Indian Journal of Science and Technology, *Vol 9(16), DOI: 10.17485/ijst/2016/v9i16/87966, April 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Survey on Signatured Xml Encryption for Multi-Tier Web Services Security

R. Menaka[1*], R. S. D. Wahida Banu[2] and B. Ashadevi[3]

[1]Anna University, Sarder Patel Road, Old Highways Building, Guindy, Chennai - 600 025, Tamil Nadu, India; menaka,murugesan@gmail.com
[2]GEC, NH 7, Banglore Highways, Salem - 636011, Tamil Nadu, India; rsdwb@yahoo.com
[3]CS Department, Kunthavai Nachiar Govt. Arts College for Women, Arulananda Nagar West Extension, Thanjavur - 613007, Tamil Nadu, India; asharajish2005@gmail.com

Abstract

Web service is the technology tied up with SOAP, UDDI and WSDL of XML format, so web services searching based on XML keyword become essential. By systematic monitoring it has been observed that internet communication is less protected than intranet communication. The transaction exchange held through internet in web which is one among the distributed application is embodied to different vulnerability. In distributed environment, messages and data are exchanged as Extensible Markup Language (XML) format for its vast compatibility in transit. For facing the competitive environment, any business teams have to find their suitable web services among the bulk services prevails in market. In apt to this, survey has been made with different searching techniques and way to boost the security container filled with access permitted service alone. Our research work on XML based Web security is concentrated on providing the privacy, certification and integrity. We investigate the way to regulate and insist the security by applying XML Encryption and Signature for data or messages in transaction and in storage form. It also proves the performance improvement in searching data from vast resources, if so security constraint is provided. Search Engines Optimization (SEO) is enhanced with parsing the descriptive tags rather than chaos data. Traders need not have prior knowledge of web farms lifecycle and its protection.

Keywords: BPEL, Multi-Tier Security, User Satisfy Profile, Web Service, XML Cryptography

1. Introduction

Web Services (WS) employ XML as in-between or intermediary medium to portray any dealing with commercial activities and interaction among their entities. Web services are used as an established model for crafting and recognizing cooperation among corporate and sharing utilities inside and across organizational boundaries. The web application of any cast of functionalities once deployed and made accessible through internet standard are summarized, collected or stored in the form of web services.

Web Security obstructs the web threats to decrease the malware assaults, helpdesk clashes and free up esteemed IT resources. The great feat of web search engine uses keyword searching approach which is the most popular search model for ordinary users in olden and recent days. As XML is standard in data representation, it is desirable to maintain keyword search in XML database. It is one of the end-user friendly ways to query XML databases, which allows users to trigger queries without the familiarity of complex query languages and the database scheme.

The XML security enforces the system design with authorization and tie up trust diplomacy capability such that emphasizing the architectural design and cooperation enforcement aspects meeting the tight security needs.

When XML encryption is employed, an encryption algorithm runs against the part of the XML document to be encrypted and XML data is restored with the resultant encrypted data inside an encrypted data element.

**Author for correspondence*

WS-Security based on XML Encryption constructs is employed in a SOAP message. The location of the resultant encrypted data element is taken from the security header element. If many elements in the body of the message are encrypted, then each is positioned by an individual referenced Data element in the reference list. In an encrypted data element, the key used for encryption is specified in the Key Info element and the encryption algorithm in the Encryption Method element. The Key Info element is indicated in the XML Signature element.

This paper work is organized as follows: Section 2 discusses the drawbacks on existing XML based web resources. Section 3 shows the study and analysis of the existing XML usage in different variant, Section 4 shows the evaluation for performance metrics and Section 5 concludes the key areas of research that make user to think of XML based security to provide the privacy, certification and integrity.

2. Related Works

Web Services depends on the standard transport protocol HTTP and the essential web architecture. It is susceptible to harsh threats and vulnerabilities. Web Service Security (WS-Security) is a flexible and feature-rich extension to SOAP protocol to provide security to web services. Identity-based Cryptography (IBC) as demonstrated in inherits [1]Identity-based Key Infrastructure for Grid (IKIG) properties. An identity-based technique offers grid security architecture but does not explain the syntax and processing of XML signatures. [2]Personalized ontology model as described and discovered ontological user profiles but failed to meet the XML security on existing web documents.

