Establishing Trust in e-Governance using Web Services

Sachidananda Patnaik

Research Scholar, Dept. of Computer Science,
Biju Patnaik University of Technology, Rourkela, Odisha, India
Sachipatnaik2008@gmail.com

Abstract Trust Management is one of the most challenging issues in the emerging Web Engineering and Internet Technologies. Over the past few years, many studies have been proposed different techniques to address trust management issues. However, despite these past efforts, several trust management issues such as privacy, security, accessibility, integrity and scalability have been mostly ignored and need to be proposed in Web Engineering technologies. Web services provide many opportunities for enterprises to built trustworthiness. In India the growing economic infrastructure with lightening speeds towards the adoption and successful implementation of e-governance. Establishing trust in e-governance services is quite important as now government has many services for common man at their door step and more services are in future. But the common man has to know about it and have used frequently for their daily requirements. This paper is emphasized to trust on the web services and what steps should be adopted for better service.

Keywords: Trust Management, Web Services, e-Governance, Trust Models.

Citation: Sachidananda Patnaik. Paper Title. *Establishing Trust in e-Governance using Web Services*. Vol. X, No. X, 2014, pp. XX-XX.

Introduction

Technological advancement has enabled governments across the globe to explore online facilities in offering a range of services to their citizens. One necessary element of offering quality online services is to understand citizen's view, opinion and perception towards using such services in contrast with the traditional service methods that they are accustomed to. E-governance has been a popular topic and countries across the world are actively investing resources to improve the public services. Despite the significant progress made in e-services, research indicates that citizens as main customers are unaware taking the advantages of different quality of services. This may be due to the poor quality of traditional services and/or lack of public trust in using them.

Trust is not a new research topic in computer science, spanning areas as diverse as security and access control in computer networks, reliability in distributed systems and policies for decision making under uncertainty. Perhaps the most notable example was the development of the Trusted Computer System Evaluation Criteria (TCSEC) in the late 70s and early 80s. Here, trust was used in the process of convincing observers that a system (model, design or implementation) was correct and secure [6].

Trust in the information society is built on various different grounds, based on calculus, on knowledge or on social reasons [7]. The notion of trust in an organization could be defined as the customer's certainty that the organization is capable of providing the required services accurately and infallibly. A certainty which also expresses the customer's faith in its moral integrity, in the soundness of its operation, in the effectiveness of its security mechanisms, in its expertise and in its abidance by all regulations and laws, while at the same time, it also contains the acknowledgement of a minimum risk factor by the relying party. The notion of security refers to a given situation where all possible risks are either eliminated or brought to an absolute minimum.

Overview of Trust Management

In reality, trust is a social problem then technical problem. Broadly speaking, Trust means as act of faith; confidence and reliance in something that is expected to behave or deliver as promised by the provider. Trust Management is originally developed by Blaze et.al [Blaze et. al 1996] to overcome the issues of centralized security systems of trust relationships, inflexibility of support complex trust relationships in large scale networks and the heterogeneity of policy makings. Policy making in trust management are responsible for setting authorization role and implementing security role. There are many issues related to the management of trust such as Control, Ownership, Prevention and Security [6]. In traditional architectures, trust was enforced by an efficient security policy, which addressed constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people [8, 9].

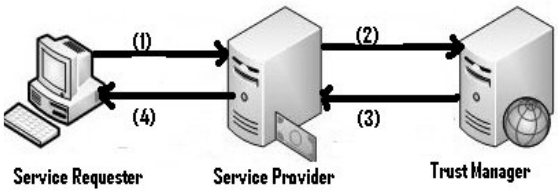

Figure 1. Overview of Trust by using Web Services

The trustworthiness of a network is reflected in three aspects: trust of web services, trust of users and trust of

network transmission. When a user accesses resource in the different domains, there is a trust issue of authentication, namely subject identity authentication for resource requester and object service authentication for resource provider. The former concerns whether a service requestor has access to the resource provider, that is to say, the access rights of service requestor; while the latter considers whether services of an object are available to the requester, namely the service trust of object [3].

Trust and reputation are related with each other closely. However, trust is quite a complicated phenomenon, the concept itself carrying many meanings. If entity A recognizes that entity B will do whatever A expects in strict way, then A will trust B. A is trustful and B is credible.

