IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Trust Management in Web Services for Prediction and Selection based on Trust Evaluation Model

G. Raj[1], M. Mahajan[2], D. Singh[3]

[1]PhD. Scholar , Computer Science Department, IKG Punjab Technical University, kapurthala, India
[2]Computer Science Department, CGC College of Engineering, Landran, Mohali, India
[3]Computer Science Department, Chandigarh College of Engineering and Technology, Chandigarh, India

Corresponding Author: er.gaurav.raj@gmail.com, Tel.: +91-8587010020

Available online at: www.ijcseonline.org

Accepted: 20/Jun/2018, Published: 30/Jun/2018

***Abstract*—** Trust, usually deal as a collaborative term for security and reliability, is also known as base parameter for defining quality of services (web services , cloud services) in cloud based environment in current research trends. In the early service communications, quality of web service was published by service provider which may be unreliable and not credible. For better verification, trust , a more refine parameters is calculated for predicting quality over all possible parameters defined in QWS dataset for evaluating trust of clustered web services. Here, We propose a Trust Management System, in which We implement security and trust policies using WS-Security and WS-Trust. Also, we had included Trust Evaluation Model (TEM) to evaluate the upcoming request /response on cloud based web server and calculate trust values. using evidence and Dempster - Shefer (D-S) rules which will help in updating the QWS dataset in clustered view of trusted web services of similar type of application.

***Keywords*—**(D-S) rules, respective trust values, Cloud Trust, WS-Security; WS- Trust

I. Introduction

Web Services is a strategy that helps two electronic systems to communicate over the Internet. They can be seen simply as a group of functions as well as methods which are depicted by WSDL & published through UDDI. Web-Services have turned in to a popular technology that yields extraordinary economic advantages to complex web application engineers.

Web Services make dispersed computing parts to be effectively coordinated crosswise over business limits and processing stages. Also, the web services present a high level of complexity of runtime operations. In Web Services, various types of business partners could be included, and it might be workable for web services to require different services offered by some third party; the ones who provide web services may or may not be from different security domains; and the clients of web services may not be known in advance. Without a doubt, trust is an important topic to be considered for conveying integrated, interoperable arrangements under web service design. There have been numerous advancements that concentrate on building blocks and particular parts of trust management. In any case it is still lacking an incorporate model and design for trust management of web services in a steady way.[1][2]

A. Security , Privacy & Trust (SP & T)

SP & T is a group of Biggest factor which leads the user not adopting cloud services as it gives up limited data control, while traditionally user have full control of the data since it in-house. But in cloud computing which gives major benefits that is outsource IT burden to the cloud provider. Security is a big concern in the virtualized environment, as if we re dealing with confidential information like personal, account information. Compliance is another big issue in the cloud which can be resolved through deploying private cloud if to secure private information. Although the cloud can limit the expenditure of the employees and cost of hardware to be used by the system, but if the cloud is not managed properly then the expenditure cost could shoot up more than we need to expend traditional systems. Security dimensions are considered as a integrated view, a combination of Confidentiality, Authorized access of information & Data integrity maintenance (C A & I). Prevention of access to, and manipulation of the data is major responsibility of security. Privacy refers to the isolation of individual's information from being disclosed. In service environment, sensitive data communicated outside in request and response format in which big possibilities of bringing an inherent intensity of risk, due to the outsourced detrusted web services bypass the physical, logical and personnel controls policies. Service consumer has to get maximum information about the provider as much as possible who are managing request and response to maintain privacy as the integrity of consumer's data. Trusted layer which is design in between consumers and providers, has to be fairly responsible of the information security and privacy when it is kept by the service provider, in communication and at consumer's node. Trust is the selection parameter, calculated based on the different quality parameters which can be calculated in this layer to find the trusted services. Every policy need to get update on regular basis that every public agencies has to desire in efforts to make sure about awareness and to put forward in comply with pertinent rules and regulations and these regulations are increasing day by day which needs transparency in operations. Big organizations are quickly adopting the use of trust based compliance and quality controls. This ensures that all necessary quality and trust based regularities can be met in distributed environment of service delivery network as we are managing it centrally in trusted layer after calculating in unit time interval.

B. Trust and Security Issues

Trust is an intangible asset that uses past experience, for decision making. Originally trust is used in context to building human beings' relationship, now it is an crucial for forming security mechanism in cloud environments, a trust comprise of many attributes, such as confidence, reliability, dependability, honest, belief, security etc. Security is main concern in web service implementation in cloud environment as it is not predictable.

Question: Are the services, provided in public/private cloud, trustworthy for organizations which are used in more sensitive and mission critical applications ?

Answer: We can evaluate and decide trust of service for consumer using consumer's feedbacks and quality statistics which can be stored in form of quality dataset of services. i.e. QWS Dataset can be used to calculate trust factor for services while trust can be calculated by 3rd-party and it can evaluate only between two entities .

Present Work is structured as follows: Sections I, contains the introduction which describe the security, privacy and trust issues related to web services followed by web service lifespan. In Section II the Web Service LifeSpan is explain as it contain the security framework for it to secure service providing to end users via specific service providers. In section III, we define the trust management and evaluation framework for WS Lifespan based on Quality and Security Considerations. In its sub section, we define Stepwise Methodology for implementation. In Section IV, Trust Calculation and Security Implementation has been done where we analyze the D-S rule based calculation, Reputation based calculation, ws-security implementation. In Section V, We examined Web pages Layout and Flow for Trustworthy Web Service(TWS) Selection. Here, we also categorized existing research and practice of trust mechanisms for web service selection and define trust value generation Methods which will be helpful in clustering trusted , detrusted and uncertain values. In last section VI, we conclude the analysis of the QWS dataset based trusted Web service selection in web application and validate the trust using mathematical derivations and graphical analysis of results held in previous section.

II. Web Service LifeSpan

In cloud based service lifecycle, There is need to include the virtualized resources for allocate and deallocate as per service requirement. It require to deallocate resources after completion of the assigned job for optimal utilization. as per the service demand we categorized them to store in sache, normal storage, archived or if we need to destroy web service i.e. if out of use from long time then destroy web service and reallocate the resources.

