Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A CLOUDLET BASED SECURITY AND TRUST MODEL FOR E-GOVERNMENT WEB SERVICES

BASSAM AL-SHARGABI [1] ,SHADI AL-JAWARNEH [2], AND SOFYAN M.A. HAYAJNEH[3]

[1] Faculty of Information Technology, Middle East University, Amman-Jordan,

[2] Faculty of Information Technology, Jordan university of science and technology, Irbid-Jordan,

[3] Faculty of Engineering, Isra University, Amman-Jordan,

E-mail: [1]bshargabi@meu.edu.jo., [2]saaljawarneh@just.edu.jo, [3]sofyan.hayajneh@iu.edu.jo

ABSTRACT

Nowadays, Cloud Computing and Web services are the main backbone of e-government applications because of its interoperability and accessibility nature. Web services that are maintained in Cloud brought much attention in research and industry in terms of securing the communicated Web services. Thus, securing and trusting between the communicated Web services has been gradually becoming more challenging for Web services consumers, administrators, and Web service providers especially the e-government services. Thus, In this paper, a Cloudlet based security trust model was proposed to guarantee a proper and secure communication between Web services through exploiting the cloud computing infrastructure . In addition, the proposed model is tackling the issues arises when Web service consumers are communicating with any of the e-governmental Web services through a trusted Cloud-based third party that is controlled by any governmental agency. Moreover, the Cloudlet is also used to measure the trustworthiness and conformance with the published policy by the provider of Web services through feedback from the Web service consumer. . The experimental result of the proposed model shows an outstanding performance regarding different size of SoAP messages using triple DES and RSA as standard encryption algorithms.

Keywords: *Web service; Security;Trust model; Cloudlet; E-government*

1. INTRODUCTION

Web services are software systems that can be published, discovered, and invoked easily due to its loosely coupled nature The Web services can be published in the Cloud environment using the Web Service Description Language (WSDL). The WSDL is expressed as an XML format to illustrate operations ,input ,output and how Web services can be invoked in Cloud using HTTP. The way how Web services can be published in Cloud or in Central registries can be explained using the Universal Description Discovery and Integration standard (UDDI). The UDDI recommends methods to publish information about the Web service provider, the services that are stored and become for service consumers to find Web service providers and Web service specification[1]. Moreover, the Web services can be invoked or communicated as defined in their description Simple Object Access Protocol (SOAP) messages, where messages are encapsulated using HTTP with an XML serialization in conjunction with other Web-related protocols as an XML formatted information exchanged among the entities involved in the Web service mode as introduced [2,3].

However, Web service consumers and providers are still concerned about security and trustworthiness issues as introduced in Midhun rt al.[4], and Sushama et al [5], such issues can be tackled by giving an identity for both Web service consumer and Web service provider thought a trusted third party. Basically, both of the Web service consumer and provider can communicate in a secure and trusted manner if there is a way to identify both parties. This is can only be done through validating incoming message between Web service consumer and provider using a solid evidence that either can be a set of claims (e.g., name, key, permission, capability, etc.). If a message arrived without having the required affirmation of the claims, the service should be discarded.

Nevertheless, Web services are constantly established with several unique security concerns, such concerns cannot be tackled like any other

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

conventional distributed messaging techniques that are mainly suitable to the widespread of Web-Services. For instance, the SOAP protocol used as a communication method between Web Services does not undertake security by itself. The SOAP protocol can be easily exceeded by a firewall, and directly processed by the Web service. Thus, SOAP messages can be exploited by an attacker to compromise the communication between Web services[6].

The emergence of Cloud Computing and Web service has opened new dawn for organizations and governmental agencies to adopt more agile and flexible interaction and harvest the prospects of Cloud Computing and Web services. Thus, to harvest these opportunities and the requirements of organizations and governmental services, each Web service provider should guarantee that the services are provided securely way and must be trusted through Cloudlet datacenters, which can be controlled by any third party to secure the communication between service consumer and provider.

Many models and approaches have been proposed to deal with security in Web services as introduced in [7] but most of them are lacking trust among Web services [8]. In this paper, a Cloudlet based approach is presented to secure the message exchange between governmental Web services and any other Web services that might interact with any Web service within governmental Web services. The Cloudlet is introduced as a trusted third party that provides an identity for communicating Web services. In addition, the Cloudlet is also used to measure the trustworthiness and conformance to the published policy by the provider of Web services through feedback from the Web service consumer

2. WEB SERVICE

Web service defined as a software system that can be recognized through URL, and can be invoked through public interfaces which described using XML . The functionality provided by Web service can be discovered by another Web service. The Web services may then interact with each other in a way as defined by its definition, the interaction can be conducted through XML-based messages conveyed by Internet protocols [1]. Three entities are the main components of the Web service architecture as illustrated in figure 1 .

