International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

Web Service Security in Business to Business (B2B) Applications using XML

AnithaGracy, J[1], Sivagurunathan, S[2], Thangavel Chandrakumar, T[3].

[1] *Thiagarajar College of Engineering, Madurai, India*
[2] *The Gandhigram Rural Institute (Deemed to be Unversity), Dindigul, India*
[3] *Thiagarajar College of Engineering, Madurai, India*

anithagracy90@gmail.com,svgrnth@gmail.com,t.chandrakumar@gmail.com

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: The Business-to-Business (B2B) e-commerce sector is poised for rapid expansion. Essential to the transformation of the B2B System is the gathering of security needs for protection, privacy, and reliability, which implies precise and Data security ready-to-go concepts for online company activities. Web Services are helpful because they provide easily available network services. Security was the major concern for B2B applications. As interest in cloud computing has grown, security concerns have been addressed and standardized. We demonstrate the fundamental characteristics and security of B2B application systems with the use of XML technology. Conventionally, a Comparison of two points currently in the XML security notion was led due to the enhancement of XML security along with the distinguished research outlines. As a starting point, XML Security refers to a collection of security techniques, such as digital signature and encryption that are strongly coupled via XML to preserve the primary qualities of the semi-structured data format of XML so long as basic security skills are provided. This paper will be investigating the Encryption from W3C and the specification of XML Signature along with its .NET implementation and a case study was carried out.

Keywords: XML, B2BIntegration, Security, XMLEncryption, XMLSignature, WebService

1. INTRODUCTION

The backbone of the IT industry was said to be Web service which started in the late 1990s as an idea. With the help of web services, there are plenty of transactions for business benefits with the goal to attain the sought objectives. The outcome of XML's (Extensible Markup Language) customizability and portability being applied to these XML and Web Service-Unleashed web services and XML for Dummies is the general language geared at these web services. An auspicious ideal model for numerous complex Web-based applications is XML Web Services. WS feature which is important is SOAP, the exchange of messages which is a strong and simple protocol that is extensible XML based [18]. In the present circumstances due to the interoperability and accessibility nature of Cloud Computing and Web services, they serve as the important key points of e-government applications [2]. In the present indeterminate and difficult environment for business, the organization which is essential is Enterprise Information Systems (EIS) [10]. Also, the main language of the Internet is said to be Hyper-ions [6]. XML technology is a set of languages, methods, and values advanced by the Hypertext Markup Language (HTML), which is not matched for conveying data and implementing managed Web Consortium (W3C). Contribution by XML has helped in many application regions like Web services, B2B interactions and also helps in the development of enterprise applications such as inter and achieving combined enterprise information systems with the help of ERP being accepted worldwide through the industries as an applied resolution [12]. Also, ERP is based on industry-driven concepts and systems. [9] discusses web service security utilizing XML innovation within endeavors. The exploration behind the B2B applications addresses the issues faced with expected frameworks by providing sensible as well as adaptable support from the IT which is done with the help of web services being disintegrated from the whole business logic of the system [22]. XML was produced so that they could uphold an assortment of online-based information transmission usages, incorporating numerous uses in B2B applications.XML has various constraints when in accordance with the region of data security and integrity [6]. All modern Web services are

produced and updated on a regular basis. It is not possible for a person to manually examine them and generate the composition plan [17]. One of the common languages is XML in the e-business revolution of B2B. Without any doubt, we could assure that XML in the future will be a part of every B2B application nonetheless.

Firstly, not being an integration solution, XML is simply a (DDL) Data Definition Language. There seems to be no business when it comes to no global XML standards among various companies extended all over the world [1][2]. Two security level that B2Bi need starts with that B2Bi demands on opening up business firewalls to permit communication through cross-boundary among enterprises. Hence, regardless of the integration mode being used, several companies should protect the inner network alongside harmful attacks over those ports that are open.

And the second level is facts and figures portrayed through focused lines that are leased which could be EDI or internet or else through any other mode which must be secured. Classified information is present within the data which also includes business transactions and corporate information and this is why it must be highly protected.

2. RELATED WORK

In order to enhance the digital sign usage so that XML documents could be signed which brings the highlights of authority party, verification, and integrity for XML sign to be the first release in W3C recommended in the wide range of web service security. Kangas Harju e. Measurements on performance which is substantially present will be exposed along with the effect on Mobile phones of usage of XML-based security in another format. Organizations implementing service-oriented architectures prefer web services as their choice for integration technology. AI-Shargabi in his paper discusses the need for XML Security Standards [3]. The standard definition regarding web services is brought up newly by W3C. The following are the concepts applied in a basic level on web service security: [4]

Availability: could DOS attack be a factor of vulnerability to the system at any cost?
Authentication: The message is sent by whom?
Integrity: could there be a tampered message?
Confidentiality: While in transit or storage, can the information be read?
Audit: are there any recorded transactions that are all secured?
Authorization: Could this target be accessed by the subject that is authenticated?
Administration: Could be management of policy be any more straightforward?

