World Applied Sciences Journal 20 (7): 941-945, 2012
ISSN 1818-4952
© IDOSI Publications, 2012
DOI: 10.5829/idosi.wasj.2012.20.07.2186

Proposed Technique of XML Base Secured Data Encryption and Transmission Technology

[1]M.K.H. Chowdhury, [2]M. Samsuzzaman, [2]T. Islam and [3]B.M. Solaiman

[1]Department of CIT, Patuakhali Science and Technology University
[2]Institute of Space Science, Universiti Kebangsaan Malaysia
[3]Masters in Software Engineering of Distributed systems, KTH

Abstract: With the development of data transmission and Web Service technology, XML is widely used in all kinds of information transformation. So, Security in XML data transmission is very important, nowadays, in most of the sensitive issue like Bank transaction, online transaction, e-commerce, Diplomatic data etc. For secure XML Transaction, several methods are proposed. In this paper we have proposed the XML's security encryption based on the importance and sensitivity of data.

Key words: XML encryption · Web security · Sensitivity of data

INTRODUCTION

Nowadays XML has become the most reliable standard for data exchange between various systems because of its nature of using plain text to encode a hierarchical set of information document tags to allow the XML [1] document makes understandable without any special reader or interpreter. Its rapid development makes the data exchange more efficient. However, the current data exchange security mechanism special e-commerce has not effective and easy to implement security mechanisms, it is sometimes limiting the amount of transaction for limiting the security risks. Although HTTPS can be used as a method for secure data transmission, XML is important for web service. For this, Security is the main issue in the XML data transaction.

XML: XML with the markup standard is similar to the HTML language to describe web pages. It is well structured, easy to use and easy to read and write data in the application. It maintains the rules of XSD. XML needs to maintain the rules of XSD strictly. With well structured data structure makes the XML application in various fields: WEB applications, electronic commerce, embedded systems, bank transaction and so on. Data can be extracted from the XML for its use and further reuse. Being a common data format it can process the data in the various formats such as text, image and sound [2]. XML data, with facilities of scalability, flexibility, readability, platform independence cannot be compared with the traditional database and binary files, which makes preferable format for all data exchanges. The next-generation network technology will be based on XML technology.

XML Security Related Technologies

XML Security: XML encryption technology is used for data encryption. After the encryption process XML formatted data is generated then reassembled the XML format data, then this encrypted XML data is sent to the one or more receivers. The main goal of XML encryption is to use the XML file element and content which purpose is make sure the data confidentiality and integrity of data storage and exchange. In the XML encryption process whole XML document is encrypted.

XML Digital Signature: XML digital signature is used to identify users, ensure data integrity and non repudiation of XML data. XML digital signature maintains the rules which make the data more secure. Accurately describes digital signature and verification process, the process includes the key pair generation [3], document signing, document delivery and signature. So by the encryption XML data Structure isn't changed. XML digital signature ensures data authentication, data integration and non-repudiation.

Correspong Author: M.Samsuzzaman, Institute of Space Science, Universiti Kebangsaan Malaysia.