Existing XML keyword search in web categorized the user search intention via node query. [3]XML Keyword Search met the intention of exact searching identification and concerned with ranking relevant searching results, but failed to handle web security up to mark. XML Signature based on RSA exists in XML Keyword Search. [9]Security framework imposes the multiple trust negotiations for decision-making but fails to extend the access control with the XML Semantic Access Control (SAC) model. Data as a service and Software as a service in web, fit for analytic functions for representing utility ratio but XML web security is not addressed at the outset of the outsourcing activity[4].

Coordination protocols on Business Process Execution Language (BPEL) identify and oversee transaction dependencies among a cluster of activities. But BPEL is not effective in controlling the right granularity and the dependencies between the operations[5]. Dual optimization approaches using the Satisfy User Profiles (SUP) algorithm[6] identified the best candidate chronon. High degree of satisfaction provided to the users with fast processing but failed to discuss about the web service security system. With help of XML Signature, guarantees the data integrity with user authentication. To analyze the complexity, insertion and deletion algorithm is constructed in 2-Hop Labeling graph[7], but XML encryption is not offered for enhancing the security level. Service Mining with BPEL[8] offered one-dimensional reporting and dashboard functionalities. Service mining is concerned with discovering web service behavior, but not confirm the web security. Trust negotiation[9] based security framework controls the secured and trusted communication among business user applications and the Entity Name System (ENS). Access control mechanisms of the COM+ architecture[10] inspected the configuration setting for security on a particular connection with an out-an-process object but never specify exactly with the XML key values.

3. Signatured XML Encryption for Multi-tier Web Services Security

With its interoperability and simplicity of utilization, standard version blocks the XML web services. This threatens limit the vast adoption of the technology across company boundaries that lack in confidentiality and integrity services. By this identification, efforts are taken to create a standardized security framework for XML Web Services. XML Web Service application is fabricated on similar setup as traditional web applications.

3.1 Web Information Gathering using Personalized Ontology Model

Data are collected in the form of resources in the web and accessed through internet. Accessing information apt to the user needs and desire is essential. One of the source through which the user need can come to forefront is through preparing profile for that user. The profiles are created from observation of the user's area of interest or willing when he surf or share in distributed environment. The result of this grasping concept identifies the users

skill base. [2]Ontology is the context of information or semantic of the content. Any word can be expressed with different context. That different pattern that represents the similar meaning can be called as semantic. The profile representing the skill set of user in semantic base can be named as personalized ontologies. An amass details of user includes his desktop information and user's native Instance Repository or Local Instance Repository (LIR). Thus, this paper introduce the construction of personalized perception model of user based on ontology and analysis of multidimensional ontology mining method. Apart from ontology thought, accessing user profiles securely is an important for attaining privacy of users.

3.2 Towards an Effective XML Keyword Search

Information retrieval is one that grasps the resources in response to query. Query framed by coining the keyword apt to our search intention. [3]Information retrieval (IR) style followed the same pattern of search but data or a resource is represented in XML form. As data representation changed, data source from where the data is retrieved is also changed from text database to XML database. The searching from XML database identify three significance such as ascertaining the surfer intention, i.e., keyword match with tag on XML node types, finalize keyword uncertain difficulties like searching keyword may exist in tag name or value of node element and the searching keyword may found in depth toward interior node. To face these challenges, IR model design novel XML based searching strategy that rank all possible intention related resources is presented on outsource scene. Examined the relevant search but lack in data safety.

3.3 Data Security Services, Solutions and Standards for Outsourcing

Web Services are significant class of knowledge emerged for the on-demand needs. The need of resources granting software like operating systems, application package, mobile apps, editor, network pack and file systems as a whole are expected for building new trade and software supporting new methods, approach and technology to control large and dynamic data repositories are invited by industrialist. For creating virtual software bed on the fly, software-as-a-service (SaaS) had been introduced. In [4]SaaS architecture, software providers warrant their applications to service requestor customers on demand based.