Web service in line of W3C is the XML artifacts which are programming requisition distinguished for being described, expanded with Definition, and identified by a URI where the interfaces are fit along with the tying so that there will be usage in interacting with various other applications of software that can use online based protocols to send messages through XML. Web services are accessed digitally so that human users do not get to access them directly. Within the case of a web broker, the HTML pages can be surfed by the user regarded by the stock acquisition, like symbol finding, price finding, entering of many requested shares, confirmation of the request acquisition, getting a confirmation number, etc. it'll be very difficult to get a program written in order to access these pages. To parse is tough in HTML and therefore the contents and organization of its pages might be changed by the website, daily. If the broker offers a stock-buying web service, the program to access is simple- an XML message over the SOAP RPC is sent and an XML message is obtained back. They are brought into various environments that integrate business operations, partners, suppliers, and employees by the Web-based enterprise systems. Enterprises are becoming ever more vulnerable to the global climate change challenge and are attempting to implement adaptation strategies [30].

ERP software vendors (www.articlesbase.com/software-articles/erp-software-and-data-security) must strike a balance between utility and security as the dangers to information security increase annually. In their paper, discuss the need to specific efforts to one of the existing measures which provide safety regarding web services, for example, let’s take SSL, "can't adjust appealing regarding security for web service " and discusses various standards and security measures in case of XML for integrity, authentication, and non-repudiation [26]. It is believed that WS-Security is a set of specifications that discusses primary security services, such as message secrecy, message integrity, and authentication. The most highlighted security requirements are discussed in various Business Models [21]. In addition to describing the recent development of Web services by a number of standardization groups, this article explains how Web services security standards address their security requirements.

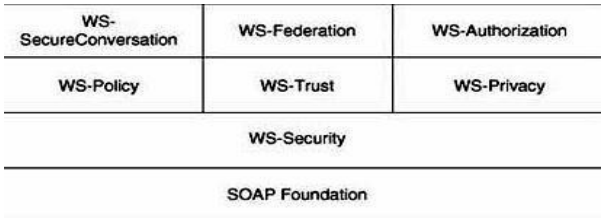

Fig. 1. WS-Security Architecture

The open neighborhood that made Web Services advanced various security measures. Figure 1 which is shown above represents an architecture charts them through principles of different layers in each constant Web Service [5]. By reducing the overhead of the key establishment, the WS-Secure Conversation is a Web Services specification that provides various SOAP message exchanges in the context of security. The tools for allowing different security realms to broker information related to identities, authentication, and identity are explained by WS Federation. WS-Policy is a collection of specifications that outline the limitations and capabilities of the safety (and other business) policies for intermediates and endpoints. The highlighted focus of WS-Security is the usage of XML Signature and Encryption part to offer prior and high end-to-end security. WS Trust provides allowances to WS-Security, exactly handling the allotting, recommencing, and authenticating of all those security tokens, also like ways to determine, evaluate the occurrence of, and generate associations among contributors during a secure message exchange. WS-Privacy depicts a model for Web Service and requester security orientation and organizational security practice explanations. Despite universal security advances like SSL, the necessity for XML Signatures are discussed by while likewise pushing on the boundaries of SSL like its ineptitude to encrypt incomplete reports and likewise its insurance of just Point-to-Point security [26]. Concern about the significance of XML Signature and the advantages of employing them, present a notion of unquestionable XML marks utilizing irrefutable RSA encryption [23]. Komienko and Mishina propose the thought of utilizing XML digital signatures within these Internet B2B conveyances without updating the present provisions, by determining capacities for marking and checking Web Services utilizing SOAP as the message [13]. The Analyst has identified bottlenecks in XML parsing and public key activities, such as RSA signature and encryption [19]. The majority of users prefer to control their personal information. But none of the mechanisms address privacy issues, which results in information leakage [7].

A full examination of the signature wrapping attack on XML Data and its solutions to detect and thwart these web security concerns is provided [15]. To resolve the above issues, we outline and implement XML Encryption & Digital Signature for the safety issues in B2B applications.

3. METHODOLOGY

A. XML & B2B INTEGRATION (B2Bi)

The structure of the information may be described using XML, which is a set of data. The platform-independent file format known as XML is used for the purpose of data representation. XML is a database management system (DBMS) that holds many things, including parser algorithms, XML documents, and Document Type Definition (DTD) schemas [16].

XML, which stands for "Extensible Markup Language," is a type of markup language. Because it is not a piece of software, it does not carry out any functions on its own. The extensible markup language, or XML, makes it possible to build a standardized system for defining, collecting, processing, and publishing data. In many respects, XML is superior to HTML as a markup language. Markup languages often have certain syntax, and HTML is no exception. To put it another way, the architecture of the language ensures that it will create a given set of characteristics in the markup that it generates. XML does not specify a set of elements, unlike HTML, which has a preset set of tags that we use to generate documents, such as H1>, P>, and Table>. In contrast, HTML includes tags such as H1>, P>, and Table>. In its place, it produces a standardized framework that either specifies our own or its defined by others depending on the criteria that they have [11].

