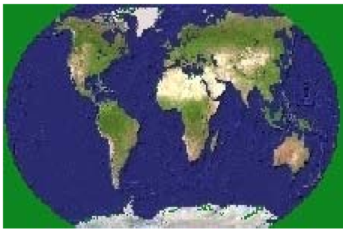

International Journal of Multidisciplinary Research and Development

IJMRD 2014; 1(6): 142-144
www.allsubjectjournal.com
Received: 17-10-2014
Accepted: 18-11-2014
e-ISSN: 2349-4182
p-ISSN: 2349-5979

Harshita
Mtech Student Mody University of science & technology, Sikar, Rajasthan, India

Sarvesh Tanwar
Asst. Professor Mody University of science & technology, Sikar, Rajasthan, India

Transmission of the secure college record over the internet

Harshita, Sarvesh Tanwar

Abstract
XML (Extensible Markup Language) is used to store the data and exchange the data across the network. In the college or university student records contains very sensitive information like grade of student, address, roll no etc., accessing of these records are done only by some authenticate person. Suppose there are several branches in college if some authority like HOD of any department wants to see the information of their respective branch student than it should includes some security measure like that person should be authorized, or data should be confidential.
In this paper, we are using XML encryption to maintain the security over the XML document while they are transmitting over unsecure web channel like internet.

Keywords: XML, XML encryption.

1. Introduction

Student record is the basic document in the college or university; there are various departments in the college which wants to access the information of their respective department students. If some authority likes HOD of any department wants to access the student record of their respective branches than it should be possible to see their student's record which includes their grades and all other information by using XML storage.

Student records are stored by using XML. Basically student records are of personal privacy, only authorized person can access, so the system requires authentication & some security measures. Teacher can access student records transparent, should rely on agent which will helps the teacher to check all the necessary student records. Due to the growth of various types of threats, hackers and other unwanted attacks over the web applications information security is one of the major issues during the transmission of data. To enhance the security system design must consider the following requirements:

1. Confidentiality: It ensures that the student records are transmitted over network without tapping by third party.
2. Only authorized person can access the information.
3. Integrity ensures the transmitted data has not been modified.
4. Non repudiation: the agent (who stores information) will not deny he/she not sent the message.

Therefore, for security of XML documents over the internet the system design must use XML encryption, XML signatures and secure socket layer.

2. XML encryption overview

As compared with traditional encryption technology, there is no such standard mechanism to encrypt a part of a document. To encrypt the entire document is very time consuming process. Hence, XML encryption provides a mean to encrypt the entire document, a part of document, and multiple encryptions over the same document. The primary goal of XML encryption is to ensure confidentiality, Authentication and verification.

3. Basic structure of XML Encryption

The structure of XML encryption given as figure 1:

```
<EncryptedData Id?Type?>
<EncryptionMethod/>?
<ds:KeyInfo>
        <Encryptedkey>?
        <AgreementMethod>?
        <ds:KeyName>?
        <ds:RetrievalMethod>?
```

Correspondence:
Harshita
Mtech Student Mody University of science & technology, Sikar, Rajasthan, India.

```
<ds:*>?
</ds:KeyInfo>?
<CipherData>
            <CipherValue>?
                        <CipherRefrence URI>?
</CipherData>
<EncryptionProperties>?
</EncryptedData>
```

Fig 1: Encryption Structure

In the above structure "?" means appears 0 or 1, "+" that appears more than once, "*" means 0 or more times. Encrypted data is the root element of an XML encryption. The sub elements of the encrypted data are encryption method, key info, and encryption properties as optional element, and cipher data as compulsory element. The encryption method describes the method of encryption with algorithm like TIPLEDES, AES128/256, and RSA etc.

KeyInfo element includes the key information such as: - private key of the receiver or a shared key. A cipher data element used to transport the symmetric key in an encrypted form. Key info element provides the information of private key of receiver to decrypt the data.