Service-Oriented Architectures (SOAs) offer service as software is named as SaaS which makes investment cost of new business establishments cheap and best option for any entrepreneur. SOA based web farm grant the application or software as services throughout this competitive world. Data needed for operation for enterprises are bumped in front of them as service from outsource. If a data management process is our need, it opt data management as service. These outsourced various functions may make its security critical where the data may fall to the wrong persons. It is essential to employ the security approaches for guarantee the confidentiality in data and the privacy for the connected individual entity.

3.4 Transaction Management in Service-Oriented Systems: Requirements and Proposal

Remote independent and inter-operability make any application prototypical to get growth over the world wide network. Service oriented computing (SOC) establish composition and coordination of sub task on the fly to formulate a complete business task. Normally the transaction operation held in database management system prepared to satisfy the ACID properties, but this may not be true if the transaction invoke remote instances from the diverse domain. So, the proposed method highlights the transaction management in SOC using Business Process Execution Language (BPEL). BPEL ties up the business logic with transcation.in form of integration and composition. The composition capability carried out especially by the guidance of transaction policy incorporated within it, but this setup needs to implant policy for safer composition of remote instances.

3.5 Targeted Online Data Delivery

There exists a major challenge for delivering data in online from the wide area network which covers the diverse data sources and vast web services. It is surveyed to note the demand changes between the execution intervals for analyzing the client or customer requirement. Data delivering demand ratio is small, online site User profiles, server notifications, and monitoring are studied and execution intervals are generated from user profiles. The attention is turned towards the formal definition of a schedule and the effectiveness of probing. A new case study using RSS[6] described where the popular designs for publishing information summaries on the web are carried

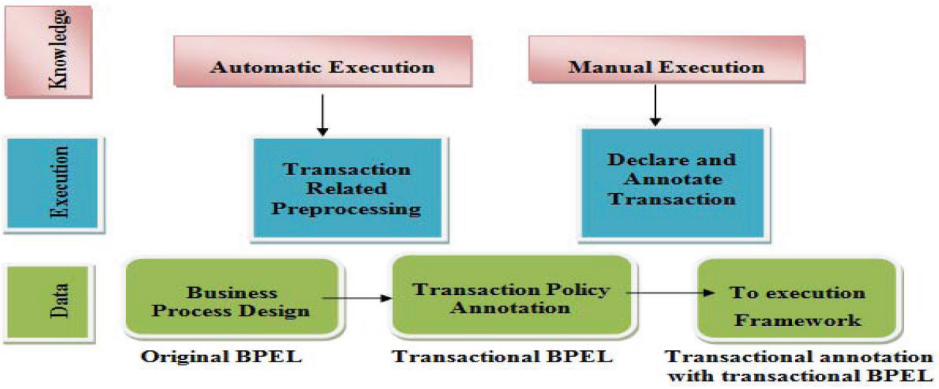

Figure 1. Integrating Transcation into BPEL process.

out. Diverse data types are the publications in RSS with news, weather updates, blog postings, media postings, Digital catalog notifications, promotions, white papers and software updates.

The application of RSS feeds is maintained by a pull-based protocol. RSS customization is offered using specialized RSS readers. A user of a reader modifies the profile by identifying the rate of monitoring each RSS feed.

3.6 Service Mining using Process Mining to Discover, Check, and Improve Service Behavior

Web services are the unit of business process or web application deployment. A web service integrates the task or business process exists across the enterprises with help of WS-Extension like WS-Business Activities, WS-Orchestrations, WS-Choreography and WS-Collaboration. [8]In service oriented approach, the more complex system is decomposed in to loosely coupled process in independent manner. These pieces run at anywhere in remote. System saves all the events in the event log along with interaction relation. Examining the logs details the services behavior is evaluated. These process is called as service mining. This offer a new form to grasp, monitoring and improve real entity like process, module and object that exists across the country and integrate to perform the complete specific business processing or transaction task.