B. B2B Integration (B2Bi)

B2B integration or B2Bi refers to the secure linkage of data between organizations' information systems. The way the business is being conducted is completely transformed between partners, suppliers, and customers or buyers. Tightly integrated partnerships raise the success and growth of the company regardless of how small, medium, or large the company is B2Bi's web service support is a crucial component of the procedure [27]. B2Bi is an effective way to comprehend the integration of enterprise information systems. Based on a thorough examination of common methods for using semantic technologies in business process management (BPM) studies of cross-enterprise cooperation or so-called business-to-business integration, we propose a framework for implementing semantic technologies in BPM research.IS academics have investigated B2B e-hubs for nearly a decade, where supply chain integration is a key topic for supply chain management. The method suggested by Belchior for estimating business-to-business integration (B2Bi) and coordination costs [5]. B2Bi aids business partners by reducing coordination expenses.

Enterprises communicate with customers, suppliers, and trading partners using a variety of strategies. Electronic data interchange (EDI) is used for commercial

communication by a variety of organizations. Using electronic data interchange (EDI) technology, corporate systems exchange structured messages based on agreed-upon message standards through private networks managed by EDI service providers. The next phase of the e-business revolution is called business-to-business (B2B) e-commerce, and it involves companies working together in real-time with their business partners and managing all of their processes online, from supply chain and purchasing to manufacturing and product development, for greater control, quicker response times, increased efficiency, a global intelligence, and unheard-of cost savings.

In today's information-intensive business environment, decision-makers throughout the whole supply chain must have access to the information necessary to make more educated business decisions on the implementation of B2B integration (B2Bi) technologies. The Business Decision Makers developed a management and orchestration model, which was validated using key-informant focus group data on worldwide B2Bi [25]. The concept is based on service-oriented B2Bi apps. They gave a practical illustration that describes and illustrates the proposed integration model. A B2B Services-oriented architecture (SOA) serves as a services layer in front of back-office systems and is often implemented via an application server or message bus. A B2B Services-oriented architecture (SOA) services layer safeguards the developer from the complexity and danger of lower layers and enables the rapid development of applications.

C. WEB SERVICE SECURITY IN B2B

a) Web Service Security

Using web services, information is transmitted over the network using SOAP (simple object access protocol). SOAP is a simple mechanism for transferring structured data in a highly decentralized setting. SOAP (Simple Object Access Protocol) uses XML (eXtensible Markup Language) to build a flexible framework for exchanging messages over a number of underlying protocols. Although SOAP is the core architecture for the exchange of information between web services, it does not provide any privacy and security protections for the data that is sent [28]. Web service modifications to provide privacy, security, trust, and other functionalities are depicted in Figure 2.

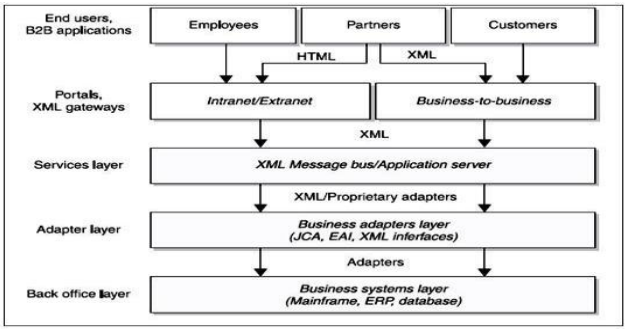

Fig. 2. B2B Services-oriented architecture

Security for web service includes factors such as integrity, non-repudiation, confidentiality, and authentication [16]. Web business procedures can compass different exchanging accomplices, for access control and authorization it requires a connection, between numerous substances (clients and also machines), and integration with corporate security approaches. In the event of highly delicate administrations, clients' authentication assumes a part of central significance [5]. No existing security solutions enable partial signature generation of email content by different signers, which could facilitate commercial scenarios [14]. According to Shakeri, enterprises must create a complete Internet security system that is tailored to the Internet business processes of today [20]. End-to-end secrecy — No one can access or copy the data while it is stored on computers or in transit.

• *Integrity* - The data is not altered on its long journey from the sender to the recipient.
• *Verification (information and client)* – The report hails from the assumed sender and is accepted by the anticipated recipient.
• *Non-reputability* - The sender cannot dispute the sent information and cannot prevent the substance from claiming the information.

