digital Signature' the ability of the Certifying Authority will be tested upon and comply with, otherwise Controller will not issue licence to Certifying Authority.
- Though the provision laid down the liberty for Certifying Authorities to set norms and standards for issue 'Digital Signature Certificate'[xxix] to the subscribers, they must observe the rules and regulation laid down by the Act and instruction given by the Controller from time to time.[xxx]
- The Certifying Authority may charge the fees for issuing 'Digital Signature' to subscriber not exceeding Rs. 25000/- [or as may be prescribed by Central Government].
- The licence issued to the Certifying Authority also has expiry date. However the provision for renewal of licence also been prescribed by the Act. [xxxi]
- The Act also prescribed the provision for issuance and suspension of licence for which Controller has been empowered by the Act. The grounds for the suspension of licences are

Providing any incorrect information asked by any statement
Failed to comply with any term and condition on the basis of which the licence has been granted
Failed to maintain standard or contravened the provision of the Act

However, Controller will give the Certifying Authority an 'opportunity of being heard' to put his stand before revocation of licence[xxxii]

Thus, as stated in the beginning of this part of research writing, the mechanism of digital signature functions to achieve authentication, non-repudiation and verification of electronic record. It provides the sense of security in the electronic environment and facilitates the electronic transaction.

Sum up

The above analysis show that 'digital signature' under the Information Technology Act, 2000, that this is not only essential aspect for creating secure environment for electronic transactions, but it create a sense of authentication and non-repudiation and thus ultimately achieve its objectives of facilitating e-commerce. Thus in its application, digital signature has not only proved an essential techno-legal requirement, but it has made the e-commerce meaningful.

However, looking to the present development across the world, it is essential to reconsider the importation of 'electronic signature' in the legal books as it ensures greater level of safety and security in electronic environment. Beside the same, the need for cross-border recognition of digital/electronic signature is already overdue which cannot be delayed further.

The study of electronic environment from legal point of view would be incomplete without scrutinizing the 'criminality' and its various dimensions. The previous and this chapter of this research writing had focused its attention on legal framework prescribe by law. However, this would be incomplete without having glance to the 'crime' being committed in cyberspace. The study of crime committed in cyberspace will provide a platform to activate the study in proper direction, as the one of the basic role of legal framework is to regulate the 'criminality' and set law and order. Thus this makes it essential to have a glance to 'criminality in cyberspace'. Therefore, next chapter of this investigative writing turn its attention towards this aspect.

References

[i] This list is not exhaustive. For e.g. Restatement (Second) of Contracts notes another function, termed the "deterrent function", which seeks to "Discourage transactions of doubtful utility." Restatement (Second) of Contracts 72 Comment c(1981). Professor Perillo notes earmarking of intent, clarification, managerial efficiency, publicity, education, as well as taxation and regulation as functions served by the statute of frauds. Joseph M. Perillo, the Statute of Frauds in the Light of the Functions and Dysfunctions of Form, 43 Fordham L. Rev. 39, 48-64.

[ii] See, Restatement (Second) of Contracts, statutory note preceding S. 110 (1982) (Summarizing purpose of the statute of frauds, which includes a signature requirement): Lon L. Fuller, Consideration and Form, 41 Colum. L. Rev. 799, 800 (1941); 6 Jeremy Bentham, The Works of Jeremy Bentham 508-85 (Bowring Ed. 1962) (1839) (Bentham called forms serving evidentiary functions "preappointed [i.e., made in advance] evidence"). A handwritten signature creates probative evidence in part because of the chemical properties of ink that make it adhere to paper, and because handwriting style is quite unique to the signer. Signed includes any symbol executed or adopted by a party with present intention to authenticate a writing.

[iii] John Austin, Lectures on jurisprudence 939-44 (44th Ed. 1873); Restatement (Second) of Contracts S. 72 comment c (1982) and statutory note preceding S. 110 (1982) (what is here termed a "Ceremonial" function is termed a "cautionary" function in the Restatement);

[iv] See, Model law on Electronic Commerce, United National Commission on International Trade Law (UNCITRAL), 29th Session, Art. 7 (1) at 3, Doc., A/CN.9/XXIX.CRP.1/Add. 13 (1996) ("Where a law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message…."); Draft Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Data Communication, United Nationals Commission on International Trade Law (UNCITRAL), 28th Session, Art. 6, at 44, U.N. Doc. A/CN./9/406 (1994). For example, a signature on a written contract customarily indicates the signer's assent. A signature on the back of a check is customarily taken s an endorsement. See U.C.C. S. 3-204 (1990).

[v] Analogizing the form of a legal transaction to minting of coins, which serves to make their metal content and weight apparent without further examination. The notion of clarity and finality provide by a form are largely predicated on the fact that the form provides good evidence. The basic premise of the efficiency and logistical function is that a signed, written document is such a good indicator of what the transaction is, that the transaction should be considered to be as the signed document says. The moment of signing the document thus becomes decision.

[vi] See, e.g. U.C.C. S. 3-401 (1990) (A Person is not liable on an instrument unless the person signed it); See generally U.C.C. S. 3-104 (1990) (requirements for negotiability).

[vii] See for details, S 20 of the Information Technology Act, 2000 which runs as under

S. 20. : **Controller to act as repository.**

(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall—

(a) make use of hardware, software and procedures that are secure its {correct after verification} intrusion and misuse;

(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

[viii] Of course, the holder of the private key may choose to divulge it, or may lose control of it (often called 'compromise'), and thereby make forgery possible. The Guidelines seek to address this problem in two ways, (1) by requiring the subscriber, who holds the private key, to use a degree of care in its safekeeping, and (2) enabling the subscriber to disassociate himself from the key by temporarily suspending or permanently revoking his certificate and publishing these actions in a "certificate revocation list." or "CRL". A verity of methods is available for securing the private key. The safer methods store the private key in a "cryptographic token" (one example is a "smart card") which executes the signature programme within an internal micro processing chip, so that the private key is never divulged outside the token and does not pass into the main memory or processor of the signer's computer. The signer must typically present to the token some authenticating information, such as a password, pass phrase, or personal identification number, for the token to run a process requiring access to the private key. In addition, this token must be physically produced, and biometric authentication such as fingerprints or retinal scan can assure the physical presence of the token's authorized holder. There are also software-based schemes for protecting the security of the private key, generally less secure than hardware schemes, but providing adequate security for many types of applications.

[ix] See, the information Technology (Certifying Authorities) Rules, 2000 Schedule V [Glossary] which define key pair as, 'KEY PAIR – In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

[x] See, for detail, S.3 of the Information Technology Act, 2000 (21 of 2000)

[xi] http://www.state.co.us/gov_dir/gss/cec3/colo_rules.htm visited on 20.10.2006

[xii] In the first phase of its operation the services being offered are government to government. NIC offers four distinct classes of digital certification services, classes 0-3 for NICNET users within the government. For all its subscribers it issues class 2 digital IDs. These digital IDs are used to identify the subscriber on the net and are legally valid as they are backed by the Information Technology Act, 2000.

[xiii] Preamble of the Information Technology Act, 2000 runs as follows :

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

[xiv] See, State of Punjab and Ors. Vs. Amritsar Beverages Ltd. and Ors. Civil Appeal No. 3419 of 2006 (Arising out of SLP (Civil) Nos. 10371-10374 of 2004) Decided On: 08.08.2006 [para 7] p. 3488. The Supreme Court observed,

We may notice some recent amendments in this behalf Section 464 of the Indian Penal Code deals with the inclusion of the digital signatures. Sections 29, 167, 172, 192 and 463 of the Indian Penal Code have been amended to include electronics documents within the definition of Page 3489 'documents'. Section 63 of the Evidence Act has been amended to include admissibility of computer outputs in the media, paper, optical or magnetic form. Section 73A prescribes procedures for verification of digital signatures. Sections 85A and 85B of the Evidence Act raise a presumption as regards electronic contracts, electronic records, digital signature certificates and electronic messages.

