An Adaptive Trust Model for Software Services in Hybrid Cloud Environment

S.UDHAYAKUMAR¹, S.CHANDRASEKARAN², LATHA TAMILSELVAN³, FAREEZ AHMED⁴

Computer Science and Engineering¹,², Information Technology Department³,⁴

B.S.Abdur Rahman University¹,³, Rajalakshmi Engineering College², Anna University²,⁴

Chennai, INDIA

mailudhay@yahoo.com, chandrasekaran_s@msn.com, latha_tamilselvan@yahoo.com,
fareez.ahamed@gmail.com

Abstract: - The objective of the research work is to propose an adaptive trust model applicable for software services deployed in cloud environment. In the earlier security modeling of cloud based applications, the trust among various services are evaluated either based on Bayesian or fuzzy approaches which are not formally verified before composition. The reputations of the constituent domain specific services are evaluated to determine the overall trust of the demanded service assuming other infrastructure and platform services. The trust relation is migrated between various virtual services in the case of emergent termination or cancellation of the customer demand. The temporal nature of the concurrent service activation and their composition processes are synchronized for each session to complete within the expected time using a Pay First Serve Next (PFSN) technique. The model is formally specified and verified using Temporal Logic of Action (TLA+) and the adapting trust level is evaluated for a SMS Cloud Service Deployment.

Key-Words: - Adaptive trust, Reputation, Domain specific services, Virtual services, Temporal service, Formal verification, Short Message.

1 Introduction

On demand paid software services are the means through which the developer community and end user community will get maximum benefit at low cost. In future internet computing, the business and scientific software services will be deployed through major cloud providers to reach the service benefits without a huge initial investment. In such a cloud computing environment, the services are expected to preserve the private and business information of the user through their service components. In preserving the privacy, the trust among the composing services may not be static and deterministic but it has to be dynamic and adaptive to assure the security of the business information assets. While the earlier Service Level Agreement (SLA) based trust model for cloud computing uses the SLA criteria and the first hand experiences of users as the main input to determine the level of trustworthiness for cloud resources [1]. This model can be used for different domains of cloud services and based on that, the trust values are awarded to the specific domain users using the same services. In the case of collaborative processes, the domain based trust models were proposed where trust relationships among members are declared into within-domain and inter-domain trust relationships along with a timely risk value table [2]. In the above trust evaluation, the feedbacks from the peer services were not considered. In reputation based trust model in addition to feedback, the transaction context factors and the community context factor were considered in a variety of online communities [3]. The next improvement in adaptive probabilistic trust model, the agents evaluate trust values of the referrers by comparing the referrals they receive with their actual experience with certainty [4]. If more number of peers and agents were involved in an online application, the priority and security features are to be considered in collecting the feedback. To avoid any security breach leading to anonymity and integrity issues, a formal approach for identity management of services, security features are to be analyzed by assigning equal priority to all registered services of different capability and security on mutual trust by the service provider [5]. For small and medium sized business applications like messaging, the authentication and access control can be achieved through services deployed in the private cloud pertaining to the organization. The accounting and context checks are performed for assuring the trusted computing over clouds. The main focus of the work is to propose an adaptive trust evaluation technique suitable for hybrid cloud messaging application through virtual services leading to identity management and content checking services.
The organization of the work is as follows; Section 2 proposes a design model of hybrid cloud for Short Message Services (SMS) with the collaboration of various services. Section 3 brings out the formal foundation using TLA+ on which the dynamic trust and the mistrust between services in the cloud are specified and verified and Section 4 addresses the adaptation policies and its types to meet the concurrency in serving the requests. Section 5 discusses a mathematical model for adaptive trust evaluation across various users through cloud services both in private and public clouds and Section 6 concludes the work with its limitations and possible future enhancements in the short message service domain.

2 SMS Cloud Design Model

In any adaptive trust based messaging service, the private cloud strengthens the reputation of the organization. In the proposed hybrid cloud model a web based SMS is designed to provide the users to send authenticated messages to the mobile recipient, that are evaluated for its trustworthiness. All the trust evaluations for a particular organization would be carried out in private cloud environment using an SMS cloud API. Then the message is sent to virtual cloud servers to check for client identification and ensures whether the recipient is in the available database, if not the trusted system enforces a restriction in the number of messages to be sent. Once the overall trust is established, the message is sent using a single commonly shared Global System for Mobile Communication (GSM) based Subscribers Identity Module (SIM), thereby trust is shared in both the clouds enabling a hybrid cloud environment as shown in Fig 1.

