Chapter 39
Securing Financial XML Transactions Using Intelligent Fuzzy Classification Techniques:
A Smart Fuzzy-Based Model for Financial XML Transactions Security Using XML Encryption

Faisal Tawfiq Ammari
University of Huddersfield, UK

Joan Lu
University of Huddersfield, UK

ABSTRACT

The eXtensible Markup Language (XML) has been widely adopted in many financial institutions in their daily transactions. This adoption was due to the flexible nature of XML providing a common syntax for systems messaging in general and in financial messaging in specific. Excessive use of XML in financial transactions messaging created an aligned interest in security protocols integrated into XML solutions in order to protect exchanged XML messages in an efficient yet powerful mechanism. However, financial institutions (i.e. banks) perform large volume of transactions on daily basis which require securing XML messages on large scale. Securing large volume of messages will result performance and resource issues. Therefore, an approach is needed to secure specified portions of an XML document, syntax and processing rules for representing secured parts. In this research we have developed a smart approach for securing financial XML transactions using effective and intelligent fuzzy classification techniques. Our approach defines the process of classifying XML content using a set of fuzzy variables. Upon fuzzy classification phase, a unique value is assigned to a defined attribute named "Importance Level". Assigned value indicates the data sensitivity for each XML tag. The research also defines the process of securing classified financial XML message content by performing element-wise XML encryption on selected parts

DOI: 10.4018/978-1-5225-9866-4.ch039

defined in fuzzy classification phase. Element-wise encryption is performed using symmetric encryption using AES algorithm with different key sizes. Key size of 128-bit is being used on tags classified with "Medium" importance level; a key size of 256-bit is being used on tags classified with "High" importance level. An implementation has been performed on a real-life environment using online banking system in Jordan Ahli Bank one of the leading banks in Jordan to demonstrate its flexibility, feasibility, and efficiency. Our experimental results of the system verified tangible enhancements in encryption efficiency, processing-time reduction, and resulting XML message sizes. Finally, our proposed system was designed, developed, and evaluated using a live data extracted from an internet banking service in one of the leading banks in Jordan. The results obtained from our experiments are promising, showing that our model can provide an effective yet resilient support for financial systems to secure exchanged financial XML messages.

INTRODUCTION

eXtensible Markup Language (XML) (Bray, Paoli, Sperberg-McQueen, Maler, & Yergeau, 2008) has been widely adopted in many financial institutions in their daily transactions; this adoption has been due to the flexible nature of XML in providing a common syntax for systems messaging in general and for financial messaging in particular. Excessive use of XML in financial transactions messaging has created an aligned interest in security protocols integrated into XML solutions in order to protect exchanged XML messages by using an efficient yet powerful mechanism. There have been several approaches proposed by researchers to secure XML messages and there is a comprehensive collection of related works.

XML is designed based on text format and has a tree structure. It is natural that data integrity, data authentication, information confidentiality, and other security benefits should be applied to entire XML data or portions of XML data. XML security solutions should provide a high level of security to ensure the confidentiality of information represented using the XML format. XML security must be integrated with XML data features and characteristics to keep the flexible nature of XML while integrating essential security technologies.

Due to the sensitive nature of financial transactions that use XML as their main messaging protocol, a security requirement should be fulfilled to protect exchanged XML messages by using a dynamic and efficient mechanism. The security mechanism should encrypt portions of XML data rather than whole messages, e.g. element-wise encryption should be used to protect sensitive parts within the XML message.

The specifications related to XML security published by W3C define the basic framework and rules that can be utilized across applications. The basic idea for XML security is to perform data encryption on XML messages whereby XML data confidentiality is achieved to ensure that the XML data structure, data content, and other sensitive information in XML data may only be accessed by legitimate parties. Confidentiality is generally associated with encryption mechanisms or access control technologies. XML key management (Hallam-Baker & Mysore, 2005) provides the basic key requirements for XML data confidentiality.

However, on a daily basis, financial institutions (i.e. banks) perform large volumes of transactions that require XML encryption on a large scale. Encrypting large volumes of messages in full will result in performance and resource issues. Therefore, an approach is needed to encrypt defined parts within the XML document, to identify syntax for representing encrypted portions, and to identify the processing rules for decrypting those portions. W3C XML encryption has a feature called element-wise encryption,