[para 8]

[xv] This shall be borne in mind that the amendment brought into effect by the Information Technology Act, 2000 in Evidence Act, 1882 has also create strong presumption in favour of electronic contracts, electronic records, digital signature certificates and electronic messages.

[xvi] Therefore, the term 'verify' has also been defined by the Act which prescribed the meaning and scope as follows :

S. 2 (1) (zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

xvii S. 2 (1) (f) of the Information Technology Act, 2000 which define "asymmetric crypto system" as follows:

"asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

xviii S. 3 (4) of the Information Technology Act, 2000. See also, Duggal Pavan, Cyber Law – The Indian Perspective, Saakshar Law Publications New Delhi, 2nd Ed. 2004, pg. 65

xix S. 2 (1) (x) of the Information Technology Act, 2000 which define "Key pair" as follows :

"key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

xx See S. 17 of the Information Technology Act, 2000 which runs as under

17. **Appointment of Controller and other officers**.

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

xxi Id. S. 18

xxii For e.g. First digital Contract Note authenticated by digital signature had been issued by Mr. K.N. Gupta, the first Controller of Certifying Authorities, Government of India, has issued the first licence to "Safe Script" to act as a Certifying Authority. Another persons who were in line for the issue of licence were (1) RBI Affiliate, Hyderabad (2) Institution of Development Research and Banking Technology and, (3) National Informatics Centre et. The "Safe Script" had issued a digital signature certificate in the name of "ICICIDIRECT.COM", Mumbai. On March 27, 2002 the subscriber "ICICIDIRECT.COM", became the first firm to issue a Digitally Signed Contract Note (DSCN) to its clients [The Economic Times, Delhi Ed. 29.03.2002 Pg. 5]. The ICICIDIRECT.COM used to issue contract notes for about 22,000 transactions carried out per day. They are physically mailed to the investors. With the introduction of the new system, the investors will investors will instantly receive a legally valid contract note electronically. A report says that the new service is expected to save around Rs. 6 crores which were payable to the brokers.

xxiii See S. 19 of the Information Technology Act, 2000 which runs as under :

19. Recognition of foreign Certifying Authorities.

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

xxiv See S. 20 of the Information Technology Act, 2000

xxv Ibid.

xxvi Id. S. 68

xxvii Id. S. 30

xxviii Id. S. 21

xxix Rule 4 of the Information Technology (Certifying Authority) Regulations, 2001 has prescribed the standards followed by the Certifying Authority for carrying out its functions.

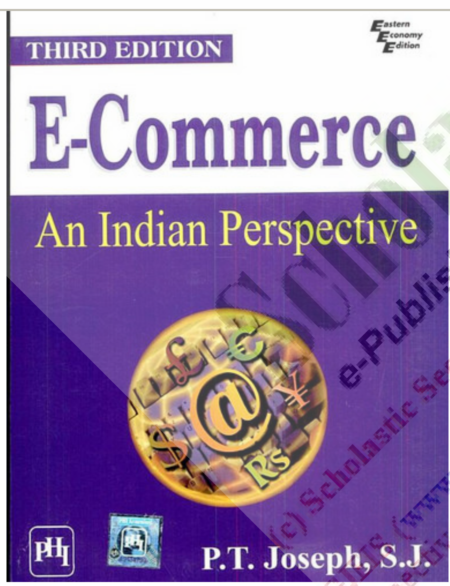
xxx See, S. 21 of the Information Technology Act, 2000

xxxi Id. S. 23

xxxii Id. S. 25

E-Commerce:
An Indian Perspective
By
P. T. Joseph, S.J.

Vinita Sharma
Assistant Professor (IT)
New Delhi Institute of Management
vinitasharma75@rediffmail.com



ABSTRACT

E-Commerce is a rapid and exciting area of development with new issues emerging everyday in this global and real time activity. The book under review highlights the latest information of e-commerce concepts, models, strategies and techniques that can be used to build useful e-commerce applications.

KEYWORD

e-commerce	India
Application	World Wide Web
e-securities	e-business strategies
Mobile Commerce	Web designing

The 3rd edition of "E-Commerce an Indian Perspective" is a thoroughly revised book. The author is back with new and improved book.

The book is useful for under graduate and post graduate students of business administration and also for students pursuing courses in computer applications information technology and information science.

The book encompasses 12 chapters covering different useful concepts and issues of e-commerce. The first chapter includes details of beginning of e-commerce in India which covers useful text and statistics for researchers of the same field.

Other part of book covers all elements of e-commerce including Customer Relationship Management, Supply Chain Management, e-payment system, e-marketing, various business models, World Wide Web technologies, e-securities, e-business strategies, mobile commerce, web designing, legal and ethical issues of e-commerce, WAP, data warehousing and data mining techniques.

The book also features many comprehensive and diverse Case Studies and statistics on Indian Corporations showing success and failure of their web based e-business models. New text on developments in technologies and general business strategies has been added in all chapters.

This fundamental treatment of the subject e-commerce coupled with a clear and practical analysis of market models, continues to make this book an invaluable source for students to improve their managerial and professional skills.

The book may also serve as valuable text book and reference book for teachers, students, researchers and other professionals.

About The Book

Title:	E- commerce: An Indian Perspective
Publisher:	PHI
Author:	S J Joseph, P T
Edition:	Paperback Third Edition
Publisher:	PHI
EAN:	9788120336216
No. of Pages:	532

http://www.karamsociety.org

Charles Møller

Center for Industrial Production,
Aalborg University,
Fibigerstræde 16, DK-9220
Aalborg Ø, DENMARK

charles@production.aau.dk

Professor, Ph.D. Charles Møller, Born: September, 2. 1962, Lives in Risskov, Denmark

Danfoss Professor in Business Process Innovation, Center for Industrial Production, Aalborg University. Teaching and researching the management of enterprise information systems in a supply chain context.

Education

Ph.D. degree in Industrial Engineering from Aalborg University (1995), M.Sc. in Electrical Engineering from Technical University of Denmark (1988).

Employment

Professor-in-residence, San Francisco State University (2005-06), Aarhus School of Business, University of Aarhus (2001-07), Department of Production, Aalborg University (1992-2001), Interconsult Management (1988-91), Brüel & Kjær (1986-88) and IBM (1985). External

Lecturer at University of Southern Denmark and University of Aarhus and External Examiner in Business Studies.

Research

Editorial board member: *Enterprise Information Systems*, *International Journal of Information Systems and Supply Chain Management* and *The Open Business Journal*. Reviewer for IBM Systems Journal, Annals of OR, Journal of IT, Journal of Strategic IS, European Journal of IS, Production Planning and Control, International Journal of Integrated Supply Management, Behaviour & Information Technology, IRMA, IDEA and Ledelse & Erhvervsøkonomi. Workshop organizer at the ICEIS and program committees for BPM, NOFOMA, IFIP 8.6, ICESAL, CONFENIS, TIGERA and ACM SAC. Program chair for CONFENIS 2010.

Major research projects and grants

Business Process Innovation (Danfoss, Aalborg University) Designing Integrated Processes based on New Advanced Enterprise Systems Technology – Establishing the Process Innovation Laboratory (ASB, Otto Mønsted), ERP management (IT University West), IMERAS (Implementation of ERP and APS systems), PITNIT (Process Integration and Transformation using Networked Information Technology), NGSC (Next-generation Supply Chain), LOKNIT, CO-IMPROVE, ULTRA (Development of future transport concepts), Center for Logistics and Goods Transportation, Center for Industrial Production (Danish Research Council).

Selected Papers Full publication list available at http://personprofil.aau.dk/Profil/100396

Total # pub exceeds 130 papers including 22 papers in Danish and international journals, 40+ refereed conference papers, and 25+ chapters or books.