The collaboration of various services in the SMS cloud is shown in Fig 2. Here the sender needs to navigate to web browser in order to send an SMS to a particular user in the cloud or in their own organization, and then the web application ensures the user to go through the necessary privacy policy check and SLA. Once the agreement is being negotiated a session is created for the user to use the various application services provided by the public cloud. For a particular service the users trust is evaluated using the formal trust metrics, and if needed the trust may be migrated to other virtual application services. Some of the other services provided by the cloud are security service for identification and authentication, billing and usage control service for pay first serve next (PFSN) of the on demand services in the cloud and scheduling and performance analysis services.

3 Formal Model of Adaptive Trust

Any applications that demands cloud services must gain trust across the constituent services like software services, network services and infrastructure services. The trust is being considered as a sum of acceptable level of uncertainties arising out of new virtual services that collaborate on the client request. Again the trust being an emergent property and not as a feature, it is an aggregated property expressed in terms of successful completion and termination of services and their consequences. An adaptive form of such a property is needed not only to collaborate but also to terminate the services based upon their reputation values. The issues are the specification of the trust and their valuation across virtual services hidden within the cloud since the uncertainty and interpretation of trust varies according to the business context. Without formal methods, it would...
be unfair to take decision in streaming a multitude of private messages through the cloud. Hence a formal method and its specification are needed before implementation to avoid any incorrect receipt of critical messages which are totally temporal in nature. The message cloud faces timing faults and Byzantine faults in streaming into the mobile service provider [7]. The first order logic should be dynamic and adaptive in forwarding the messages into both private and public clouds. The trust evaluation service is the core of the work which has been specified and verified in TLA+ as given below for minimization of transient faults within the application itself.

4 Adaptation Policy, Level and Type
In a cloud environment where a web client application, specific to SMS services must gain trust or evaluate the uncertainties prevailing among the individual services inside the private and public clouds. There may be possible forms of trust based on their values say zero trust, absence of trust, mistrust, distrust and adaptive trust [6]. When the trust between services breaks, it is defined as zero trust. The absence of trust indicates that the entities are not dedicated to the services assigned to them, while the mistrust is the act of believing that a particular service has a hidden policy or agenda. The distrust is a formal way of not trusting any service in a cloud environment leading to grave risk or deep doubt. The proposed adaptive trust model forces a verification technique irrespective of the zero trust, mistrust, distrust and positive trust among the services and evaluate the overall trust in both public and private cloud and decide the action before the task is handed over to the next services. If the uncertainty level is low when compared with the cloud service provider specification, then the trust is positive, if not it leads to mistrust or zero trust.

The adaptation policy in any cloud on demand service is to pay first and serve next (PFSN). That is the organization needs to pay first a minimum charges in sending a multitude of corporate messages to their customers through mobile services depending on the number of messages. In signing this agreement, the cloud vendors will give their trust and privacy policy to accommodate the customer request. While streaming the messages, the dynamic trust between the services as well as the trust on the recipients will be taken into consideration. If the evaluated trust falls below the minimum threshold, then based on the type of message whether it is a normal or emergency, the trust level will be recalculated. If not, the total session will be terminated. The accounting service monitors and meters the delivery of the batch of messages and calculate the actual charges to be paid by the client organization based on the usage time towards various software, platform and infrastructure services utilized by the demanded task. The public cloud API throws an exception in the case of excess services utilized by the client to pay for it. If not paid, then the reputation of the client organization will get a major decrement and pushed into non trusted clients table. An initial advance payment to meet the average message transactions will be demanded during the client registration phase itself to avoid any misuse of valuable services.
5 Adaptive Trust Evaluations
The cloud based message service can gain or lose its trust across the various constituent services deployed in both private and public cloud. The static trust based messaging may result the information received by a illegitimate recipient where in the case of corporate messages that may lead to business collapse even. The trust evaluation of heterogeneous software services sitting inside and outside the cloud has to be carried out based also on the initiator of that task. All the cloud vendors may or may not be trustworthy, so the critical and individual tasks are checked with the help of a private cloud exclusive for that organization and uploaded into software processes into a public cloud for streaming and accounting the submitted messages. The nature and the priority of the messages along with the status of the community who logged into the cloud are to be taken into consideration to evaluate the dynamic run time trust of that service for the task. Let the total trust can be evaluated based on the individual trust established between the services during run time. The connectivity services and the network management services are also taken into consideration. For a sample scenario, the total trust is the algebraic sum of all the trust values of individual services as per the weightage accepted during the service level agreement (SLA) session which can be expressed in Equation 1.