The Previous WS Lifespan is the amalgamation of following phases:

P- 1 : Before Beginning Development
within Design and Development
P- 2 : Within Deployment
P- 3 : Within Maintenance and Operations

As per cloud based web service development, resources are assigned in virtualised manner. We have included the concept of virtualization in resource allocation in web service development. So by the property of virtualization, until we de-allocate the resources which are used in WS, these resources will not utilize effectively and reduce the resource optimization possibilities. In order to overcome this issue, we include WS archive and WS destroy as new phases in modified WS Lifespan.

Table 1 : Web Service Lifespan using Cloud based Service Management

	Phase 1: **WS Development (Without Cloud Service)**	**Phase 2:** **WS Deployment (With Cloud Services)**	**Phase 3:** **WS Maintenance (With Cloud Services**	**Phase 4:** **WS Archive (With Cloud Services**	**Phase 5:** **WS Destroy (Without Cloud Services**
1	Requirement Collection	Virtual Infrastructure Selection	Continuous Feedback	Secure Storage of WS	Uninstall the WS
2	Planning and Design	Platform Selection	Problem Identification	Problem Solution Synchronization	Uninstall the Platform
3	WS Development WS Testing	SLA Verification and Validation	Problem Domain Selection	Disaster / WS Loss Identification	Delete Virtual Machine

4		WS Installation	Problem forwarding	Start Recovery from Secure Storage	Free Virtual Resources
5			Provide Solution		Update Resource Repository

WSL Lifespan needs complete and all time association with web (24 × 7) and it's linked virtualized resources in cloud. Monitoring security issues at regular interval will be possible and become easy for maintaining with its all time availability. Our framework follows DnD (Defence in Depth) method and logic for management of security issues in individual stage.

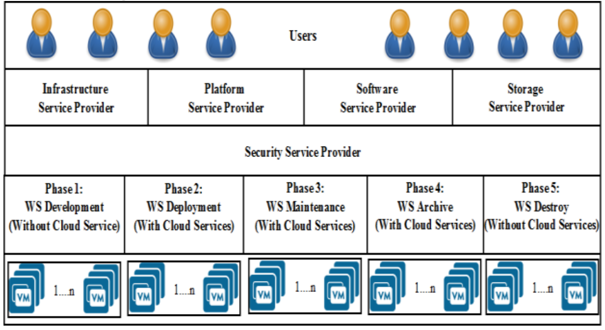

Users
Infrastructure Service Provider
Platform Service Provider
Software Service Provider
Storage Service Provider
Security Service Provider
Phase1: WS Development (Without Cloud Service)
Phase2: WS Deployment (With Cloud Services)
Phase3: WS Maintenance (With Cloud Services)
Phase4: WS Archive (With Cloud Services)
Phase5: WS Destroy (Without Cloud Services)
VM
1...n

Fig. 1: Specialized Security Framework for Web Service Lifespan (WSL)

As per proposed framework, WSL phases are stacked in second layer from base where base layer is collection of dedicated VMs, a group of VMs defined as per load and requirements of each phase. Security Service Provider is handling security management for which a Single entry exit point is required to established with complete monitoring features which should act like a root monitoring node for conducting security crosschecks of all phases and provide effective firewall. Here we set crosscheck nodes in between phases to sub phases to verify the access permissions and identify as verification gateway. Each gateway, is configured as per security policies defined for phases in standard policies as per defined protocol stack which is updated in random time interval.

One of our objective is to test the security for which we design functional test cases. In Security Testing characteristic defined for SoapUI 5.4.0 is extremely easy to validate and the functional security of web services can be test using these test cases to assess the vulnerability exist in the system for security attacks. Security Testing of web service with SoapUI 5.4.0 can be demonstrated as follows:

1. *__Create a Functional Test Case__*

Initiate the process with including the trustworthy demo project by importing it into workspace to explore the Test Case.

2. *__Add a Security Test__*

An empty "Security Tests" as a New Security Test can include by right click. Here, we can add number of security scans and declaring them for making sequence of Test Steps.

3. *__Execute the Test for Security Testing__*

Execute the Test to monitor undergoing development for every TestStep to configured scan of security in the main window of security test as the different Security Scans are executed here.

4. *__Analyze the Results__*

The Security Log shows detailed information on failed Security Scans. We can review in this log by double clicking individual scan to check for unanticipated observant that forces indicating a likely possible thread for security in marked service and to see their actual message exchanges.

5. *__Create a Report__*

A report which representing the constant and trustworthy services which provide the innovative and effective idea to predict and select the service which is secure and trustful.

III. Trust Management System for WS LifeSpan

From the security testing reports and related quality parameters, we find that trustworthiness of web service can be calculated based on following three perspectives:

i. Trust that clients have in web services,
ii. Trust that the web service has in its clients,
iii. Trust that both clients and the service have regarding the network transmission.

Because of the expanding interest of these web services, the security of these web services is of great importance. To give security of web services to the clients, different security policies are created. By giving security to the clients, we are given protection, confirmation and classification due to which this security has a vital role in providing efficient Trust Management System (TMS).

A. Framework of Trust Management [TM] System

In TMS, On the basis of the type and nature of a particular web service, a security policy set is connected on it so as to give security to the clients. Web service security comprises of five primary segments: "'WS-Security; Web-Services-policy; WS Security-Policy, WS Trust, WS Secure-Conversation".