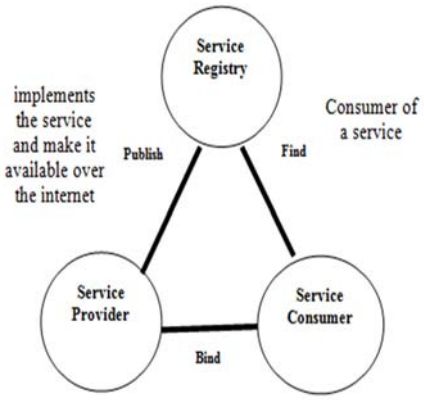

Figure 1: Web service Architecture

The Web Service Provider offers functionality as described in a standard format, which is available in a central Service Registry or in CLoud. The Web Service Consumer can then find and retrieve the information from the registry and exploit the description to interact or bind with the Web service. The proper scheme of Web service is illustrated in Figure 1 by the keywords “publish”, “bind” and “find”.

The emergence of Web services applications such as finance, accounting, order procurements, customer relationship management, and manufacturing has established further opportunities for enterprises to adopt more agile and flexible collaborations. in other words, enterprises can use Web service to conduct Business-to-Business in an interoperable way through exploiting Web services offered by other business partners based on certain business processes.

3. WEB SERVICE SECURITY CHALLENGES

The utilization of Web services in e-governments applications and services or any enterprise, the security is a key obstacle that must be tackled, In this section, the regular security threats that might affect the use of Web services are demonstrated as follows:

Message Assertion: This security threat is related to alter the messages that exchanged between communicated Web services, where the attacker may modify the SOAP message content that was originated either by the service consumer or provider. The altered SOAP message is then mistaken by the receiving service as being the originator’s real intention. Besides, an attacker might also establish a new fake SOAP message to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

deceive the receiving Web service into that message arrived from a valid Web service as presented in [9].

Loss of confidentiality: such threat can occur when an unauthorized entity might read the intercepted SOAP message that transmitted between Web service consumer and provider

Man in the middle attack: this security threat can occur when an attacker positioned between the Web service consumer or Web service provider, where the attacker can read and alter the messages between both parties the provider and consumer and then send a modified SOAP message to each of the two parties.

Replay of message parts: this security threat can occur when the attacker uses parts of the intercepted SOAP message to the receiver with the intention of gaining access to an unauthorized system, or causing the receiver of SOAP message to take unnecessary action.

Denial of service: this security threat can occur only when an attacker modifies the SOAP message contents that will lead Web service provider or consumer to devote all resources to a certain task so that it cannot be provided by any services to valid requests[2]

4. WEB SERVICE SECURITY COUNTERMEASURES

The description of the basic standards and approaches presented in the literature is presented in this section. Such approaches and standards are mainly established to overcome Web service major security issues. The approaches and standards are summarized below :

W3C XML Encryption: this is a method to encrypt and decrypt the exchanged SOAP messages between interacted Web services through using an XML encryption method, but such a method shows that encrypting SOAP messages using XML encryption methods can be decrypted easily by an attacker [10].

W3C XML Signature: this approach relies on creating a signature for the SOAP messages that are exchanged between the communicated Web services in a way to offer integrity, signature assurance and non-repudiation[11].

WS-Security Tokens: in this approach, the WS-Security is used to identify and verify the source of SOAP messages for both Web service provider and consumer. However, WS-Security relies on transmitting security information called token within a SOAP message, where this token is described in XML. Besides, more enhancement has been presented to WS-Security to improve Web service security as in [12,13,14], where the majority of improvements are lean on SOAP message authentication along with WS-Addressing with the aim of protecting against a message replay attack [14].

. **WS-Secure Conversation**: such an approach relies on using an encryption key to be shared among communicated Web services in a special session. The encryption key must be originated by Web service providers using an encryption algorithm in order to generate the key. This key is embedded with the SOAP message, where this key also can be used to decrypt messages. Accordingly, when the Web service consumer receives a SOAP message can decrypt the message and retrieve the session key as this key can be used to secure communication between provider and consumer through the session [14].

WS-Policy: this approach relies on imposing a policy for the communicated Web services, where this policy defines and specifies the properties of the Web services. While requesting Web services can use this policy to ensure and accept the request. Accordingly, such policies can be attached to SOAP messages using WS-policyAttachment, where WS-MetadataExchange is used to retrieve the policies from the SOAP message. Encoding the text can be associated with Policy assertion, where SOAP protocol can be used to enforce the header combinations existing between SOAP messages that are defined through WS-PolicyAssertions as approached in [14] .

WS-Trust: this is a protocol that is designated to ensure a trusted way to exchange SOAP messages for interacted Web services. The WS-Trust protocol relies on the reciprocity of a Security Trusted Tokens (STS), where these tokens are generally a set of assertions about a service or resource by the source of such token. The tokens can be attached to SOAP messages that are exchanged between the communicated Web services .