Snabe, J. H., Rosenberg, A., Møller, C., & Scavillo, M. (2008). Business Process Management: The SAP Roadmap. Bonn, Boston: Galileo Press; Pérez, M. L., & Møller, C. (2008). The Predictive Aspect of Business Process Intelligence: Lessons Learned on Bridging IT and Business. In A. t. Hofstede, B. Benatallah & H.-Y. Paik (Eds.), Business Process Management Workshops (pp. 11-16). Berlin, Heidelberg; Møller, C., Chaudhry, S., & Jørgensen, B. (2008). Complex Service Design: A Virtual Enterprise Architecture for Logistics Service. Information Systems Frontiers, 10(5), 16; Møller, C. (2006). The Role of Enterprise Systems in Supply Chain Networks: A Taxonomy of Supply Chain Strategies. International Journal of Networking and Virtual Organizations, 3(2), 156-171; Møller, C. (2005). ERP II: a conceptual framework for next-generation enterprise systems? Journal of Enterprise Information Management, 18(4), 483-497.

Volume-2 Issue-1

January 2010-June 2010

Kripa Shanker

Vice Chancellor, U P Technical University, INDIA

ks@iitk.ac.in

Kripa Shanker obtained his B.Sc.Engg. (Mechanical) from Banaras Hindu University, M.Tech. in Mechanical Engineering from IIT Kanpur; and M.S and Ph.D. in Operations Research and Industrial Engineering from Cornell.

His main areas of teaching and research include production/operations management, supply chain and logistical management, quantitative and statistical decision models, computer integrated/flexible manufacturing systems, cellular manufacturing, and simulation.

He joined IIT Kanpur as a faculty member in the Industrial and Management Engineering Department in 1978 where he has been serving as a Professor since 1987. He had been a visiting Professor at the Asian Institute of Technology from 1882-84, and again from 1998-2000. He has also taught at Cornell, AITCV Hanoi, Vietnam; and Mazandran University, Iran.

He has supervised over 120 Masters and 9 Doctoral theses. He has published seventy papers in international journals and conference proceedings. He has been associated with more than a dozen sponsored projects in the field of CAM, CIMS and FMS from various sponsoring agencies. He has organized several continuing education courses for engineering college teachers, and engineers and managers from industry on the topics of inventory control, quality and reliability, DSS, CIMS, FMS and IMS.

He has received several scholastic awards and prizes for his studentship and also for his professional accomplishments. He is a recipient of Gold Medal for standing first in Mechanical Engineering at BHU. He has also been recipient of National Merit Scholarship and Government of India Scholarship for Studies Abroad. He has been awarded ISTE National Award for Outstanding Academic, 2001, and Distinguished Alumunus Award from BHU in 2007.

He is affiliated with many professional bodies which include Operations Research Society of America, Operations Research Society of India, Institute of Industrial Engineers (IIE) (Sr. Member), Fellow of Indian National Academy Engineering, Institution of Engineers, India Fellow (Life Member), Indian Institution of Industrial Engineering, Indian Society for Technical Education (Life Member). He is reviewer of several international journals in the areas of FMS, CIMS, and production and operations management.

During the last 30 years at IIT/K as a faculty, he has held various positions like founder and Head for several years of Data Processing Cell (now Office Automation), Warden, Head of Department, Head Counselling Service, Dean of Students Affairs etc. At the national level, his participations include as Member, CII National Committee on Technical Education and Training, Chairman, Institution of Engineers (India) Kanpur Local Centre, Member, AICTE National Broad of Accreditation, Board of Management Studies, member of Board of Governors of several institutions including NITs, Chairman Board of Apprentice and Training (Northern Region), He has represented various bodies of the Government of India at several international fora.

His major professional/administrative achievements with national impact include his initiating at IIT Kanpur, teaching and research in the field of computer integrated/flexible manufacturing systems (CIM and FMS), Supply chain and logistical management, Data-Processing Centre (now office automation) and starting a 2-year MBA programme.

He has been the Deputy Director of IIT Kanpur for the two consecutive terms (2002-08).

@R@MS

Volume-2 Issue-1

January 2010-June 2010

Biographical Note of the Luminary in an Area of IS

Global Journal of Enterprise Information System

Blockchain Federation of India [BFI]

Blockchain Federation of India is the primary and principal body of blockchain professionals in India. It was founded on 13th March 2019 by a few academician and Cyber professionals including its co-founders Col. Inderjit Singh Barara and Dr. Subodh Kesharwani which has now grown to be the national body representing blockchain professionals on a PAN India basis, in fact informally through social networking cites group exists from 2017 onwards. BFI is a non-profit professional meet to exchange views and information learns and share ideas. The wide spectrum of members is committed to the advancement of theory and practice of Blockchain and Technology Systems, Science and Engineering, Information Processing and related Arts and Sciences. The Federation also encourages and assists professionals to preserve truthfulness and aptitude of the profession and fosters a sagacity of partnership amongst members. Besides formulating the activities held at the chapters and student branches, the society will also conducts periodic conferences, seminars. The society will be in touch with various International bodies of blockchain for an international alliance.

BYLAWS OF BLOCKCHAIN FEDERATION OF INDIA

Blockchain Federation of India known for its acronym (BFI) is an Indian customized international organisation dedicated to raising digital competence standards in the workforce, education and society in blockchain perspectives. BFI have a certain vision and mission:

- To bring all block chain researcher and technocrats under one roof
- Formulation of Block chain Virtual university
- Developed Own Teaching Contents in Block chain

BLOCKCHAIN VIRTUAL UNIVERSITY

Blockchain Federation of India is an international organisation dedicated to raising digital competence standards in the workforce, education and society vis-à-vis blockchain. Our proposed certification programmes, delivered through an active network in multiple countries, enable individuals and organisations to assess, build and certify their competence in the use of blockchain tools to the globally recognized BFI standard, known as BFI worldwide. As a nonprofit social enterprise Blockchain Federation of India (BFI) benefits from the exclusive support of experts from national technical societies and partners international to enlarge vendor-independent standards which define the skills and knowledge required to use blockchain technology in actual fact. We work with education and training partners, local and regional authorities, national governments, international development organisations as well as public and private sector employers in all sectors, in the delivery of our programmes. The quality and reputation of BFI is built on years of expertise earned by it's founders and associated office bearers. Our accomplishment is maintained by our forthcoming innovation in certification programme development, our commitment to rigorous test design methodologies, and consistent adherence to our quality assurance standards. Blockchain Federation of India planning to support the initiatives of National Operators of the programme in various parts of world. All Blockchain Federation of India operations work closely with regional, national and local partners to develop the global network of BFI Accredited Test Centers.

BYLAWS OF THE BLOCKCHAIN FEDERATION OF INDIA

ARTICLE I. NAME

- The name of the Federation shall be the "Blockchain Federation of India", and it shall be incorporated as a nonprofit corporation in Republic of India with a Headquarter in New Delhi.

ARTICLE II. PURPOSE

- The purpose of the Federation shall be to promote Blockchain education through faculty development and to encourage that the teaching and learning \ related to blockchain implementation in various upcoming field.

ARTICLE III. RESTRICTIONS ON ACTIVITIES

- Section 1. No part of the earnings of the Federation shall inure to its members, officers, or other private persons, except that the Federation shall be authorized and empowered to pay reasonable compensation for services rendered in direct support of its purpose.
- Section 2. No part of the activities of the Federation shall be directed towards influencing legislation or intervening in political campaigns.

ARTICLE IV. MEMBERSHIP

- Section 1. The Board may establish and/or change the membership classes. The Board of Directors shall set the dues amount and the criteria for each class of membership.
- Section 2. All individuals who are members in good standing shall have the right to vote, hold office, and serve on committees. To be in good standing, a member must not be more than six months in arrears in his/her dues and financial obligations to the Federation. Individuals more than six months in arrears in their dues will be declared inactive, but retained on the membership rolls for an additional six months. Inactive members can reinstate their good standing by payment of current and all past dues.
- Section 3. Individuals whose dues are more than one year in arrears shall be dropped from the membership rolls.

