AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Securing XML Web Services using enhanced Elliptic Curve Cryptographic signature for e-business transactions

[1]R. Menaka and [2]Dr. R.S.D. Wahida Banu

[1]*Research Scholar, Anna University, Coimbatore, Tamil Nadu*
[2]*Supervisor, Anna University, Coimbatore, Tamil Nadu*

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form
19 September 2014
Accepted 29 September 2014
Available online 6 November 2014

Keywords:
Extended Markup Language,
Encryption,
Enhanced ECC Signature, Key Value,
E-business Transactions, ECC Palm
Print Signature Tag, Parent Element.

ABSTRACT

Web security using Extended Markup Language (XML) has become a standard for E-business processing. Though XML Keyword Search (XML-KS) in web identifies the user search intention via node query and ranked the results of the queries in an efficient manner, but it failed to handle web security by conforming to a highly recursive schema. Personalized Ontology Model (POM-WIG) learns ontological user profiles for personalized Web Information Gathering using multidimensional ontology mining method, but failed to attain XML security on existing web documents. The XML Signature is also not covered with ECC (Elliptic Curve Cryptography) based algorithms in XML-KS. To address the problem, we present an XML based web security with key values, Enhanced ECC (XML-Enhanced ECC) mechanism in this paper. Initially, XML-Enhanced ECC allows signing in multiple tags for a specific XML document. Compound (i.e.,) multiple signature processing is carried out using the hash values of the information with the procedures, structure and processing resulting in the increased system utility ratio. The signature processing with the key values handle the web security using the high recursive schema resulting in higher precision rate. Secondly to compute the hash value for multiple signatures, Enhanced Elliptic Curve Cryptography Algorithm is developed in the encryption side. The ECC algorithm is enhanced by extracting the palm print as the primary signature information. XML-Enhanced ECC sign takes the information as the child element and XML signature group as the parent element. The information is enveloped with the "Enhanced ECC Palm print Signature Tag". Finally, Enhanced ECC Signature provide optimal element at the receiver (i.e.,) decryption side with appropriate key value that efficiently validates the signature and fetch the original information by minimizing the decryption time. XML- Enhanced ECC Sign attains improved security on web while performing e-business transactions. Web security using XML attains effective result on several metrics such as web security level, precision, recall, system utility ratio, and decryption time.

To Cite This Article: R. Menaka and Dr. R.S.D. Wahida Banu, Securing XML Web Services using enhanced Elliptic Curve Cryptographic signature for e-business transactions. ***Aust. J. Basic & Appl. Sci.,*** *8(17): 10-19, 2014*

INTRODUCTION

With the massive growth of transactions level conducted through electronic media, there is an increasing need for the development of significant support tools to enhance the degree and sophistication for the automation of E-Commerce. Though most of the conventional type of Internet-based E-Commerce was designed with the consideration of B2C, B2B the future constitutes a much larger part of the entire E-Commerce community. It is highly perceived that with the increasing amount of information available in Internet, B2B will grow continually and will become the most predominant means of doing business in the coming future.

With increasing success in the field of web, information retrieval (IR) on the web, searching keyword on XML has emerged as an interesting topic. In an IR-style method which uses the measure of XML data to provide solution for searching keyword was presented. The author initially mentioned certain amount of guidelines for search engine for identifying the search intention and ranked according to the search results. Though XML Keyword Search (XML-KS) in web identifies the user search intention via node query and ranked the results of the queries in an efficient manner, but it failed to handle web security by conforming to a highly recursive schema.

In an effective indexing method called as IR-tree, was presented that with the help of top-k document search algorithm provided four different tasks during document search including provisioning for spatial filtering, filtering of textual contents, measuring the relevance factor and ranking the document efficiently.

Corresponding Author: R. Menaka, Research Scholar, Anna University, Coimbatore, Tamil Nadu.

Though with the help of IR-tree search efficiency was achieved, search for different access patterns remained unaddressed. An integrated approach addressing semantic and nonfunctional criteria to measure the quality in web services was presented for balancing the new dimension of semantic quality and was further used as a basis for ranking and optimization criteria with an acceptable computation costs. Though computation cost was highly relied on pre-computed tasks that may result in unsatisfied goals based on the context.