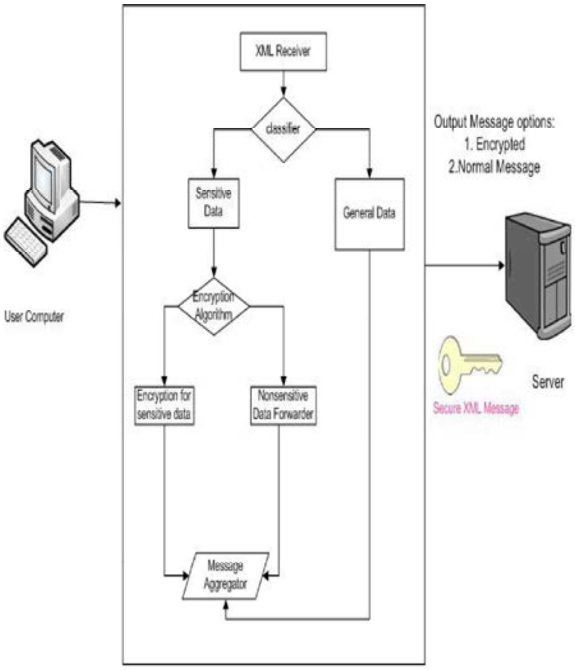


Fig. 1: System overall structure

Proposed XML Based Information Security System

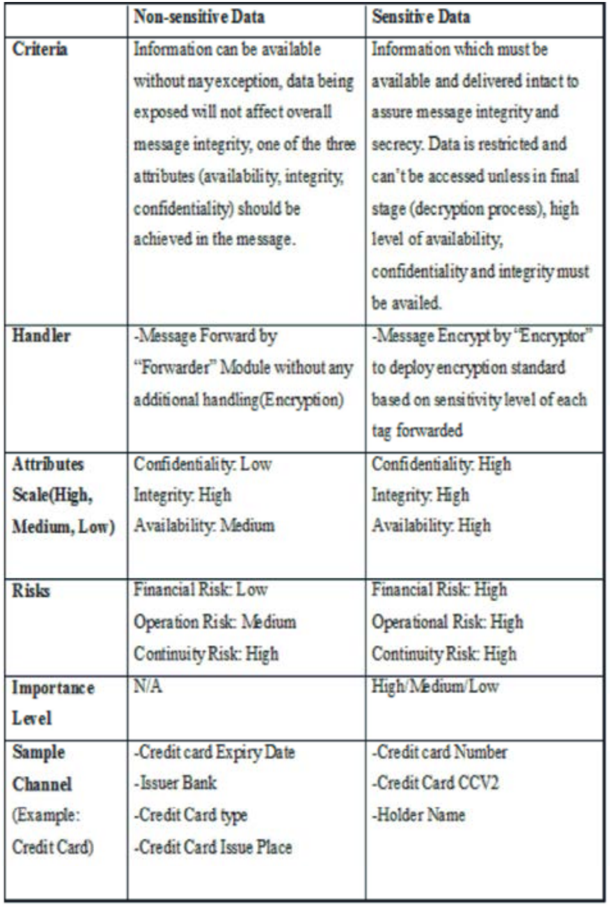
System Overall Structure: This system works using the following few steps:

- Receiving all the XML data from the user
- Divide the collected XML data based on their sensitivity
- Forward the data based on their sensitivity-
- If data are non sensitive, forward it without encryption
- Else use XML Data Conversion module based on their sensitivity.
- Aggregate the encrypted data
- Forward them to the server

The whole process is given in the figure 1:

Our study gives more emphasize on data sensitivity. User normally sends different types of documents, data. Some of them are normal, non-sensitive and some of them are sensitive depending on their business policy. If the data are non-sensitive, then it will forward without any encryption mechanism. For the sensitive data, the data are divided into two parts, namely, sensitive part and non-sensitive part. Sensitive part is encrypted by the cryptography mechanism and non sensitive part is forward without encryption. These data are aggregated in the aggregator. Then overall data interaction with the server.

Table 1: Data Classification based on sensitivity [4]



	Non-sensitive Data	Sensitive Data
Criteria	Information can be available without nayexception, data being exposed will not affect overall message integrity, one of the three attributes (availability, integrity, confidentiality) should be achieved in the message.	Information which must be available and delivered intact to assure message integrity and secrecy. Data is restricted and can't be accessed unless in final stage (decryption process), high level of availability, confidentiality and integrity must be availed.
Handler	-Message Forward by "Forwarder" Module without any additional handling(Encryption)	-Message Encrypt by "Encryptor" to deploy encryption standard based on sensitivity level of each tag forwarded
Attributes Scale(High, Medium, Low)	Confidentiality: Low Integrity: High Availability: Medium	Confidentiality: High Integrity: High Availability: High
Risks	Financial Risk: Low Operation Risk: Medium Continuity Risk: High	Financial Risk: High Operational Risk: High Continuity Risk: High
Importance Level	N/A	High/Medium/Low
Sample Channel (Example: Credit Card)	-Credit card Expiry Date -Issuer Bank -Credit Card type -Credit Card Issue Place	-Credit card Number -Credit Card CCV2 -Holder Name