ARTICLE V. OFFICERS

- Section 1. The Officers of the Federation shall be the President, President-Elect, Secretary, Treasurer, and the Immediate Past-President. The election procedure is as described in Article VII.
- Section 2. President & Secretary. The President and Secretary of BFI is the highest ranking officer of the Federation and are directly accountable to the membership and the Board. The President leads the Board of Directors as a chairperson and Secretary will be the Convener in development of the strategic goals and objectives of the organization and provides direction and leadership. The President serves as the Chair of the Board of Directors, Executive Committee and Annual General Meetings. A detailed position description, approved by the Board, shall be maintained on the Federation's website.
- Section 3. Immediate Past-President. In those years when a new President is elected, the current President assumes the office of Immediate Past-President. The Immediate Past-President remains in office until a new Immediate Past-President assumes the office. A vacancy in the office of Immediate Past-President cannot be filled by appointment. A detailed position description, approved by the Board, shall be maintained on the Federation's website.
- Section 4. President-Elect. The President-Elect is the third highest ranking officer of the Federation and shall support the President and secretary to advance the work of the Federation. At the end of the term, the President-Elect shall assume the office as President of the Federation. In the event that the President is temporarily unable to fulfill her/his duties to the Federation, the President-Elect may be appointed Acting President by the Board of Directors. If the President resigns or is unable to fulfill their duties for an extended period, the President-Elect shall become the President and a new President-Elect shall be elected by a majority vote in a special election of the Board of Directs within 30 days. A detailed position description, approved by the Board, shall be maintained on the Federation's website.
- Section 5. Secretary: The Secretary oversees the recording of proceedings of meetings of the Federation and the Board of Directors, and is responsible for the Federation's correspondence. A detailed position description, approved by the Board, shall be maintained on the Federation's website.
- Section 6. Treasurer: The Treasurer oversees the financial records of the Federation according to standard accounting practices, and, whether performed personally or through the Federation's administrative office, is responsible for safeguarding the Federation's funds. The Treasurer presents periodic reports on the financial status of the Federation to the Board of Directors and a full report to the membership at the Annual Federation Meeting. A detailed position description, approved by the Board, shall be maintained on the Federation's website.

ARTICLE VI. BOARD OF DIRECTORS

- Section 1. The Board of Directors shall be the principal governing body of the Federation. The Board of Directors shall consist of eleven (11) Directors plus four (4) Officers plus the Immediate Past-President,

if the Immediate Past-President is not an elected Director. When the Immediate Past-President is not an elected Director, the Immediate Past-President would be an ex-officio member of the Board of Directors and the Executive Committee until a new Immediate past President assumes the office. In that capacity, the Immediate Past-President has a vote only to prevent a tie (so when an even number of Directors and/or Officers is present).

- Section 2. Directors shall be elected for a three (3) year term. The terms shall be staggered and at least three (3) seats will be elected annually. Directors may not be elected to serve consecutive terms but may be reelected after an absence of one year. The election procedure for Directors is described in Article VII.
- Section 3. The Board shall meet quarterly, or more often if the need arises, at the call of the President or at least three members of the Board. Board meetings may be held in person, by teleconference, or other electronic means. A proposed agenda and supporting materials shall be made available to Board members prior to a Board meeting.
- Section 4. A quorum shall consist of one more than half the current number of Board members and must include at least two members of the Executive Committee.
- Section 5. In the event a vacancy occurs on the Board in a Director position, the President shall, with the approval of the Board, appoint a member to fill the vacancy. These appointed members shall serve out the term of the individuals they replace on the Board. The new Director shall complete the term of the former Director and shall be eligible for reelection if the remaining term is less than two years. Individuals joining the Board of Directors by appointment as a Director shall not serve more than three consecutive years in that office as a Director in addition to the partial term they served as replacement. In the event a vacancy occurs in an Officer position, the Board will immediately elect a new officer to that position in accordance with Article VII. The elected member takes office immediately, shall serve out the term of the individual she or he replaces as an Officer and will still be eligible for one complete term (of two years) in that same Officer position in addition to the partial term she or he served as a replacement.
- Section 6. With the approval of the Executive Committee, the President may recommend that any Board member be removed from office by the following procedure: 1) reasons for the proposed action must be provided in writing to the member, 2) the member shall have 60 days in which to represent themselves at a meeting of the Board, 3) a two-thirds vote of the current number of Board members shall then decide.

ARTICLE VII. NOMINATIONS AND ELECTIONS

- Section 1. Nominations. The Nominating Committee shall on or before January 25th submit to the Federation Manager a list of candidates for each position subject to election in that year. The names of these individuals, and other such supportive materials as deemed appropriate by the Nominating Committee, shall be posted to the Federation's website on or before February 1. The Federation's administrative office shall mail or fax a copy of these materials to those BFI members who have previously indicated they do not have Internet access. Between February 1 and February 15, members may petition for additional candidates to be added to the ballot. Such nomination petitions may consist of either a single document or separate letters. To be nominated by petition, each candidate must have the support of at least 15 BFI members in good standing. All petitions and letters must be addressed to and received by the Federation Manager on or before midnight (IST) of February 15.
- Section 2. Elections. On March 1, a secured, electronic ballot shall be activated on the Federation's website, along with instructions for electronic voting. All ballots must be electronically submitted to the website on or before midnight (IST) March 15 to be counted. Results shall be posted to the Federation's website by April 1. A plurality of the votes cast is needed for election. In the event of a tie, the election shall be decided prior to April 1 by a majority vote of the current number of Board members.
- Section 3. Newly elected Directors will assume their office at the conclusion of the Federation's annual meeting.
- Section 4. The Officers (of the Federation President, President-Elect, Secretary and Treasurer) shall be elected by a majority vote of the Board of Directors by electronic vote before December 15th, and assume their duties on January 1st. If the elected Officer is a current Director, the newly elected Officer must resign as a Director before assuming the role as an Officer. Officers serve a two-year term of office, and may not serve consecutive terms. However, they may be reelected to the same office after an absence of one year. An Officer may be elected to a different position on the Executive Committee immediately following his/her current term. There is no limit on the number of times an individual may serve as an Officer. The President-Elect, Treasure, and Secretary shall be elected by the Board of Directors as described in Section 5 below. Officers may be removed by a two-thirds vote of the entire membership of the Board of Directors.
- Section 5. Nominations for Officers. In the year the Officers are to be elected, a special Officer Nominating Committee will be formed, composed of the Immediate Past-President, President-Elect, two members from the BFI Nominating Committee (elected by the Nomination Committee) and one current Director

(elected by the Board of Directors). No committee member can be a concurrent candidate for an Officer position. The special Officer Nominating Committee shall on or before November 1st submit to the Federation Manager a list of candidates for each Officer position. Candidates must be BFI members in good standing. The names of these individuals, and other such supportive materials as deemed appropriate by the Nominating Committee, shall be posted to the password protected Board website on or before November 7th.

- Section 6. If a conflict arises concerning elections of Directors or Officers, the current Chair of the BFI Nominating Committee and 2 recent Past Presidents will be appointed to resolve any conflicts.

ARTICLE VIII. STANDING COMMITTEES

- Section 1. Membership and Term of Service. Standing Committees are defined in these Bylaws of BFI and can only be removed or redefined by majority vote of the membership. Other committees may be created by the Board to serve specific duties important to the organization
  - Chairs of Standing Committees, except the Executive Committee, are nominated by the President and approved by the Board. They serve three-year terms until the close of the next Annual Business Meeting and may be reappointed.
  - Members of Standing Committees, except the Executive Committee, the Professional Development Committee and the Nominating Committee, are appointed by the committee Chair, who will notify the Board of all committee membership changes. All appointed members shall serve one-year terms until the close of the next Annual Business Meeting and may be reappointed.
- Section 2. Executive Committee. The Executive Committee, which consists of the Officers, shall make decisions and take actions on behalf of the Board in between Board meetings. The President shall call meetings of the Executive Committee.
- Section 3. Nominating Committee. The Nominating Committee shall be responsible for determining a suitable group of candidates for election to the Board of Directors. It shall consist of five members who are neither current members of the Board nor current Committee Chairs. They may not be current candidates for the BFI Board. The President shall appoint a Chair plus two members with the approval of the Board of Directors. Two members shall be nominated and elected by the membership at the Annual General Meeting.
- Section 4. Professional Development Committee. The Professional Development Committee shall be responsible for recommending the overall scientific and educational programs of the Federation to the Board. Membership will include the current BFI President, President-Elect and Chairs of the Publications Committee and of other Committees with missions relevant to professional development activities, as determined by the Board.
- Section 5. Publications Committee. The Publications Committee shall be responsible for oversight and management of all publications of the Federation. They will work in concert with the Editorial Board of the Federation's journal.
- Section 6. Membership Committee. The Membership Committee shall be responsible for evaluating the needs of the membership and recommending appropriate ways to meet those needs. The committee will develop methods and programs for active membership recruitment and retention.
- Section 7. Finance and Organizational Development Committee. The Finance and Organizational Development Committee shall assist the Treasurer, who shall serve as Committee Chair, in maintaining the financial health of the Federation, including preparation of the annual budget. It will also be responsible for pursuing appropriate federal, foundation, corporate, and private funding to support the work of the Federation. The Committee shall be chaired by the Treasurer.