Over the last decades, the amount information based on web has increased substantially. To gather the most wanted information from the web has become one of the challenging problems for the users. A novel mechanism called as the personalized ontology model was designed for representing knowledge and deriving the reason over user profiles was discussed. Personalized Ontology Model (POM-WIG) learns ontological user profiles for personalized Web Information Gathering using multidimensional ontology mining method, but failed to attain XML security on existing web documents. In an approach was presented with the main aim of applying the extraction of information in an automatic manner that was learned in prior way from a specified web site to a new site using text-related clues. Though promising performances were achieved but at the cost of time.

One of the critics observed in search engines is that whenever a user issues a query, most of the search engines return the similar type of results to the users. A large scale framework was presented for personalized search designed with the help of query logs evaluated using five personalized search algorithms that helped to increase the search accuracy. But the methods provided were not optimal. To address the problem of optimality in Web database scenario, an unsupervised framework was presented called as the online record matching method. The advantage was that given with a query, duplicates were identified in an effective form from the result of the query from multiple Web databases. Though duplicates were removed by minimizing the burden of users by increasing the precision value, the iteration level was increased with the increase in the number of queries.

A new approach based on vision was presented that was based on web-page programming and language independent. This language independent approach used the features related to visual on the deep Web pages and implemented deep Web data extraction, consisting of extraction of data record and data item for one data region. Issues related to multi-data region were not discussed.

With the increasing use of Internet, web services have resulted in communication revolution where efficient cooperation between different parties is important, i.e., in e-commerce and e-business. A framework called as the Web service discovery framework was presented which showed better performance on loading and resulted in increase of precision and recall using grouping filters for single Web services. But Web service compositions based on abstract descriptions remained an open issue.

Based on the aforementioned technique described, we focus on securing the XML web services using enhanced elliptic curve cryptographic signature by applying palm print signature elements. An elaborate description is provided in the forthcoming sections. The rest of this paper is organized as follows: The structure of our enhanced elliptic curve cryptographic signature and their service requirements with a detailed architecture are described . The design of key value generation using palm print key element is discussed. The design of the enhanced ECC signature algorithm is described. The design for experiment and results of performance evaluation are described in following section. Related work also discussed. Finally, conclusion was made.

Securing Xml Web Services Using Enhanced Elliptic Curve Cryptographic Signature:

In this section, the overall structure of securing XML web services is discussed. The goal of XML based Enhanced Elliptic Curve Cryptographic Signature mechanism is to protect the web services by implementing a signature procedure. The signature procedure improves the security on E-business transaction. The XML-Enhanced ECC Sign developed using the compound signature framework sign of multiple tags on the XML document. The XML based Enhanced ECC Signature mechanism on web services removes the malfunction, and repudiation on E-business transactions. The signature on the XML document support all type of encryption and decryption algorithm to improve the web service security level by avoiding falsification. Using XML based Enhanced ECC Signature algorithm, key values of the data are computed in an efficient manner. Compound tag signing using XML document is depicted in Figure 1.

The compound (i.e.,) multiple tag signing uses the key value to perform the structure processing and two procedures namely, key value generation procedure and key validation procedure. The structure processing analyzes the markup language in XML-Enhanced ECC Signature mechanism and passes structured information to any e-business application. Two components, Signature Method and Signature Value are used by the Enhanced ECC signature mechanism in order to store the information and to fetch the resultant value respectively**.** Followed by this, the key value generation procedure in XML-Enhanced ECC Signature mechanism provides the receiver a suitable key value to attain higher level of recursive scheme on E-business transaction.

Australian Journal of Basic and Applied Sciences, 8(17) November 2014, Pages: 10-19

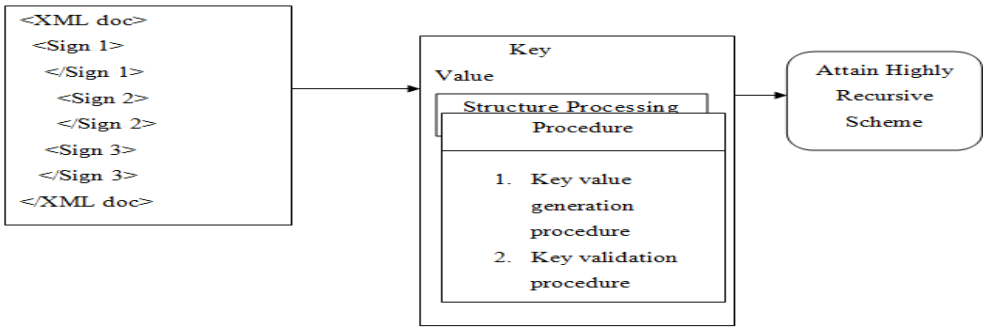

Fig. 1: Procedure of compound tag signing using XML document.