The consumer of a Web service can determine the availability of token and requests for the needed token to STS else service consumers may hand over the liability of finding the token to STS itself and state only available token and just ask for the exact token. This can be made by the Web Service consumer with including a parameter called a time variant as entropy while requiting the token, STS will be returned using a secret key that is called proof-of-possession. As this token can be handled as certificate and the use of a private key to the proof-of-possession.

eXtensible Access Control Markup Language (XACML): which is an XML access control model to secure the Web service communications, through

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

exchanging an XML framework for the process of authentication and authorization of interacted Web services. XACML is dictated to impose an access control policy between Web services. Another promising Web service approach that relies on including WS-Security and WS-Policy, where the WS-Security is used to secure SOAP messages through XML Encryption and XML Signature standards while the WS-Policy framework is used to specify the security policies of Web services that can be defined in regards of their characteristics and features such determining the encryption algorithms and security tokens, and privacy rules as proposed in [4]. In addition, the encryption of XML is used to allow an end-to-end security for Web services to guarantee the confidentiality by encrypting the XML data. As XML Encryption is not anticipated to replace or exceed Secure Socket Layer (SSL), but it can be used with SSL to cover security issues that are not handled by SSL. Therefore, the .XML encryption algorithm can be used to ensure confidentiality issues. Eventually, XML Encryption does not provide new cryptography algorithms or techniques as explained in[13].

Moreover , methods and techniques also have been proposed in the literature to handle the Denial of Service attack (DoS) by using a mechanism for filtering the malicious requests[14], to avoid using the internet users from taking part in DoS attacks without their knowledge to protect Web services from DoS attacks. One method that is based on replicating Web services in a control and robust way since the Web services are more vulnerable to the DOS attacks and such a method can be exploited to protect Coudlet and Web services against DOS attacks [15].

5. CLOUDLET

A Cloudlet can be considered a new architectural component that is introduced from the concourse of mobile computing and Cloud Computing. Cloudlet consists of a set of trusted datacenters that are connected to the Internet and its available to be used by any nearby mobile devices [16]. A Cloudlet can be seen as a datacenter with only one goal which is to bring the capabilities of Cloud more rapidly.

Cloudlet requires slight power, Internet connection with an access control authority. However, the security framework within Cloudlet can handle the process of authentication and authorization[17]. Accounting and auditing is still handled within the Cloudlet framework. All Cloudlet requests and responses can be monitored and logged by the accounting module as presented in Serrano et al [18]. Therefore, in the context of using Cloudlet as an access control layer, the proposed security trust model in this paper, relays on Cloudlet access control authority feature to secure communication between e-government Web services and others. Although, due to the simplicity of managing Cloudlet, Cloudlet must be controlled and managed by any governmental agency to provide trust for the Web service consumer and provider as proposed in this papered.

6. WEB SERVICE TRUST

Measuring the trustworthiness of the Web services can be characterized as qualitative or a quantitative over a certain numeric range. However, the trust level as in this paper is represented numerically to pinpoint the trust ranking of registered Web services in Cloudlet and the feedback for each of the invoked Web services . Nevertheless, trust relies upon the perspective of the users and it can't be described as an objective property of certain trustees. Several approaches that focus on the quantitative measurement of a Web service's trustworthiness have been proposed in the literature [19]. Most of the trust evaluations as seen in the literature are based on quality of service(QoS) in terms of probabilistic form.

Other approaches are considering that Web service trust as a subjective uncertainty that includes the randomness and fuzziness. Probability metrics might be expressed as the randomness of trust, but not appropriate to convey concepts of fuzziness. Actually, the human perception of a trust can be expressed through the natural languages not in terms of mathematics, It's better to let human rate and evaluate the trust in a discrete statement form rather than using continuous measures as introduced in [20,21]. Therefore, people tend to abstract some typical concepts from numerical values of trust to express and understand the degree of trust. This process must establish a subjective fuzziness. For instance, we say that a Web service consumer trusts a provider, if we only use a probability number between [0, 1] to quantify the degree of trust, we cannot decide if 0.88, 0.92, or 0.95 can more accurately signify the trust degrees. In order to bridge numerical values to concepts, the fuzzy set is used as a way to express the fuzziness. However, to characterize the fuzzy concepts as a subjective perception the fuzzy sets to use a fixed number . The fuzziness can be described by the membership function approach that will not take the randomness into account [22]. In general, it is difficult to differentiate randomness and fuzziness during the subjective perception process. The Cloud model can consistently express the randomness and fuzziness according to a mathematical and fuzzy set theory, which already

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

has been used in more related areas of trust evaluate and modeling[22]. In this paper ,we adopt the cloud model in order to represent computable factors of trust relation in order to rationalize and express the subjective uncertainty of trust from the perspective of the consumer of Web services.