ARTICLE IX. MEMBERSHIP MEETINGS

- Section 1. Annual General Meeting Time, Place, and Purpose. The Annual General Meeting of the Federation shall be held at such time and place as may be selected by the Board of Directors and stated in the Notice of Meeting. The Annual General Meeting shall include the transaction of such other business as may properly be brought before the membership.
- Section 2. Notice of Meetings. The Federation Manager shall give notice of all Federation meetings stating the place, day, and hour of the meeting and, in case of a Special Meeting, the purpose for which the meeting is called. Such notice of special meetings shall be not less than ten or more than fifty days before the date of the meeting. Notice of the Annual General Meeting is to be given no later than the prior Annual General Meeting.
- Section 3. Quorum. A quorum for transaction of business shall be not less than 10% of the total membership in good standing.
- Section 4. Voting and Representation. Each member who is present shall be entitled to one vote at all BFI meetings. A membership roll showing the list of members as of the record date, certified by BFI's Secretary, shall be produced at any meeting of the members upon request. All persons appearing on such membership roll shall be entitled to vote.

ARTICLE X. AMENDMENTS

- Section 1. Amendments of the bylaws may be proposed by a majority of the Board of Directors or by a petition, sent to the Secretary, bearing the signatures of at least 15 members in good standing.
- Section 2. Notice of proposed amendments, shall be posted to the Federation's website on or before March 1. The Federation's administrative office shall mail or fax a copy of these materials and the slate of nominees, described in Article VII, Section 1, to those BFI members who have previously indicated they do not have Internet access. On April 1, a secured, electronic ballot shall be activated on the Federation's website, along with instructions for electronic voting. The Federation's administrative office will mail or fax a ballot containing the proposed changes and the slate of candidates, described in Article VII, Section 2, to those BFI members who have previously indicated they do not have Internet access. All ballots must be electronically submitted to the website or received in the post by the Secretary on or before midnight (IST) of April 30 to be counted. The Secretary shall tally the votes and send the results to the Federation Manager for posting on the Federation's website by May 15.
- Section 3. In the event of an urgent requirement for an amendment, the Board of Directors, by a two-thirds vote, may authorize posting a proposed amendment to the members at any time. Notice of proposed amendments shall be posted on the Federation website for a 30-day period prior to balloting. At the end of the posting period, a secured electronic ballot shall be activated on the Federation's website, along with instructions for electronic voting. The Federation's administrative office shall mail or fax appropriate information and a ballot to those BFI members who have previously indicated they do not have Internet access. All ballots must be electronically submitted to the website or received in the post by the Secretary within 30 days of the opening of balloting. The Secretary shall tally the votes and send the results to the Federation Manager for posting on the Federation's website.
- Section 4. All amendments of the bylaws require an affirmative vote of two-thirds of the members in good standing who submit valid ballots.

ARTICLE XI. INDEMNIFICATION

The Federation shall defend and indemnify any qualified person against any threatened, pending, or completed legal action resulting from actions taken in good faith on behalf of the Federation. Qualified persons shall be present and former officers, employees, and officially elected or appointed members of boards, councils, committees, and other components of the Federation.

Indemnification will not be provided to any person who shall be adjudged in a legal action to be liable for negligence or willful misconduct in the performance of duty, or when such person did not reasonably believe that the action was within the law and in the best interests of the Federation.

Indemnification shall cover cost of defense and any judgments, fines, and amounts paid in settlement actually and reasonably incurred by a qualified person, up to a limit of one-million dollars in any single case except in circumstances expressly prohibiting such limitation under the law. Such indemnification shall be in accordance with the established policy of the Federation.

ARTICLE XII. OTHER PROVISIONS

- Section 1. The fiscal year of the Federation shall be on a calendar year basis (1st April to 31st March).
- Section 2. The Federation shall be governed Income tax rules of Order, as currently revised. In case of a conflict between Rules of Order and these bylaws, the bylaws shall take precedence.

ARTICLE XIII. DISSOLUTION OF THE FEDERATION

In the event of the dissolution of the Federation, the Board shall give all its assets to one or more nonprofit, tax-exempt organizations. If the Board cannot decide, the decision shall be made by the applicable Court in the Union territory of Delhi, India

ARTICLE XIII: MODE OF OPERATION & SIGNING AUTHORITY

Founder President and Secretary will be the whole time signing authority and operates banking transaction physically & virtually jointly

Col. Inderjit Singh Barara
President

Dr. Subodh Kesharwani
Secretary

Scholastic Seed Inc.
e-Publishing Aggregator & Periodical Mentor

SUBSCRIPTION FORM

Blockchain Federation of India

Mr ☐ Mrs ☐

Last Name: .....

First Name: .....

University/Organization/Company: .....

.....

Address:.....

.....

E-mail: ..... **Telephone:** (__).....

Complete Invoice Address (i.e your University/Organization/Company):

.....

.....

.....

Subscription Fees

Country	Indian Membership			Corporate Membership		
Year	One Year	Two Year	Three Year	One Year	Two Year	Three Year
National	₹ 1800	₹ 4000	₹ 6000	₹ 50,000	₹ 1,00,000	₹ 2,00,000
International	$120	$ 200	$300	$1000	$ 1500	$2000
Membership years run 1st January to 31st December of every year						

Please check appropriate registration fee for BFI:

- Student BFI Member ☐
- Student Non BFI Member (includes 1 year membership) ☐
- Senior/Industry BFI Member ☐
- Senior/Industry non BFI Member (includes 1 year membership) ☐

PAYMENT METHOD

Payments should be made by bank transfer at:

Bank Name	:	IDFC Bank
Bank Account No.	:	10020469746
Payment Favouring	:	Scholastic Seed Inc.
IFSC Code	:	020102
MICR Code	:	110751003
Account Branch	:	New Friends Colony (NFC)

For inquiries, please contact Scholastic Seed Inc.

COPYRIGHT TRANSFER FORM

(Please Compile This Form, Sign and Send By E-mail)

Global Journal of Enterprise Information System
Scholastic.seed@gmail.com
Editor-in-Chief : Dr. Subodh Kesharwani
Online ISSN : 0975-1432 | Print ISSN : 0975-153X
Frequency : Quarterly | Published since : 2009
Publisher(s) : KARAM Society & Scholastic Seed Inc.

Please complete and sign this form and send it back to us with the final version of your manuscript. It is required to obtain a written confirmation from authors in order to acquire copyrights for papers published by GJEIS a quarterly international periodical.

Full Name and Surname			
Title	Dr./ Mr./ Ms./		
Organisation			
Address			
Postal code		City	
Country			
Mobile with Country code			
Fax /landline			
E-mail			
Paper Volume, Issue & Year	Volume-11, Issue-2, July-Sep, 2019		
Paper Title			
Authors			
Paper Pages			

Copyright Transfer Statement

The copyright to this article is transferred to GJEIS an international periodical and its Publisher Scholastic Seed Inc. & KARAM Society if and when the article is accepted for publication. The undersigned hereby transfers any and all rights in and to the paper including without limitation all copyrights to GJEIS. The undersigned hereby represents and warrants that the paper is original and that he/she is the author of the paper, except for material that is clearly identified as to its original source, with permission notices from the copyright owners where required. The undersigned represents that he/she has the power and authority to make and execute this assignment.