The highly recursive scheme in web services provides effective transaction for the massive volume of information which can then be employed to wide range of business fields. The multiple signed XML document provides improved security on Enhanced ECC encryption algorithm. The compound signed information from the XML document includes the signed data with specified Enhanced ECC SignatureInfo element. The SignatureInfo elements, includes two elements namely, the position element that denotes the key value position and alter element that denotes the arbitrary number of times the key value to be altered to improve the security level on E-transaction services. Followed by this using the key validation procedure, the receivers fetch the original information embedded in the XML document.

Overall Structure:

Figure 2 shows the architecture diagram of Enveloping XML based Enhanced ECC Signature (XML-Enhanced ECC Sign) mechanism for providing security to e-business transaction. It consists of the signing of multiple tags, enhanced ECC signature encryption and enhanced ECC signature decryption. Using the key values, multiple tags are signed in. Using Enhanced (Palm print) ECC Signature encryption is performed using enhanced ECC Signature encryption algorithm and the corresponding signature is validated with the help of enhanced ECC Signature decryption algorithm.

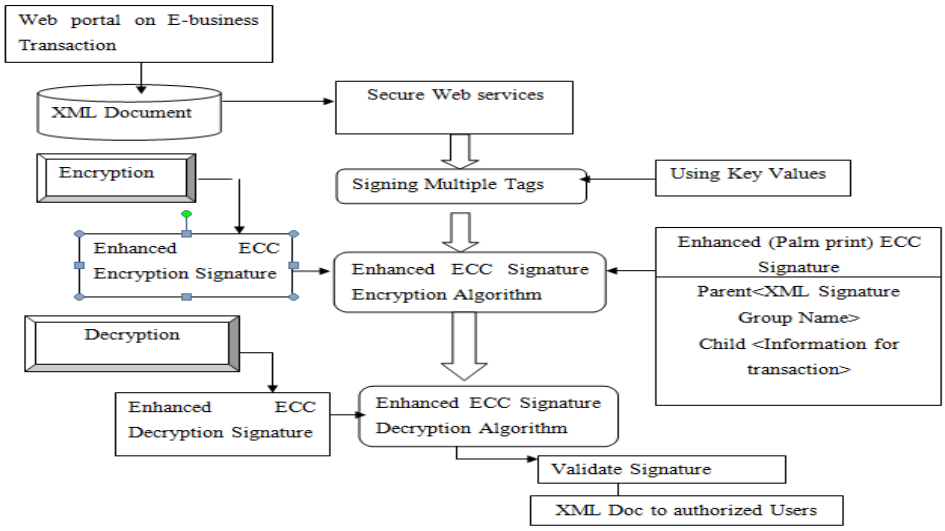

Fig. 2: Architecture diagram of XML-Enhanced ECC Sign Mechanism

As illustrated in Figure 2, the Enhanced Sign mechanism is implemented for E-business transaction. The web portal provides secure web services to the end users using the compound sign tag. The compound sign tag is developed using different key values to enhance the security factor using elliptic curves over the finite fields. The compound sign tag in the XML-Enhanced ECC Signature Mechanism is developed using the ECC Signature encryption and decryption algorithm. Palm print Signature is employed in XML with Elliptic Curve Cryptography that further enhances the ECC signature mechanism for effective validation of signature using parent and child element information. The key validation procedure helps the receivers to fetch the original information embedded in the XML document.

Australian Journal of Basic and Applied Sciences, 8(17) November 2014, Pages: 10-19

To convert the business transaction document into a comprehensible form for the unauthorized users, Enhanced ECC Signature Encryption Algorithm is employed as described in Figure 2. The input, XML document is encrypted using the Enhanced ECC Encryption signature, SignatureInfo element which provides the information to the receiver about the keying substance used to validate the signature. The authentication of signature is ensured using the Enhanced ECC Signature Decryption.

Key Value Generation:

The key value is generated by each user in XML-Enhanced ECC Sign Mechanism using individual palm print key element. The palm print key element is used to map the information with slight modifications from the input information. The key value generation procedure is represented through Figure 3.

