# Xml-Based Security for E-commerce Application

**Ms. Pradnya B. Rane, Dr.B.B.Meshram**

Computer Department,VJTI,Matunga Mumbai, India

***Abstract-*** E-commerce applications now a day are becoming very popular as it saves a lot of time and at the same time it is very secure. Developing E-commerce application from scratch is a tedious job. The requirements for securing e-commerce transaction are privacy, authentication, integrity maintenance and non-repudiation. In this paper we are suggesting security concerns for payment details of customer. We are using XML watermarking in combination with digital signature for this purpose. This can be done to check integrity of the payment details data. This paper provides directions for web and ecommerce applications security. In particular, XML security and payment database security issues pertaining to the web and e-commerce applications are discussed.

***Index Terms***- Watermarking, Integrity, Digital Signature, Xml watermarking, SHA-512, SHAwithDSA..

## I. INTRODUCTION

Electronic commerce (e-commerce) is one of the fastest growing application areas for the World Wide Web. For the effective operation of the web and e-commerce applications, security is a key issue. The security threats include access control violations, integrity violations, sabotage, fraud, privacy violations, as well as denial of service and infrastructure attacks[1][2].

Web services security requires authentication (establishing identity), authorization (establishing what a user is allowed to do), confidentiality (ensuring that only the intended recipient can read the message, accomplished with encryption), and integrity (ensuring the message hasn't been tampered with, generally accomplished with digital signatures)[3].

The success of the Internet has made the communication very easy between parties and XML is one of the most used standard for information representation and exchange. A huge amount of data is crossing the Internet on the daily basis. Since the Internet is an unreliable network, XML data can be easily captured and tampered by unauthorized users. XML data is generally presented in plain text, thus hackers can access it during transmission across a network. Vendors have generally avoided encrypting the data because this would add size to already bulky XML files.

In this paper we are concentrating only on transaction data security of e-commerce application. This study is proposing a scheme that uses XML watermarking and digital signature to detect and localize any modification made to an XML data. The watermark embedding and detection processes are done online and use only a constant memory. Section I gives introduction to security concerns of e-commerce application, Section II describes the related work in the area of xml security. Section III discusses the proposed system for securing transactional xml data. Paper concludes in section IV.

## II. RELATEDWORK

The purpose of Web security is to meet the security expectations of users and providers. To that end, Web security is concerned with

- client-side security,
- server-side security, and
- secure transmission of information.

Client-side security is concerned with the techniques and practices that protect a user's privacy and the integrity of the user's computing system.
Server-side security is concerned with the techniques and practices that protect the Web server software and its associated hardware from break-ins, Web site vandalism and denial of service attacks.
Secure transmission is concerned with the techniques and practices that will guarantee protection from eavesdropping and intentional message modification.

The wide acceptance of XML as the format for data representation and exchange clearly demonstrates the need for a general and flexible framework of secure access for XML databases. While security specification and enforcement are well established in relational databases, their methods and approaches cannot be easily adapted to XML databases. This is because an XML document stores information not only in its data nodes but also in the way it is structured. Consequently, the problem of secure access to XML databases has its own particular flavour and requires dedicated solutions. Watermarking is a known technique for hiding a copyright mark in a digital document, in a resilient manner. While such methods already exist for numerical streams, they do not meet the specific requirements of XML streams..Watermarking in the contexts of image, audio or video data is well-known to be an effective technique to protect the intellectual property of electronic content. Essentially, the technique embeds a secret message into a cover message within the content in order to prove the ownership of materials.
The existing watermarking technology has mostly been developed in the context of multimedia data, since such data has a high tolerance to noise and thus it is not easy to detect the watermark. Unlike multimedia data, XML data are diverse in nature: some are data-centric and numeric (e.g. regular scientific data) while some are document-centric and verbose (e.g. book chapters). It is challenging to develop an effective watermarking scheme which is invisible and is able to resist various kinds of attack[4][5]. Agrawal presents an effective watermarking