3.7 On Incremental Maintenance of Semantic Web Represented as Graphs

The current usage on web to share the resources depends upon the technology like SOAP, a WSDL protocol that depends upon XML. XML based web ontology and semantic web forcing to adapt the interest in graph structured database. The relational database allows the operation like creating, inserting, updating and deleting the table or data in the form of SQL query. But the basic operation allowed in [7]graph structured database is to trace the reachability nodes. Graph structures database is represented by directed Graph denoted as G(V,E). The node represented as V is linked with a Label L that have two lists of node Listin(V) and List out(V). Both list combined to call as 2-hop labels. Here the proposed heuristic functions uses cut vertex or minimum graph bisection to produce node separation property that leads to incremental maintenance algorithm. However, the work have motivated to enhance the optimization while searching the data in nodes or tag of XML document but still lacks on privacy and integrity.

3.8 ANSI RBAC Support in COM+

The person working with computer may be surfing, chatting, mailing, hacking, updating and eavesdropping through their own compactible browser. He get into and able to access the restricted resources through login module if he has recognition to do so. Ability to access resources can be granted under pay or free mode. Either way makes an assurance of resource level utilization based on role he possesses. Depends upon the role he possess the suitable permission are granted in [10]Role-based Access Control (RBAC) systems. A role is expertise with specific tasks and responsibility. The objective of RBAC is to support review and control access management. RBAC is accepted as prevailing access control model approved by American National Standard for

Information Technology in 2004 and known as ANSI RBAC. This model is suitable for enterprise comprises diverse cooperating community. This diverse community coordinated successfully in open access by adoption of middleware technology. Examples for middleware is CORBA that define the access control based on user's characteristics, essential, and admitted rights and in EJB controls are defined apt to his role planning and systematic life cycle. In COM+, the role plays by grouping the user having the identical permission to retrieve services for load balancing and distributed transcation. The COM+ has its own semantics for providing protection schema to upkeep ANSI RBAC. The ANSI RBAC provides the categories of function like creating and maintaining of role sets and mapping, assigning role and users and creating session, activating and deactivating role. CORBA, COM+ and EJB are request oriented one whereas ANSI RBAC COM+ is session based. Even though COM+ support short fall of ANSI RBAC, COM+ is better than CORBA and EJB. Lack to support session specific operation, CORBA and EJB not suit for real world distributed application, But COM+ with the support of ANSI RBAC, suit for real world distributed application.

3.9 3.9 Histogram of Gradients (HOG) Method

Information generally can be retrieved either using text, images or voice. For retrieving the information through image like the hand drawn sketches of any objects, it is proposed to use the method Histogram of Gradients (HOG) method based on entropy. Entropy[11] defined the statistical measure of the randomness that gives the object content present in the image. In this entropy based methods, we follow three steps (i) Computation of gradient after partitioning the images in to blocks (ii) Orientation Binning and prioritizing (iii) Fast nearest neighbour calculations. The estimated results produce the improvement of retrieval for image.

3.10 Hybrid Approach for Extraction

Information retrieved through the web pages is adopted either by supervised or unsupervised learning. More irrelevant data is retrieved while retrieving information by unsupervised. The proposed Hybrid Approach[12] for Extraction methods mines the relevant data and removes the duplicated data.

4. Comparison of Signatured XML Encryption for Multi-tier Web Services Security & Suggestions

Various parameters are taken to evaluate performance ratio to study the privacy level, integrity of the signatured XML encryption for multi-tier web services security.