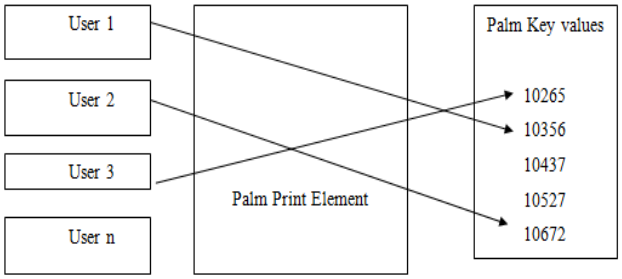

Fig. 3: Key generation Steps.

As described in Figure 3, key generation in XML-Enhanced ECC Sign Mechanism quickly performs the secure E-business transaction on web services. The key is generated with even distribution of values by the users. The key generation formula is

Key generation = (i*n)/N (1)

Eqn (1) takes the input as the integer 'i' which ranges from 0 to N-1. The value 'n' is used as the arbitrary number generators on the palm print based signature. The collision on the leading digits occurs but varies with each user key value. The key value is returned at the receiver side using the Enhanced ECC Signature Decryption algorithm. The key value generation in XML-Enhanced ECC Sign detect the duplicate users (i.e.,) malfunction users.

Enhanced ECC Signature Algorithm:

The Enhanced elliptic curves use the palm print signature in the cryptographic form to secure the web services. Prime curve points over Z_p and binary curve takes value of 2^m . The enhanced ECC is evaluated using a cubic equation that take on variables and coefficient values with a set of integers from 0 through p-1 and the computation is carried out with respect to modulo p. In order to encrypt the signature in an efficiency manner in the XML document, Enhanced ECC encryption algorithm is introduced with the generated palm print key values. The elliptic curve point is described as,

Elliptic Curve (E) = d[0,1….255] (2)

The elliptic curve point (E) generates the key using the hash functions ranging from 0 to 255. The key used for the Enhanced ECC Encryption and decryption work is carried out as,

Begin:

<XML Document>
<Parent: "Signature Group Name">
<Child: "User Information">

// Enhanced ECC Encryption Algorithm:

Step 1: Elliptic curve $E_p(x,y)$ where p is a prime number and a random elliptic curve 'E'.
Step 2: Sender keeps the random number α with cryptographic signature
Step3: G 1 and G2 as general public keys
Step 4: Computes G1 = α (E +G) and G2 = α G.

// Enhanced ECC Decryption Algorithm:

Step6: Enhanced Elliptic curve with palm signature cryptography key decrypt information
Step7: Computes I1 = β (E+I) and I2 = β I
Step 8: Selects large random number β and point I
Step9: I1 and I2 as his general public keys

Australian Journal of Basic and Applied Sciences, 8(17) November 2014, Pages: 10-19

</Child: "User Information">
</Parent: "Signature Group Name">
</XML Document>
End

Elliptic curve Ep (x,y) where p is a prime number for a random elliptic curve 'E'. The sender selects a huge arbitrary number α which is less than the order of $E_p(x, y)$ and a point G on the enhanced elliptic curve. Followed by this the sender computes G1 = α (E +G) and G2 = αG. The sender keeps the random number α with cryptographic signature and the point G as private keys and publishes G1 and G2 as general public keys.

Similarly on the other hand, receiver selects a large random number β and a point I on the enhanced elliptic curve. The receiver side evaluates I1 = β (E+I) and I2 = β I. Followed by this the receiver keeps the random number β and the point I as private keys and publishes I1 and I2 as his general public keys. After publishing the public keys, the enhanced elliptic curve cryptography calculates the following palm print signature in XML tag. The signature on decryption side helps to secure the web service on the XML document.

Enhanced ECC Encryption Algorithm:

The enhanced ECC encryption algorithm flows in such a way that the message is encrypted using the enhanced elliptic curve points. The elliptic curve points (e1e2) is described as

e1=αE and e2=Information (α+β)G1-αG1 (3)

Elliptic curve points (e1, e2) with random point values 'α' and 'β' send the pair of points to the decryption side for securing the web services.

Enhanced ECC Decryption Algorithm:

The decryption work is carried out in the receiver side using the encrypted XML document. The receiver removes the original information from the encrypted side using the public key component. The decrypted form in XML-Enhanced ECC Sign is described as,

Information =e2-(α(e1)+β(I1)) (4)

After receiving the information in Eqn (4), security rate is improved on using the palm print signature based elliptic curve points. The enhanced elliptic curve clearly describes the decryption process using large random points and hash key values.