technique for the relational data[6][7]. This technique ensures some bit positions of certain attributes contain the watermarks.
Gross-Amblard [6][8] investigates the problem of watermarking XML databases while preserving a set of parametric queries. His work mainly focuses on performing queries on different structures and pay less attention to the watermarking scheme.
In [9], the scheme proposed is called WmXM. WmXM is described as a system for watermarking XML, which generates queries from essential semantics to identify the available watermarking bandwidth in XML documents. As further described, it uses query templates to represent data usability, generate queries from semantic, which allows elements identification and structure units for watermarking. It also considers the internal semantics to walk through vulnerabilities that come with redundancy found in XML data. This watermarking scheme starts with the initialization, where a schema is specified and XML data are validated . A set of query templates is specified to represent data usability. Using a secret key, a number of data elements or structure units is selected for the watermark embedding. Queries are then created. The process ends up with the Watermark Insertion. Just as above in [10], we note that this technique falls into robust watermarking.
In [11], a scheme for watermarking semi-structured data that uses a graph labelling is proposed; As other schemes mentioned before this one also falls into robust watermarking.
In [12], a scheme for fragile watermarking is proposed. The technique used here is a proven method for detecting and localizing malicious alterations made to a database relation with categorical attributes. Furthermore, the scheme is distortion free, which means there is no distortion made to the actual data. It prevents illegal embedding and verification, since the watermarking process is governed by a key. The watermark embedding process and verification can only be done by a person who possesses the necessary key. The original database relation with no embedded watermark is not required for watermark verification. Finally, in case the watermark verification fails, the embedded watermarks indicate where the modifications are.
The algorithm used in this scheme can be resumed as follow: In the watermark embedding phase, first a primary key hash value is calculated for each tuple according to a watermark key and the primary key of the tuple. According to their primary key hash value, all tuples are partitioned into relative groups. After grouping, all tuples in each group are sorted according to their primary: this is done for the purpose of synchronization. The watermark embedding process ends up by watermarking each group independently. One main thing to keep in mind which is very important is that the grouping and sorting operations are only virtual operations: there is no change of physical position of the tuples. In the watermark detection phase, the same operations as in the watermark embedding phase are repeated except that when the extracted bits from a group hash are retrieved; They are checked against the position of the tuples to verify the watermark.
In [13], several techniques for hiding information in an XML document has been proposed.

## III. PROPOSED SYSTEM

Transaction database security module provides stable storage for security -related data objects, including cryptographic keys, user information, customer transactional data etc against session hijacking attack. Transactional data, cryptographic keys are stored in XML files.
It has two sub-modules as shown in Figure 1.

### *A. XML Watermarking*

In this module, watermarking of payment details is done to avoid session hijacking attack as user can see only the watermarked data. With development of data for copyright protection, Xml file watermarking can be used. At sender side payment details are stored in xml file, then we are partitioning the xml file, embedding hash values in bit positions of xml file. The working of watermarking of xml data has following sequence.
1.For watermarking we are using SHA-512 algorithm to get hash of transactional data or payment detail XML file.
2. Read xml file, partition xml data.
3. Then this Hash value is embedded in the bit positions of xml file.
4. Then we are computing digital signature of watermarked xml file.

### *B. Digital Signature*

A digital signature's purpose is to ensure integrity and non-repudiation when files are transmitted. For calculating digital signature of watermarked xml data, we are using SHA1withDSA algorithm. It works in the following sequence.
1. It takes watermarked xml data.
2. SHA1withDSA hashing code is used to generate hash code of the message.
3. Message is sent to the receiver side with public key.
4. At receiver side the message is again watermarked first as mentioned above. Then the digital signature is generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic. That means payment details are secured. The combination of watermarking and digital signature provides an effective digital signature scheme.