Sources of XML information with a procedural access interface are compared to sources of social information with a database interface. Each new user must first register by providing a supported or self-declared password. It is anticipated that the conventional approach for Internet validation would be the use of certificates issued and verified by a Certificate Authority (CA) as a fundamental component of public key infrastructure (http://www.ibm.com/developerworks/XML/library/x-encrypt/). Using XML to implement security standards is the main goal of XML security. While several countermeasures propose the XML rewriting attack, finding a common technique for secure and fast substantiation of XML input to SOAP web services still remains an open issue. For a primary approximation, An XML web service is a service of RPC within which, responses and requests are encoded in XML as SOAP envelopes and transported over to HTTP [8]. To increase the security of XML archives, many methods have been developed in B2B Projects. A brief description of a few of these technologies is provided below.

b) XML Signature

In XML transactions, it is planned to use digital signatures similar to signatures in extensible Markup Language (XML). This concept of digital signature is not new, and other additional methods have been presented to the community (such as public-key cryptography standards) [1]. Digital Signatures have become a crucial component of electronic security, as they may be used to assure the validity, integrity, and non-repudiation of data. The Structure of the extensible Markup Language (XML) Signature is shown in Figure 3. Generally, existing browser-based security systems, for the most part, satisfactory for flat esteem business-to-buyer transactions, don't furnish the improved security or adaptability needed for ensuring high-quality business transactions and the touchy information trades that embody them. extensible Mark-up Language (XML) Digital Signature furnishes requisitions with validation, information uprightness, and non-renouncement capabilities.

Extensible Mark-up Language (XML) Digital Signature could be connected to 1 or more things of advanced substance. These things of the computerized substance may be any sort of information yet are as a rule extensible mark-up Language (XML) reports, and are alluded to by URIs. The present trend is that for data communication between applications, extensible mark-up Language (XML) has become a standard means. Algorithms such as Pretty Good Privacy (PGP), Digital Signature Algorithm (DSA), and RSA addresses the issue of sending and receiving data and it is the recommendation from W3C. These local data objects are mentioned via a fragment identifier if the data items are within the same XML document.

The extensible Mark-up Language (XML) Digital Signature is typically utilized in various application areas like electronic mail and electronic fund transfer, software distribution, Electronic Data Interchange (EDI), etc. However, it's critical to create an alternate serialization format that is compatible or agreeable to security features of extensible Mark-up Language (XML) such as signing and encryption. Web Sphere Application Server uses an extensible Mark-up Language (XML) signature with existing algorithms such as HMAC, SHA1, and RSA, but XML signature does not build new cryptographic techniques.

Signatures in Extensible Markup Language (XML) establish vital information and the discovery of new techniques. Extensible Markup Language (XML) Signature Wrapping attack is one of the most serious attack methods in Web Services [9]. The quality establishes a blueprint for representing the results of a digital signature operation that is applied arbitrarily but often extensible Mark-up Language (XML) data

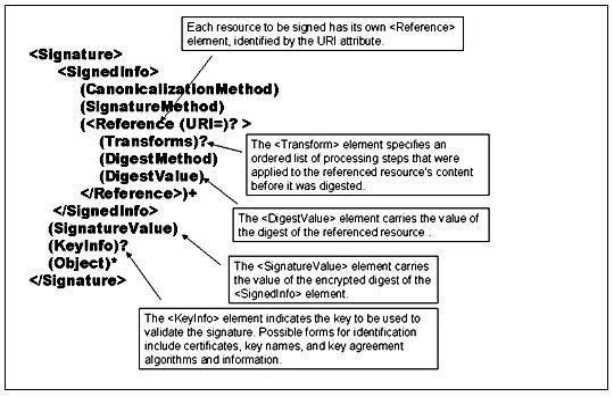

Fig. 3. Signature XML Basic Structure

XML Encryption

Encryption is the procedure for change of the fragile record into a structure that is not sensible to unauthorized customers. Approved clients need to decrypt the figured substance remembering the finished objective to handle the substance. It is an amazingly old technique to accomplish informative data security. In 2002, the W3C Consortium did an improvement to Extensible Markup Language (XML) encryption to hold the steps for the encryption of information, the steps for decryption of encrypted data, the syntax to speak to the data that XML encrypted, the informative data used for decryption of the data, and a record of algorithms for encryption, for example, Advanced Encryption Standard (AES), triple Data Encryption Standard (DES), and Rivest-Shamir-Adleman calculation (RSA)and this is called as Encryption using XML. It enhances the security of requisition that requires a safe exchange of arranged qualified information. XML is the most notorious enhancement of composing information, and in this way, XML-dependent encryption is the trademark approach for handling complex requirements of security in qualified information trade requisitions. The following Figure 4 shows the illustration of the encrypted document. The Encrypted Data component signifies the element of an encrypted Credit Card. The Encryption Method part depicts the connected encryption algorithm, which is AES in the following illustration. To recover a decryption key, the Key info element holds the informative data, which is a Key Name element in this sample. By using serializing and encrypting in the Credit Card element, cipher value texts are obtained which hold the cipher text. XML encryption and decryption rely on pre-existing encryption methods. XML Encryption is used to add secrecy and security to XML documents.

```
<PaymentInfo xmlns='http://example.org/paymentv2'>
 <Name>WEB SERVICE SECURITY</Name>
 <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
  xmlns='http://www.w3.org/2001/04/xmlenc#'>
  <EncryptionMethod
   Algorithm='http://www.w3.org/2001/04/xmlenc#aes-cbc'/>
   <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
    <KeyName>SECURED NAME</KeyName>
   </KeyInfo>
   <CipherData>
    <CipherValue>ydUNqHkMrD...</CipherValue>
   </CipherData>
 </EncryptedData>
</PaymentInfo>
```

