Chapter 13 Building a Secured XML Real-Time Interactive Data Exchange Architecture

Yousef E. Rabadi
University of Huddersfield, UK

Joan Lu
University of Huddersfield, UK

ABSTRACT

TCP and UDP communication protocols are the most widely used transport methods for carrying out XML data messages between different services. XML data security is always a big concern especially when using internet cloud. Common XML encryption techniques encrypt part of private sections of the XML file as an entire block of text and apply these techniques directly on them. Man-in-the-Middle and Cryptanalysts can generate statistical information, tap, sniff, hack, inject and abuse XML data messages. The purpose of this study is to introduce architecture of new approach of exchanging XML data files between different Services in order to minimize the risk of any alteration, data loss, data abuse, data misuse of XML critical business data information during transmission; by implementing a vertical partitioning on XML files. Another aim is to create a virtual environment within internet cloud prior to data transmission in order to utilise the communication method and rise up the transmission performance along with resources utilisation and spreads the partitioned XML file (shredded) through several paths within multi agents that form a multipath virtual network. Virtualisation in cloud network infrastructure to take advantage of its scalability, operational efficiency, and control of data flow are considered in this architecture. A customized UDP Protocol in addition to a pack of modules in RIDX adds a reliable (Lossless) and Multicast data transmission to all nodes in a virtual cloud network. A comparative study has been made to measure the performance of the Real-time Interactive Data Exchange system (RIDX) using RIDX UDP protocol against standard TCP protocol. Starting from 4 nodes up to 10 nodes in the domain, the results showed an enhanced performance using RIDX architecture over the standard TCP protocol.

DOI: 10.4018/978-1-7998-5339-8.ch013

INTRODUCTION

From the industrial age the world has become more in need to connect businesses together and globally migrate to an informational age, and exchanging information has increasingly become a part of its requirements. However, technology is used not only by ethical users but unfortunately by unethical users too; they grab any opportunity to manipulate or spy on the data during transmission for their immoral purposes. The need to set up an interoperable framework for exchanging data between different domains plays an important and essential role in doing business. As XML increasingly becomes a standard format for transmitting data on networks between different businesses, the need for finding secured and efficient techniques of transmitting XML data files is an essential matter. Real-time interactive data exchange system (RIDX) aims to place a multi-layer of defence of exchanging XML data information electronically between businesses, organisations, and other groups using Internet cloud network as a platform. The RIDX goal in this study is to build a clear infrastructure required for managing XML data real-time interactive exchange, taking into consideration the enormous security threats that face XML data files during transmission. The proposed system adapts as part of its transport protocol by using a multicast data distribution mechanism in order to reduce network resources, minimise the hindrance and expenditure. Thus far, there has been little stimulus to utilise multicast data distribution, because it lacks a protection mechanism for the data being delivered.

Although there has been significant progress in presenting secured multicast data distribution different drawbacks, threats and attacks can be addressed during the traditional transmission process:

- Communication channels that are not secured will jeopardise data integrity, from modification, data misuse, and data abuse. A man-in-the-hub can tap the stream of data including encryption keys, sensitive data etc.
- Operating system security breaks including memory observation; invaders can forecast sensitive secrets concealed inside memory.
- To prevent a service from providing its ordinary functions that may result to a noncontemporary information, this denial of service (DoS) can cost the organisation a large amount of service time and money.
- When transmitting data across a shared network, some tools can be used to sniff network packets in order to reveal sensitive information especially if no data encryption measurements have been taken.
- When encryption methods are applied on sections of XML file assumable confidential parts, cryptanalysts can generate statistical information and extract some useful data that can be used unlawfully, and if the encryption is applied on XML as one block of data, efficiency problems might occur.
- Validating messages transmitted from the originator is always a concern. Therefore an authentication process as a security measurement has to be established.
- Failing to preserve data integrity from any alteration, maliciously or accidentally, is a challenge during data transmission.
- Failing to guarantee that the data transferred can stay confidential and convey assurances that the data is not revealed by any unauthorised parties.