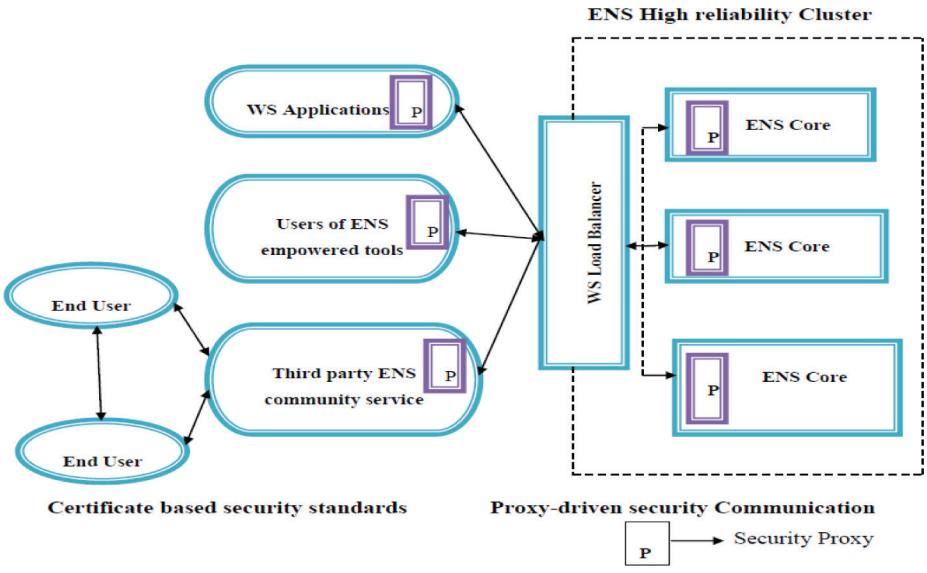

Figure 2. OKKAM security architecture and communications.

4.1 System Utility Rate

System utility rate refers to the effectiveness to measure the number of attacks prevented through segregated linear decision rule. The System Utility Rate takes place on existing Effective XML Keyword Search, Personalized Ontology Model and ANSI Role-Based Access Control (RBAC) Support. Figure 3 describes the system utility rate. As the number of user's increases, system utility rate also increases automatically. The experiment as per value in Table 1 shows that greatly Personalized Ontology Model lifts up the system utility rate when compared with Effective XML Keyword Search and ANSI RBAC support. Research in system utility rate of Personalized Ontology Model is 25-31 % higher when compared with the effective XML Keyword Search and 15-20 % higher when compared with the ANSI Role-Based Access Control (RBAC) Support.

Table 1. Tabulation for System Utility Rate on Signatured XML Encryption

Number of Users (Number)	System Utility Rate (%)		
	Effective XML Keyword Search	POM	ANSI RBAC Support
10	45	65	50
20	49	69	53
30	51	72	56
40	54	75	59
50	56	78	61
60	58	82	65
70	60	85	69

4.2 Execution Time

Execution time is measured as the amount of time taken to complete the data delivery task in milliseconds. The execution time compared with existing Targeted Online Data Delivery, Service Mining using Process Mining and Transaction Management in Service-Oriented Systems (TMSOS). Figure 4 describes the execution time compared with other as tabulated in Table 2. The experiment shows that greatly Transaction Management in Service-Oriented Systems reduces the execution time when compared with Targeted Online Data Delivery and Service Mining using Process Mining. Research in execution time of Transaction Management in Service-Oriented Systems is 16–25 % lesser when compared with the Targeted

Table 2. Tabulation for Execution Time on Signatured XML Encryption

Number of Users (Number)	Execution Time (ms)		
	TMSOS	Targeted Online Data Delivery	Service Mining using Process Mining
10	25	31	38
20	28	34	42
30	32	37	45
40	35	43	49
50	39	47	52
60	43	51	56
70	47	55	61