\[
T_{ij}^t = \sum_{i=1}^{M} (\text{Trust}_{ij}^{\text{Pri Cloud}} + \text{Trust}_{ij}^{\text{Pub Cloud}}) - \text{Mistrust}_{ij}^{\text{Private and Public Cloud}}
\]

(1)

Let i be the sender and j be the recipients, and M be the total no of messages from the web client, then during any particular session the trust between sender and the recipient can be estimated based on the trust between the individual check-in services. For example if the sender sends an SMS to a particular recipient the trust is calculated from its initial value which has been already stored in the cloud storage. In the case of a Mozilla client tries to send a message to Android mobile recipient then, the private cloud of that organization assigns an initial trust value to that request. If the initial trust \(T^t\) value is 0 or below the threshold, the cloud must prompt to the web client for registration or renewal. Once the value has been assigned the trust report service adds the weighted trust due to the presence of the needed identification \(T^d\). Similarly authentication \(T^{auth}\) of the web client in order to activate that particular service is checked and the weightage for the authentication trust service is added, if not subtract from the initial trust value. In the same way the weightage for the trust due to correct message format, \(T^{mf}\) and acceptable legitimate content, \(T^c\) are also added up. If the web client is a frequent user of highly privileged community, then these two privileges \(P^f\), and usage factors \(N^f\), are also considered and summed up till the session completes. The trust between services in the private cloud while forwarding a message can be evaluated as per the Equation 2. In Fig 3 depicts how the user gains the trust value from the initial trust by passing through various services in the private cloud and then gains the reputation to migrate to the public cloud where the information is sent to the recipients.

\[
T_{ij}^d = \sum_{i=1}^{M} (T_{ij}^{id} + T_{ij}^{auth}) * N_{ij}^f + (T_{ij}^{mf} + T_{ij}^c)
\]

(2)

![Fig.3. Trust Migration in Hybrid cloud](image)

The trust between the private cloud interface with the public cloud API and all other trust of the constituent services in the public cloud can be represented as per the Equation 3.

\[
T_{ij}^{sl} = \sum_{i=1}^{M} (T_{ij}^{gc} + T_{ij}^{ppc} + T_{ij}^{slac} + T_{ij}^{simc})
\]

(3)

After having gone thru the history or empirical data of the client over the message services, it is also possible to evaluate the percentage of suspicion based on its validity, authenticity and its content.
Let, $S_{U_i}$ be the number of messages that are suspected by the system. A message is said to be suspected if the recipient is not in the official database. The suspicion factor $P_{U_i}$ can be calculated as the percentage of suspected messages over the total no of messages M sent by the user $U_i$. Hence the trust between two end services over a series of request on to the public cloud through the private cloud is adaptable with respect to the instantaneous values of the mutual trust existing between the individual services, and their mistrust between them as shown in the Equation 4.

$$T_{i,j}^A = \sum_{i=1}^{M} \left( T_{i,j}^p \pm (T_{i,j}^{id} \pm T_{i,j}^{auth}) \right) \times N_{i,j}^{f} \pm (T_{i,j}^{mf} \pm T_{i,j}^{id} \times P_{U_i}^f)$$

$$+ \sum_{i=1}^{M} T_{i,j}^{gc} \times T_{i,j}^{ppc} \times T_{i,j}^{slac} \times T_{i,j}^{simc}$$

$$- \left( \frac{P_{U_i}^f}{Initial\ Trust} \right)$$

(4)

If there is no trust between any services over the same task then the trust will be adapted as shown in Equation 5.

$$T_{i,j}^A = \sum_{i=1}^{M} \left( T_{i,j}^p \pm (T_{i,j}^{id} \pm T_{i,j}^{auth}) \right) \times N_{i,j}^{f} \pm (T_{i,j}^{mf} \pm T_{i,j}^{id} \times P_{U_i}^f)$$

$$+ \sum_{i=1}^{M} T_{i,j}^{gc} \times T_{i,j}^{ppc} \times T_{i,j}^{slac} \times T_{i,j}^{simc}$$

$$- \left( W_{i,j}^2 - (W_{i,j} - P_{U_i}^f)^2 \right)$$

$$Initial\ Trust$$

(5)

The list of entity services available within the cloud with different types of trust among them are shown in Table 1, and the list of services available based on the message priority is show in Table 2.