We declare that: This paper has not been published in the same form elsewhere.

1. It will not be submitted anywhere else for publication prior to acceptance/rejection by this periodical.
2. A copyright permission is obtained for materials published elsewhere and which require this permission for reproduction.

Furthermore, I/We hereby transfer the unlimited rights of publication of the above mentioned paper in whole to GJEIS. The copyright transfer covers the exclusive right to reproduce and distribute the article, including reprints, translations, photographic reproductions, microform, electronic form (offline, online) or any other reproductions of similar nature.

The corresponding author signs for and accepts responsibility for releasing this material on behalf of any and all co-authors. This agreement is to be signed by at least one of the authors who have obtained the assent of the co-author(s) where applicable. After submission of this agreement signed by the corresponding author, changes of authorship or in the order of the authors listed will not be accepted.

Yours Sincerely,

Date: …… Place: ……

Corresponding Author's Full Name …….... Signature……

Co-Author's Full Name……..... Signature……

Co-Author's Full Name……..... Signature……

WE JUST WANT TO SAY... THANK YOU!

10 Incredible Years of GJEIS 2009-2019

To,

Prospective Contributors & Researchers
Global Journal of Enterprise Information System
Peer Reviewed/Refereed/ Quarterly

Dear Mam/Sir,

2019 is really a benchmark for the GJEIS Journal as it had completed the ten year service of serving the researcher and facilitates learning by and large in totality. GJEIS published four times annually (January, April, July, and October). Accordingly, 40 issues have been published in the first 10 years. GJEIS is a methodological journal that focuses on articles about mixed methods research across the Enterprise, Information & System. GJEIS is also an international and multidisciplinary journal that publishes manuscripts in two various categories: methodological/ theoretical papers and original empirical studies. Although there are other methodological journals that publish mixed methods studies, GJEIS focuses exclusively on mixed methods research and solicitants different types of article in GJEIS Journal which mainly focuses on research issues in the EIS and IT related areas.

1.	Empirical Research Papers (ERP) report on completed EIS research that complies with rigorous scientific standards. ERP present original results of completed research studies with the aim of obtaining feedback from fellow researchers. [Limit 16 Pages]
2.	Theme Based Papers (TBP) are short papers that present the design and preliminary results of ongoing EIS research studies with an endeavor of obtaining early feedback and further guidance from experts and peers. TBP will be evaluated using the same academic standards as regular research papers (except for completeness requirements). [Limit 12 Pages]
3.	Case Study Based Papers (CSBP) describes real-life experiences with EIS that authors wish to share with fellow practitioners and EIS researchers. They focus on problems and solutions in specific contexts. Their aim may be to help other practitioners facing similar problems or to solicit help and possible solutions from other practitioners (or EIS researchers). [Limit 10 Pages]
4.	Review of Literature (RoL) aim is to review of the suitable "literature" (books, journals, magazines, URLs, Videos) discussing the topic one want to investigate. It discusses modus operandi and mechanism that are apposite for investigating the subject matter just a simple summary of the sources, but it usually has an organizational pattern and combines both summary and synthesis with intent to explore gap. Objective behind creating this type of phenomenon in GJEIS is to give grassroots researcher a roof to synthesize and weigh up the guiding notion of research questions. [Limit 8 Pages]
5.	View Point (VP) is a situation for which something is pragmatic or considered as a point of view. The purpose of VP is to share different views about the IT related products and what individual think about that. [Limit 6 Pages]
6.	Research Thought (RT) can refer to the opinion or arrangement of research ideas that effect from thinking, the act of producing thoughts on diverse interdisciplinary collaborative research areas or tools with which researcher can formulate it's research paper, choose a method for undertaking a study, write up for findings and discuss the outcomes in a discussion section. In this head author can throw a light on various research tools which can be helpful in formulating a research paper. [Limit 5 Pages]

7. Student Research Initiatives (SRI) is a research initiative by a grass-root researcher and technocrats. This head facilitate students/learners to pursue independent academic and imaginative effort and engage in research under the supervision of a faculty mentor with an intention to heighten student research as a means of collaborative learning, critical thinking and the establishment of knowledge. [Limit 12 Pages]

8. Dissertation Snapshot (DS) is an excerpt from a researcher's own thesis or dissertation which had been previously published or submitted in the form of research project or its own doctoral work. The rationale is to raise the curtain on an application and thought used by researcher in a brief manner with an intention to promote the future researchers to sequel their thoughts. [Limit 10 Pages]

9. Questionnaire Format (QF) A new philosophy called "Questionnaire Format" had been introduced, in which we are going to publish distinguish questionnaires that navigates the usefulness of it in building research and how to communicate with the respondents. The rationale behind introducing this QF is to give a glimpse about the structure and the pedagogy. QF on the other hand provides a niche to grass-root researcher about their various thoughts related to preliminary research and facilitates them in linking with a respective research papers which the researcher had visualize or going to plan in a coming future. This is a new inventiveness under the GJEIS Academic Social Responsibility (GASR) and would be complimentary/charitable in nature. [Limit 5 Pages]

10. Book Review (BR) is a literary criticism in which a book is analyzed based on content, style, and merit. BR can be a primary source opinion piece, summary review or scholarly review. Books can be reviewed for printed periodicals, magazines and newspapers, as school work, or for book websites on the internet. A book review's length may vary from a single paragraph to a substantial essay. Such a BR may evaluate the book on the basis of personal taste. Reviewers may use the occasion of a book review for a display of learning or to promulgate their own ideas on the topic of a fiction or non-fiction work. [Limit 3 Pages]

11. Biographical Note of the Luminary in an Area of IS We as per our culture acknowledge in every issue a great leader, Entrepreneur, Technocrats, Academician etc., who contribute a lot to a society in an area of IS. [Limit 2 Pages]

12. Great Enterprise Contribution to Society in Information System Perspectives deals with those enterprises contributing a lot to the society, and considering themselves a wizard in the field of Information System, we publish their profile, with the intention that their creation/contribution would be viewed and duly appreciated by the corporate and academics, all-around the globe. The purpose behind this is to broadcast the most visually powerful, immersive and engaging rich media applications on the Web. [Limit 2 Pages]

13. Award is something given to a person or a group of people to identify their fineness in a definite field especially in an area of EIS, it is rather a certificate of excellence for their contribution in academia or in a corporate world. This start throws a light on an entity or a gamut of researcher who had been honored for their extra ordinary input. [Limit 2 Pages]

14. Homage means great respect and tribute, or something done to honor a person. We in GJEIS pay homage to our ancestor's and say prayers in admiration to their memory which includes academicians, technocrats and great thinkers. The special respect would be shown publicly by sharing their achievements and contributions in writing which includes images, excerpts, testimonials, write-up, etc. [Limit 2 Pages]

Scholastic Seed Inc.
e-Publishing Aggregator & Periodical Mentor

Scholastic Seed Inc.
e-Publishing Aggregator & Periodical Mentor

About New Submission Policy (NSP) 2019

The NSP-2019 consists of following features:

1. Paper will be strictly submitted online at : **www. gjeis.com**
2. Priority would be given to pure empirical article which revolves around first hand information and backed merely by primary data collection will be accepted promptly as these article uses data based on actual observation or experimentation during formulation.
3. It is mandatory for Indian authors to submit research article along with a foreign co-author as a first author or corresponding authors due to journal global in nature characteristics and its wide international presence and listing in various directories across the globe. The submission by the foreign authors will fulfill the global mandate of journal and facilitate in listing and enhanced impact factor in future course of action. Though the journal have been listed in various directories and had a good impact factor but we expect in 2019 to be listed in few leading indexing.
4. There will be a waiting time of minimum **12 months** from the date of submission i.e. April 2019, as paper require rigorous review by **3 internal reviews** from India and **3 blind reviews from outside India** based on the subject expertise and themes.
5. From April 2019 we are putting a Reviewer comment in a Paper under Category Called: Anonymous Reviewer-1, Anonymous Reviewer-2, and Anonymous Reviewer-3. Though tracking record from Submission to online first would depict with various dates in a paper. Visit sample article and reference style. Journal also publishes a similarity index detail of ithenticate plagiarism report at the end of an article.