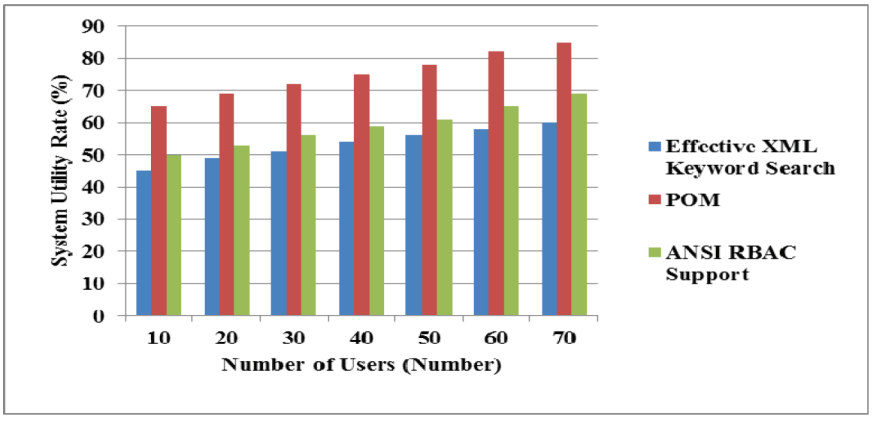

Figure 3. System Utility Rate on Signatured XML Encryption.

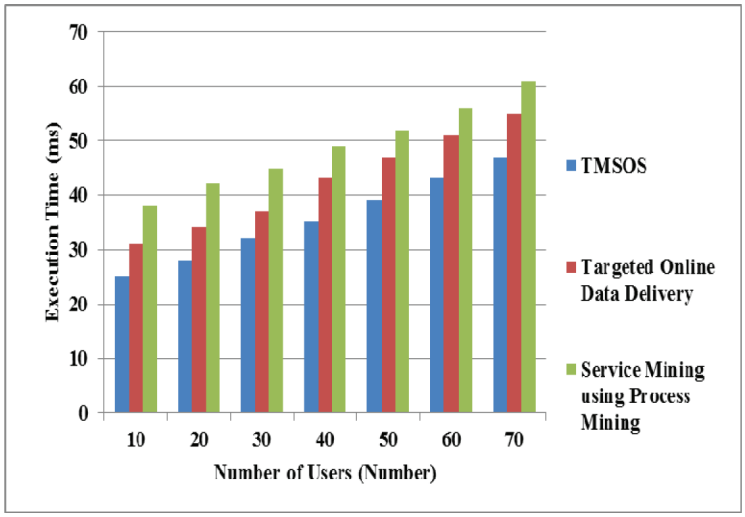

Figure 4. Execution Time on Signatured XML Encryption.

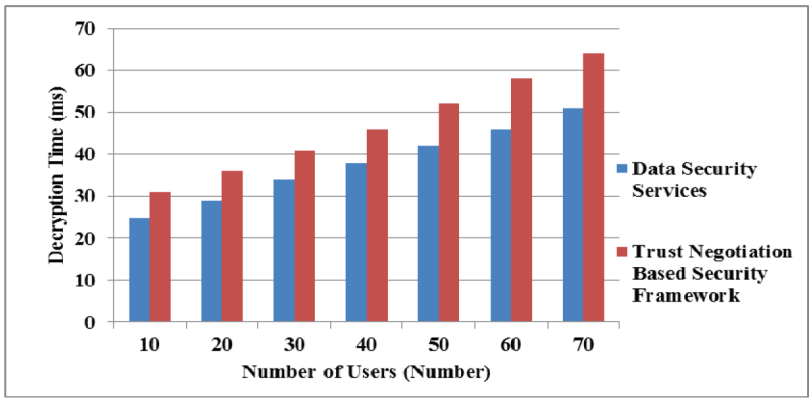

Figure 5. Decryption Time on Signatured XML Encryption.

Online Data Delivery and 28-52 % lesser when compared with the Service Mining using Process Mining.

4.3 Decryption Time

Decryption time specify the time taken to decrypt the documents received from the source by using the decryption key in milliseconds (ms). The decryption time compared with the existing Data Security Services and Trust Negotiation Based Security Framework. Figure 5 describes the system utility rate using Table 3 based on the Signatured XML Encryption compared with other mechanism. As the number of user's increases, system utility rate also increases automatically.

The experiment shows that greatly Data Security Services reduces the decryption time when compared with Trust Negotiation Based Security Framework. Research in decryption time of Data Security Services is 13–25 % lesser when compared with the Targeted Online Data Delivery.

4.4 Web Security Level

Web security level is of the level at which the data is successfully delivered to the destination point. The web security level comparison takes place on existing Targeted Online Data Delivery, Service Mining using Process Mining and Transaction Management in Service-Oriented Systems (TMSOS).

