ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on 'Trusted Model for Securing the E-Government Web Services'

Sooraj Bagdia[1], Afraj Attar[1], Shubham Chaudhary[1], Rohan Gaikwad[1], Swati Keshari[2]

Students, Dept. of Computer Engineering, MESCOE, Savitrabai Phule Pune University, Pune, India[1]

Asst. Professor, Dept. of Computer Engineering, MESCOE, Savitrabai Phule Pune University, Pune, India[2]

ABSTRACT: In rise of the web applications of web services which provides a easy and convenient way for the citizens. Trust is one of the most critical factors for a service requester when selecting the required e-government web service. Adopting Web services in e-government enables government agencies to provide value-added services by defining a new service that can overcome the limitations of the previous e-government services. It is most likely due to the fact that web services are interoperable. However, some of these government web services are loosely coupled and therefore are unreliable. So, we need to develop a Security trust model which helps in securing and providing are liable communication. These Security trust model will be controlled by a third party under the supervision of governmental agency. The trust model helps to achieve the objectives: secure the communication and interaction between e-governmental web services. It is based on a trusted third party controlled by any governmental agency in order to provide an identity for both, web service consumer and provider. This can be used when both parties are communicating or interacting and they can identify each other through this identity provided by the third trusted party.

KEYWORDS: Authentication; Web based services; information flow control; online information service, verification; cryptographic controls

I. INTRODUCTION

The web based services are widely used now a days. This application needs to be secured and reliable for the user. If any of the attacker attacks on the website then, the sensitive data can be misused. It is also necessary to test the weather both parties(user and web service) are genuine or not. Thousands of people rely on the E-governmental services. So this data should be protected.

The third party plays an important role in E-governmental web services. The third party will use JSON web token for verification purpose. The third party will send an token request to both the parties. If the parties token verification is successful then only further communication will process. If any of the parties does not seems to be genuine then third party rejects further communication. The intermediate third party makes E-governmental web service more reliable to use. With this token verification process many of the unauthorized users are not able to use the E-governmental web service data.

Another way through which data can be protected is encrypting and decrypting. Through encrypting and decrypting algorithms data packets can be encrypted at the sending side and will be decrypted at the receiver side. Sending side and receiving can be user and E-governmental web service or vice versa. If the data gets attacked and attacker captures the packets then attacker cannot read the information as the data is encrypted. This makes web service more secured compared to the other web services. So, token verification and data encryption, decryption are main focus of this paper. The privacy of the E-governmental web service will be maintained. This trust model can be implemented on various governmental projects in which privacy, integrity and reliability is much needed.

II. RELATED WORK

In this paper the author's have used open source web technologies. The main reason for choosing open source technologies are it makes the project cost very cheaper, on many of the platforms this technologies are accepted, plenty of information are available on the internet which guide fresher's and experience people in field of technology. The open source technology is widely used. The whole concept depends upon token verification. For the token verification JSON(JavaScript Object Notation) will be used. JSON are quick, faster in work process and verifies token from both

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

parties very easily. JSON Web Token (JWT) is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA. This is a stateless authentication mechanism as the user state is never saved in server memory. The server's protected routes will check for a valid JWT in the Authorization header, and if it's present, the user will be allowed to access protected resources. As JWTs are self-contained, all the necessary information is there, reducing the need to query the database multiple times.JST can handle multiple token requests from both parties without any conjunction or mismatching problems. JSON web tokens serves the purpose. For the encryption & decryption purpose JSON Web Encryption can be used. JSON Web Encryption (JWE) represents encrypted content using JSON-based data structures. Cryptographic algorithms and identifiers for use with this specification are described in the separate JSON Web Algorithms (JWA) specification and IANA registries defined by that specification. Related digital signature and Message Authentication Code (MAC) capabilities are described in the separate JSON Web Signature (JWS) specification. For this trust model many of the protocols will be used such as SOAP, HTTP. This protocols allows less costly interactions on the internet. The systems interact with the web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP in conjunction with other web related standards. XML is the data format used to contain the data and provide metadata around it. Different web application may use different programming languages , and hence there is a need for a method of data exchange that doesn't depend upon a particular programming language. Most types of software can, however, interpret XML tags. Thus, Web services can use XML files for data exchange.

III. WEB SERVICE SECURITY CHALLENGES

Security is critical to web services. However, neither XML-RPC nor SOAP specifications make any explicit security or authentication requirements. There are three specific security issues with web services.

Confidentiality: If a client sends an XML request to a server then we need to ensure that the communication remains confidential. To maintain confidentiality we need to make use of XML-RPC and SOAP which will run primarily on top of HTTP. HTTP has support for Secure Socket Layer (SSL).The communication can be encrypted via SSL. SSL is a proven technology and widely deployed over the network.

A single web service may consist of a chain of applications. For example, one large service might tie together the services of three other applications. In this case, SSL is not adequate so the messages need to be encrypted at each node along the service path. In this each node represents a potential weak link in the chain. Presently, there are no good solution to this issue, but one promising solution is the W3C XML Encryption Standard. This standard provides a framework for encrypting and decrypting entire XML documents or just portions of an XML document.

Authentication: If a client connects to a web service then we need to identify the user. Whether the user is authorized to use the service. There are various options that can be considered but there is no clear consensus on a strong authentication scheme. One option is to use HTTP that includes built-in support for Basic and Digest authentication, and services can therefore be protected in much the same manner as HTML documents are currently protected. Another option is to use SOAP Digital Signature (SOAP-DSIG) that leverages public key cryptography to digitally sign SOAP messages. It also enables the client or server to validate the identity of the other party. The Organization for the Advancement of Structured Information Standards (OASIS) is working on the Security Assertion Markup Language (SAML).