7. RELATED WORKS

Many approaches and models have been proposed in the literature to secure communication between Web services. However, few of those approaches or models are based on access control models or using reputation manager for Web services.

In [20], the authors introduced an access control method, which is based on multifactor trust management for each Web service provider. The introduced access control calculates a trust value for Web service providers at each time Web service consumer request or invokes the Web service provider. The access control models are located on the provider side, which calculates the trust value statically and analysis of behavior, activities of previous access attempts of the Web service consumer. The trust value can be decreased due to any violation by the service provider and the feedback from the service consumer, but this won't solve the dilemma of restricting the of malicious services as in [23] . The trust model here only serves the service provider interest not the service consumer and does not provide an authentic way for both service provider and consumer .

Another trust model in [21] also serves the service provider interest, which is based on four attributes : availability, reliability, turnaround efficiency and data integrity of the service provider in the Cloud. The four values are used to compute the trust value of the provider. The AVANTSSAR Platform proposed to secure Web service communication in service oriented architecture, Its platform is a policy to enforce and validate security [24]. A distinction must be made between hard trust involves features such as authenticity, encryption, and security between communicating services, while the second type of trust is soft trust that involves the nature of human, loyalty of brand, and user-friendliness as in [25]. Furthermore, the above-mentioned approaches do not consider the dynamic nature of trust that will change over time due to many reasons. The proposed trust model relies on soft trust security measures and feedback from the services consumer which will keep the trust level updated.

A trust model was presented in. [26], which modeled the trust relationship between service provider and consumer based on three factors: reputation, trustworthiness and risk. The presented model takes advantage of Cloud to compute and quantify those factors. However, a weighting schema can be used to provide weights for the three factors to represent the interests of service consumer as presented in the proposed model[19].

A certification based approach was introduced in [27], where the certification is given to a Web service based on service description model. This certification is based on security and supports a test-based security certification scheme for communicating Web services. The certification schema of this approach is motivated by the security features that can be computed by using a model-based testing approach that begins with the service model, and automatically creates the test cases to be used in the service certification.

An access control method implemented on OPENi introduced in [17], which allows users to control how services can use their data. The access control method is implemented through the use of REST based endpoints along with the use of stateless JSON Tokens . This model allows users of mobile applications to share, reuse, and control access to their data while maintaining Cloud scalability.

A security trust model introduced in [28] to evaluate communicated agents in multi-agent platform, the model used to detect which agent can be trusted or not through a heuristic algorithm, the algorithm uses heuristics to compute truest for each connected agent. Furthermore , another approach in [29] was introduced to select the trusted providers, the selection procedure relies on how the Cloud provider satisfy the consumer security and privacy requirements based set of probabilities and weights. Although, deterministic and probabilistic methods were proposed in the literature to evaluate the Web services trust to replace the uncertainty that brought from the inconsistencies of rates supplied by Web consumers over time and the inconsistency of the assessed QoS values as in[31,32,33].

8. PROPOSED SECURITY TRUST MODEL

The Cloudlet security trust model proposed in this paper is presented in this section, the proposed model is based on the existence of Cloudlet that acts as a trusted third party between communicating Web services . The Cloudlet should be controlled by a governmental agency, which is responsible for ensuring a valid way for all the governmental Web services and others to communicate in a secure and trusted way.

Moreover, the Cloudlet is responsible for defining an identity for all consumers and provider

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of Web services to guarantee a valid identity for each of the communicated services. The identity generated by Cloudlet data storage and also maps their identities for both services as illustrated in Figure 2.

Figure 2: Proposed Security Trust Model

The Proposed Cloudlet Model Works as follows:

- A citizen or enterprise (Web service consumer) initializes a request.
- The request is appended into the data storage of the Cloudlet, the Cloudlet assumed to be an authenticated third party. This means that the third party has a valid digital certificate.
- Web server of Cloudlet processes and analyzes the citizen or enterprise request (citizen or enterprises are authenticated by ID and the e-government Provider for the service).
- The Web server also processes a valid connection with the data storage of Cloudlet.
- If the connection is passed, the data is appended to the citizen or enterprise file and e-government file at the data storage.
- If the connection is passed, the identity of the Web service provider is sent to be validated.
- Web server processes a connection: maps the identity of both e-government Web service and citizen or enterprise Web service to ensure that both services are connected in a secure manner, where citizens or enterprise Web service will be on the table, and all e-governments Web services also will be stored in another table. The tables contain the identities of both parties.
- Whenever the Web service consumer can provide feedback regarding the trustworthiness of the provider which will be stored in Cloudlet as a score for that provider.