Trust can be defined as "Trust T is a function of a pair (TR, TE) where TR is a trustor who has a certain level trust on others and TE is the trustee who is trusted by the trustor. The output of this function TV is a trust level which is often represented by a value. T: TR * TE -> TV.

An overview of the trust management approach to authorization and access control is given in Fig 1.

- Requester request for service.
- Provider gathers information and sends to trust manager for trust verification.
- Trust manager verifies trust and give the result to provider.
- Accept/deny request of requester based on trust manager result.

Feature & Need of Trust

Although the definition of trust is not strict standard, but overall, the trust has the following features.

- Subjectivity, there may be different trust degree for the same entity among different entities.
- Context it is not only to consider the influences of subjective consciousness, but also to contact with the specific environments and context, when entity evaluates the trust relationship. Namely, it is context dependency.
- Asymmetry A trusts B. whereas, it may not correct.
- Dynamic Trust relationship between entities is not eternal. It will be changed dynamically when the requestor's behaviours change. For example, the trust degree will decrease with the passage of time.
- Measurable the subjective trust evaluation can be measured accurately by many decisive factors.

Trust is a measure of relation between a pair of entities. This measure can be used as a calculus to make further decisions. Trust can be helpful in solving many problems, including resource access, filtering information, and resolving inconsistencies [2].

There are two broad types of trust 1. Direct Trust 2. Indirect Trust. The direct trust of an entity can be determined directly from the history of interactions of entity. The indirect trust of an entity can be determined by other entities experiences indirectly.

Trust Model using Web Services

Typical interactions on the Service Web involve four types of entities: (i) Web Services, (ii) Service Providers, (iii) Service Registries, and (iv) Service Consumers

- Web Services: A Web service is a software application identified by a URI (Uniform Resource Identifier), whose interface and binding are defined, described and discovered by XML artefacts, and supports direct interaction with other software applications using XML messages via Internet-based protocols. A Web service may be viewed as a set of operations, where each operation is a "processing unit" that consumes input values (called its parameters) and generates output values called the result of that operation's invocation. For the sake of focus and clarity, we assume only a single operation per service.
- Service Providers: The service provider is the entity that provides the service, i.e., makes it available to consumers. A service provider may be a business, a government agency, an academic institution, etc. A provider may provide one or more services. A service is provided by a single provider. Providers have publicly known identities. The provider owns the service. It may or may not actually manage the service.
- Service Registries: A service registry is a searchable directory that contains a collection of descriptions of Web services. A service registry has two components: a repository of service descriptions and a registry engine that answers the requests sent to the registry by service providers and service consumers. A service registry may be private or public. Any provider may advertise its capabilities by publishing the Web service in a public registry. A private registry may be used only by a limited, known set of providers to publish services.
- Service Consumer: A service consumer is any entity that invokes a Web service, e.g., an intelligent agent, a Web application, or another Web service. A human user may also invoke a Web service, but we assume that each user is represented by a software component (defined: proxy) in the system.

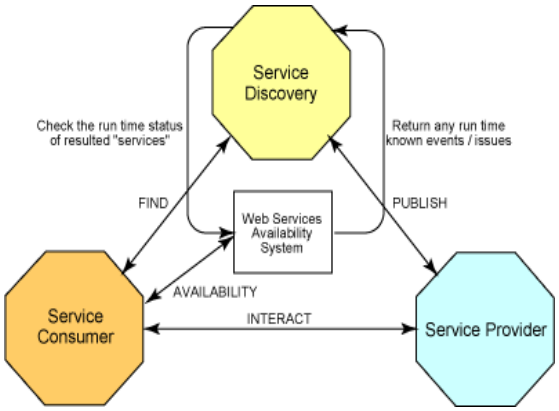

Figure 2. Architecture of Trust based Services

The following key steps are performed by the Trust Engine of a Web Service:

- Verify that the claims in the token are sufficient to comply with the policy and that the message conforms to the policy.

- Verify that the attributes of the claimant are proven by the signatures. In brokered trust models, the signature may not verify the identity of the claimant – it may verify the identity of the intermediary, who may simply assert the identity of the claimant.
- Verify that the issuers of the security tokens (including all related and issuing security token) are trusted to issue the claims they have made. The trust engine may need to externally verify or broker tokens (that is, send tokens to a security token service in order to exchange them for other security tokens that it can use directly in its evaluation).