Network Security: Presently it is difficult to provide a agreed-upon solution to this problem and it has been the subject of much debate. For now to filter out SOAP or XML-RPC messages, one possibility is to filter out all HTTP POST requests that set their content type to text/xml. Another alternative is to filter the SOAPAction HTTP header attribute. Firewall vendors are also currently developing tools explicitly designed to filter web service traffic.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

IV. PROPOSED SECURITY TRUST MODEL

We are going to describe the proposed trusted model with the help of which we are trying to establish a secure communication between the government services and the users. This will be controlled by a third party which will be under the supervision of governmental agency. This will help in providing a secure communication channel.
This third party will get requests from both the parties which will be requesting for identity. The third party will provide them identities through JSON Web Tokens**.** This JWT will be then used for verification purpose for providing a secure communication. The JWT is a compact and self-constrained that provides secure transmission of information between two parties as a JSON object. The third party will encrypt the data by using the JWE before sending the data through a SOAP communication channel. Also JWS will ensure that the data that is being encrypted is digitally signed and authenticated. This whole communication will be controlled by the Security trust model.

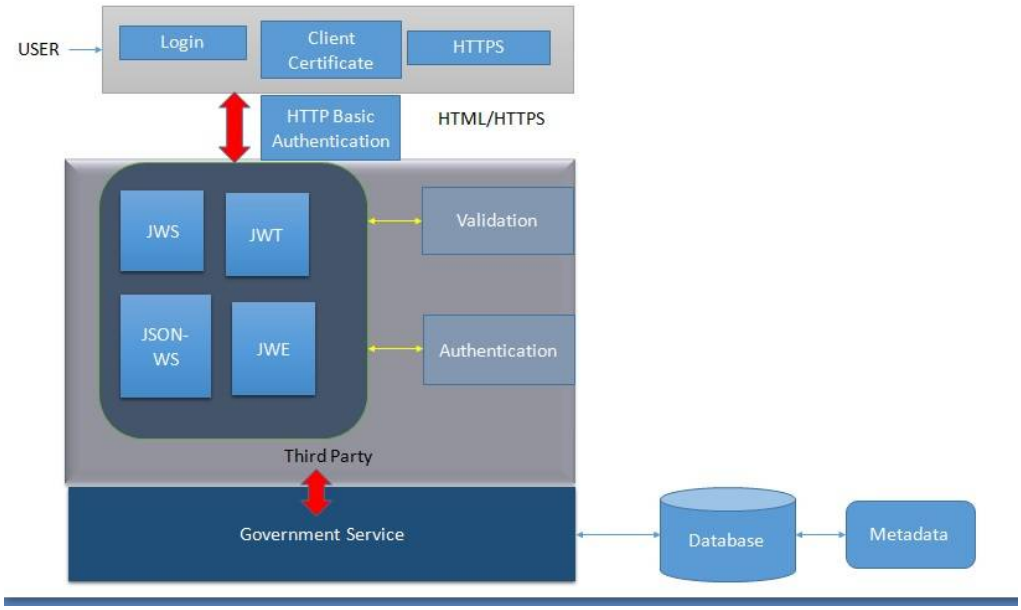

Fig.1. Architecture Diagram

V. CONCLUSION AND FUTURE WORK

We have improved security of E-Governmental web agencies. We have integrated third party in middle of user and web agencies for secured communication. The report reviews the implementation of trusted model for securing the E-Government web services. It is a secured web service so the user can rely for communicating with these agencies. The report outlines two approaches of web application that are token is verified from both the parties for securing the data and data is encrypted-decrypted to protect the data from attacks.

REFERENCES

1. Bassam Al-Shargabi ,"Security Engineering for E-Government Web Services:A Trust Model" , International Conference on Information Systems Engineering, 2016
2. Love Adedayo ,Ron Ruhl, Dale Lindskog, "E-Government Web services and Security of Personally Identifiable Information in Developing Nations", The 8th International Conference for Internet Technology and Secured Transactions , 2013
3. Rui Song, Bixin Li, XiaonaWu, Cuicui Liu, Shanshan Qi, "A Preference and Honesty Aware Trust Model for Web Services" 19th Asia-Pacific Software Engineering Conference, 2012
4. Zhendong Ma, Christian Wagner, Thomas Bleier, "Model-driven security forWeb services in e-Government system: ideal and real", 7th InternationalConference on Next GenerationWeb Services Practice, 2011
5. Wang Shao-Jie Shen Gui-Cheng Zheng Xue-Feng ,"A Trust Model of Web Services Based on Individual Experience" , IEEE Computer Assurance Systems Engineering , 2011

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

6. Wei She, Bhavani Thuraisingham, and I-Ling Yen , "Delegationbased Security Model for Web Services" , IEEE High Assurance Systems Engineering Symposium ,2010
7. Yumi Yamaguchi1, Hyen-Vui Chung2, Masayoshi Teraguchi1, and Naohiko Uramoto1 , "Easy-To-Use Programming Model for Web Services Security" , IEEE Asia-Pacific Services Computing Conference , 2007
8. Brahim Medjahed, Athman Bouguettaya "Customized Delivery of E-GovernmentWeb Services", IEEE Computer Society , 2005