Furthermore, The identity is encrypted by an XML encryption algorithm determined by the Data Web server in Cloudlet and to be transmitted through SOAP message the intended Web service. The identity can be used by the communicated Web services and to be validated through third party as illustrated in figure 3. Accordingly, the integrity and non-repudiation of the transmitted SOAP message can be ensured. Moreover, The communication between Web services and Cloudlet can be handled by the use of PKI technique as presented in [34,35,36,37,38], as the public key can be published by the Cloudlet for communicated Web services through the Cloudlet private key.

The key primary process steps in the proposed model that shows the rule of Cloudlet to secure and ensure trust communication between involved Web services. The Cloudlet can ensure the validity and authenticity of both Web service consumer and provider by verifying that the claims in the identity are satisfactory and to be confirmed with the policy that determines the rule of each Web service. The Cloudlet can verify that the attributes of the provider in order for the requester to ensure and trust the provider.

The Cloudlet can store information about providers through the feedback from consumer regarding trustworthiness and conformance with the published policy of the provider. This information can be used by Cloudlet to give a score for the provider trustworthiness, the scoring for the trust can be computed using equation 1.

$$TS = \frac{\sum_{i=1}^{n} T}{n} \quad \text{..... (1)}$$

Where T is the trust score provided based on Web service consumer , where n is the number of times the Web service provider has been scored . Usually, trust scores are given a range to rank Web services. For example, in Amazon.com, the range is [0, 5].

Figure 3: The Rule Of Cloudlet Between Web Services

The higher value of TS for Web service provider means a high trust. The Web service consumer can set the value to the accepted trustworthiness value in the discovery process and can be validated throughout the Cloudlet as illustrated in figure 2.

The strength of the proposed model is that the authentication process through the Cloudlet can manage issuing, renewing and validating the identity of both service requester and provider which leads to a trust relationship. The proposed model defines a request/response protocol by which Web services can request of Cloudlet that a particular identity security of the provider and the trust score of give and stored in the Cloudlet based on provider history.

9. EXPERIMENTAL STUDY AND DISCUSSION

In order to validate the proposed model, an experimental study was conducted on CloudSim platform, which is an open source platform. We

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

conducted two experiments using two encryption algorithms such as RSA, triple DES along with varying size of the SOAP message, number of rounds along with block size for triple DES. All communication between the services provider and consumer are handled through the Cloudlet. When producing a digital certificate for a Web services , we no longer need to encrypt the entire SOAP message with a sender's private key. The whole time taken to encrypt the SOAP message in the Cloudsim platform for the varying size of SOAP message such 32, 64,128,256,512(in MB) is calculated and illustrated in the table1.

Table: Time and size of SOAP message

SOPA message size	Encryption Algorithms (Milliseconds)	
	Triple DES	RSA
32	522	312
64	845	413
128	1281	688
256	1653	912
512	2123	1346

As shown in figure4, the encryption time taken by triple DES and RSA for different SOAP message size in CloudSim platform environment, where the result shows that it would better to use RSA as an encryption algorithm in Cloudlet in term of time as compared to the triples DES.

Figure 4: Time analysis

10. CONCLUSION

Nowadays , most of e-government services migrated to the Cloud due its accessibility and interoperability nature, in this matter most of consumer of services or the services provider whether they are enterprises or governmental agencies are still having concerns about the security and trust issues. In this regards the communication between the service providers and consumer must be done in a secure and trusted manner. Accordingly, a Cloudlet based security and trust model was introduced to ensure and guarantee a secure communication and interaction between e-governmental Web services and other service consumers.The model is based on exploiting the Cloudlet data storage as a trusted third party managed and controlled by any governmental entity in a way to distribute identities for both parties (Web service consumer and provider). The identity can be used when both parties are communicating or interacting and they can identify each other through this identity managed and distributed by a trusted third party through the use of Cloudlet. In addition, the proposed model provides a way to measure the trustworthiness of the e-government Web services through feedback approach. The experimental result of the proposed model shows an outstanding performance regarding different size of SoAP messages using triple DES and RSA as standard encryption algorithms. As future work, we intended to improve the proposed model to be used for the Constraints devices such as Internet of Things devices.

ACKNOWLEDGMENT

The authors are grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

REFRENCES:

[1] Booth, H. Hass, F. Mccabe, E. Newcomer, M. Champion, C. Ferris, D. Orchard, . Web services architecture, 2015. W3C Working Group Note 13 September 2015, W3C Technical Reports and Publications, http://www.w3.org/TR/ws-arch/

[2] Al-Shargabi, B. El Shiekh, A. Sabri, A ." Web service composition survey: State of the art review". Recent Patent on Computer science Journal, 3(2),pp 91-107 (2010).