Experimental evaluation:

The proposed XML based Enhanced ECC (XML-Enhanced ECC Sign) mechanism for securing the web services is implemented in JAVA platform. The Amazon Access Samples Data Set from UCI repository is taken as the input value to analyze the security on web. The dataset used for analyzing the web services consists of 30000 instances with 20000 attribute values. The information related to the business is clearly defined in the Amazon Access Samples Data Set, and as a result the parametric factors are easily determined.

XML-Enhanced ECC Sign compares the result against the Existing XML Keyword Search (XML-KS) and Personalized Ontology model for web information gathering (POM-WIG). The experiment is conducted on the factors such as web security level, system utility ratio, Decryption time, Precision and Recall.

The system utility ratio (SUR) defines the ratio of XML document with the signed data to the effective retrieval of XML doc to authorized users measured in terms of %.

$$SUR = \frac{(\text{No.of XMLDoc- Retrieval Rate of XMLDoc})}{\text{No. of XMLDoc}} \quad (5)$$

Decryption time using Enhanced ECC Signature mechanism is the time taken to respond to the web portal on E-business transaction measured in terms of milliseconds.

$$DT = Time\ (Enhanced\ ECC\ Decryption + CPU\ time) \quad (6)$$

Let us consider an Amazon Access Samples Data Set with 30000 instances. The Recall value (as shown in eqn (7)) based on Enhanced ECC Signature mechanism measures the number of relevant XML doc retrieved to the total number of relevant XML doc. It is expressed in terms of percentage (%).

The precision value based on Enhanced ECC Signature mechanism is the ratio of retrieved XML doc that is relevant (as shown in eqn (8)). Let XMLR represents the relevant XML doc retrieved, XMLNR denotes the relevant XML doc not retrieved and XMLIRR denotes the irrelevant XML documents retrieved, the recall value and precision value is given as below in (7) and (8)

$$RV = \frac{XMLR}{(XMLR + XMLNR])} * 100 \quad (7)$$

$$PRV = \frac{XMLR}{(XMLR + XMLIR)} * 100 \quad (8)$$

Result analysis of xml-enhanced ecc sign mechanism:

The XML-Enhanced ECC Sign mechanism is compared against the existing XML Keyword Search (XML-KS) and Personalized Ontology model for web information gathering (POM-WIG). The experimental results using JAVA are compared and analyzed through table and graph form given below. To support transient performance, in Table 1 we apply an efficient ECC sign mechanism to obtain the system utility ratio and comparison made with two other existing methods XML-KS and POM-WIG

Table 1: Tabulation for System Utility Ratio.

Document Size (MB)	System Utility Ratio (%)		
	XML-Enhanced Sign mechanism	XML-KS	POM-WIG
5	65	60	58
10	68	66	63
15	72	70	65
20	70	69	64
25	74	71	67
30	78	74	70
35	80	77	71
40	79	78	73

Table 2: Tabulation for Decryption Time.

Document Size (MB)	Decryption Time (ms)		
	XML-Enhanced Sign mechanism	XML-KS	POM-WIG
5	45	48	51
10	50	53	54
15	52	55	58
20	51	54	52
25	55	59	64
30	58	63	67
35	62	65	69
40	64	70	72

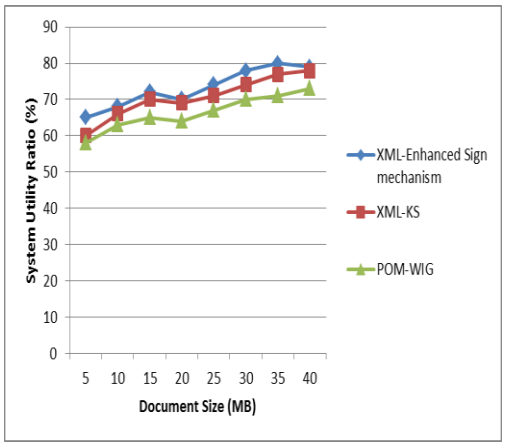

Fig. 4: Document Size versus System Utility Ratio.

Figure 4 show that the proposed XM-Enhanced Sign mechanism provides higher system utility ratio when compared to XML-KS and POW-WIG . This is because of the application of compound signature processing carried out using the hash values with the help of two components Signature Method and Signature Value resulting in the increased system utility ratio by 2 – 7 % when compared to XML-KS. In addition to that with the use of the appropriate key value, the signature is validated and fetches the original information by increasing the system utility ratio by 7 – 12 % than the POM-WIG.