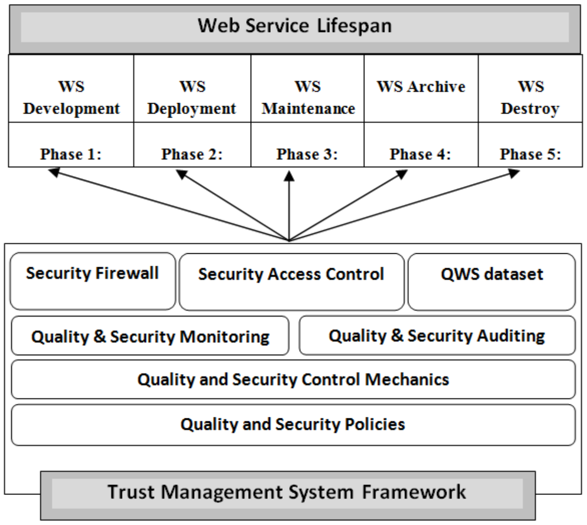


Fig.2: Trust Management System [TMS] Framework for WS Lifespan based on Quality and Security Considerations

Web Service Trust, which is *firm faith in the truth about security, reliability and quality of an element,* is a critical part of decision making process for Web Services prediction and selection. It especially impacts the determination of security policy and its configuration as WS-Security configuration in SoapUI, i.e., which is allowed to carry out activities as Outgoing WS-Security Configuration, Incoming WS-Security Configuration , Keystores /Truststores and Certifications. It includes the techniques which are expected to oversee and actualize security to and for the web services i.e. encryption /decryption, adds SAML assertion and Timestamp token, Signs outgoing message, configuring JDBC connection, testing environment and event-handling functionality.

Trust is a critical aspect in web service selection in cloud computing environment. We inspect and characterized number of research in web service selection in trusted mechanisms for cloud environment in following categories based on–

1. Reputation,
2. Evidence
3. SLA,
4. Security Policy Selection (Security Monitoring)
5. QWS Analysis (Controlling and auditing)

Trust which is multifaceted social occurrence, and a systemic observation of trust system investigation which is very necessary. Here, we illustrate a broad analysis of trust and expand a somewhat relaxed, easy and conceptual framework. Particularly, we include following:

i. Policy-based trust judgment and trust evaluation based on QWS dataset and its statistical analysis, by which web service consumer or service provider can trust / detrust.

ii. Evidence-based trust judgment, by which particular quality elements of web services which are used as verification for trust decision.

iii. Cloud attribute qualifications or selection, by which few attributes of web service are officially authorized, and the belief in those attributes is based on official recognition and verification done based on chains of trusted attributes.

Trust models generally have some basic requirements. Some of these relationships deal with the access control of the web services specifically. They have this special feature that they exist only in the web services paradigm and protects them It capture the access control requirements for them as well. Based on the previously defined trust relationship model, we can have relations like:

i. Trustor set (set of one or more similar web service)

ii. Trustee set (entities that request for the web services).

iii. The condition set requires the trust mechanisms like credentials, data storage, and reputation and environment parameters.

iv. Basic operations performed on the web services are includes in the property set as execute , update and find.

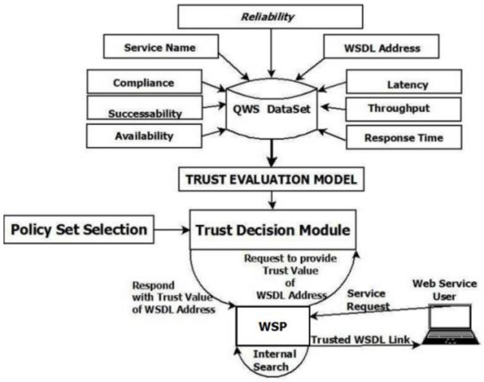


Fig. 3 : Working of Trust Decision Model(TDM)

B. *Trust Evaluation Model[TEM]*

Before understanding TEM, need to explain working the Trust Decision Module where TEM and Policy set Selection is required for providing Trusted Service to user which is defined as follows:

1. User request for specific type of web service from WSP.
2. WSP ask for decision about trusted web service from Trust Decision Module(TDM).
3. TDM use the Policy set selection based on User predefined policy requirements.
4. TDM use the feedback provided by TEM and combine the both outcomes and decide the web service which is most trusted and suitable as per User requirements.

TEM, is the model which define with the following objectives:

1. To evaluating trust of all web services at runtime as per request of web service users and service providers.
2. If parameter values of requested web service are out of the QWS database model provide process to develop and update the data set by using missing value generation based on neural network and other techniques to evaluate the trust value of the web service which will be used in evaluation of web service trust.

The process of completing first objective is explained as follows:

Evaluation can be done by three ways

1. Dempster Shafer(D-S) Rule Based Trust Calculation
2. Reputation based Trust Evaluation
3. WS- V&V security policy based Evaluation

Explanation of them are described in next section here we introduced there utility and architectural placement in TEM.

Working of TEM is explain through workflow methodology of TEM as follows:

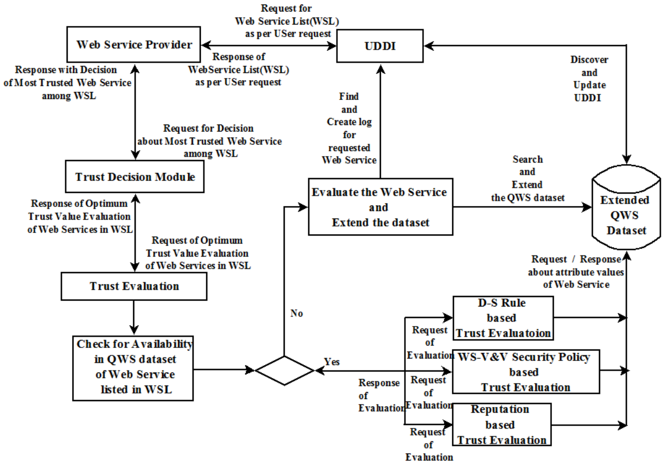


Fig. 4: WorkFlow Methodology in Trust Evaluation Model

C. Stepwise Methodology Design

The methodology adopted for trust and security implementation needs to design steps which can be easily explain for what to achieve and how to achieve in terms of final outcome of the research:

Step 1: Analyze the existing Trust Management and Evaluation Models for web services

A large number of research papers and surveys have been published regarding Trust, Trust Management and Evaluation. But specifically for "Web Service Trust Evaluation and Management", very less work has done till now. Objective of this research paper is to study and analyze the work that has been done in the field of Trust Evaluation and find suitable Truest Evaluation by comparing them and selecting the optimized trust value using our proposed Web Services Trust Management Models to other related Trust Models.