In addition, the proposal provides a general mechanism for multi-message exchanges during token acquisition. One example use of this is a challenge-response protocol. This is used by a web service for additional challenges to a request or to ensure message freshness and verification of authorized use of a security token. This model is a deterministic trust model. It proposes a recursive schema to establish trust relationships.

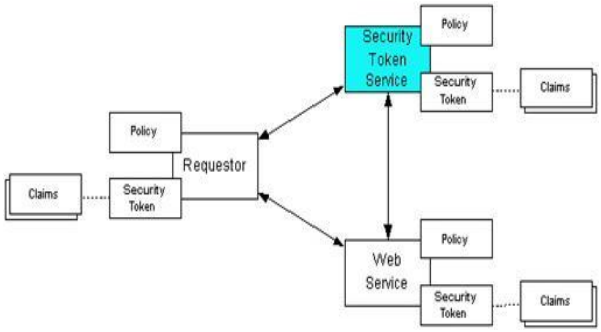

Figure 3. Web Service-Trust Trust Model

Web Service Trust in e-Governance

E-Services can be defined as the web services which are delivered through the internet. In e-service customer's interaction contact with service providers is through different web technologies such as their web sites, web applications or mobile applications. Zeithmal, Parasuraman and Malhotra [8] conceptualize the e-service as an information service where the primary value is swapped between the buyer and seller in the form of information. Services in e-Government play a very important role with specific, dynamic, explicit and implicit needs. A common classification of service in e-government is related to the users: Government-to-Citizen (G2C) services provide full support to the common citizen, Government-to-Business (G2B) services to support different organization that includes government organization, private organization and volunteer organizations, Government-to- Government (G2G) services to the same or different administrations within the circles and Government-to-Employee (G2E) service for the employability.

In e-Governance, the government to citizen (G2C) has identified factors facilitating citizen's adoption of e-government websites and also their consequent impact. Trusting beliefs that an e-government website will act responsibly when a citizen or public visits with it are central to e-government website success. If the goal is to develop and implement e-governance then it is useful to examining functional objectives. Functional objectives of e-governance system and services includes

a) Availability of information in the form of data across multiple delivery channels.
b) Reliable and secure transaction across the channels.
c) Reasonable social, political and economical returns.
d) Trustworthy and transparency in services.
e) Wide rich of citizens in respect of multilingual.
f) Collaboration and partnership among government, private sector and community organization.

Government, like most businesses, has a number of core processes that are essential to the successful operation of the enterprise, some of which may be more important in specific socio-economic and cultural situations than others. Based on extensive experience with businesses, government agencies and other organizations of the second author, we define these core processes as:

- *Procurement:* Enables government to procure or tender.
- *Receipts:* Enables government to receive monies from the general public towards taxes, services, fines and other dues
- Payments: Enables Government to pay the recipients (suppliers, citizens for pensions, refunds, etc.)
- *Information:* Enables the government at all levels to access/create/acquire, gather, manage, organize, preserve, remove, and disseminate information about citizens, organizations, companies, research and development, activities, etc. Enables the citizen to access information about actions of the government, rules, regulations, services, etc.
- *Lodgment/Transact:* Enables the general public to submit and/or process applications, register documents to the government for various services and obligations, and obtain other services
- *Public Complaints:* Enables the public to relay grievances effectively and conveniently to the government
- Public Safety and Health: Enables public awareness and involvement in their safety and health.
- *Public Records and Archives:* Enables citizens to access records generated by and for the government that are not exempted by law.

Establishing Trust in e-Governance

Trust is the biggest issue in web services as well as in services of e-governance. In respect of Cloud Computing as services, security is an important issue while utilizing storage service on a remote location, the consumers are generally unaware of what happen about the data they processed or accessed. In fact, consumers themselves have less control to secure the data they host on the cloud. The trust mechanism has proven to be an appropriate substitute to the aforesaid security issues as it establishes entities' relationship quickly and safely. Since trust is purely an abstract and a subjective term; therefore, it is ordinarily difficult to tangibly measure and effectively manage it.

A security architecture can be defined in three levels such as *Software Security* (identity authentication,

Management, access control), *Platform Security* (Framework security, component security, interface security) and *Infrastructure Security* (virtual environment security, shared storage security).

Nepal et al. proposed a framework to built trust communities for secure access of data

- *Personal Background*: A user's personal information must require for future use that what type of user and what about his hobbies and activities and his/her requirements.
- *Social Capital*: The basic purpose is to create an environment for interaction with other services and also services can provides what actually the user wants.
- *Social Trust*: In this step, the social trust of an individual member and of the community as whole is evaluated based on social capital. We refer to the latter two steps as creating a *social model.*
- *Recommendation*: The last step in our approach is the generation of recommendations based on trust. The aim of the recommender is to make the online community relevant to the members so that we can increase the social capital and social trust, which in turn is used again by the recommendation system to recommend new activities or content. This cycle continues, first to build the trust community and then to ensure its sustainability. This is required because trust decays with time (which is sometimes refers to as *ageing*).

Conclusion

This paper presents concepts of trust management using web services in e-governance application and services. The existing research is concentrated on trust based on reputation, behavior, recommendation and identity. Government has many policies for the common consumer and that has in the form of services. But most of consumers are not exactly using the services due to trustworthiness. Trust on services is very important scenario and consumers has to trust on services. We emphasize on establishing trust model and trust procedures in e-governance application and for this purpose web services is very important. The future research of this work leads to development of different trust model for e-governance.

References

[1] S. Patnaik "Trust Management in E-Governance Services", 2nd National Conference on Advanced Computing Techniques & Applications-2014, pp. 54 – 58.

[2] R.J. Manoj and A. Chandrasekar "A Literature Review on Trust Management in Web Service Access Control", International Journal on Web Service Computing (IJWSC), Vol. 4, No. 3, Sep 2013.

[3] H. Limam and J. Akaichi "Managing Web service Communities: A Cache for Queries Optimization", International Journal on Web Service Computing (IJWSC), Vol. 1, No. 1, Sep 2010.

[4] Z. Malik and A. Bouguettaya "RATEWeb: Reputation Assessment for Trust Establishment among Web Services", The VLDB Journal (2009) 18:885-911.

[5] Thompson S.H. Teo, Shirish C. Srivastava and Li Jiang "Trust and Electronic Government Success: An empirical Study" Journal of Management Information Systems/Winter 2008-9, Vol. 25, No. 3. Pp. 99-131.

[6] W. Zhao and V. Varadharajan "Trust Management for Web Services" IEEE 2008 Int. Conference on Web Services.

[7] Y.L. Sun, Z. Han, W.Yu and K.J.R. Liu "A Trust Evaluation Framework in Distributed Networks Vulnerability Analysis and Defense Attack" IEEE INFOCOM, pp 1 – 3, 2006.

[8] G.U. Lize, W. Jingpei and S. Bin "Trust Management Mechanism for Internet of Things" China Communication 2014, pp 148 – 156.

[9] D. Lekkas "Establishing and Management Trust within the Public key Infrastructure", Computer Communications 26(16) (2003).

[10] Syed F.H. Zaidi, F. Marir and S.Siva "Accessing e-Government Service & Trust: Government to Citizen" ICDS 2013: The Seventh International Conference on digital Soecity.

[11] S.K. Prajapati, S. changder and A. Sarkar "Trust Management Model for Cloud Computing Environment" Proceedings of ICCCAN – 2013.

[12] V.A. Zeithaml, A. Parasuraman and A. Malhotra "Service Quality Delivery Through Web Sites: A Critical Review of extant knowledge" Journal of the Academy of Marketing Science Vol. 30, No.40, pages 358-371.

[13] A. Agraval, P. Shah and V. Wadhwa "EGOSQ – Users' Assessment of e-Governance Online-Services: A Quality Measurement Instrumentation" CSI Publications.

[14] J. Sun, Z. Sun, Y. Li and S. Zaho "A Strategic Model of Trust Management in Web Services" SciVerse Science Direct Physics Procedia 24 (2012) 1560 – 1566.

[15] W. Zhao and V. Varadharajan "Trust Management for Web Services" IEEE 2008 Int. Conference on Web services.

[16] S. Patnaik and A.K. Misro "Different Test Cases for e-Governance using Web Services" ICDCIT-2011, International Journal of Computer & Communication Technology (IJCCT), Vol. 2, Issue 5, pp. 30 – 34, ISSN: 0975 – 7449.

[17] S. Patnaik, R.K. Das and A.K. Misro "Adoption of Clod Computing in e-Governance" CCSIT – 2011, Springer – Communications in Computer & Information Science (CCIS) 133, Part III, 2011, pp. 161 – 172, ISSN: 1865 – 0929, ISBN: 978-3-642-17880-1.