The comparison of decryption time is presented in table 2 with respect to the XML documents in the range of 5 – 40 MB. With increase in the size of the XML document, the decryption time is also increased.

Australian Journal of Basic and Applied Sciences, 8(17) November 2014, Pages: 10-19

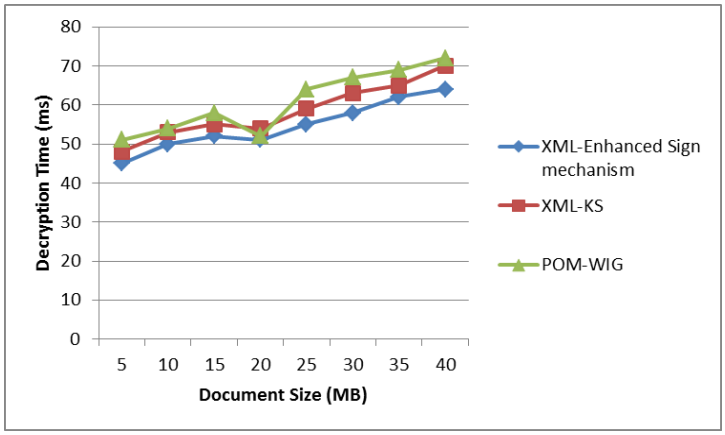

Fig. 5: Document Size versus Decryption Time.

To ascertain the performance of the decryption time, comparison is made with two other existing works XML Keyword Search (XML-KS) and Personalized Ontology Model for web information gathering (POM-WIG) . In figure 5, the document sizes are varied between 5 and 40. From the figure it is illustrative that the decryption time is lesser using the proposed XML-Enhanced Sign mechanism when compared to the two other existing works. This is because with the application of Enhanced ECC Signature the documents are retrieved accurately by minimizing the decryption time by 4 – 9 % when compared to XML-KS . Furthermore, by providing optimal element at the receiving side, with the help of the public key, the time taken to decryption is minimized by GDDND model by 8 – 16 % than when compared to POM-WGI .

The precision value for XML-Enhanced Sign mechanism is elaborated in table 3. We consider the model with a document size of 40 MR for experimental purpose using JAVA.

Table 4: Tabulation for Recall.

Document Size (MB)	Recall (%)		
	XML-Enhanced Sign mechanism	XML-KS	POM-WIG
5	74	69	65
10	70	68	64
15	68	66	63
20	72	67	65
25	63	60	58
30	58	55	53
35	56	54	48
40	63	52	46

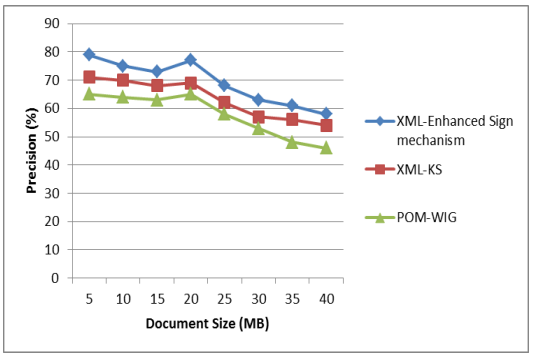

Fig. 6: Document Size versus Precision.

In figure 6, we depict the precision value attained using the document of size 5 to 40 MB for the purpose of experiment. From the figure, the value of precision achieved using the proposed XML-Enhanced Sign mechanism is higher when compared to two other existing works XML

Keyword Search (XML-KS) and Personalized Ontology Model for web information gathering (POM-WIG). Besides we can also observe that by increasing the size of the document, the precision value is decreased using all the methods. But comparatively, it is higher in XML-Enhanced Sign mechanism because with the signature processing, the key values handle the web security using the high recursive schema resulting in higher precision rate by 6 – 10 % than XML-KS . In addition, with the application of Palm print key element, quickly

performs the E-business transactions on web services using arbitrary number generators on the palm print based signature. As a result, the precision value is improved by 14 – 21 % than compared to the POM-WIG .

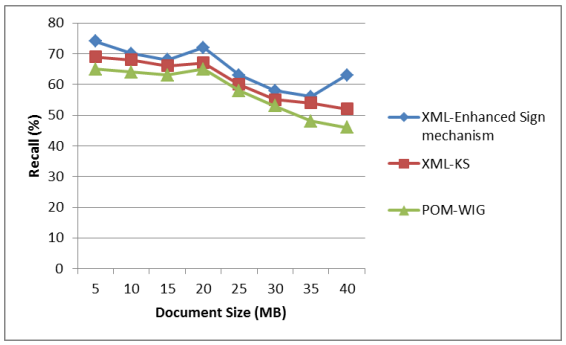

Fig. 7: Document Size versus Recall.