The following table 1 given below shows the classification [4] of Sensitive Data and Nonsensitive data:

Characteristics of Suggested System: Efficiency: System is designed for XML documents based on the classification to determine which are a sensitive data and non-sensitive data for every message from their importance level.

Compatibility: System compatibility is the key factor in data design. At first all the data are being processed by XML which gets its structure from the XSD. Then data are processed in the XML format and although these are encrypted or decrypted data, these are also in XML format. All the XML data are compatible with the environment.

Security: Communication between sender / receiver, data encryption/decryption, message handling and message assembly process has a secure architecture in the proposed system.

Functional Module: Data security Exchange Module The system uses a data conversion module for achieving the security and efficient XML data transmission in the network. This module keeps both the feature of XML and security related technology.

For XML sensitive data transmission through the network, the system integrates the XML encryption, XML digital signature, XML access control and key management technology which makes a framework for sensitive transmission of data with digital envelope [5]. Digital envelope packaging and un-packaging is used in the digital envelope. For the digital envelop packaging is to use each other's public key to encrypt the encryption key and only each other's private key can restore the encrypted data. For digital envelop un-packaging the private key is used to decrypt the encrypted data. Digital envelope wants to ensure that only the prescribe receiver can read the content of the information thus it has a very high security. If the encrypted file is illegally intercepted by others, because by the interceptor don't have the communication key, so it is not possible to decrypt the file. This fully ensures the data transmission security, authenticity and integrity.

Suppose A is the sender, B is the receiver, the data exchange process to ensure the data integrity or confidentiality.

Here algorithm for symmetric encryption is used to encrypt sensitive xml documents. We know from the symmetric encryption algorithm technique, it uses the same key (symmetric key) for both encryption and decryption. So we need to ensure the transport security [7]. So to ensure the transportation security of symmetric key, an asymmetric algorithm is also used with the symmetric key encryption algorithm. This kind of security technology of combining a symmetric algorithm and non symmetric algorithm is called Hybrid Key system.

The whole process of the encryption and decryption is given below:

- Uses the symmetric key algorithm for encryption
- A public key algorithm is used then to encrypt the symmetric key of the previous step
- If there are multiple receivers that time public key of different receivers are used to encrypt the same symmetric key for different receivers.
- Receivers use their own private key to decrypt and receive the message.

Thus we can say that this process ensure the confidentiality and access control.

XML Data Conversion Module: The main idea of the module is XML data conversion through the network is common data model which communicates with the system. Sensitive and non-sensitive XML data both are passed through the data model. XML two-way mapping to achieve the data transfer between different system and becomes a uniform XML format after encryption and decryption. In the data conversion process, source XML file and output target files are XML formatted for heterogeneous system. They can take data from database or any other system XSLT mapping that can map the input and output file into XML documents [8]. Then the converted file is again called to convert XML standard into target files, to complete a conversion process. This module is mainly orthodox of data conversion module and XSLT data mapping.

Data Aggregation and Forwarding: This is the final stage of the process. Assembled sensed data comes from the Data Conversion module and non-sensitive data come from the forwarder. These data are aggregated and then send to the server.

System Evaluation and Performance Evaluation: Generally users or clients send or request data to/from the web server and the server process the request forwarding the request to the database server. The process achieves the data using this encryption and signature and return data to the requester. So, we need transportation security between the user and web server. Here, we need three security aspects as follows, security in data exchange protocol, security in Key transmission and security in Encryption algorithm. When the user requests a large number of data, XML serialization is used here to save these data and so we need to achieve the security of these data storage. Its security is depended on the security of the encryption algorithm and key. The encryption process suggested in the data conversion module can effectively prevent the attacks that could suffer in data exchange and storage. So it will be able to achieve the data exchange From the figure2, we can see that in the receiving part we will get a hash value. We need to match received a hash MD' with the sender's hash value MD. If both are matched, then no any tamper happened. If any kind of tamper recurred, the hash value will mismatch. By this study, we can also say that the XML signature module gives the function to effectively handle the unauthorized users who can leak the encrypted data files and documents. So, we can opine that this security conversion module suggested here can provide integrity, availability and confidentiality of the secured data and documents.

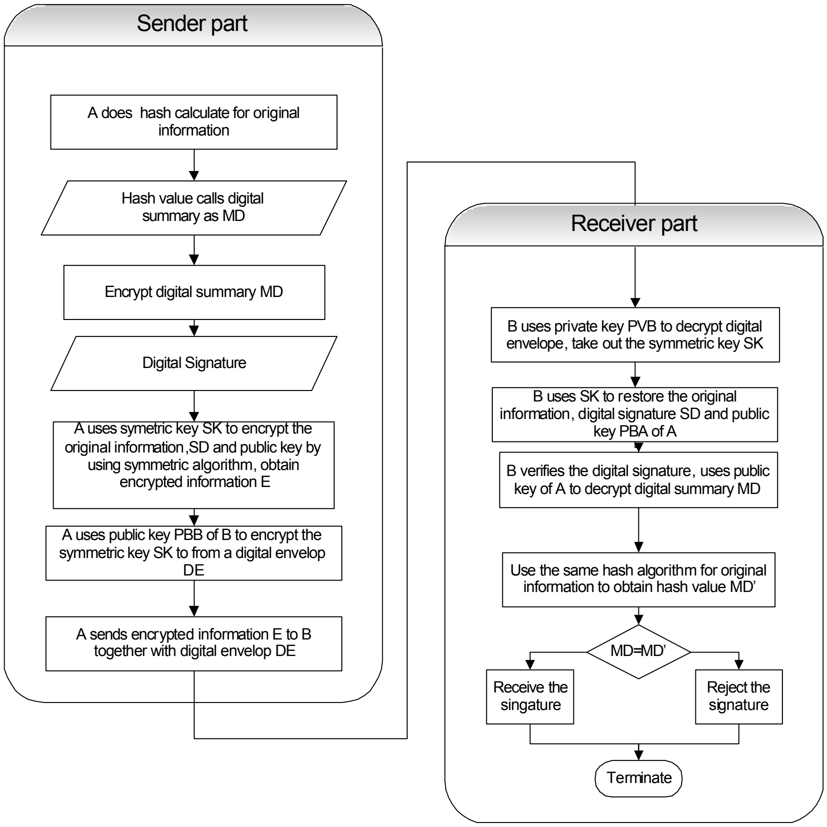

Sender part
A does hash calculate for original information
Hash value calls digital summary as MD
Encrypt digital summary MD
Digital Signature
A uses symetric key SK to encrypt the original information ,SD and public key by using symmetric algorithm, obtain encrypted information E
A uses public key PBB of B to encrypt the symmetric key SK to from a digital envelop DE
A sends encrypted information E to B together with digital envelop DE
Receiver part
B uses private key PVB to decrypt digital envelope, take out the symmetric key SK
B uses SK to restore the original information, digital signature SD and public key PBA of A
B verifies the digital signature, uses public key of A to decrypt digital summary MD
Use the same hash algorithm for original information to obtain hash value MD'
MD=MD'
Receive the singature
Reject the signature
Terminate

Fig. 2: Data Exchange process [6]

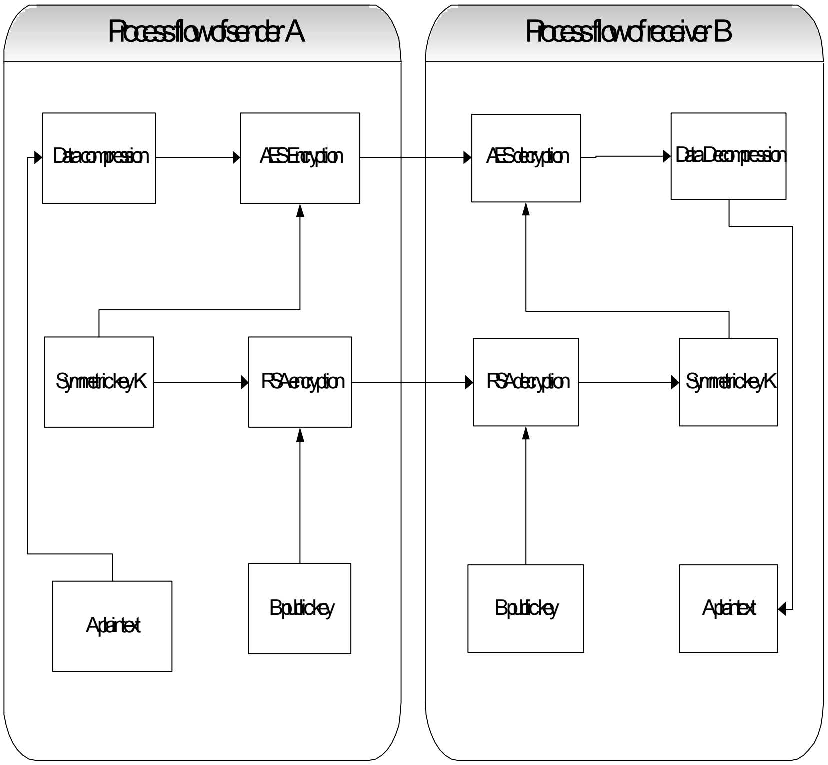


Fig. 3: Structure of Hybrid system [6]

CONCLUSION

With the development of XML technology, XML becomes memory efficient, fastest data exchange format. Being with loosely coupled, well structured, hierarchical data structure is XML become a hot cake after solving XML security problems it will have done more mature in rapid development. In the design and implementation of XML data exchange security program, this paper helps to make a secure and effective XML based data exchange. The program provided data confidentiality, integrity and secure data exchange moreover it achieved the expected functions to secure data transfer and storage.

Appendix: XML: Extensible Markup Language
XSD: XML schema definition
XSLT: Extensible Stylesheet Language Transformation

REFERENCES:

1. Bray, T., J. Paoli and C.M. Sperberg-McQueen, 1998. Extensible Markup Language (XML) 1.0. W3C.
2. Harn, L., C.Y. Lin and T. Wu, 2004. Structured multi signature algorithms. Computers and Digital techniques, IEE Proceedings, 151(3): 231-234.
3. Hardwick Martin and Dvorak Paul, 2000. What you should know about STEP, Machine Design. 7(13): 98-100.
4. Ammari, F.T. and J. Lu, 2010. Advanced XML Security Framework for Building Secure XML Management System (SXMS), Seventh International Conference on Information Technology.
5. Sun Microsystems, 2000 Inc Connected Limited Device Configuration (CLDC) Specification, ver.1.0a, Sun Microsystems, Inc.
6. Zhihong, X., Y. Yu and Z. Wei, 2010. XML-based Information Security Technology Study, 2nd International Conference on Software Technology and Engineering (ICSTE).
7. Kudo, M. and S. Hada, 2004. XML document security based on provisional authorization,Proc of the 7th ACM Conf on Computer and Communications Security, 33(4): 379-389.
8. Donald Eastlake, Joseph Reagle and David Solo, 2000. XML-Signature Syntax and Processing, W3C Working Draft.