A Study On Trusted Model For Securing The E-Government Web Services

[1]Dr. Harshali Patil, [2]Dr. Ashish Kulkarni, [3]Dr. Swapnil Undale
[1,2,3]Assistant Professor,
Dr. Vishwanath Karad MIT World Peace University,
Pune, India.

Abstract: In rise of the web applications of web services which provides an 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. By establishing a new service that can overcome the limits of earlier e-government services, government agencies can create value-added 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. The model 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**.**

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 day. 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 a 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. LITERATURE REVIEW

Al-Shargabi Bassam (2016) researched in the area of the application of web services opens new dawn for e-government applications due to its interoperability that brought by application of web services. Securing the communication between web services has been progressively becoming more demanding requirement for users, administrators, and web service providers. Thus, the need for a security trust model to ensure a proper and secure communication between web services. In this paper, a security trust model is introduced to secure the communication and interaction between governmental web services through a trusted third party controlled by any governmental agency.

Adedayo L, Butakov S, Ruhl R (2013) explored the processing of PII data in e-Government web services in developing countries. It presents a secured framework intended for protecting Personally Identifiable Information (PII) data in e-Government web services in developing nations where such do not already exist. The framework is based on the OWASP ASVS security requirement for data protection in the web environment, which was used as the basis of assessment for the respective website by analyzing the security of the web portal used in processing citizens' registration data using a non-invasive web site analysis method.

Yen I-Ling Yen (2007) noted that web service is the emerging standard that supports the seamless interoperation between different applications. While the interoperability, flexibility and automated composition are continuously enhanced, security is still the major hurdle. In recent years, lots of studies

have been conducted in web service security and various security standards have been proposed. But most of these studies and standards focus on the access control policies for individual web services and do not consider the access issues in composed services. Consider a simplest service chain wherein a user x accesses service s1, and s1, in turn, accesses service s2. The current web service security framework assumes s1 accesses s2 based on its own privilege; thus sensitive information may be incorrectly revealed to x. A better solution is that x delegates its privilege to service s1 for this access. However, problems such as how much privilege to delegate, how to confirm cross-domain delegation, how to delegate additional privilege when needed, etc. arise. The problem becomes more complex when workflow involves many layers of services. In this paper, we propose a delegation-based security model to address all these issues. It extends the basic security models and supports flexible delegation and evaluation-based access control.

Medjahed B, Bouguettaya A, (2005) reported that web is revolutionizing the way citizens interact with businesses and government agencies. Almost all key functions of modern society are being reshaped to exploit opportunities the Web opens. As part of an effort to improve government- citizen interactions, government agencies are providing a wide spectrum of online services.Virginia Tech is collaborating with the Virginia Department for the Aging (VDA) on a project called WebSenior. A middleware infrastructure, WebSenior automatically delivers e- government services customized for seniors. It uses ontologies to automatically generate Web services customized to senior citizens needs and government program laws and regulations.

Attar A (2007) noted that in rise of the web applications of web services which provides an 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. By establishing a new service that can overcome the limits of earlier e-government services, government agencies can create value-added 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.

Curran, Kevin, Paul, (2007) reported that in the world of information technology, a security model is only as secure as its weakest link. There are several layers of security and different measures that can currently be implemented. However, they lack coordination, and therefore potential security breaches might compromise the network. With wireless access becoming the norm, and users requiring & the move communication & quota, even within a campus, networks are expanding past the traditional wired networks by adding wireless access points. This gives customers the flexibility they require but leaves a net threat vector to the network. There have been various encryption and security steps taken to validate the communication and authentication of the devices and end users connecting. This project addresses the critical problem of secure authentication using the 802.1x standard, which will be implemented using Microsoft's Radius server elements. It will involve the enrollment of secure certificates on Windows mobile devices, thus securing mobile devices from physical attacks. To ensure that all steps are adhered to, that all necessary applications have been installed, and to handle Web service communication, an application will be created that will provide an automated solution.