Figure 6 describes the web security level using the value in Table 4. The experiment shows that greatly Targeted Online Data Delivery has higher security when

Table 3. Tabulation for Decryption Time on Signatured XML Encryption

Number of Users (Number)	Decryption Time (ms)	
	Data Security Services	Trust Negotiation Based Security Framework
10	25	31
20	29	36
30	34	41
40	38	46
50	42	52
60	46	58
70	51	64

Table 4. Tabulation for Web Security on Signatured XML Encryption

No of users	Web Security Level (%)		
	TMSOS	Targeted Online Data Delivery	Service Mining using Process Mining
10	51	65	56
20	54	68	59
30	57	72	63
40	61	75	65
50	65	78	68
60	68	81	72
70	71	85	75

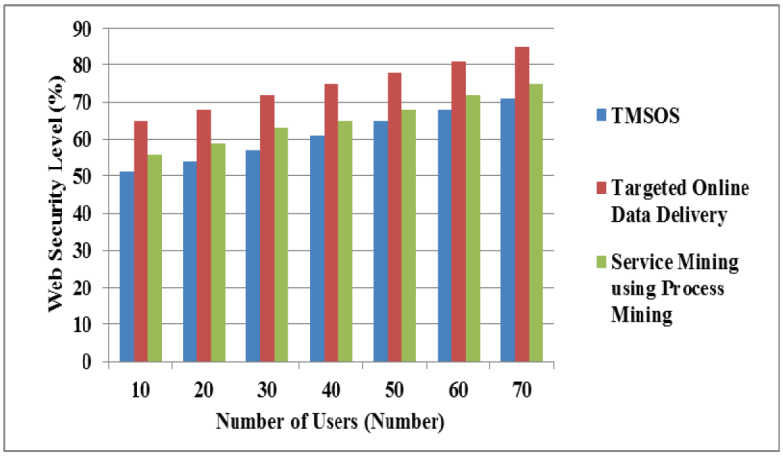

Figure 6. Web Security Level on Signatured XML Encryption.

compared with Transaction Management in Service-Oriented Systems (TMSOS) and Service Mining using Process Mining. Research in Targeted Online Data Delivery is 14–16 % highly secured when compared with the Transaction Management in Service-Oriented Systems (TMSOS) and 10-15 % higher secured when compared with the Service Mining using Process Mining.

5. Discussion on Adapting Signatured XML Encryption in Web

Our new era of the internet community, walk around with massive on-the-fly resource usage application. This high tech community prevails with the fast access to large quantities of data and commensurately fast computational resource. Each and every organization has its own local authorities to administrate the resources which may be in the form of software or hardware. It is impractical to execute this immense computational or storage entailing application using resources exist in individual organization. The internet technology grants the facilities to share the data from any location. The user running an application on this distributed environments have to get integrity assurance on their digital assets and to ensure that proprietary application remains safe while traveling, processing, accessing and updating.

One of the ways to secure connection was ensured by employing firewalls. It's run through was to establish a constructive rules to allow restricted IP address tied by that network. But, now Internet usage of accessing any

application and business logic became ubiquitous and we cannot have sharing option alone through IP community only. Next level improvement preceded by HTTPS that secure the connection establishment by transmitting request and response through HTTP over SSL. Even though, HTTPS hold pervasive web sharing facilities, its license validation through certificate slow down the system performance. Moreover, it provides transport level security (i.e. point to point) where connection alone is secured excluding the data, because of exposing the packet header information to each intermediate node due to encoding or decoding operation. Switching to message level security is needed that saves data while in transport and in storage.