Continues re-evaluation about trust values and updation in QoS data set based on Trust of Service is missing in current developments. In General, Trust management build trust decision, evaluation of relationship type, Trust value and monitoring but re-evaluation of existing trust, relationships and values are regularly changing based on user demand and requirement changes. So ultimate objective id to keep ourselves update as per Trust of Service(ToS) i.e., 'monitoring and re-evaluation' of trust which is not perfectly achieved till now , will be achieved in proposed one.

Step 1: *Service Provider request to UDDI to get list of web services as per user request.*

Step 2: *UDDI provide the list as per Extended QWS dataset and other repository.*

Step 3: *WSP send the list to TDM for getting most trusted web service known as Trustworthy Web Service (TWS).*

Step 4: *TDM Send request to TEM where it check the availability of web service data of WSL in QWS dataset.*

Step 5: *If NO, send information to evaluate web service on runtime and extend the parametric information in QWS dataset.*

Step 6: *If Yes, it Calculate the Trust value of Web services in WSL*

- ***a.*** *D-S Rule based Trust Evaluation*
- ***b.*** *WS-V&V Security policy based Trust Evaluation*
- ***c.*** *Reputation based Trust Evaluation*

Step 7: *Compare and Store the optimized value of trust in QWS dataset.*

Step 8: *Forward the optimum and Most Trusted Web Service information as response to TDM to WSP to User.*

Step 9: *This Trustworthy Web Service feedback from the user will be updated in QWS dataset for future discovery, trust evaluation and user request.*

IV. TRUST CALCULATION AND SECURITY METHODOLOGY

We use the sample case study for understanding Trust Evaluation by all three methods. The steps of the case study to find trust value and cluster them in three categories as trusted , detrusted and uncertainty using Dempster–Shafer theory for calculating reputation and trust of service.

A. D-S Theory Based Trust Calculation

The Dempster Shafer Theory(DST) of evidence was originated by Arthur Dempster with respect to statistical inference methods, this theory was later remodeled as theory of evidence by Glenn Shafer. This theory lets the user to integrate the evidence by collecting from different users to conclude at specific degree of belief and understanding in trusted values. In our research work as we use the QWS dataset as a collection of beliefs which are derived from collection of interaction evidence so each attribute/

parametric information of web service is introduced as the belief.

As per statement of D-S theory all evidences have degree of the belief whose value is in range from '0' to '1'. Here, '0' indicate that the fact has no supportive evidence and '1' it has full support. The possible conclusion can be define as Δ set :

$$\Delta = \{\alpha_1, \alpha_2, \alpha_3 \ldots\ldots \alpha_n\} \qquad (1)$$

Where, Δ = The set of concluding belief that can be drawn based on the evidence

$$\alpha_n = \text{The number of evidence} \qquad (2)$$

Each α is mutually exclusive of each other where at least one α needs to be true

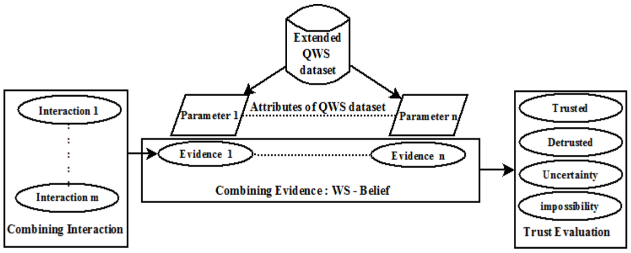


Fig. 5: D-S Theory used for QWS dataset for Trust Evaluation

We have used combining interactions in trust value evaluation using the interaction's evidences. Here all user interaction with web services are stored as instance and marked as evidence in the set *E*. *E* can be further divide in 3 subsets as α (positive), β(negative) and ∏(uncertain) interactions.

Attributes which are acting as a evidence and number of interactions are the no of users whose feedbacks are recorded to find the value of evidence. These evidences combined and form a combined belief about the web service as WS-belief, a specific generalized attributes in row of QWS dataset for a defined WSDL linked Web service.

Let's assume the '*i*' is user entity which denote the number of users who are using web services and '*j*' is provider entity which denote number of web service providers. At time '*t*' the interaction among these entity '*i*' and '*j*', It can be marked as positive interaction($\alpha_{i,j}^{t}$), negative interaction ($\beta_{i,j}^{t}$) , and uncertain interaction($\prod_{i,j}^{t}$).

The trusted, detrusted and uncertainty can be assign using distinguished framework by $\Delta = \{t, -t\}$, *where* $2^{\Delta} = \{\{t\}, \{-t\}, \{t, -t\}, f\}$, according to the D-S rule, where the values represent the trust as $\{t\}$, distrust as $\{-t\}$, uncertainty as $\{t, -t\}$ and impossibility as f.

For the time '*q*', the entity '*i*' evaluates the degree of direct trust on entity *j* as:

$$dt_{i,j}^{q} = \{ dm_{i,j}^{q}\{t\},\ dm_{i,j}^{q}\{-t\},\ dm_{i,j}^{q}\{t,-t\} \} \qquad (3)$$

for the time $q = 0$, the $dt_{i,j}^{0} = \{0,0,1\}$, and the function of basic probability assignment $dt_{i,j}^{q}\{(.)\}$ can be defined as:

$$dm_{i,j}^{q}\{t\} = u \times dm_{i,j}^{(q-1)}\{t\} + (1-u) \times \frac{\alpha_{i,j}^{t}}{\alpha_{i,j}^{t} + \beta_{i,j}^{t} + \prod_{i,j}^{t}} \qquad (4)$$

$$dm_{i,j}^{q}\{-t\} = u \times dm_{i,j}^{(q-1)}\{-t\} + (1-u) \times \frac{\beta_{i,j}^{t}}{\alpha_{i,j}^{t} + \beta_{i,j}^{t} + \prod_{i,j}^{t}} \qquad (5)$$

$$dm_{i,j}^{q}\{t,-t\} = 1 - dm_{i,j}^{q}\{t\} - dm_{i,j}^{q}\{-t\} \qquad (6)$$

Here *u* belongs to the weight factor, it can either be 0 or 1.

B. WS- V&V security policy based Evaluation

As per implementation in research studies done in the field of regression testing to get Service Verification and Validation, WS -Security policy is very helpful and give the following understandings:

i) Trust models can be utilized for studying the trust choices and for working on existing models of trust. Trust modeling depicts processing of trust, and is mostly about the brain research or human science for the disintegration of what it includes. It ranges from basic access control polices to investigations of ability, convictions, chance, significance, utility, and so on.

ii) A few metrics can be utilized to catch the conduct of a WS through these feedbacks. Some of them are recorded underneath:

(a) TM_C = Trust Metrics for Cloud based Web Service Consumer to check Service's Trust

$$TM_C : \{ S_{ID}, R_T, T_H, A_V, R_L, S_C, L_T \}$$

$$\forall i, \exists j \ \ TM_{C1}(i, j)\ S_{ID}, (i)$$

(b) TM_p = Trust Metrics for Cloud based Web Service Provider to check Consumer's Trust

$$TM_P : \{ U_{ID}, R_P, VR_F, VL_D \}$$

The level of trust on a Web Service depends on following three points:

T_1 = *Trust that clients have in web services,*

$$T_1 = \sum_{i=1}^{7} \frac{\sum_{j=1}^{4} TM_{C1}(i,j)}{4} - \sum_{i=1,j=1}^{i=7,j=2} TM_{C2}(i,j) \quad (13)$$

Where form

$TM_{C1} \subset \{T_H, A_V, R_L, S_C\}$
$TM_{C2} \subset \{R_T, L_T\}$

T_2 =Trust that the service provider has in its clients,

$$T_2 = \sum_{i=1,j=1}^{i=n,j=3} TM_{p1}(i,\ j) \quad (14)$$

$TM_{P1} \subset \{R_P, VR_F, VL_D,\}$

R_P : Reputation of Client in terms of probability and
VR_F, :Security Policies return 1 if Service Request is Verified, else return 0
VL_D :Security Policies return 1 if User ID is valid, else return 0;
T_3= Trust that both clients and the service providers have regarding the network transmission
$T_3 = TM_C \cup TM_P$

As per these Levels trust of each service *i* can be formulated as:

$$\forall i \ \ T_i = T_1(i) \wedge T_2(i) \wedge T_3(i) \quad (15)$$

Where T_1, T_2, T_3 Derived using parameters assigned in related sets.

C. Reputation based Trust Evaluation

Reputation is extended form of D-S theory where indirect trust can also be calculate and considered for recommended system. The entities that have made direct interaction with the evaluated entity can obtain the recommendation; those entities who have not made any direct interaction cannot access the trust recommendation using reputation based evaluation.

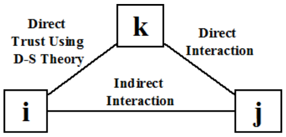


Fig. 6: Reputation based Indirect Interaction in Trust Evaluation

If i and k has same requirement we can assume, the research scenario where entity k has a direct interaction with entity j, then we can state that the entity i can get recommendation information of entity k with entity j, through direct trust degree from entity k and entity j. This indirect interection is known as Trustworthy Reputation (Rt) of entity.

Trustworthy Reputation can be calculated using function as follows:

$$Rt_{k,j}^{q} = \{\ Rm_{k,j}^{q}(\{t\}),\ Rm_{k,j}^{q}(\{-t\}),\ Rm_{k,j}^{q}(\{t,-t\})\ \} \quad (7)$$

Here, $Rm_{k,j}^{q}(\{X\})$ is the basic probability assignment as defined in D-S theory.

As per discussion above , we can use direct trust $dt_{k,j}^{t}$ for trust recommendation in Reputation based trust calculation as $Rt_{k,j}^{t}$ for the entity k, thus $Rt_{k,j}^{t} = dt_{k,j}^{t}$ and

$$Rm_{k,j}^{t}\,\{x\} = dm_{k,j}^{t}\,\{x\}. \quad (8)$$

In our trust decision model, a recommendation may come from different methods as one is reputation based recommendations D-S theory based recommendation and other sources also. We integrate these recommendations. However the result may be inconsistent as it may happen the recommendation may be contradictory, here the weight of each recommendation are taken the weight Ω_k can be defined as

$$Rp_{i,j}^{t}\,\{t\} = \Omega_k + Rp_{i,j}^{t}\,\{t\} = \Omega_k + dm_{i,j}^{t}\,\{t\} \quad (9)$$
$$Rp_{i,j}^{t}\,\{-t\} = \Omega_k + Rp_{i,j}^{t}\,\{-t\} = \Omega_k + dm_{i,j}^{t}\,\{-t\} \quad (10)$$
$$Rp_{i,j}^{t}\,\{t,-t\} = \Omega_k + Rp_{i,j}^{t}\,\{t,-t\} = \Omega_k + dm_{i,j}^{t}\,\{t,-t\} \quad (11)$$

Lastly, the integrated form of all the recommended trust combines to build reputed trust of Web Service '*A*', which can stated as

$$Rp_{i,j}^{t}\{A\} = Rp_{1,j}^{t}\{A\} \pm Rp_{2,j}^{t}\{A\} \ldots \pm Rp_{q-1,j}^{t}\{A\} \pm Rp_{q,j}^{t}\{A\} \quad (12)$$

where; $q= 1,2,\ldots.m,\ \ A \neq f,\ \ A \in 2^{\Omega}$

These parameters as also used in QWS dataset of web service quality for analytical study defined as follows:

i. <u>Response Time</u> :Time taken to send a request and receive a response.
ii. <u>Throughput</u> : Total Number of invocations for a given period of time.
iii. <u>Availability</u> : Number of successful invocations/total invocations.
iv. <u>Reliability</u> : Ratio of the number of error messages to total messages.
v. <u>Latency</u> : Time taken for the server to process a given request.
vi. <u>Execution Time</u> : Time taken to execute one request on the server.

Quality Web Services Testing basically involves:

i. To understand WSDL file.
ii. To determine the operations that the web service provides.
iii. To determine the XML request format which is needed to be send.

iv. To determine the response XML format.

v. To use a tool or writing code to send request and validate the response.

V. IMPLEMENTATION AND RESULT ANALYSIS

Home Page: It is the welcome page for visitor, cloud user or the cloud service provider. It gives brief idea of cloud entities i.e, Web Service User(WSU) or Web Service Provider(WSP). As we selects type as per role, our corresponding next web page open.

Role based Login page: If visitor wants to use service, he will select the WSU else WSP option from the home page. As per role based selection, the login page for the Cloud will come up. Enter credentials, like username and password (encrypted/decrypted by DES / AES). After authentication, the user can access their account.

Service selection: Here, Select the type of services which we want to use. Select will be from the list of available web service types. Here in our case study we select the validation services from QWS dataset for which total 24 instances are in record for quality analysis based on previous user statistics.

Parametric search : After selection of service type, system will ask for the quality parametric requirements of the user, where we have to fill in their requirements, like priorities in cost , time, performance, etc. (List of parameters are based on how we are planning to calculate Trust Factor using QWS parameters)

Cloud based Web Services List : Once the requirement have been set a list of cloud service providers have come up, from where they can select the cloud based trusted web service from CSP list where each web service has updated with unique trusted value at runtime.

Cloud Based Web Services provided : After selection, This window shows up the current service statistics being provided by service provider, as here user can assess the Service providers capability and check whether it fulfill their requirements or not.

Trust, Distrust And Uncertainty : Based on the trust values and personal experience , consumer can submit feedback of used web service, as service provider provides level of predection as follows:

Pred$_1$: Trusted (When the provider is trustable)

Pred$_2$: Detrust (When the provider is not trustable)

Pred$_3$*: Uncertainty (When trust Cannot be determined)*

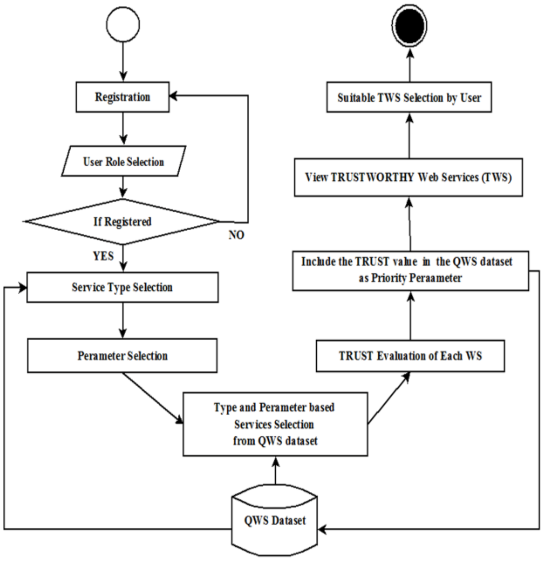
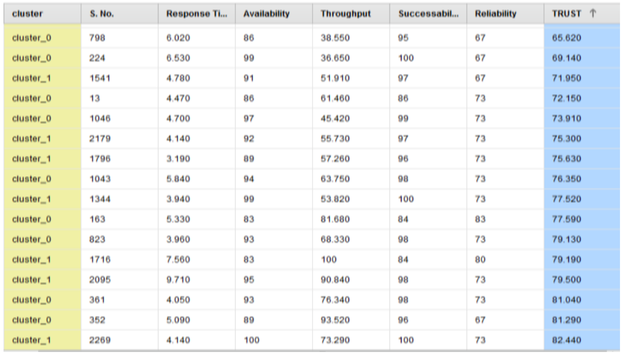
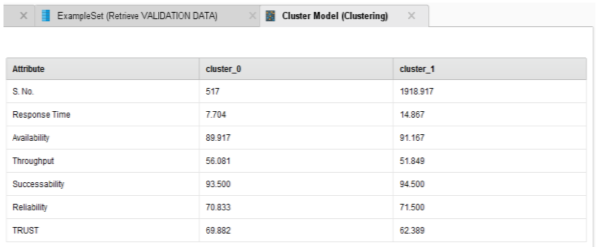


Fig. 7: Web pages Layout and Flow for Trustworthy Web Service(TWS) Selection



cluster	S. No.	Response Ti...	Availability	Throughput	Successabil...	Reliability	TRUST ↑
cluster_0	798	6.020	86	38.550	95	67	65.620
cluster_0	224	6.530	99	36.650	100	67	69.140
cluster_1	1541	4.780	91	51.910	97	67	71.950
cluster_0	13	4.470	86	61.460	86	73	72.150
cluster_0	1046	4.700	97	45.420	99	73	73.910
cluster_1	2179	4.140	92	55.730	97	73	75.300
cluster_1	1796	3.190	89	57.260	96	73	75.630
cluster_0	1043	5.840	94	63.750	98	73	76.350
cluster_1	1344	3.940	99	53.820	100	73	77.520
cluster_0	163	5.330	83	81.680	84	83	77.590
cluster_0	823	3.960	93	68.330	98	73	79.130
cluster_1	1716	7.560	83	100	84	80	79.190
cluster_1	2095	9.710	95	90.840	98	73	79.500
cluster_0	361	4.050	93	76.340	98	73	81.040
cluster_0	352	5.090	89	93.520	96	67	81.290
cluster_1	2269	4.140	100	73.290	100	73	82.440

Fig.8: Trust calculation and clustering on QWS datasets of validation services using RapidMiner


ExampleSet (Retrieve VALIDATION DATA)
Cluster Model (Clustering)

Attribute	cluster_0	cluster_1
S. No.	517	1918.917
Response Time	7.704	14.867
Availability	89.917	91.167
Throughput	56.081	51.849
Successability	93.500	94.500
Reliability	70.833	71.500
TRUST	69.882	62.389