Fig. 4. Common secret key of Extensible Markup Language (XML) document

```
<PaymentInfo xmlns='http://example.org/paymentv2'>
 <Name>WEB SERVICE SECURITY</Name>
 <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
  xmlns='http://www.w3.org/2001/04/xmlenc#'>
  <EncryptionMethod
   Algorithm='http://www.w3.org/2001/04/xmlenc#aes-cbc'/>
  <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
   <EncryptedKey xmlns='http://www.w3.org/2001/04/xmlenc#'>
    <EncryptionMethod
     Algorithm='http://www.w3.org/2001/04/xmlenc#rsa-1_5'/>
    <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
     <KeyName>SECURED NAME</KeyName>
    </KeyInfo>
    <CipherData>
     <CipherValue>yMTEyOTA1M...</CipherValue>
    </CipherData>
   </EncryptedKey>
  </KeyInfo>
  <CipherData>
   <CipherValue>ydUNqHkMrD...</CipherValue>
  </CipherData>
 </EncryptedData>
</PaymentInfo>
```

Fig.5. XML document encryption along with the public key recipient

Its purpose is to give a security edge to existing Extensible Markup Language (XML) documents by encrypting the enormous amount of data it stores. In Figure 4, it is expected that both the sender and beneficiary have a regular secret key. Provided that the beneficiary has an open and private key pair, which is in all probability the case, the Credit card element might be encrypted as demonstrated in Figure 5. The Encrypted Data element is the same as the Encrypted Data element discovered in Figure 4. On the other hand, the Key Info element holds an Encrypted key.