[3] Kaur,J. Singh, N."Web Vulnerabilities Caused By Social Media Web Service Integration".International Journal of Innovative Research in Computer and Communication Engineering.. 3, (1), pp 66-70 (2015).

[4] Midhun, T. Prasanth, K. Anoop, J . "A Survey on Authorization Systems for Web Applications . Journal of Computer Engineering (IOSR-JCE). 17(3), pp 01-05 (2015)

[5] Sushama, K. Anna, S. "A Large Scale Study of Web Service Vulnerabilities". Journal of Internet Services and Information Security (JISIS). 5(1),pp53-69 (2015).

[6] Li, Y. Lin, C. "QoS-aware service composition for workflow-based data-intensive applications". In Proc. of International on Web Services (ICWS'11), USA ,Washington DC, pp 452–459 (2011).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] Jia-ju, W, Zhu, X. Liu, Z .and Cheng,Z. "Research on Security Model of Web Service." DEStech Transactions on Engineering and Technology Research eeta (2017).

[8] Al-Shargabi, B. "Security Engineering for E-Government Web Services: A Trust Model." In Information Systems Engineering (ICISE), 2016 International Conference on, pp. 8-11(2016).

[9] Holgersson, J. Soderstrom, E. "Web service security - vulnerabilities and threats within the context of ws-security". In Proc. of the 4 th International Conference on Standardization and Innovation in Information Technology (SIITT'05), Geneva, Switzerland, pp 138–146, (2005).

[10] Tibor,J. Juraj,S. "How To Break XML Encryption." In The 18th ACM Conference on Computer and Communications Security (CCS), (2011).

[11] Bertino, E. Martino,L. Paci, P. Squicciarini, A." Security for Web Services and Service-Oriented Architectures". Springer, (2009).

[12] Brahim, M.B. Chaari, T . Jemaa, M. B. . nd Jmaiel, M. Sema"ntic matching of ws-securitypolicy assertions". In the 10 th Internation Conference on Service-Oriented Computing Workshops (ICSOC'12), Cyprus, Paphos, pp 114–130 (2012).

[13] Sinha, S. Sinha, S. K. "Security Issues in Web Services: A Review and Development Approach of Research Agenda". Assam University Journal of Science & Technology: Physical Sciences and Technology. 5(2),pp 134 -140 (2010)

[14] Siddique, H. Syed S.H ." Security Issues in Web Services". International Journal of Computer Science and Telecommunications. 5(5) ,pp24-27 (2014).

[15] Priyadharshini, M.Baskaran, R. Srinivasan, M. K. Paul, R. "A Framework for Securing Web Services by Formulating an Collaborative Security Standard among Prevailing WS-Security Standards." Communications in Computer and Information Science .4,pp 269-283 (2011)

[16] Bahtovski, A and Gusev, M. "Cloudlet Challenges," Procedia Engineering, 69, pp.704-711(2014).

[17] McCarthy,D. Malone. P.Hange, J. Doyle, K..Robson, E Conway,D. Ivanov, S. Radziwonowicz, L. Kleinfeld, R. Michalareas, T. Kastrinogiannis, T. Stasinos, N. and Lampathaki, T." Personal Cloudlets: Implementing a user-centric datastore with privacy aware access control for cloud-based data platforms." In Proceedings of the First International Workshop on TEchnical and LEgal Aspects of Data pRIvacy, TELERISE '15. USA,Piscataway, NJ, pp 38–43 (2015).

[18] Serrano, J. E. Leguizamón, J. and Martínez-Santos, J. C. "GridUI, a RESTful Web service and ubiquitous UI for accessing HPC resources," 8th Euro American Conference on Telematics and Information Systems (EATIS), Cartagena, pp. 1-4 (2016).

[19] Talluri, S. "Novel Techniques In Detecting Reputation based Attacks And Effectively Identify Trustworthy Cloud Services." International Journal of Science Engineering and Advance Technology , 4(6),pp 287-289 (2016)

[20] Manoj, R. J., & Chandrasekhar, A. " An Access Control Model of Web Services Based on Multifactor Trust Management". International Review on Computers and Software (IRECOS), 8(10),pp 2460-2466 (2013).

[21] Manuel, P. "A trust model of cloud computing based on Quality of Service". Annals of Operations Research, 233(1),pp 281-292 (2015).

[22] Deyi,L. Changyu,L, and Wenyan ,G. "A new cognitive model: cloud model." International Journal of Intelligent Systems 24(30),pp 357-375 (2009).

[23] Manoj, R. J. Sheeba, A. and Praveena, MD.A. "User Behavior based Trust Estimation for Web Service Access Control Model" Int J Adv Engg Techl. 11(1),pp 791-796 (2016).