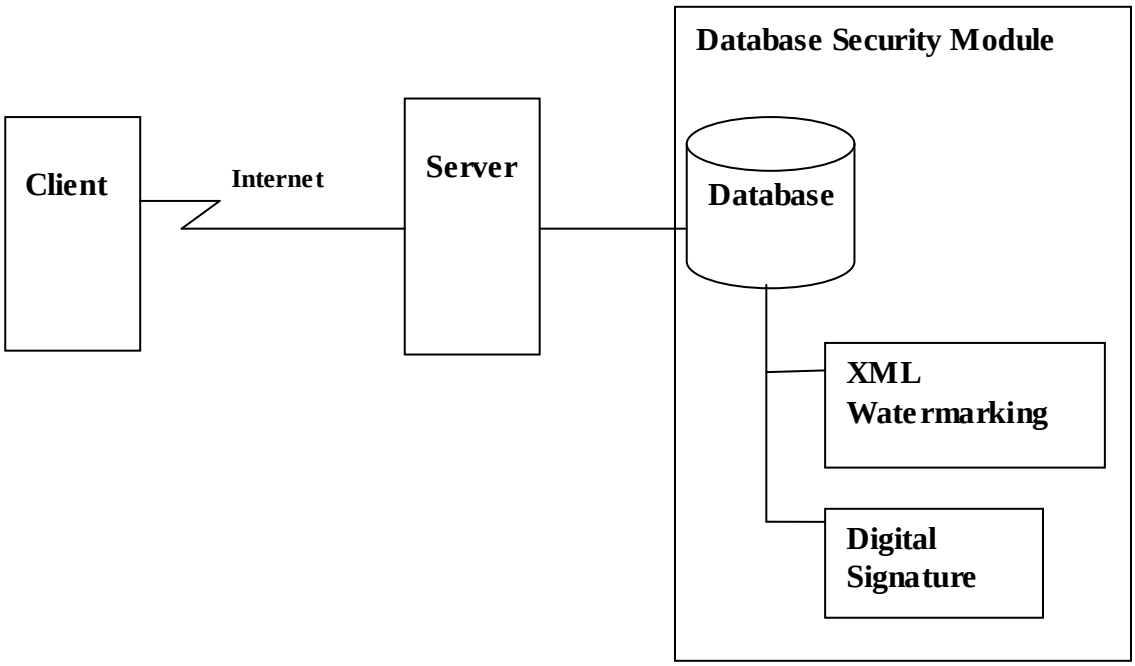


**Figure 1: Proposed System Architecture**

## IV. CONCLUSION

For securing transactional databasee against message sniffing, session hijacking attacks we are watermarking the payment details xml file and then we are applying digital signature at client side. Finally sending it to the server side system. At server side system same decoding process will be done to check integrity of the original data.In this system even an attacker hacks the digital signature of the file still he/she can not get payment details as they can see only the watermarked xml data which is not in the human readable format.

## REFERENCES

[1] Abdul Monem S. Rahma1, Rabah N. Farhan2, Hussam J. Mohammad," HYBRID MODEL FOR SECURING E-COMMERCE TRANSACTION ", International Journal of Advances in Engineering & Technology, Nov 2011. ISSN: 2231-1963, Vol. 1, Issue 5, pp. 14-20

[2] Rhavani Chris Clifton Amar Gupta Elisa Bertino Elena Ferrari," Directions for Web and E-Commerce Applications Security ",IEEE/2001

[3] David Geer , "Taking Steps to Secure Web Services ", Editor: Lee Garber, Computer, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org

[4] Steven J. Vaughan-Nichols ," XML Raises Concerns as It Gains Prominence ", http://computer.org/publications/dlib ,May-2003.

[5] Wilfred Ng and Ho-Lam Lau ," Effective Approaches for Watermarking XML Data ", L. Zhou, B.C. Ooi, and X. Meng (Eds.): DASFAA 2005, LNCS 3453, pp. 68–80, 2005. _c Springer-Verlag Berlin Heidelberg 2005

[6] Jules R. Nya Baweu and Huiping Guo," Integrity veri¯cation for XML data ", Proceedings of the World Congress on Engineering and Computer Science 2007 WCECS 2007, October 24-26, 2007, San Francisco, USA

[7] R. Agrawal and J. Kiernan. Watermarking Relational Databases. In Proc. Of VLDB, 2002.

[8] D. Gross-Amblard. Query-preserving Watermarking of Relational Databases and XML Documents. In Proc. of Principle of Database Systems, 2003.

[9] X. Zhou, H. Pang, K. Tan and D. Mangla WmXML:A System for Watermarking XML Data In Proceedings of the 31st VLDB Conference, 2005.

[10] W. Ng and L. Lam Effective Approaches for Watermarking XML Data In 10th International Conference on Database Systems for Advanced ApplicationsDASFAA, 2005.

[11] R. Sion, M. Atallah and S. Prabhakar Resilient Information Hiding for Abstract Semi-Structures a In Proceedings of the Workshop on Digital Watermarking IWDW, Seoul, Korea, 2003. Proceedings of the World Congress on Engineering and Computer Science 2007 WCECS 2007, October 24-26, 2007, San Francisco, USA ISBN:978-988-98671-6-4 WCECS 2007

[12] H. Guo, Y. Li, A. Liu and S. Jajodia A Fragile Watermarking Scheme for Detecting Malicious Modifications of Database Relations In Information Sciences , Vol. 176, No. 10, pp 1350-1378, 2006.

[13] S. Inoue, K. Makino, I. Murase, O. Takizawa, T. Matsumoto and H. Nakagawa A Proposal on Steganography Methods using XML In Symposium on Cryptography and Information Security, pp.301-306 , 2002.

**First Author** – Pradnya B. Rane, MTech computer, pradnyarane@gmail.com