XML Encryption in the WSS-Core

For the advancement of Structured Information Standards (OASIS), WSS-Core specification is a work in progress by the Organization. The particular portrays upgrades to SOAP (Simple Object Access Protocol) informing to furnish through message integrity - the quality of protection, the confidentiality of the message, and authentication through a single message. The message classified is acknowledged by encryption dependent on extensible Mark-up Language (XML) Encryption. The WSS-Core specification backs encryption of the mixture of header blocks, body blocks, their sub-structures, and connections of a SOAP (Simple Object Access Protocol) message. The reference might be an intimation for a beneficiary to recognize which encrypted parts of the message to decrypt. The extensible Mark-up Language (XML) syntax of the reference changes depending on what information is encrypted and also how it is made. For example, suppose that the Credit Card element in Figure 6 is encrypted with either a public key common or the secret key of the recipient.

```
<SOAP-ENV:Envelope
 SOAP-ENV:encodingStyle='http://schemas.xmlsoap.org/soap/encoding/'
 xmlns:SOAP-ENV='http://schemas.xmlsoap.org/soap/envelope/'>
 <SOAP-ENV:Body>
  <PaymentInfo xmlns='http://example.org/paymentv2'>
   <Name>WEB SERVICE SECURITY</Name>
   <CreditCard Limit='12,000' Currency='INR'>
    <Number>2359 3456 1243 5544</Number>
    <Issuer>HDFC BANK</Issuer>
    <Expiration>04/16</Expiration>
   </CreditCard>
  </PaymentInfo>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Fig. 6. Sample Soap Message

Implementation of Web Service Security Techniques

We have implemented XML Signature specification and Encryption from W3C using the platform named as Microsoft .Net with C#. The framework is named as .Net which delivers a platform for system implementation that is complete when it's combined with the SDK version 2.0, Microsoft 2006 with the WS-Trust standard supported by web service enhancement (WSE) along with WS-Security [24]. Figure 7 illustrates the B2Bi system architecture for a secured web service Business system. The exchange of business messages helps in interaction with Buyers and Sellers in B2Bi architecture which is based on a messaging model. The standard for message exchange with Encryption and Signature which is the ebXML as an electronic business eXtensible Markup Language framework is through Enterprise A. OASIS group facilitates an open, non-proprietary, industry-standard platform which is known as ebXML.

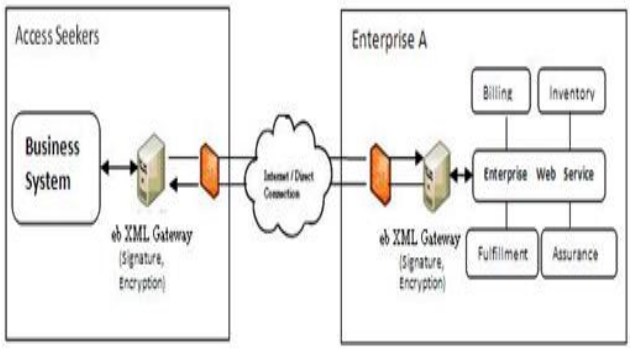

Fig. 7. B2Bi Architecture High-Level

Between two messaging gateways, the distribution and acceptance of messages is known as ebXML Gateways as you could see in Figure 7, is involved in B2B transactions. Hosting a gateway that is ebXML to distribute and accept messages to/from the Enterprise-A gateway that is ebXML shall be needed by an Access Seeker.

4. DISCUSSION

The relationship in B2B e-Market applications is established by certain paper contracts along with a number of certificates till now, due to the operation based on papers which are still dominant in the e-Market even still. The privacy leakage is led due to third-party-issued paper certificates. Security using web services is provided by illustrating the proposed mechanism and architecture to a real e-Market which is given below as a case study. A new relationship is built with the help of web services as seen clearly in Figure 8 to illustrate the real workflows.

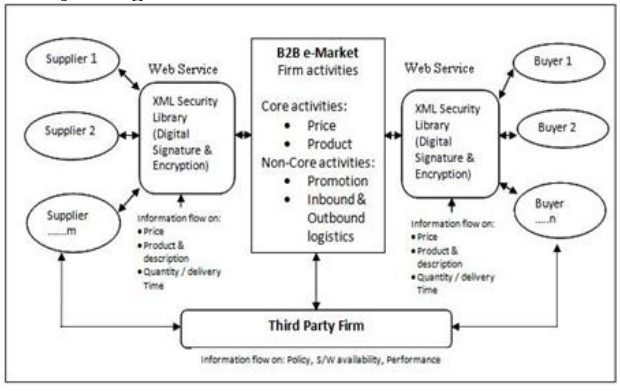

Fig. 8. A case study with interactions in B2B e-market network

The business of supplying materials to vendors who hailed from other states of India is referred to as "NAUTIX". Clients join in affiliation with other businesses which is similar to plenty of affiliates joining the vendor who has a remarkable growing business. Routing of data enabled by XML along with verification into the system of affiliation helps in doing business operations along with a solution that can deliver searching through online, availability checker as well as ordering as their standards were taken by NAUTIX.

Some of the features expected were:

Online credit card information is accepted to order the materials which are XML service. Order is canceled by XML service. The rate and accessibility of each material in the trusted network are updated where service using XML is managed. Data that gets directed through the affiliated wide network alone is ensured by username and password for security where the entire XML service of transactions is authenticated. When there are any types of mistakes and catastrophes present in connecting to the other system in the trusted wide range of networks, then the XML system must be responsible, that is it should not break down. Once the valid verification of every transaction is being done among a system of two systems trusted range of networks, only then will the entire answer featuring XML services like online ordering and handling rate and accessibility of materials and plenty of those other services present through XML work. XML helped in doing data providing or data consuming. It is needed in the system to fetch other systems' real-time rate and availability and show it to the customer in order so that the data is consumed and the system can work itself in affiliation with other systems.

Achievement