[24] Armando, A., Arsac, W., Avanesov, T., Barletta, M., Calvi, A., Cappai, A., and Erzse, G." The AVANTSSAR platform for the automated validation of trust and security of service-oriented architectures". In International Conference on Tools and Algorithms for the Construction and Analysis of Systems ,pp 267-282 (2012)

[25] Pearson, S. " Privacy, security and trust in cloud computing". In Privacy and Security for Cloud Computing ,pp. 3-42 (2013).

[26] Wang, S. X., Zhang, L., Wang, S. and Qiu, X. "A cloud-based trust model for evaluating quality of Web services." Journal of Computer Science and Technology, 25(6), pp1130-1142 (2010)

[27] Anisetti, M., Ardagna, C. A., Damiani, E., & Saonara, F. A test-based security certification

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

scheme for Web services. ACM Transactions on the Web (TWEB), 7(2), (2013)

[28] Das, A., & Islam, M. M."SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems". IEEE transactions on dependable and secure computing, 9(2), pp261-274 (2012)..

[29] Pavlidis, M., Mouratidis, H., Kalloniatis, C., Islam, S., Gritzalis, S. "Trustworthy selection of cloud providers based on security and privacy requirements: Justifying trust assumptions". In: Proceedings of the 10th International Conference on Trust, Privacy, and Security in Digital Business (TrustBus 2013). pp185–1 (2013).

[30] Saoud, Z., Faci, N., Maamar, Z., & Benslimane, D." A fuzzy-based credibility model to assess Web services trust under uncertainty". Journal of Systems and Software. 122, pp 496-506 .(2016).

[31] Saoud, Z, Noura, F, Zakaria ,M, and Benslimane,D. "Sybil Tolerance and Probabilistic Databases to Compute Web Services Trust." In East European Conference on Advances in Databases and Information Systems, pp. 458-471 (2015).

[32] Vigil, M. A. Moecke, C. Cust, R.¸sdio, A. and Volkamer, M. “The notary based PKI,” in Public Key Infrastructures, Services and Applications, ser. Lecture Notes in Computer Science, S. Capitani di Vimercati and C. Mitchell, Eds. Springer Berlin Heidelberg, vol. 7868, pp. 85–97 (2013).

[33]Al-Shargabi, B. Alhadithy.H, " Web Service Composition in Cloud: A Fuzzy Rule Model " Recent patent on computer Since, 2018

[34]Al-Shargabi, B. Alhadithy.H, " Fuzzy Rule Based Web Service Composition in Cloud " In proceeding of The International Conference on Data Science, E-learning and Information Systems, 2018

[35] Kalpana G, Kumar PV, Aljawarneh S, Krishnaiah RV. Shifted Adaption Homomorphism Encryption for Mobile and Cloud Learning. Computers & Electrical Engineering. 2018 Jan 1;65:178-95.

[36] Aljawarneh S. Cloud Security Engineering Concept and Vision: Concept and Vision. InCyber Security and Threats: Concepts, Methodologies, Tools, and Applications 2018 (pp. 93-101). IGI Global.

[37]Al-Rousan, T., Abualese, H., & Bassam, A. S. (2019). A New Trust Framework for E-Government in Cloud of Things. International Journal of Electronics and Telecommunications, 65(3), 397-405.

[38]Al-Rousan, T., Abualese, H., & Al-Shargabi, B. (2019). A New Security Model for Web Browser Local Storage. International Journal of Advanced Computer Science and Applications (IJACSA), 10(8).

Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

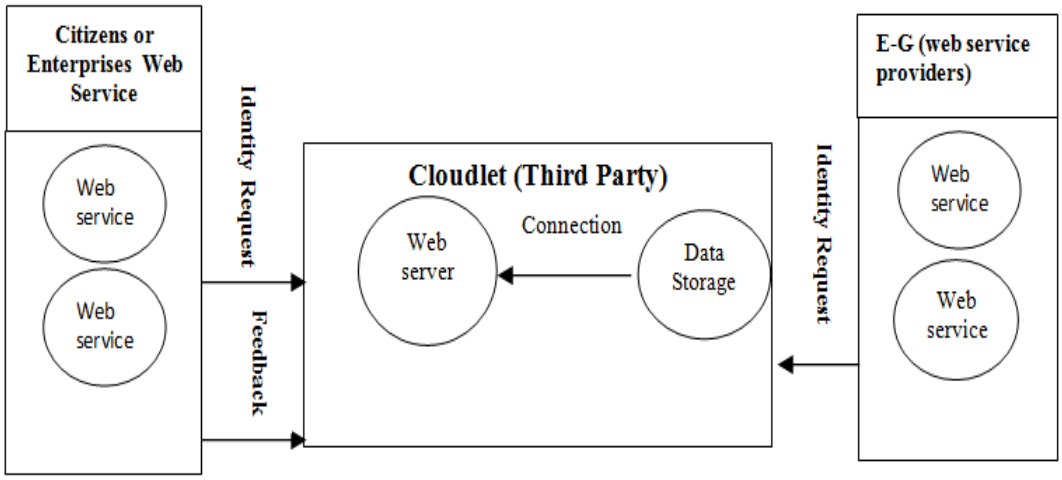

Figure 2: Proposed Security Trust Model

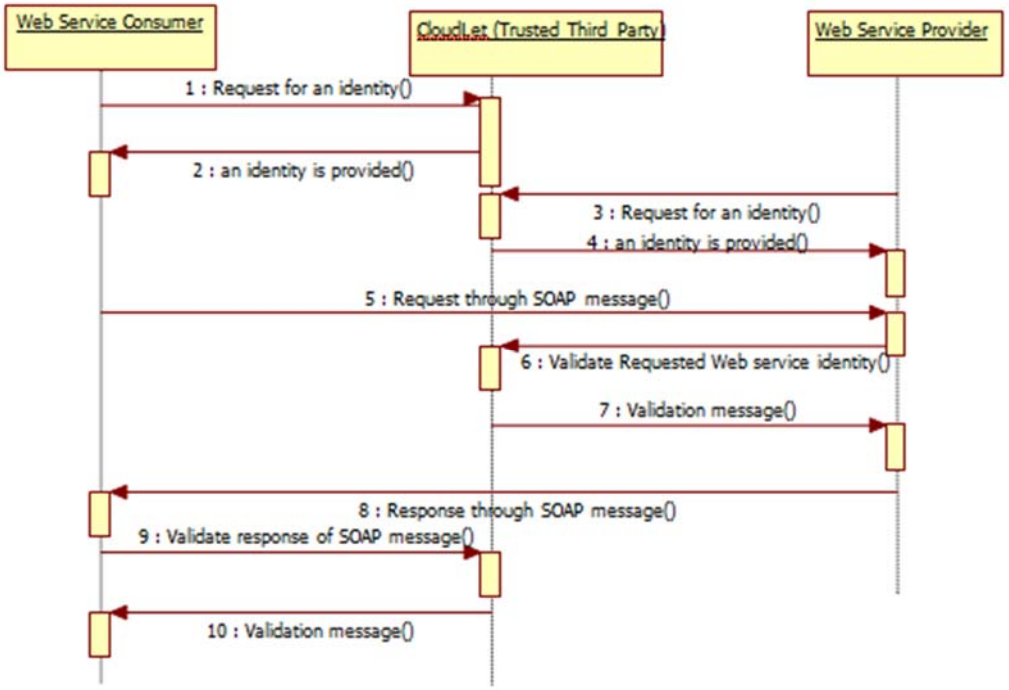

Figure 3: The Rule Of Cloudlet Between Web Services

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

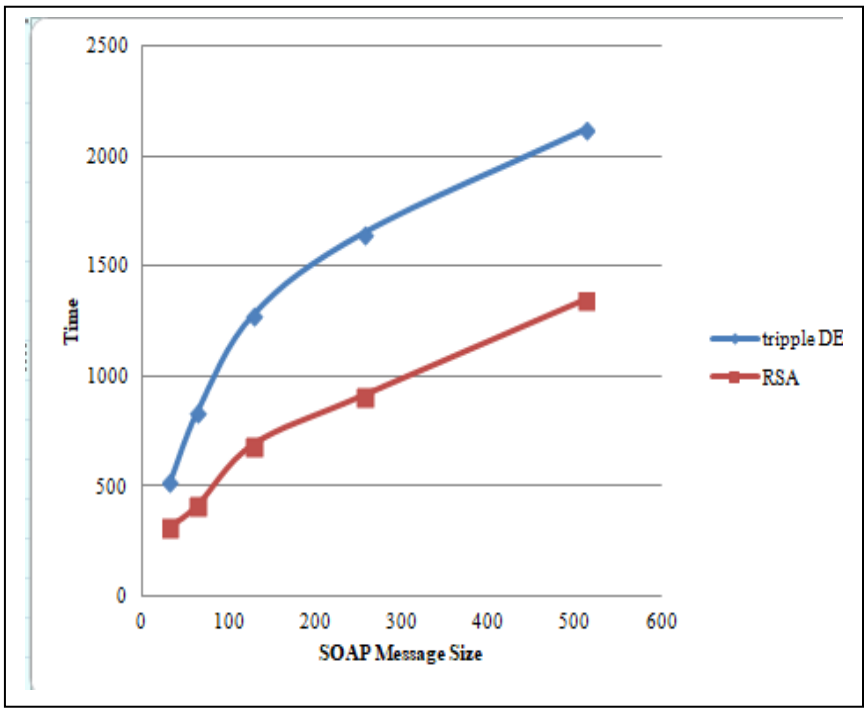

Figure 4: Time Analysis