Table 4 and Figure 7 illustrate the recall value versus the XML document of size measured in terms of MB for experimental purpose conducted using JAVA. From the figure we can note that the recall value attains 4.76 % improved for an XML document size of 25 MB when compared to XML-KS and 7.93 % improved when compared to

POM-WIG which shows that there is a significant gain using the proposed XML-Enhanced Sign mechanism. This is because, Prime curve point over Z_p and binary curves takes the value of 2^m using a cubic equation that take on variables and coefficient values with a set of integers from 0 through p-1 and increases the recall value by 3 - `17 % when compared to XML-KS. Further using XML-Enhanced Sign mechanism, with the generated palm print key values the elliptic curve point (E) generates the key using the hash functions ranging from 0 to 255 and improves the recall value deployment by 7 – 26 % when compared to POM-WIG.

Related works:

The World Wide Web comprises of massive amounts of data. But with the increasing amount of information, benefit cannot be attained using the raw web pages until the information is extracted properly and organized in a well manner. A novel framework presented was called as the WebNLP, that enabled integration of page in bidirectional manner and a deep understanding of text in an iterative manner. But the complexity involved during bidirectional access was high. A cross-layer security mechanism was introduced for better communication and providing authentication, integrity using XML Encryption and Signature and enhanced the security level at the cost of complexity during computation.

Using XML technique in web has become the standard of e-Business services. This is because of the fact that many companies post their financial statements that consists of disclosure of balance sheet, detailed statements of profit and loss, and so on. Web Services security was applied, than the traditional transport-level security and resulted in enhanced level of security, providing integrity and confidentiality in extensible business reporting language documents that were encoded by SOAP. Though security was provided, the encryption algorithm followed was a time consuming process and attack related issues were not discussed.

We security testing methods were introduced called as, Web Services security (WSSecurity) and Security Tokens were introduced to identify the access control level of the sender for the SOAP messages being exchanged with new vulnerabilities being unaddressed. A new standard was introduced to address the new vulnerabilities by introducing a gateway both at the client side and at the server side to provide counter attacks introduced due to WS-Security standards as well as other attacks. Hardened SOAP schema was introduced for validating both the requestor and provider and assured of security, but composite services remain unaddressed.

With higher amount of XML data exchanged between the customers in business, there is an increasing requirement for significant query processing using XML data. The massive amount of XML tree pattern were explored and referred to as the extended XML tree pattern to demonstrate the method effectiveness. Context-aware systems, for web services were designed that interacted with different users and provided access rights, security and privacy of information to the end users. But with the rapid behavioral change of the users, predication based context-aware systems remain unaddressed.

The web service methodology is an important instance of the Simple Object Access paradigm. A matching based on conceptual indexation was designed to exploit the service interface and domain ontology, with the main objective of indexing the web services. Also, the method evaluated similarity score amongst the request placed by the user and the web services that were indexed using cosine measure with less efforts made on security.

An effective model was presented for providing securing by way of introducing the access control list for each web services and the consumers of web services were provided with high level authentication. In addition a trust based model was introduced that provided a fair exchange between the web service producers and web services consumer by enhancing the level of security. Though communication time was reduced, but sufficient certification authority was unaddressed.

A two-phase was designed that were used for building services for web from existing web applications. The two phases were, namely abstraction phase that extracted UML conceptual schema and an implementation phase that generated JAVA code of web service from the UML using the rules of mapping using static abstraction. Dynamic aspect of web service construction remained an open issue.

Conclusion:

An XML based web security with key values, have been designed to attain XML security on web documents and to increase the system utility ratio using the hash values of the information with the procedures, structure and key value generation and validation processing. We adopt Enhanced Elliptic Curve Cryptography Algorithm, design a high recursive schema with the key values handle the web security and propose an Enhanced ECC Palm print Signature Tag which attains improved security on web while performing e-business. The proposed ECC Encryption and Decryption algorithm is adaptive because of the introduction of prime number and a random elliptic curve 'E' during encryption and Enhanced Elliptic curve with palm signature cryptography key during decryption. In addition, Enhanced elliptic curves use the palm print signature in the cryptographic form to secure the web services which in turn increases the security. Experimental evaluation is conducted with the Amazon Access Samples Data Set extracted from UCI repository to analyze the security on the web and measured the performance in terms of system utility ratio, decryption time, precision and recall. Performances results reveal that the proposed XML-Enhanced Sign mechanism provides higher level of precision and accuracy and also strengthen security by consuming less decryption time for E-business transactions. Compared to the existing XML based web security, the proposed XML-Enhanced Sign mechanism 21% high in precision and system utility ratio by 12 % compared to state-of-art works.