Message level security is injected by either XML Cryptography or WS-security. The Web provides a collection of protocols for data transmission. That data is defined in form of XML representation. XML derives much of its strength in combination with the Web. XML structure the document suitable for variant device format, diverse application area format, and being used as the common data format and protocol to make easy accessibility in unsuited systems. For this XML aptness, we choose XML cryptography. The major issues of this standard is

- Specified parts of structured data can be encrypted and signed.
- Many specified parts of structured data with different algorithm or key can be encrypted or signed.
- Multiple parties can access encrypted or signed structured data storage

This standard pinned to work with many symmetric algorithms like DES, TDES, RC4 etc. and asymmetric algorithms like RSA, DSA as default. The implementation if fitted with asymmetric algorithm such as ECC cryptographic algorithm provide more security level in small bits than granted by RSA algorithm. Any document converted to XML form can be encrypted and signed with any algorithm chosen above. The information matching the keyword or extraction of user profile can be a confidential asset of any concern. Even though authorization provided by login to user, some secure activities to be followed to maintain the confidential.

For facing the competitive environment, any business teams have to find their suitable web services among the bulk services prevail in market. Web service is the technology tied up with SOAP, UDDI and WSDL of XML format, so web services searching based on XML keyword become essential. Once the requesting query matches tags in WSDL of services, the accessing cannot be made open to all. Those specified part or whole has to be secured from malpractice.

Evaluating the performance metric like decryption time, system utility, precision is essential to find the optimization in secured E-business transaction.

5.1 Future Directions

The future direction of using the signatured XML encryption in multi-tier web service security can be in the following ways:

- Designing a new algorithm to attain the XML web security with key
- Planning a new technique in order to effectively design the BPEL based web security
- Introducing a new architecture to forecast the combination of different inputs and outputs on web security

6. Conclusion

Surveillance about the existing signatured XML encryption in multi- tier web service security with different system and support has been discussed. This examination increases the need of privacy and integrity of data in multi-tier web service security. Finally, the result shows that the security services on web increases the data delivery ratio and privacy level of the data and also reduces the execution time over a wide range of experimental parameters.

7. Refereences

1. Lim HW, Paterson KG. Identity-Based Cryptography for Grid Security. International Journal of Information Security. 2011 Feb; 10(1):15-32.
2. Tao X, Li Y, Zhong N. A Personalized Ontology Model for Web Information Gathering. IEEE Transactions on Knowledge and Data Engineering. 2011 May; 23(4):496-11.
3. Bao Z, Lu J, Ling TW, Chen B. Towards an Effective XML Keyword Search. IEEE Transactions on Knowledge and Data Engineering. 2010; 22(8):1077-92.
4. Hamlen KW, Thuraisingham B. Data security services, solutions and standards for outsourcing. Computer Standards & Interfaces. 2013 Jan; 35(1):1-5.

5. Sun C, El Khoury E, Aiello M. Transaction management in Service-Oriented Systems: Requirements and a proposal. IEEE Transactions on Service Computing. 2011; 4(2):167-80.
6. Roitman H, Gal A, Raschid L. A Dual Framework and Algorithms for Targeted Online Data Delivery. IEEE Transactions on Knowledge and Data Engineering. 2011 Jan; 23(1):5-21.
7. Bramandia R, Choi B, Keong Ng W. Incremental Maintenance of 2-Hop Labeling of Large Graphs. IEEE Transactions on Knowledge and Data Engineering. 2010 May; 22(5):682-98.
8. Van der Aalst W. Service Mining: Using Process Mining to Discover, Check, and Improve Service Behavior. IEEE Transactions on Services Computing. 2013 Nov; 6(4):525-35.
9. Mana A, Koshutanski H, Perez EJ. A trust negotiation based security framework for service provisioning in load-balancing clusters. Computers & Security. 2012 Feb; 31(1):4-25.
10. Darwish W, Beznosov K. Analysis of ANSI RBAC Support in COM+. Computer Standards & Interfaces. 2010 June; 32(4):197-214.
11. Aarthi R, Anjana KP, Amudha J. Sketch based Image Retrieval using Information Content of Orientation. Indian Journal of Science and Technology. 2016 Jan; 9(1):1-5. Doi: 10.17485/ijst/2016/v9i1/73218.
12. Abarna R, Pradeepa S. A Hybrid Approach for Extracting Web Information. Indian Journal of Science and Technology. 2015 Aug; 8(17):1-6. Doi: 10.17485/ijst/2015/v8i17/61595.