Paper Code (DOI): $$$$$ **Originality Test Ratio:** @@%**; Submission Online:** DD-MM-YYYY**; Manuscript Acknowledged:** DD-MM-YYYY**; Originality Check (ithenticate):** DD-MM-YYYY**; Peer Reviewers Comment:** DD-MM-YYYY**; Double Blind Reviewers Remark:** DD-MM-YYYY**; Author Revert:** DD-MM-YYYY**; Camera-Ready-Copy:** DD-MM-YYYY**; Editorial Board Citation:** DD-MM-YYYY**; Published Online First:** DD-MM-YYYY

---

6. Corporate/Institution who take the GJEIS annual subscription will get a 4 complimentary publication in a year of their employees and faculty
7. Certificates for Article Publication and Reviewers effort would be endorsed and acknowledged with a separate certificate and exclusively send by the Research & Academic Management Society and Scholastic Seed Inc.
8. Form will be submitted with a new link using Google form link available on a GJEIS portal.
9. One indicator of GJEIS's kudos is the impact factor of 2.219 which is coming up gradually due to peer review procedure followed by journal. GJEIS an inaugural impact factor of 2.219. Regarding the topics examined in these editorials, the reflections are about diverse issues: research questions, perspectives, training, data analysis, paradigms, integration, and challenges for mixed methods research, among others. Moreover, some editorials examine the same topic. Thank you for the ten noteworthy years of tenderness, acquaintance, and hold up. We enormously couldn't have made it without you, nor can we catch the next steps without your backing. I hope you'll keep holding us to high standards, and telling us when we've congregates your expectations and when we've let you alongside.
10. Fast Track Publication (FTP) will be enabled for Indian Author with a complimentary subscription of one year either by the Research Institute. Reviewers and other compliance will be managed by the editorial office on a priority basis and paper published in a same quarter if fulfill the eligibility and able to adapt suggestion by a blind reviewers.
11. FTP consist of a features like "Online First" in which article published in a fast track basis and uploaded online without the Volume and Issue date and automatically transfer to the routine forthcoming issue. www. gjeis.com

Subodh K. Kesharwani

Editor-In-Chief
Notified Tenure 2018-2020

Fast track journals are crucial for research articles that are amazingly noteworthy and necessitate essential propagation, or where there is a funding policy raison d'être for urgent publication. Fast-track peer review prioritizes a manuscript and decreases its publication time. GJEIS offers this opportunity by fast tracking as just speedy review and quick publishing. When a paper is marked for fast track during submission line www.gjeis.com it is recurrently reviewed and a publication decision is made swiftly. Fast tracking might also shrink the amount of time allocated for peer review and editing as it will parallel send to blind and peer reviewer and constantly dedicated publishing team would be allocated simultaneously. It typically cuts the overall publication time by at least one-third.

GJEIS have developed fast-track peer review options to restrain some of the needless instance that lapses between a manuscript being submitted and its periodical. GJEIS Fast Track Publication service which better known as FTBS is an **"optional service"** which provides author a platform to publish their papers in **just 9 weeks**, usually a journey time from submission to publication takes 12 Months. The purpose of creating **FTPS** is to facilitate the author in publication of their paper in a prescribe time frame and do all the process in a fast track mode without compromising with quality. There are certain prerequisites which are mandatory to include under FTPS:

- ✓ Article should be Plagiarism Free and pass the Originality Test by http://www.ithenticate.com (Prevention Plagiarism tool) with similarity test index below (10%)
- ✓ Expedited review will be offered, on request, for submitted research articles after the editorial board consist of 5 members approved.

GJEIS has started a non-compulsory speedy examination for fast-track publications to draw attention to noteworthy developments in the various fields of the academic research without compromise with superiority. GJEIS goal is to endow with the research group of people with rapid and on the spot entrée to freshly completed research works in a variety of research vicinity that are speedily developing with great impending impact. The research community as a whole advantageous from the realism that primary edge research is made reachable to a extensive audience more punctually. Kindly note that we acknowledge a limited number of the article under fast track in one quarter due to it's frequency and further email journal's primary contact for the inquiry. After receiving express review request for the article, we will tell to our contributor in a week time whether we can offer rapid review for the submission or not. If we decide not to we may offer to think about your paper either in the normal mode or provide you date from when we can consider it under rapid review.

FASTTRACK Publication Service

There are certain amount attracted by the author if they avail this FTPS service, which is not pre-decided but based on the article creditability and its testimonial, nonetheless it takes into contemplation the following cost levied:

1. Fast track Plagiarism check Cost
2. Suggest method to rectified plagiarism and facilitating the same
3. Facilitate in reviewing the article by the in-house team of experts and 6 subject expert reviewer (3 India & 3 Abroad)
4. Research Orientation by the subject expert and help in connecting and navigating
5. Subscription Cost of a Journal both Print & Online
6. Given the number of high quality submissions and the associated production costs, we are only able to grant a limited number of FTPS waivers and discounts, with priority given to some first generation students residents.

Waiver from Cost Occurred under FTPS

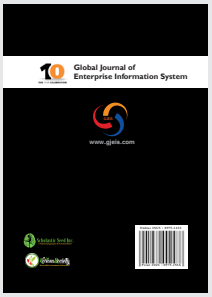
- If the Editorial Board thinks that the submitted articles are exceptional in nature and sound good amount of research then to facilitate and acknowledge the author, editorial board automatic initiate waiver partially or fully by exempting fees levied under FTPS. Thus these academic responsibility initiatives would facilitate in safeguarding the author in newly developed concept.
- Article having Zero% Plagiarism checked by iThenticate a plagiarism detection service with a research orientation automatically comes under waiver list and published within 9 Weeks from the date of Submission or generation of DOI from Crossref USA www.gjeis.com

Note

This facility is an optional service, hence the price quote would be based on article-to-article and would be intimated by the editorial office depend on the submission and subject to aforementioned points under waiver list

Disclaimer

GJEIS is a Peer Review restricted access subscription base Research Journal started in a year 2009 and does not charged any fees or Article Processing Charges(APC) from the author during or after publication. Fast Track Publication service (FTPS) is an optional service which had been originated to facilitate the submitter to reduce the time-frame and helping in strengthen their rights.



Scholastic Seed Inc. is in the e-publishing business from last one decade. The first creation the group had originated was the Peer Review Research Journal founded in the year 2009 known as Global Journal of Enterprise Information system (GJEIS). At the later stage group has come up with a sequel in the form of a medical journal in collaboration with it academic and research consortium NGO, KARAM Society & MEDANTA Hospital doctors in a name of AGEMS (Annals of Geriatric Education and Medical Sciences). The consortium currently having contemporary out-of-box approach and are now well acknowledge as an e-publishing aggregator and periodical mentor. The company till date had published few journals and facilitates/consulted lots of Brick-&-Mortar periodcials into a digital dynamic format. Till date we had consulted 20 periodical and entered into a book publishing business.

Journal Initiated under Scholastic Seed Ambit

GJEIS-2009
KARAM Society & Informatics Publishing Ltd.

AGEMS-2014
KARAM Society & Innovative Publications

SIRIFORT-2018
Sirifort Institute of Management Studies & KARAM Society

CYBERNOMICS-2018
Scholastic Seed Inc. & KARAM Society

E-GOVERNANCE-2018
Scholastic Seed Inc. & KARAM Society

Scholastic Seed helps to scholar in publishing Paper in an impact factor indexed journal

When a scientific paper, dissertation or thesis is published the author(s) have a duty to report who has contributed to the work. This recognition can take several forms such as authorship, relevant acknowledgments and by citing previous work. There is a growing industry where publication consultants will work with authors, research groups or even institutions to help get their work published, or help their dissertation/thesis. This help can range from proof reading, data collection, analysis (including statistics), helping with the literature review and identifying suitable journals/conferences.