Fig. 9 : Centroid Table for QWS data for clustered web service of validation

B. Trust, Distrust And Uncertainty:

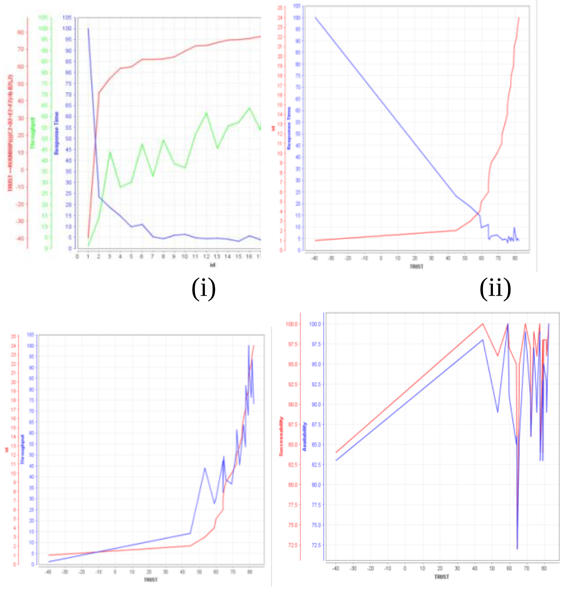
These RapidMiner graphs predicts that the provider which we are evaluating based on QWS dataset, can be trusted if trust value is increasing as throughput of web service increased. If response time is decreasing trust will increase and if availability and successability are increasing Trust has more probability of increasing. From Fig. 10(i) which shows the relation of each Trusted web service with response time and throughput, stated that

If response time is proportional to Trust factor that will be called Detrusted graph as per Fig. 10(ii).

If throughput is proportional to Trust factor that will be called Trusted graph as per Fig. 10(iii).

If in trusted graph , we found sudden changes in form of increment or decrement that will identified as Uncertainty. Uncertainty can be occur due to sudden change in success ability and availability as per Fig. 10(iv).

We had also done statistical analysis of web service quality in our case study and find the Minimum, Maximum, average and deviation values of each parameter used which is used in analysis of quality distribution in clustered data by curve distribution graphs as per Fig. 11.



(i) (ii)

(iii) (iv)

Fig. 10: Trust, Distrust and Uncertainty graph

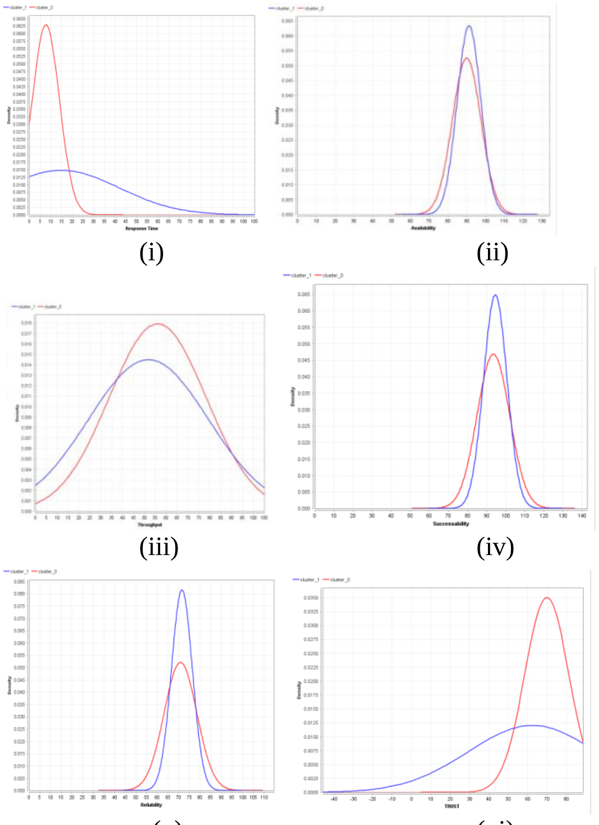
Table 2: Statistical analysis of Validation Service Clusters in QWS dataset

Table 1 : QWS dataset Analysis of attribute values

	Average	Deviation	Min	Max
Response Time	11.28583333	19.55474	3.19	100
Availability	90.54166667	6.852351	72	100
Throughput	53.965	24.59318	1.15	100
Successability	94	7.289063	72	100
Reliability	71.16666667	6.294695	58	83
TRUST	66.1358333	24.54157	-39.72	82.4

	3			4

We also observed the relation in between QWS parameters and trust based on quality clustering in defined cluster 0 & 1 through which we can described as follows:



(i) (ii)

(iii) (iv)

(v) (vi)

Fig. 11: Normal Curve Distribution of QWS parameters between cluster 0 and cluster 1

Now, the web application being develop and integrate the web service based on considerations as security policies and trust values that provides trusted access control to the data of the user. The user needs to have the authentication token that is unique everytime the user log-in. Without this token or after the expiry of this token the user will not be able to access the page that is requested using trusted web service. This token is a secret key between the application and the web server and hence the information of the user cannot be misused and cannot be accessed by an unauthorized person. Trust is considered anonymous with the cloud and web security, but it is much more than that. If we want to make cloud businesses more secure and trustworthy then we have to apply these policy based Trust Management System and techniques to over cloud based web service providers so that the At the same time the cloud service providers can prevent themselves from getting attacked by the malicious user.

VI. CONCLUSION AND FUTURE SCOPE

The scope of security research of Web Services is very high and large enough in today's business environment, which plays an important role in providing efficient system. Hence, if the system is insecure, it will lead to failure. Hence testing a system is equally important for security of a system. In this article, we had achieved the outcome as a secured web application over that consumers can trust. Through in this paper we have focused on implementation based on ws-policies and evidence based modelling for secure web application. it provides good analysis of the data generated as well as QWS dataset. Trust values which is calculated dynamically based on quality parameter's behaviour used in dataset and based on the evidence and D-S rule theory. Finally through this research, we have tried to imbibe trust among both the web service consumer and web service provider. The web service and its application can be tested using postman which provide quality assurance and efficiency. We can test whether the WS-policies helps in access control and security of web services. Trust integrates the security and quality which on which the working of web services depends.