Marwell, Nicole, (2015) noted that much existing scholarship on nonprofit organizations' receipt of government funds appears to assume that there is something highly problematic about the relationship. Although rarely articulated in these studies, the concern about the negative effects of government funding turn on a view of nonprofits that privileges their private character. In this article, rather than examining how public funds constrain private action, we inquire about how government deploys private organizations, via the mechanism of government funding, to secure a public good. Using a case study of the nonprofit child welfare sector in New York State, we theorize a deficit model of collaborative governance in which nonprofits have been deputized by the state to secure children's social rights but do not receive sufficient resources to cover the costs of securing those rights. Then, we connect this theory to organization-level financial management practices that pose challenges to the nonprofits of both survival and service quality. This nonprofit organizational instability concerns the state insofar as it threatens the securing of individuals' social rights.

Jaamour, Rami (2005) provided perspective of security operations in the light of Web services, seeking to further the discussion concerning the security implications of Web services and their oversight. It should be mentioned that safeguarding one's Web services is a critical component of a successful deployment.

Only secure Web services can provide an acceptable integration solution when deployed externally for consumption by partners or consumers, because the benefits they disclose should far outweigh the risks. Using the right tool for the job is important, both in terms of products and technologies.

Sturtevant, Cameron (2005) analyzed the issues raised by following three new security specifications: WS-Security Policy, WS-Secure- Conversation and WS-Trust. The three specifications submitted to the Organization for the Advancement of Structured Information Standards define the process of working with security tokens, brokering trust relationships, securing messaging, establishing security context and defining security policy assertions-- basically, how Web services can establish a trusted relationship and then carry out reliable communication inside the trust domain. The submission of these specifications continues a tradition, started in 2002, where International Business Machines Corp. and Microsoft Corp. first announce the evolution of their Web services security work at Burton Group's Catalyst Conference North America. The announcements at the conference came at the same time that attendees were voicing concerns about identity management. Many attendees raised the issue that the growth of service-oriented architecture will depend on the reliability of user identity. INSET: Security and identity.

III. RESEARCH METHODOLOGY

The study was conducted on the basis of questionnaire through which we get to know that how much people are aware about the e-governance web services. The method used for the research purpose is the questionnaire method is that method in which a number of questions ask for collecting the data. This list of questions is handed over to the respondents either by the investigator personally or via google form link submit over E-Mail. After providing their feedback by filling up the questionnaire, they return it to the investigator. The details of the project design are as follows:

IV. SCOPE AND LIMITATIONS

4.1 Scope: The study was conducted in to the particular region that was in pune city. Here the investigation was done on 'The E-Government Web Services' used in our day today life. Here we find that how much the people are aware about the government web services. Weather they use this kind of services, how much they trust on this services and the last thing is that how much they trust on this government web services.

4.2 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.

4.3 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).

4.4 Network Security: Presently it is difficult to provide an 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. The Another alternative way to filter the HTTP header is Firewall vendors are also currently developing tools explicitly designed to filter web service traffic.

4.5 Limitations: Security is critical to web services. However, specifications make any explicit security or authentication requirements. Here are three specific security issues with web services that we faced during the research.

V. DATA ANALYSIS

Table 1. Descriptives of Demographics

Variable		Frequency	Percentage
Age	10-20	5	15.6
	21-30	19	59.4
	31-40	5	15.6
	> 40	2	6.3
Gender	Male	22	68.8
	Female	9	28.1
Occupation	Student	22	68.8
	Business	5	15.6
	Employee	4	12.5
Education	10 th	2	6.3
	12 th	2	6.3
	Graduate	9	28.1
	Post Graduate	18	56.3
Area	Rural	9	28.1
	Urban	22	68.8

Table 2. Descriptive Statistics of Dependent Variables

	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Private web services are secure than E-government web services	3.84	.779	-.156	.421	-.357	.821
Government has to spend more on the securing E-government web services.	3.87	.885	-.043	.421	-1.118	.821