- Plagiarism Check by (iThenticate, turnitin,Plag scan, Urkund)
- Language, Grammar Check, Punctuation Check, Writing Style Check, References Check
- Rearrangement, expansion, or summarizing of sections
- Ensuring logical flow between sentences and paragraphs
- Cross-checking appropriateness and presence of sections
- Content Accuracy & Enhancement, Logical Flow
- Specialized Subject-area Matching
- Formatting and Artwork Editing
- Enhanced Pre-submission Peer Review
- Journal Selection and Submission
- Review Correction and Re-Submission
- Confirmed Journal Publication

What will happen if you don't involved an aggregator and publishing mentor like scholastic seed?

- If you will involve your own intellectual capital in whom you're spending lucrative amount per month. The in-house team will not commit fully due to other obligation and teaching assignment. On the other hand Scholastic team facilitate in doing your job from underneath to pinnacle with the same cost and do some add-on like applying Algorithm and Citation, mentoring of in-house team in the same institution at later stage and make this e-publishing auto mode with a span of time.

How the Credit ability of an institute deteriorated without periodicals

- As we know that Institution creditability would be judged on the basis of the periodicals they published as these periodicals such as newsletters, journals, magazines, annual reports, etc are their front face and if these front face are digitally equipped it would be definitely a win-win stage for the students and the institutions and further by adding a feather in a cap.

Why there is a need of Online Periodicals

- Free access • Self-archiving • Repository • Author foot fall • Pre or post publication irrational fear Eradication

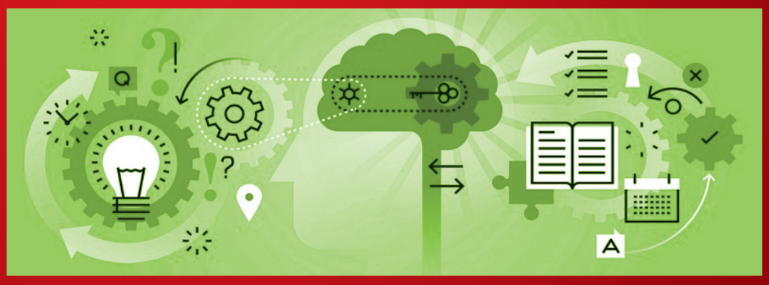
DO's AND DON'T

- Digital Publication is as good as print publication
- Always Prefer Open Source Journal and Digital Format as it circulate fast and perpetual in nature.
- Have a Digital Object Identifier (DOI)
- Have a good team of editorials and reviewers
- Google Scholar and Citation is an important ingredients for choosing a journal
- Scopus, ICI, WoS and UGC Listing is a parameter to select journal
- Always check the H-index of an author
- Know the Impact factor of journal before Publishing an article
- Check the Ethical issue and Privacy Policy of the journal
- Frequency and consistency would be an important ingredient to judge the creditability

- It is suggested to an editor not to publish anything without Originality check
- Don't Prefer Pay and Print Model

Services

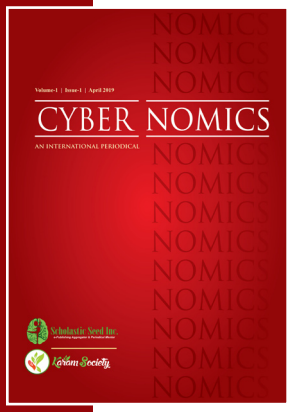
How Scholastic Seed Involved with institution in E-publishing and Journal making



- Website Creation includes coding in PHP and SQL Database Ready-to-Run Software with a Source code right transfer model.
- Sub-domain and hosting on a pro-rata basis (domain and hosting will be given to the respective institute with an ownership transfer)
- Digitalizing the Content Electronically and Uploading on Web (Frequency: Monthly, Quarterly, Bi-annually & Annually)
- Online tracking of articles submitted.
- Online manuscript submission.
- Updates about your manuscript delivered via e mail and SMS.
- Blind Peer-Reviewed Format and pedagogy to accomplish
- Facilitate in Papers abstract/indexed by all the major scientific indexing services.
- Aligned with various Impact Factor agency
- Converting Text into PDF and Final Camera Ready Shape(CRC)
- Call For Paper Arrangement of Article Plag Check, Interaction with Author, Proof Reading
- Other Indexing would be done by the society/ Scholastic Seed Inc. time-to-time, but other expenditure incurred would intimate and levied accordingly if charge by the agency on time-to-time basis.
- Process for Both eISSN and ISSN and Documentation
- Facilitate in Getting RNI No. From Registrar Of Newspapers For India

CYBER NOMICS

CYBERNOMICS is being published as a co-published peer-reviewed magazine by KARAM Society and Scholastic Seed Inc. The subjects covered by the magazine are IT linkages in business and management and others field related to cyber and its economics fields. It also covers many aspects in Information System and related areas which are burgeoning. The Magazine provides an international forum for the exchange of ideas, principles and processes concerning the application of diverse topics of Cyber to organizations, institutions and the world at large. CYBERNOMICS considers research submissions in several categories but revolves around Cyber threats, Security remedies, etc.



CYBERNOMICS magazine aims at achieving the growing demands for understanding and addressing issue pertaining to real-worlds Cyber-Attacks, Cyber Threats, Cyber threat Intelligence, Cyber Warfare, Cyber Terrorism, Darknet and Crypto Currencies and threats to information infrastructures critical to the national security of country.

The magazine publishes articles and reviews in the areas including, but not limited to:

- Cyber Threats
- Cyber Warfare
- Darknet and Darkweb
- Cryptography and its applications
- Network and critical infrastructure security
- Hardware security
- Software and System security
- Cybersecurity data analytics
- Data-driven security
- Adversarial Reasoning
- Malware Analysis
- Privacy-enhancing technologies and anonymity
- IoT Security
- Blockchain Security
- Cryptocurrencies
- Machine Learning
- Big Data Analytics
- Artificial Intelligence

Global Journal of Enterprise Information System

GJEIS Indexing till 2019

GJEIS in collaboration with Scholastic Seed Inc. and KARAM Society, publishes a new peer-reviewed open access e-journal in Enterprise Information System (EIS) areas of business which covers IT linkages in business, finance, marketing, management, organizational behaviour, buyer behaviour and other relevant fields. It also covers many aspects in Information System and related areas. The journal provides an international forum for the exchange of ideas,principles and processes concerning the application of diverse topics of EIS to organizations, institutions and the world at large. GJEIS considers research submissions in several categories but revolves around three buzzwords Enterprise Information and System Journal takes into consideration professional plagiarism detection and prevention technology for it's scholarly publication and research article in order to ensure the originality of written text before publication. The GJEIS receives submissions only through it's journal website www.gjeis.com. The journal has a very good impact factor and is listed and indexed in almost fifty directories and libraries all around the globe. GJEIS is also a scholarly publisher that uses services of Crosscheck offered by CrossRef, USA and facilitated by iThenticate software. The journal had implemented a Search Engine Optimization (SEO) and web analytics dedicatedly for it's online portal to provide glimpse about the articles having highest citation. GJEIS is also associated with International DOI Foundation (IDF) USA. GJEIS is also concomitant of Publsher International Linking Association, Inc (PILA) a not-for-profit membership organization. USA.

Scholastic Seed Inc.

www.gjeis.com

global Journal of ENTERPRISE INFORMATION SYSTEM

Certificate of Outstanding Contribution

awarded to

XXXXXXXXXXXXX

in recognition of the contributions made to the quality of the Magazine.

Publisher **Editor-in-Chief**

Scholastic Seed Inc.

www.gjeis.com

global Journal of ENTERPRISE INFORMATION SYSTEM

Certificate of Excellence in Reviewing

awarded to

XXXXXXXXXXXXX

in recognition of the contributions made to the quality of the Magazine.

Publisher **Editor-in-Chief**

Deep Learning Architectures is a class of Machine Learning Algorithms

11TH ANNIVERSARY

Global Journal of Enterprise Information System

GJEIS

www.gjeis.com

Online ISSN : 0975-1432

Print ISSN : 0975-153X

Scholastic Seed Inc.
e-Publishing Aggregator & Periodical Mentor

Karam Society
Since 2009 in Academic & Research