REFERENCES

[1] Gaurav Raj, Muhammad Sarfaraz, "Survey on Trust establishment in Cloud computing", Confluence- The Next Generation Information Technology Summit, Amity University, Noida, 25-26 Sept. 2014, IEEE

[2] Weiliang Zhao, Vijay Varadharajan, "Trust Management for Web Services", IEEE International Conference on Web Services, (pp.818-821),Beijing, (2008).

[3] Ayesha Kanwal. , Rahat Masood. and Muhammad Awais Shibli., "Evaluation and Establishment of Trust in Cloud Federation", 8th International Conference on Ubiquitous Information Management and Communication, Article No. 12, pp. 1-5, 2014, ISBN: 978-1-4503-2644-5 doi>10.1145/2557977.2558023

[4] Xiaonian Wu, Runlian Zhang, Bing Zeng, Shengyuan Zhou, "A Trust Evaluation Model for Cloud Computing " Elsevier Procedia Computer Science, Information Technology and Quantitative Management, Science Direct, Volume 17, 2013, Pages 1170-1177

[5] E. Chang, T. Dillon, F. K. Hussain"Trust and Reputation for Service-Oriented Environments", Wiley, 2006.

[6] Tyrone Grandison and Morris Sloman, "A Survey of Trust in Internet Application", IEEE Communications Surveys and Tutorials, Fourth Quarter 2000.

[7] R.Joseph Manoj and Dr.A.Chandrasekar, "A Literature Review on Trust Management in Web Services Access Control", "International Journal on Web Service Computing", Vol.4, No.3, September 2013

[8] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management", IEEE Symposium on Security and Privacy, 1996. Proceedings, ISSN: 1081-6011, Oakland, CA, USA, USA , 1996.

[9] Rich Mogull, J. Arlen, F. Gilbert, A. Lane, D. Mortman, G. Peterson, M. Rothman, "Security Guidance for Critical Areas of Focus in Cloud Computing", Security Guidance v4.0 © Copyright 2017, Cloud Security Alliance.

[10] National Institute of Standard and Technology, "NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291,Version 2, (Supersedes Version 1.0, July 2011)" , NIST Cloud Computing Standards Roadmap Working Group , July 2013

[11] Ahmed Taha, Salman Manzoor, Neeraj Suri, "SLA-Based Service Selection for Multi-Cloud Environments", Edge Computing (EDGE) 2017 IEEE International Conference on, pp. 65-72, 2017.

[12] Loubna Mekouar, Youssef Iraqi, "TrustWS: A Trust Management System forWeb Services", Conference: International Symposium on Web Services, At Dubai, UAE, 2010

[13] Jagpreet Sidhu, Sarbjeet Singh, "Design and Comparative Analysis of MCDM-based Multi-dimensional Trust Evaluation Schemes for Determining Trustworthiness of Cloud Service Providers", Journal of Grid Computing, pp. , 2017, ISSN 1570-7873.

[14] Mohammad Mehedi Hassan, Mohammad Abdullah-Al-Wadud, Ahmad Almogren, SK Md. Mizanur Rahman, Abdulhameed Alelaiwi, Atif Alamri, Md. Abdul Hamid, "QoS and trust-aware coalition formation game in data-intensive cloud federations", Concurrency and Computation: Practice and Experience, pp. n/a, 2015, ISSN 15320626.

[15] Talal H, Quan Z. "Trust as a Service: A Framework for Trust Management in Cloud Environments", ACM 12th international conference on Web information system engineering, pp. 314–321, 2011.

[16] M. D. Priya, A. Lavanya, "Intrusion Detection System Using Raspberry Pi Honeypot in Network Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 3, pp. 41-45, January-February 2018.

[17] E. Manigandan, C. Kalaiarasi, E. Manigandan, Prof. C. Kalaiarasi, "Cryptography in Cloud Computing : A Basic Approach to confirm Security in Cloud", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 3, pp. 58-63, January-February 2018.

Author's Profile

Mr. G. Raj pursed Bachelor of Technology from UPTU, Lucknow, India in 2006 and Master of Technology from MNNIT, Allahabad, India in year 2010. He is currently pursuing Ph.D. from Punjab Technical University, Kapurthala , Punjab, India and currently working as Assistant Professor in Department of Computer Sciences, Amity University Uttar Pradesh, India since 2013. He has worked in Lovely Professional University as Assistant Professor from 2010 to 2013. He is a professional member of IEEE since Jan.,2018. He has published more than 40 research papers in reputed international conferences and journals including IEEE, ACM , Springer and it's also available online. His main research work focuses on Web Service, Software Engineering, Cloud Security and Privacy, Service Prediction, IoT and Computational Intelligence based education. He has 10 years of teaching experience and 5 years of Research Experience.

Dr M. Mahajan pursed Bachelor of Technology and Master of technoology from MMEC, Mullana in Information Technology and Ph.D. in Computer Science from Punjab Technical University, Kapurthala in 2016 . He is currently working as Assoc. Professor and HOD in Department of CSE in CGC, Landran from 2015. He is a professional member of IEEE,. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cloud Security and Privacy, Big Data Analytics and Data Mining,. He has 5 years of teaching experience and 4 years of Research Experience.

Dr D. Singh Presently working as Associate Professor in Computer Science & Engineering Department at Chandigarh College of Engineering & Technology (CCET), Chandigarh He has published and presented 82 research papers in National & International Journals (Including IEEE, Springer, ELSEVIER & having good impact factor) /Conferences. He is having 12 years of experience of teaching at reputed Engineering Colleges.Had done B.E.(Computer Science & Engineering.), M.Tech(Computer Science & Engineering.), PhD(Computer Science & Engineering.)He has guided 8 PhD Thesis, 10 M Tech Thesis, 19 B Tech Projects. He is Member of reviewer Panel of International Journal of Information Technology & Knowledge Management and Member of reviewer Panel of International Journal of Research in Engineering & Technology, Life member of IETE. His main research work focuses on Web Enginering, Software Engineering, Cloud Security and Privacy, Big Data Analytics and Data Mining.