XML helps in the working of authentication (username, password-based) networks. The particular methods of XML named Push and pull are implemented using XML-based transferring of various data. HTTP and Soap XML helps in data transfer techniques in XML along with Socket. Saving crosswise over pages of all these data and putting them together in one XML document. Submission of a request to the respective department for products, notifying the branch which delivers to transport the request also requesting the department for paying to charge the Visa are a variety of things that could happen out of sight. As the informative data is transmitted between applications, these could happen in stages. We must take a few things into consideration. With the help of FTP, the qualified data from one organization can head off to different organizations could be considered as a scenario. The perfect result is the Public-key Cryptography used by Encryption. A digital signature is preferred if the information is not discriminating however still ought to be verified to check legitimacy. Standards and Algorithms such as DSA, PGP, RSA, etc., are the ones that are defined through W3C which is supported by XML signature [29]. The deciphering of the XML signed using Microsoft. NET is done if W3C would suggest some applications so that it may understand the XML which is said to be a signed one.

5. CONCLUSION

Protecting data allotted on the B2B applications on the Internet is helped through the technologies which exhibit XML security specifically signature and Encryption regarding XML whereby could be viewed through the paper. Digital Signatures of XML and Encryption mechanism are supposed to be in usage through upkeep and security which is enhanced whilst the use of XML in Business Applications are confirmed as the goal of the usage of XML in B2B applications which is mentioned in this paper. Extensible Markup language used to be advanced to enable a broad vary through Online-based data alternate uses, along with ERP, E-Commerce of B2B, etc. due to the fact the main linguistic of the Online whereabouts also HTML abbreviated for hypertext mark-up language that is now not appropriate for spreading information and execution of transactions.

The issue of safely sending and appropriating information that accords to the vast majority of the Algorithms such as DSA, PGP, RSA, etc., and so on is addressed by determinations from W3C. From World Wide Web where the implementation using C#.NET through Signature requirement in XML is explored throughout this paper. The ability to comprehend Signed XML and validate the signature in any Java- or Microsoft-based programming language is one of the greatest advantages. XML signature is addressed to uncover a namespace in particular by Microsoft.net Framework. In order to make signatures in XML and to encrypt those keys with the usage of C#.net language, different namespaces, and methods are shown in this paper. Two key initiatives, XML signature, and XML encryption, were outlined in order to address the problem of securing relevant information that is disseminated throughout an internet network. Software developers and Internet users have access to a variety of methods for conducting transactions online. This paper discusses and demonstrates the creation of Signature and Encryption of XML, which is facilitated by the fact that the management of the Internet is centered on security-related issues.

The exploration of examples that involve applications on a wider range with many signatures will be our future research which also defines adequate visualization styles for those applications. Given that an XML document and an XSLT transform which are both in a signed form would be in favor of the display of WWW signed documents so that it may be made possible for the enhancement of existing web browsers such as the XML signature verification included, which is defined clearly in another area. Also, in order to improve the Web service security, we must apply smart card equipment XML which is treated through XML communication procedures.

ACKNOWLEDGMENT

This research work was supported by the TRF Scheme (Thiagarajar Research Fellowship) provided by Thiagarajar College of Engineering, Madurai, India.

REFERENCES

1. Abidi, S., Essafi, M., Guegan, C. G., Fakhri, M., Witti, H., & Ghezala, H. H. B. (2019). A web service security governance approach based on dedicated micro-services. Procedia Computer Science, 159, 372-386.
2. Al-Shargabi, B. A. S. S. A. M., Al-Jawarneh, S. H. A. D. I., & Hayajneh, S. M. (2020). A cloudlet-based security and trust model for e-government web services. Journal of Theoretical and Applied Information Technology, 98(1), 27-37.
3. Akramov, A., Mirzaraimov, B., & Akhtamova, Y. (2020). Foreign experience related to the legislation and practice of trust management of property in business activities. Збірник наукових праць ΛΌΓΟΣ, 12-14.
4. Antonova, R., & Georgiev, G. (2019, January). ERP Security, Audit, and Process Improvement. In Smart Technologies and Innovation for a Sustainable Future: Proceedings of the 1st American University in the Emirates International Research Conference—Dubai, UAE 2017 (pp. 103-110). Cham: Springer International Publishing.
5. Belchior, R., Guerreiro, S., Vasconcelos, A., & Correia, M. (2022). A survey on business process view integration: past, present and future applications to the blockchain. Business Process Management Journal.
6. Bhargavan, K., Corin, R., Fournet, C., & Gordon, A. D. (2007). Secure sessions for web services. ACM transactions on information and system security (TISSEC), 10(2), 8-es.
7. Bhuvaneswari, N. S., & Sujatha, S. (2022). Integrating SOA and web services. River Publishers
8. Chen, M. (2003). Factors affecting the adoption and diffusion of XML and Web services standards for E-business systems. International Journal of Human-Computer Studies, 58(3), 259-279.
9. Cristescu, M. P. (2019). CHARACTERISTICS OF OPEN GRID SERVICES ARCHITECTURE. Knowledge Horizons. Economics, 11(1), 8-14.
10. Cui, M., Li, W., Cui, L., Jia, Y., & Wu, L. (2022). How do keystones govern their business ecosystems through resource orchestration?. Industrial Management & Data Systems, (ahead-of-print).