H_1-There is significant difference between male and female

Table 3. T-Test: Group Statistics-Gender

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Private web services are secure than E-government web services	Male	22	3.68	.716	.153
	Female	9	4.22	.833	.278
Private web services are secure than E-government web services	Male	22	3.91	.971	.207
	Female	9	3.78	.667	.222

Table 4. Independent Samples Test-Gender

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Private web services are secure than E-government web services	Equal variances assumed	.455	.505	-1.820	29	.079	-.540	.297	-1.148	.067
	Equal variances not assumed			-1.705	13.110	.112	-.540	.317	-1.225	.144
Private web services are secure than E-government web services	Equal variances assumed	3.292	.080	.370	29	.714	.131	.355	-.595	.858
	Equal variances not assumed			.432	21.698	.670	.131	.304	-.499	.762

Result-p value>0.05 we accept the NULL hypothesis. So, gender wise as per their opinion that private web sites are more secure than government website and government have to spent more for securing their website.

H_1-There is significant difference between Student and Business/Employee person

Table 5. T Test- Group Statistics-Occupation

	Occupation	N	Mean	Std. Deviation	Std. Error Mean
Private web services are secure than E-government web services	Student	22	3.68	.780	.166
	Business/Employee	9	4.22	.667	.222
Private web services are secure than E-government web services	Student	22	3.91	.971	.207
	Business/Employee	9	3.78	.667	.222

Table 6. Independent Samples Test-Occupation

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Private web services are secure than E-government web services	Equal variances assumed	.676	.418	-1.820	29	.079	-.540	.297	-1.148	.067
	Equal variances not assumed			-1.947	17.389	.068	-.540	.278	-1.125	.044

Private web services are secure than E-government web services	Equal variances assumed	3.292	.080	.370	29	.714	.131	.355	-.595	.858
	Equal variances not assumed			.432	21.698	.670	.131	.304	-.499	.762

Result-p value>0.05 we accept the NULL hypothesis. So, Occupation wise as per their opinion that private web sites are more secure than government website and government have to spent more for securing their website.

H_1-There is significant difference between Rural and Urban

Table 7. T-Test- Group Statistics- Area

	Area	N	Mean	Std. Deviation	Std. Error Mean
Private web services are secure than E-government web services	Rural	9	4.11	.601	.200
	Urban	22	3.73	.827	.176
Private web services are secure than E-government web services	Rural	9	3.89	1.054	.351
	Urban	22	3.86	.834	.178

Table 8. Independent Samples Test- Area

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Private web services are secure than E-government web services	Equal variances assumed	2.852	.102	1.258	29	.219	.384	.305	-.240	1.008
	Equal variances not assumed			1.438	20.510	.165	.384	.267	-.172	.940
Private web services are secure than E-government web services	Equal variances assumed	.333	.569	.071	29	.944	.025	.356	-.703	.753
	Equal variances not assumed			.064	12.310	.950	.025	.394	-.830	.881

Result-p value>0.05 we accept the NULL hypothesis. So, Area wise as per their opinion that private web sites are more secure than government website and government have to spent more for securing the website.

H_1-There is significant difference between Graduate and Post graduate

Table 9. Independent Samples T-Test- Group Statistics- Education

	Education	N	Mean	Std. Deviation	Std. Error Mean
Private web services are secure than E-government web services	Graduate	11	3.82	.874	.263
	Post Graduate	18	3.78	.732	.173

Private web services are secure than E-government web services	Graduate	11	3.55	.820	.247
	Post Graduate	18	4.11	.758	.179

Table 10. Independent Samples Test- Education

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Private web services are secure than E-government web services	Equal variances assumed	1.386	.249	.134	27	.894	.040	.301	-.578	.659
	Equal variances not assumed			.128	18.424	.899	.040	.315	-.620	.701
Private web services are secure than E-government web services	Equal variances assumed	.390	.538	-1.890	27	.069	-.566	.299	-1.180	.048
	Equal variances not assumed			-1.854	19.972	.079	-.566	.305	-1.202	.071

Result-p value>0.05 we accept the NULL hypothesis. So, Education wise as per their opinion that private web sites are more secure than government website and government have to spent more for securing the website.

VI. FINDINGS

A majority of respondents, i.e. 61.29% of the respondents are of the age group 21-30, moderately responses is given by the age group of 10-20 and 31-40 have same response of 16.13% and the minor response is given by the age group of above 40 and i.e.6.5%. A majority of respondents, i.e. 73.20% of the respondents are Male and 26.80% are Female. Almost all the respondents are student i.e. 70.97 and rest of business person and employee the percent are 16.13% and 12.90% respectively. Almost all the respondents are post graduate i.e. 58.06%, graduate are 29.03% and the other respondent are from 10^{th} &12^{th} and their %is 6.45% respectively. Almost all the respondents are from urban i.e. 70.97% and rest of the other are 29.03% they are rural respectively.

Almost all the respondents are the user which always use the internet and their percentage is 48.39, often user are 25.81%, rarely user are 9.68% and the person who don't use internet are 3.23%. Majority of the respondent reply that they use the E-Government Web Services sometime and their percentage is 45.16, and rarely user, often user, and always user have the percentage 16.13 and never users are 6.45% respectively. Majority of the respondent are agreed with that the E-government web-sites are safe Majority of the respondent are sometime aware about the inappropriate use of "Data" on web sites. Majority of the respondent are sometime prefer using the E-government web services than other web sites. Majority of the respondent think "Bio-metric" login will help to securing the E-governments web-services and their percentage is 86.21.and 13.79%responces are in NO. Majority of the respondent think "OTP" login will help to securing the E-governments web-services and their percentage is 97.10.and 12.90% responses are in NO. Majority of the respondent think "photo/picture" login will help to securing the E-governments web-services and their percentage is 83.87.and 16.13% responses are in NO. Majority of the respondent think "By integrating the third party in middle of user and web agencies for secure communication is going to be useful and their percentage is 77.42.and 22.58% responses are in NO. Majority of the respondent think that hacking and phishing are the major factor affecting the government web services and their percentage is 28.57 and 26.19 and the less responses are for sql and spam and their percentage are 25 and

20.Majority of the respondent think "HTTPS" is secure for web services and their percentage is 96.77.and 3.23 % responses are in NO. Majority of the respondent think "WAF" (web application firewall) secure the web sites of E-government and their percentage is83.87% and 16.13% responses are in NO. Majority of the respondent think "JWT" (Json web tokens) is good for using verification purpose for web sites and their percentage is70.97% and 29.03% responses are in NO. Majority of the respondent agree that the private web services are secure than E-government web services and neutral are 29.03% and strongly agree are 19.35%Majority of the respondent are neutral their percentage is 35.48% agreed are 32.26% strongly agreed are 29.03% and disagree are in percentage of 3.23 to spend more on the securing E-government web services.

VII. Conclusion

This report provides the implementation of trusted model for securing the E-Government web services in two ways. first is a secured web service, so that user can rely for communicating with these agencies, in this token is verified from both the parties for securing the data and the other way is data is encrypted-decrypted to protect the data from attacks.

VIII. Future scope of research

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. we can implement such more models to secure the sensitive data that can be misused.

IX. 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 Lindsborg," 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.

[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.

[9] ABDUL-RAHMAN, A. AND HAILES, S. 2000. Supporting trust in virtual communities. In Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00). IEEE Computer Society, 1–9.

[10] ADALI, S., ESCRIVA, R., GOLDBERG, M. K., HAYVANOVYCH, M., MAGDON-ISMAIL, M., SZYMANSKI, B. K., WALLACE, W. A., AND WILLIAMS, G. 2010.

[11] Measuring behavioral trust in social networks. In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI'10). 150–152.