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

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

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,

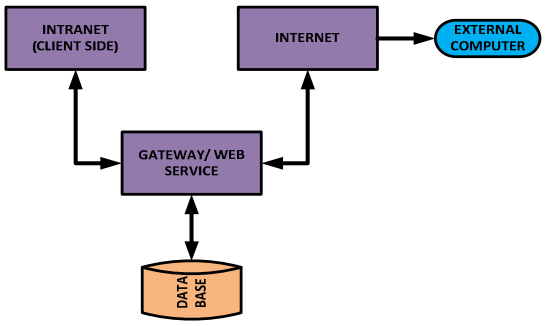

Figure 1: Basic Design of the System

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.

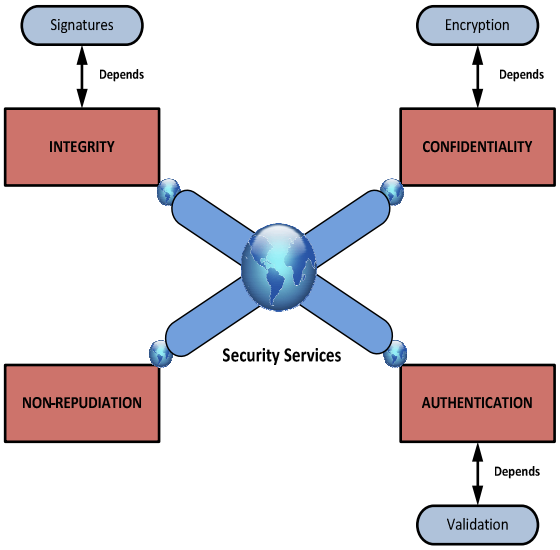

Figure 2: Security Factors

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.

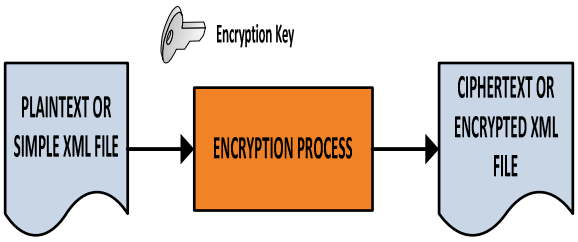

Figure 3: XML Encryption

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.

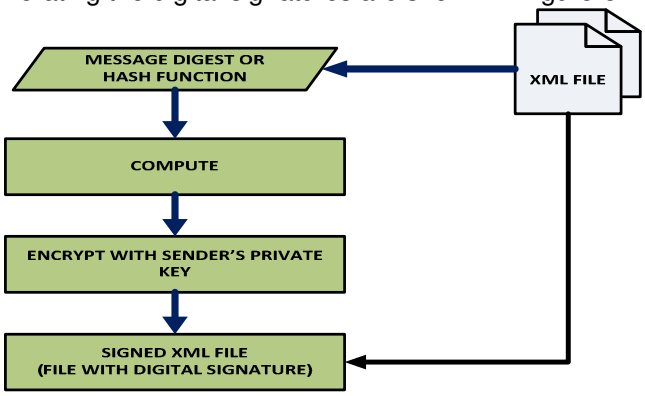

Figure 5: Steps for generating XML Signatures

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.

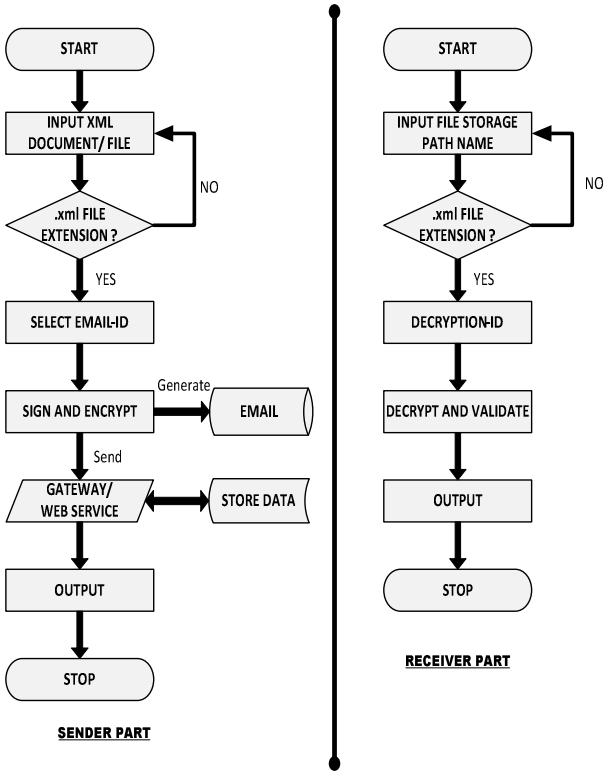

Figure 6: Flowchart of the System

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],

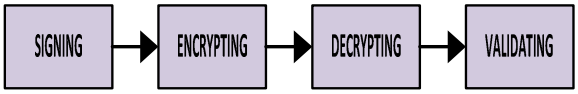

Figure 7: Steps for performing Security Services

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.

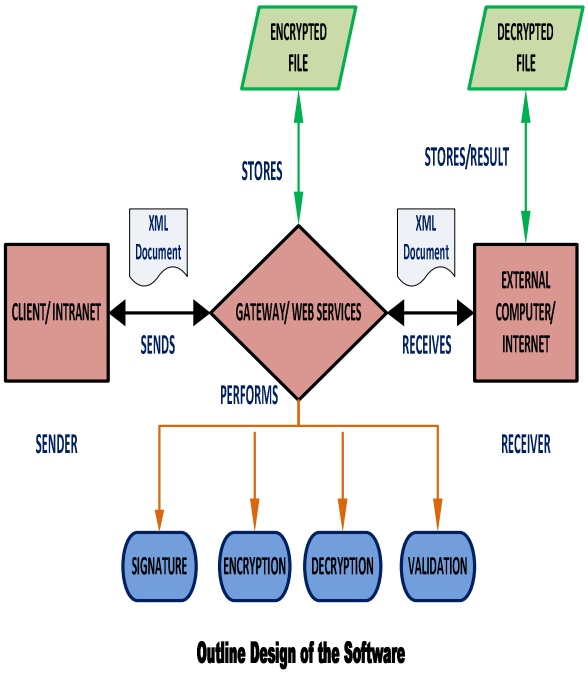

Figure 8: Outline Design of the Software

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