11. Hallam-Baker, P., Hondo, V. M., Lockhart, H., Martherus, B. R., Maruyama, O. H., Nadalin, A., ... & Waite, D. (2005). Web Services Trust Language (WS-Trust).
12. Hasnain, M., Pasha, M. F., Ghani, I., Imran, M., Alzahrani, M. Y., & Budiarto, R. (2020). Evaluating trust prediction and confusion matrix measures for web services ranking. IEEE Access, 8, 90847-90861.
13. Kornienko, D. V., Mishina, S. V., & Melnikov, M. O. (2021, November). The Single Page Application architecture when developing secure Web services. In Journal of Physics: Conference Series (Vol. 2091, No. 1, p. 012065). IOP Publishing.
14. Lee, C. D., & Chen, T. H. (2021). New Secure and Practical E-Mail Protocol with Perfect Forward Secrecy. Symmetry, 13(7), 1144.
15. Mohdhar, A., & Shaalan, K. (2021). The future of e-commerce systems: 2030 and beyond. Recent Advances in Technology Acceptance Models and Theories, 311-330.
16. Moon, Y.B. (2007). 'Enterprise Resource Planning (ERP): a review of the literature'. International Journal Management and EnterpriseDevelopment, Vol. 4 No. 3.

17. Muthukrishnan, P., Sakthivel, V., Ramachandran, B., & Srihari, K. (2020). Technical analysis on security realization in web services for e-business management. Information Systems and e-Business Management, 18, 427-438.
18. O'REILLY, P. A. T. R. I. C. K., & Rigopoulos, K. (2022). Fiscal Year 2021 Cybersecurity & Privacy Annual Report. NIST SPECIAL PUBLICATION, 800, 220.
19. Samuel, A. S. G. (2020). Implementation of Service Oriented Architecture Using Web API & SOMA in E-commerce Web Application. International Journal, 8(7).
20. Shakeri Aski, B., Toroghi Haghighat, A., & Mohsenzadeh, M. (2020). Trust optimization in the single web services using a neuro -fuzzy system. Iranian Journal of Optimization, 12(2), 187-201.
21. Skala, A. (2022). Sustainable transport and mobility—Oriented innovative startups and business models. Sustainability, 14(9), 5519.
22. Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., ... & Kim, K. I. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. Electronics, 10(15), 1811.
23. Tekli, G. (2021). A survey on semi-structured web data manipulations by non-expert users. Computer Science Review, 40, 100367.
24. Tekli, J., Damiani, E., and Chbeir, R. (2021). 'Using XML-Based Multicasting to Improve Web Service Scalability'. International Journalof Web Services Research (IJWSR) doi:10.4018/jwsr.2012010101, Vol. 9No. 1, pp. 1 - 29.
25. Thangavel, C. and Sudhaman, P. (2011). 'Enhancing Data Security in ERP Projects Using XML'. International Journal of Enterprise InformationSystem, IGI Global, Vol. 8 No. 1, pp. 1- 15.
26. Thuraisingham, B., Kantarcioglu, M., & Khan, L. (2022). Secure Data Science: Integrating Cyber Security and Data Science
27. Wang, S., Guo, M., Hu, Y. X., Chiu, Y. K., & Jing, C. (2022). Smart manufacturing business management system for network industry spin-off enterprises. Enterprise Information Systems, 16(2), 285-306.
28. Weck, M., Jackson, E. B., Sihvonen, M., & Pappel, I. (2022). Building smart living environments for ageing societies: Decision support for cross-border e-services between Estonia and Finland. Technology in Society, 71, 102066
29. Yue-Sheng, G., Meng-tao, Y., & Yong, G. (2010). Web services security based on XML signature and XML encryption. Journal of Networks, 5(9), 1092.
30. Zhang, Q., Gossai, A., Monroe, S., Nussbaum, N. C., & Parrinello, C. M. (2021). Validation analysis of a composite real-world mortality endpoint for patients with cancer in the United States. Health services research, 56(6), 1281-1287.

J.Anitha GracyJ. Anitha Gracy is currently a full-time Ph.D. research scholar at Anna University Chennai pursuing her research at the research center – Department of Applied Mathematics and Computational Science, Thiagarajar College of Engineering, Madurai, India since January 2023. She has rich teaching experience in Research. Her current research interest includes software engineering, information systems, and data mining.

Dr.S.Sivagurunathan Sivagurunathan is an Assistant Professor in the Department of Computer Science and Application at Gandhigram Rural Institute. He received his Ph.D. from Anna University specializing in Computer Science. His research interests include Computer Networks, Cloud Computing and IoT, and Network Security. He has completed a few projects receiving funding from the University Grants Commission (UGC) and Rajiv Gandhi National Institute of Youth Development (RGNIYD)India. He has been organizing several National level Workshops, seminars,

Dr.T.Chandrakumar Chandrakumar is an Associate Professor in the Department of Applied Mathematics and Computational Science at Thiagarajar College of Engineering. He received his Ph.D. from Anna University specializing in Computer Science. His research interests include software engineering, Analytics, Enterprise Resource Planning (ERP), and software quality. He has completed a few projects receiving funding from University Grants Commission (UGC) India. He is been regularly funded by the DST (Dept of Science and Technology), and DRDO (Defence Research Development Organization) for organizing National level Workshops and seminars. He has published more than 15 research papers in refereed conferences and journals such as Computer Standards & Interfaces (Elsevier-SCI), International Journal of Project Management (Elsevier-SCI), IJEIS of IGI-USA, IJICT, and IJBIS. He has authored 03 Book chapters in the refereed edited book of SPRINGER from Jan 2014 to date. He also serves as a reviewer for the International Journal of Project Management (Elsevier), Computer Standards and Interfaces (Elsevier), International Journal of Industrial Engineering: Theory, Applications and Practice etc. He has guided many postgraduate scholars and teaches several courses on Computer Applications and data science engineering.