REFERENCES

Bouchiha Djelloul, Malki Mimoun and Mostefai Abd El Kader, 2009. Towards Reengineering Web Applications to Web Services, The International Arab Journal Of Information Technology, 6(4).

Chunyu Yang, Yong Cao, Zaiqing Nie, Jie Zhou and Ji-Rong Wen, 2010. Closing the Loop in Webpage Understanding, IEEE Transactions on Knowledge and Data Engineering, 22(5).

Freddy Lecue and Nikolay Mehan, 2011. Seeking Quality of Web Service Composition in a Semantic Dimension", IEEE Transactions on Knowledge and Data Engineering, 23(6).

Georgios Meditskos and Nick Bassiliades, 2010. Structural and Role-Oriented Web Service Discovery with Taxonomies in OWL-S, IEEE Transactions on Knowledge and Data Engineering, 22(2).

Hadjila Fethallah, Chikh Mohammed, 2013. Automated Retrieval of Semantic Web Services: A Matching Based on Conceptual Indexation, The International Arab Journal Of Information Technology, 10(1).

Jiaheng Lu, Tok Wang Ling, Zhifeng Bao and Chen Wang, 2011. Extended XML Tree Pattern Matching: Theories and Algorithms, IEEE Transactions On Knowledge And Data Engineering, 23(3).

JunWu, Ming Zhan, Bin Duan and Jiang Liu, 2013. A Cross-Layer Security Scheme of Web-Services-Based Communications for IEEE 1451 Sensor and Actuator Networks, International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation.

Nayat Sánchez-Pi, Javier Carbó, José Manuel Molina, 2012. A knowledge-based system approach for a context-aware system, Knowledge-Based Systems, Elsevier.

Priyadharshini, M., I. Suganya, N. Saravanan, 2013. A Security Gateway for Message exchange in Services by Streaming and Validation, International Journal of Innovative Research in Computer and Communication Engineering 1(3).

Salas, M.I.P., E. Martins, 2014. Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security, Electronic Notes in Theoretical Computer Science, Elsevier.

Sawsan Abu-Taleb and Hossam Mustafa, 2010. Improving Web Services Security Models, The International Arab Journal Of Information Technology, 7(4).

Sun Park1, Seung-Jung Shin, 2013. WS Security of XBRL Financial Documents Encoded by SOAP, International Journal of Security and Its Applications, 7(4).

Tak-Lam Wong and Wai Lam, 2010. Learning to Adapt Web Information Extraction Knowledge and Discovering New Attributes via a Bayesian Approach, IEEE Transactions on Knowledge and Data Engineering, 22(4).

Wei Liu, Xiaofeng Meng and Weiyi Meng, 2010. ViDE: A Vision-Based Approach for Deep Web Data Extraction. IEEE Transactions on Knowledge and Data Engineering, 22(3).

Weifeng Su, Jiying Wang and H. Frederick Lochovsky, 2010. Record Matching over Query Results from Multiple Web Databases, IEEE Transactions On Knowledge And Data Engineering, (22)4.

Xiaohui, Tao, Li. Yuefeng and Ning Zhong, 2011. A Personalized Ontology Model for Web Information Gathering, IEEE Transactions on Knowledge and Data Engineering, 23(4).

Zhicheng Dou, Ruihua Song, Ji-Rong Wen and Xiaojie Yuan, 2009. Evaluating the Effectiveness of Personalized Web Search, IEEE Transactions On Knowledge And Data Engineering, 21(8).

Zhifeng Bao., Lu. Jiaheng, Tok Wang Ling and Bo Chen, 2010. Towards an Effective XML Keyword Search, IEEE Transactions on Knowledge and Data Engineering, 22(8).

Zhisheng Li, Ken C.K. Lee, Baihua Zheng, Wang-Chien Lee, Dik Lun Lee and Xufa Wang, 2011. IR-Tree: An Efficient Index for Geographic Document Search, IEEE Transactions on Knowledge and Data Engineering, 23(4).