4. Problem description

To encrypt the student record as given in figure 2:

```
<?xml version="1.0"?>
<student record number="201">
<information>
<student name>Harshita</student name>
<course information>
              <name>Cryptology</name>
            <grade>A</grade>
</course information>
<branch>cse</branch>
<enrollment>130390</enrollment>
</information>
</student record>
```

Fig 2: Student Record

The above figure includes the details of student of CSE branch if we want to transmit the information of student to its particular branch's HOD than we have to encrypt the data, so that only authorized person will access the particular data.

The encryption can be done by using symmetric encryption, asymmetric encryption or combination of both (hybrid approach).

The steps of encryption are given as follows:-

1. Choose the symmetric key algorithm for encrypting the data here we choose AES128cbc (cipher block chaining) mode.
2. Encrypt the symmetric key by using public key algorithm here we are using RSA public key algorithm.
3. Store the encrypted data in the cipher value.
4. Sends the message

The steps of decryption are given as follows:-

1. Decrypt the symmetric key by using private key of the receiver.
2. Now decrypt the content by using symmetric key (or shared).

Here both sender and receiver know the shared key for encrypting and decrypting the content. While private key will be known only by the intended receiver and sender is going to encrypt the data by using receiver's public key.

Like for above record, it contains student of CSE branch than sender will encrypts the message by using public key of that branch HOD and later only HOD is going to decrypt the message because he/she only knows its private key.

After encrypting the information the record will become as figure 3:-

```
<? xml version="1.0"?>
<EncryptedData
xmlns=http://www.w3.org/2001/04/xmlenc#
type='http://www.isi.edu/in-notes/iana/assignments/media-
types/text/xml'>
<EncryptedMethod algorithm='
http://www.w3.org/2001/04/xmlenc #aes128-cbc'>
<ds:KeyInfo>
------here the information of symmetric key will be store------
-
</ds:KeyInfo>
<CipherData>
<CipherValue>
-----Contains cipher value of content------</CipherValue>
</CipherData>
</EncryptedData>
<EncryptedKey>
<EncryptedMethod algorithm='
http://www.w3.org/2001/04/xmlenc #rsa-1-5'>
<ds:KeyInfo>
------here the information of private key will be store-------
</ds:KeyInfo>
<CipherData>
<CipherValue>
cipher value of symmetric key will be store---------
</CipherValue>
</CipherData>
</EncryptedKey>
```

Fig 3: structure of record after encryption

5. Conclusion

We describe the secure transmission of student record over the unsecure web channel like internet by using the XML encryption technology. In this paper, a full XML document of student is encrypted and access by student respective branch's HOD only. In our future work we can apply multiple encryptions over the same document.

6. References

1. El-Aziz AA, Kannan A. A comprehensive presentation to XML signature and encryption. *Recent Trends in Information Technology (ICRTIT), 2013 International Conference on*. IEEE, 2013.
2. Aravanaguru RA *et al.* Securing Web Services Using XML Signature and XML Encryption. arXiv preprint arXiv*:1303.0910,* 2013.
3. Seak Sea Chong, Ng Kang Siong. A file-based implementation of XML encryption." *Software Engineering (MySEC), 2011 5th Malaysian Conference in*. IEEE, 2011.
4. Gu Yue-sheng, Meng-tao Ye, Yong Gan. Web Services Security Based on XML Signature and XML Encryption. Journal of Networks 2010; 5(9).
5. Hashizume Keiko, Eduardo B Fernandez. Symmetric

encryption and XML encryption patterns." *Proceedings of the 16th Conference on Pattern Languages of Programs*. ACM, 2009.

6. Yu Ge. Applications of XML encryption in electronicdocument. Computer Engineering and Design 2007; 28(4):935-938.
7. Miyauchi Koji. XML Signature/Encryption–the Basis of Web Service Security. NEC journal of advanced technology, 2005, 2.1.
8. Naedele, Martin. Standards for XML and Web services security. *Computer* 2003, 36.4.