**Table 1 Trust Weightage in Private Cloud**

<table>
<thead>
<tr>
<th>Community</th>
<th>Trust Weightage for Services in Private Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ID Check (T''')</td>
</tr>
<tr>
<td>Commmon</td>
<td>+w1</td>
</tr>
<tr>
<td>Corporate</td>
<td>+10</td>
</tr>
<tr>
<td>CEO</td>
<td>100</td>
</tr>
</tbody>
</table>

**Table 2 Trust Weightage in Public Cloud**

<table>
<thead>
<tr>
<th>Message Priority</th>
<th>Gateway Check (T''')</th>
<th>Privacy Policy Check (T'''')</th>
<th>SLA Check (T''''')</th>
<th>SIM Check (T'''''')</th>
</tr>
</thead>
<tbody>
<tr>
<td>+w1</td>
<td>-w1</td>
<td>+w2</td>
<td>-w2</td>
<td>+w3</td>
</tr>
<tr>
<td>Normal</td>
<td>+1</td>
<td>-1</td>
<td>+2</td>
<td>-2</td>
</tr>
<tr>
<td>Urgent</td>
<td>+10</td>
<td>-10</td>
<td>+5</td>
<td>-5</td>
</tr>
<tr>
<td>Emergecy</td>
<td>100</td>
<td>100</td>
<td>200</td>
<td>200</td>
</tr>
</tbody>
</table>

The SMS cloud module with trust evaluation for checking the suspicious messages is implemented in a Linux environment using java. The coding that implements the trust evaluation and sending of SMS via Linux server is given below.

```java
DriverManager.getConnection("jdbc:mysql://localhost:3306/smsscloud", "root", "tiger");
PreparedStatement stmt = conn.prepareStatement("select * from pbook where number=?");
stmt.setString(1, request.getParameter("phno"));
ResultSet rs = stmt.executeQuery();
if(!rs.next()) {
    double trust = Math.pow((double)user.getNoofSuspectedMsgs()/user.getNoofMsgs(),2)/user.getNoofMsgs();
    out.println("<h1>"+trust+"</h1>");
    if(trust>user.getThreshold())
        {out.println("<h1>Stoped</h1>");
        return;
        }
    DataOutputStream acm = new DataOutputStream(new FileOutputStream("\dev\ttyACMO"));
    acm.writeBytes("AT+CMGF=1\r\n");
    acm.writeBytes("AT+CMGS="+request.getParameter("phno")+"\"\r\n");
    acm.flush();
    try { Thread.sleep(500); }catch (InterruptedException ex) {
        Logger.getLogger(SMSRequest.class.getName()).log(Level.SEVERE, null, ex); }
    acm.writeBytes(request.getParameter("msg"));
    acm.write(26);
}
```

The trust model proposed for the SMS Cloud is based on giving various trust levels to various levels of authority. Let $U_1, U_2, U_3, ..., U_n$ be the various levels of authority where the level of authority decreases as n increases. The graph in Fig 4, shows the number of messages that are sent by a user for the adapted trust values $U_i$, and how $U_i$ varies with different weightages. Its is inferred from the table that if we set a threshold for the user $U_i$ to be 20,
then the system allows only up to 23 SMS to the recipients that are not in the existing database, like wise for TU₄ where the threshold is higher, the allowable SMS is only 10.

Table 3 Trust Values for Different User Levels

<table>
<thead>
<tr>
<th>No. of Messages</th>
<th>Adapted Trust Values of Different User levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TU1</td>
</tr>
<tr>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>9</td>
</tr>
<tr>
<td>20</td>
<td>16</td>
</tr>
<tr>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>

Hence as the allowable number of SMS is directly proportional to the Trust value gained by the sender is shown in the Table 3.

Fig.4 Messages verses Adapted Trust values

6 Conclusion

An adaptive trust model for assuring short messages delivery based on trust evaluation of multitude of services in a hybrid cloud environment is proposed. The design model for such SMS Cloud is also achieved after formally verifying the trust that is moderately adaptive based on several context and contents. The suspicion factors and the reputation factors are plying a vital role for enhanced performance of the proposed model. The adaptive trust evaluation within two clouds is having a constrain rising from the unknown clouds and mobile service providers. The different priorities and length of the messages are other constraints which limit the deployment of the application after SLA between two cloud vendors. The cost effectiveness of the hybrid cloud for SMS services and the stochastic nature of requests for multimedia messages will be considered in the future work.

References: