A Review on Trust Mechanisms in Cloud Environment

1SubramanianAnbazhagan and Dr. K. Somasundaram

1Department of Computer Science and Engineering, Karpagam University, Coimbatore, Tamilnadu-641021, Tel:0422 647 1115, India.
2Department of Computer Science and Engineering, Jaya Engineering College, Chennai, Tamilnadu, India.

ABSTRACT

Background: A Review on Trust Mechanisms in Cloud Environment. Objective: Cloud computing is the new paradigm for sharing computational or storage resources. It is an emerging technology for sharing services through internet. In cloud computing, trust management is more important for the use of information and communication technology. There are two levels of trusted environment in the cloud. First one is user based trust and the second one is service provider based trust. Generally, trust value is computed by determining the attributes like, confidentiality, integrity, reputation, security, etc. These parameters are obtained from the user access log, which is present in the cloud server. Service composition provides value-added services via composing web services, which are provided by various organizations. Service composition in multi-cloud environment coordinates self-interested participants, automate service selection, and also deals with cloud providers and their services. Due to the dynamic nature of the cloud, continuous monitoring on trust attribute is mandatory to enforce Service Level Agreement (SLA). A SLA is a formal contract used to guarantee the consumers service quality. This paper covers an extensive survey of various security mechanisms for cloud environment, which can contribute in developing efficient trust mechanisms. Results: The analysis is done based on the access record and the trust evaluation is carried out. Service composition provides. Trust model aims to reconfigure servers dynamically and allocate high quality computing resources to users. Service Level Agreement is done between a network service provider and a customer. Conclusion: The existing trust evaluation schemes lacks in security and privacy in cloud computing environment. Evidence based trust has low fault detection and high conflicting rate. From the survey, it is proven that the SLA based ontology technique effectively computes the trust for cloud user and server.

INTRODUCTION

Cloud computing is an emerging technology that changes the IT architectural solutions. It is a new pattern of computing, which dynamically provides computing services by Virtual Machine (VM) technologies. It is a model for enabling convenient, on-demand network access to a shared pool of configurable resources. Cloud provider host their resources through internet on virtual computers and make them available to multiple clients. Virtualization provides the ability to providers to sell the same hardware resources among multiple clients. The clouds have different architecture based on the service they provide. The data is stored on a centralized location called data centers having large size of data storage. The Service Level Agreement (SLA) is a legal contract between the service provider and cloud user. SLA is a document, which defines the relationship between two parties, namely, the provider and cloud user. It contains the following properties:

- Identify and define the customer’s need
- Provide a framework for understanding
- Simplify complex issues
- Reduce areas of conflict
- Encourage dialog in the event of disputes
- Eliminate unrealistic expectations

Cloud computing SLA is maintained when dealing with outsourced cloud service providers and specialized cloud vendors. Access control is one of the most important measures to ensure the security of the cloud computing. Cloud could not solve the uncertainty and vulnerabilities by applying traditional access control. A party might be authenticated and authorized but this does not ensure the authorizations in an efficient manner. Therefore it is important to identify the trustworthiness of the services or service providers. Trust management is a
fundamental technique to detect the malicious, selfish, and compromised nodes. The trust management comprises of two trust relations namely,

1. Objective trust
2. Subjective trust

Objective trust can be defined as a hypothesis based on reasoning augmentation, which includes Burrows, Abadi and Needham (BAN) logic in security protocols. Subjective trust principal component is an estimate of specific character or behavior level of trust objects. The trust can be explained in the following ways,

- Trust plays a role when the environment is uncertain and risky
- Trust is the basis, based on which certain decisions are made
- Trust is built using prior knowledge and experience
- Trust is a subjective notion based on opinion and values of an individual
- Trust changes with time and new knowledge while experienced one influences the old ones
- Trust is context dependent
- Trust is multi-faceted

The security of the cloud is enhanced by analyzing the user behavior. The analysis is done based on the access records and evaluation is carried out. Service Composition provides value-added services via composing basic web services, which are provided by various organizations. In cloud service composition, collaboration between brokers and service provider is essential to satisfy the incoming cloud consumer requirements. These requirements are mapped to cloud resources, which are accessed through web services in an automated manner. The challenges faced in automated service composition are

- Dynamically contracting service providers, which set a service fees based on supply-demand basis.
- Dealing with incomplete information regarding cloud resources.

Service composition can be either static or dynamic. In static composition model, the process is built manually and the web service is automatically selected by the system. In dynamic composition, both the process model and service selection are done automatically by programs. Trust is an important factor in the cloud system. It is the main concern for all interaction between service providers and consumers in such a changing environment. Trust evaluation factors include scalability, availability, security and usability. Trust model aims to reconfigure servers dynamically and allocate high quality computing resources to users. Trust models consider specific cloud-related attributes while selecting the cloud providers. Cloud ontology provides a meta information, which describes the data semantics. It provides a shared understanding of a domain of interest to support communication among human and computer agents. Ontology comprises set of concepts and relationships between concepts that can be applied for information retrieval to deal with user queries. This paper surveys about various techniques and algorithms to enhance the cloud security.

This paper is organized as follows. Section 2 describes the various trust mechanisms involved in cloud platform. Section 3 depicts the results and discussion. Section 4 discusses about the summary. Section 5 provides proposed work and section 6 discusses conclusion.

**Trust Mechanisms in Cloud:**

The trust mechanisms provides a good way for improving the system security. It provides security states, access control, reliability and policies for decision making by identifying and distributing the malicious entities based on extracting the detected results from security mechanisms in different systems.

A. User Behavior Based Trust Evaluation:

In trust mechanism, the user behavior analysis plays a vital role. During this analysis process, various behavior of individual user are identified according to their usability.

1) Analytic Hierarchy Process (AHP) based Evaluation Strategy:

AHP is a combination of qualitative and quantitative analysis of multi-objective decision (Vaidya, O.S.and S. Kumar, 2006). It can be defined as a division of series of levels of attributes in which each attribute represent a number of small sets of interrelated sub-attributes. It simplifies the complexity of the problem analysis and test the consistency of the major subjective mistakes. In AHP, the user behavior trust can be assessed by receiving the evidence from the user’s access to cloud resources. The trust evaluation is done based on “divide and treat” method, which is a hierarchical structure model. Top-down hierarchical structure shows how to decompose the trust and down-top hierarchical structure illustrates how to integrate the behavior evidence to form the evaluation of user behavior trust. In AHP, the low-level behavior evidence affect the higher-level sub-trust. This depends on the expert’s expertise, which results in low security.

2) Fuzzy Analytic Hierarchy Process based Evaluation Strategy (FAHP):

It is based on Triangular Fuzzy Numbers (TFN), which makes the evaluation results more objective (Tang, Y.-C.and T.W. Lin, 2011). It is an efficient tool to handle the fuzziness of the data involved in deciding the preferences of the variables. FAHP method has a decision support system to help
decision makers making better choices both in relation to tangible and intangible criteria. Fuzzy set theory is used to provide an effective way of dealing with the uncertainty of subjective interpretation. Triangular Fuzzy Numbers are constructed to identify the preferences of one criterion over another. TFN can be defined by a triplet (l,m,u) and its membership function \( \mu_A(x) \) can be defined as the following equation

\[
\mu_A(x) = \begin{cases} 
\frac{x-l}{m-l}, & l \leq x \leq m \\
\frac{u-x}{u-m}, & m \leq x \leq u \\
0, & \text{otherwise}
\end{cases}
\]

\[ S_i = \sum_{j=1}^{m_i} m_i \left( \sum_{j=1}^{m} m_j \right)^{-1} \]

Where \( x \) is the mean value of \( A \) and \( l, m, u \) are real numbers. The value of fuzzy synthetic set consist of criteria set \( C \), where \( n \) denotes the number of criteria and \( m \) is the number of decision alternatives. The decision alternative set is denoted by \( A \) (Mehregan, M.R., et al., 2014). This method is easy to compute the trust than the other approaches.


It evaluates the user behavior by combining the advantages of ANP and FAHP (Dewangan, M.B.K.and M.P. Shende, 2012). In AHP, the low-level behavior evidence affect the higher-level subtrust, while the high-level sub-trust does not affect lower-level evidence. FANP evaluates an user behavior trust to reflect relationship between various behavior evidence. It has a strong disadvantage of subjectivity which depends on the expert’s expertise.

4) Double Sliding Window based Evaluation Strategy:

In the evaluation of user behavior, the sliding window carry out the evaluation of node behavior trust (Reddy, C.N.K.and G.V. Murthy, 2013). The trust calculation is based on time, actual contacts of nodes and size of the window, which involves in control evaluation scale. The movement of window is involved with two factors

1. Time (t)
2. New node intercourse

As the time goes by, the window moves forward and some overdue trust records gradually out of the windows. In this way, the overall trust value of the node is decreased when the node does not exchange information with others for a long time. When a new node comes, the size of the window is fixed so the records, which has the farthest time from current wasn’t overdue and squeezed out by the windows movement. By computing the user behavior trust of effective trust records the security is increased.

B. Service Composition in Cloud:

Service composition provides value-added services while composing basic web services, which are provided by various organizations. Some of the service compositions are Priority based, Dynamic, QoS aware, Agent based and Compatibility based service compositions.

1) PriorityBased Service Composition:

In priority based service composition, each requirements are prioritized based on the service (Khushbu, D.D.Y., D. Virani, MadhuriVaghasia, 2013). The services with smaller length are executed first. Services are available with different provider, these services are combined and delivered to the consumer. These services are integrated together and delivered to the customer. In this service composition, consumer requirements are read and the values of requirement are stored in requirement list. Then, for each request the priority is assigned with different parameter and the values are stored. For each parameter the total value of each priority is calculated. For each proposal Call For Proposal (CFP) message is sent to the broker agent. Then if the agent has a particular service, the user is allocated with particular service and the agent accepts for the proposal or else the agent rejects the proposal. It requires very less effort and time to provide service and decreases the energy consumption.

2) Dynamic Service Composition:

Dynamic service composition accelerates application development. It is the process of creating new services at run time from a set of service components (Zhou, J., et al., 2012). This process includes activities that must take place before the actual composition such as locating and selecting service components. It also provides considerable flexibility for modifying and extending the operation of software systems during runtime. A service component is a self-contained unit of service that encapsulates some service functionality and appropriate data (Tosic, V., et al., 2002). A service component is independent from other service components in a particular composition. It is easily detached and replaced with other service component.

3) QoS AwareService Composition:

QoS aware service composition consists of a set of QoS constraint values and these constraints are defined by an end user based on QoS expectation about the composite solutions (Chen, Y.M.and Y.J. Peng, 2012). In this situation, service selection composition are failed and more time is wasted on solution discovery. QoS selects a service from pool to execute, then a functional qualified composite solution is derived. This stage is called as combination. The qualified functional composite solutions are computed to determine their own
composite value over QoS constraint. The QoS values of a composite service are determined by the value of the component services and by the composition structure used (e.g. sequential, parallel, conditional and loops), Table 1. Shows the examples of QoS aggregation functions (Alrifai, M., et al., 2010).

<table>
<thead>
<tr>
<th>Aggregation type</th>
<th>Examples</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summation</td>
<td>Response time</td>
<td>( q(cs) = \sum_{j=1}^{n} q(s_j) )</td>
</tr>
<tr>
<td></td>
<td>Price</td>
<td>( q(cs) = \frac{1}{n} \sum_{j=1}^{n} q(s_j) )</td>
</tr>
<tr>
<td></td>
<td>Reputation</td>
<td>( q(cs) = \prod_{j=1}^{n} q(s_j) )</td>
</tr>
<tr>
<td>Multiplication</td>
<td>Availability</td>
<td>( q(cs) = q(s_j) )</td>
</tr>
<tr>
<td></td>
<td>Reliability</td>
<td>( q(cs) = \min_{s=1}^{n} q(s_j) )</td>
</tr>
<tr>
<td>Minimum</td>
<td>Throughput</td>
<td>( q(cs) = \min_{s=1}^{n} q(s_j) )</td>
</tr>
</tbody>
</table>

4) Agent-based Service Composition:

Agents are semi-recursive contract net protocol and service capability tables that composed of information catalogs about cloud participants (Gutierrez-Garcia, J.O. and K.M. Sim, 2013). Agents are independent problem solvers that collaborate to attain global objectives. Agents are appropriate tools for automating cloud resource management such as autonomous resource mapping. Cloud service composition are augmented in two dimensions namely,

1. Horizontal service composition
2. Vertical service composition

Horizontal service composition deals with the combination and integration of heterogeneous services. Vertical service composition combines the homogeneous services. Tasks performed by agents are called as behaviors. An agent is also defined as a single execution thread in which a set of behavior objects are instantiated. Each agent behavior handles an agent tasks are activated in response to different events. A set of behaviors can be added, stopped or removed from a pool of agent behaviors to handle multiple current actions.

5) Compatibility-aware Service Composition:

This approach helps the non-expert users with limited or no knowledge on legal and virtual appliance image format compatibility issue to deploy the services flawlessly (Dastjerdi, V. and R. Buyya, 2014). The knowledge is used for reasoning an algorithm that detects a set of cloud services comprising of virtual appliance and units are compatible or not. This technique allows non-expert cloud users to set their preferences using high level composition solutions. The majority of end users avoid system that incur complexity in capturing their constraints, objectives and preferences. In this, users find a way to prioritize their preferences and then map them to weights. When multiple cloud services are composed together they should be compatible to each other. It minimizes the deployment cost and deployment time and increases the reliability while adhering to composability constraints.

C. Various Trust Mechanisms in Cloud:

Trust model aims to reconfigure servers dynamically and allocate high quality computing resources to users. Trust evaluation factors include scalability, availability, security and usability. Some of the trust mechanisms are reputation based trust, SLA verification based trust, Evidence trust and Bayesian Network based Trust Mechanisms.

1) Reputation based Trust:

Trust and reputation are different where trust is between two entities. But the reputation of an entity is the aggregated opinion of a community towards the entity (Wang, S.-X., et al., 2010). An entity with high reputation is trusted by many entities in the community. Trust judgment on an entity is made by trustee and the reputation is used to compute the trust level of the trustee. The reputation of cloud users provides an impact on cloud users. Reputation is represented by a comprehensive score reflecting the overall opinion. Reputation is more useful for the cloud users in choosing a cloud service from many options without particular requirement. A large number of raters are needed for meaningful and objective ratings. The advantage is that the data used for assessment covers more situation and wider time-window of observations. It also maintains overall credibility level of the system. It affects the reliability of the system and misuses the resource providers to gain popularity.

2) SLA verification based Trust:

A Service Level Agreement is a legal contract between a cloud user and a cloud providers (Dash, S.). SLA concentrates on the visible elements of cloud service performance and does not address invisible elements such as security and privacy. Cloud users lack in the capability to do fine grained QoS monitoring and SLA verification on their own. In a private cloud, the trust authority takes care of the QoS monitoring and SLA verification. In a public cloud, an individual user and small organization use cloud entity as trust brokers without technical capability. If the monitoring is conducted by a cloud broker, then the belief in the results of monitoring is dependent on the trust with respect to professional
monitoring. It gives clear idea about the cloud service providers and has high sustainability. It also gives a transparent view about the service providers. The service providers do not provide better service or support to the cloud users. Due to this reason, the SLA does not provide efficient trust in cloud environment.

3) Evidence-based trust:

Trust belief in the expected behavior of trustee is based on the evidence of the trustee’s attributes of competency, goodwill, and integrity with respect to the expectation (Wang, G.and J. Wu, 2011). The evidence-based trust is represented as follows:

\[
\text{Believe} (u, \text{attr}_1(s, v_i)) \land \ldots \land \text{Believe} (u, \text{attr}_n(s, v_n)) \rightarrow \text{trust}_*(u, s, x, c)
\]

which states that if an individual u believes a subject s has attribute attr1 with value v1, ..., attribute attrn with value vn, then u trusts s with respect to x, the performance of s or information created or believed by s, in a specific context c. Table 2 shows the various sources of trust involved in evidence based trust. It is highly scalable and deals with integrity of service providers. It has low fault detection rate and high conflicting rate.

<table>
<thead>
<tr>
<th>Table 2: Various Sources of Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain-Specific expectation</strong></td>
</tr>
<tr>
<td>Performance</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Privacy</td>
</tr>
</tbody>
</table>

4) Bayesian Network based Trust Management (BNBTM):

It uses multidimensional application specific trust values and each dimension is assessed using a single Bayesian network (Wang, Y.and J. Vassileva, 2003). The distribution of trust values is denoted by beta probability distribution functions based on the interaction history. Trust value of peer i is indicated by,

\[
\tau_i = \frac{a_i}{a_i + b_i}, (i \in \{G, L, C\}, \tau \in \{G, L, C\})
\]

Where \(a_i = r_i + 1\) and \(b_i = S_i + 1\) and \(r_i\) and \(S_i\) are number of interactions with outcome i and \(\bar{i}\) respectively. It is a flexible method, which provides differentiated trust in different aspect of each other’s capability and integrate different aspects of trust. It does not identify the key parameters, which influence the system performance.

D. Sla Based Techniques:

SLA are a formal means of identifying key services and processes required to meet business needs (Patel, P., et al., 2009). The SLA process is a quality improvement process, which includes five stages

- Awareness and negotiation
- Documentation
- List of services and quality levels
- Reports
- Monitoring and Reviewing

Awareness and Negotiation:

In this phase, a broker discusses the business requirements and service capabilities with both parties. It is not carried out in small services, which
altered (3 or 6 monthly), or appropriate resource re-allocation considered — e.g. standby/redundant equipment purchased.

**RESULTS AND DISCUSSION**

Various Trust based mechanisms for cloud environment are shown. The results of the survey are illustrated in Table 3. In cloud environment, trust is evaluated based on the user behavior analysis. The analysis is done based on the access record and the trust evaluation is carried out. Service composition provides. Cloud service composition includes several tasks such as discovery, compatibility checking, selection and deployment. Trust model aims to reconfigure servers dynamically and allocate high quality computing resources to users. Service Level Agreement is done between a network service provider and a customer. The aspects of this agreement includes scope, quality and responsibility, which are agreed between the service provider and user.

---

**Table 3: Information about Various Trust Mechanisms in Cloud Platform**

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Performance</th>
<th>Quality Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Behavior Analysis</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Double Sliding Window based Evaluation Strategy (Reddy, C.N.K. and G.V. Murthy, 2013; Ghanem, T.M., et al., 2007)</td>
<td>Fuzzy set theory is used to provide an effective way of dealing with the uncertainty of subjective interpretation.</td>
<td>1. Fuzzy judgment matrix&lt;br&gt;2. Pairwise comparison&lt;br&gt;3. Fuzzy evaluation</td>
</tr>
<tr>
<td><strong>Service Composition in Cloud Environment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority Based Service Composition (Khushbu, D.D.V., et al., 2013; Calheiros, R.N., et al., 2011)</td>
<td>This trust calculation is based on time related, actual contacts of nodes and size of the window, which involves in control evaluation scale.</td>
<td>1. Expert dependent&lt;br&gt;2. Subjectivity&lt;br&gt;3. Correlation between elements&lt;br&gt;4. Consistency check&lt;br&gt;5. Hierarchical decomposition</td>
</tr>
<tr>
<td>QoS selects a service from pool to execute, then a functional qualified composite solution is derived.</td>
<td></td>
<td>1. QoS deviation rate under different system load.</td>
</tr>
<tr>
<td>It has the ability of reflecting self-interested characteristics of distributed and parallel executing cloud participants.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Time to complete task</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Exchanged messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatibility-aware service composition (Constantinescu, L. et al., 2004; Dastjerdi, V. and R. Buyya, 2014)</td>
<td>This method is easily extended to deal with partial matches of data types and ranges by incorporating software switches.</td>
<td></td>
</tr>
<tr>
<td>This technique allows non-expert cloud users to set their preferences using high level composition solutions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Complete type matching</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Partial type matching</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Layered domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust Mechanisms in Cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation based Trust (Wang, S.-X. et al., 2010; Zhou, Z.-x., H. Xu and S.-p. Wang, 2011)</td>
<td>This system integrates the trust model and defines trust as the outcome of observation leading to the belief that depend on a risky situation.</td>
<td></td>
</tr>
<tr>
<td>It achieves the complete description of trust concept and the obtained trust information contains more semantic contents, which provides a strong basis for trust related decisions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Computable factors of trust relation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Scoring Trust Degree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Response time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Success Execute Rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLA verification based Trust (Maurer, M. et al., 2010; Van, H.N., et al., 2009)</td>
<td>It defines QoS goals for arbitrary parameters between the cloud providers, where it optimizes the resource usage.</td>
<td></td>
</tr>
<tr>
<td>It has the ability to automate the dynamic provisioning placement of VMs by considering application level SLA and resource exploitation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. SLA violations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Resource Allocation Efficiency (RAE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidence-trust (Wang, G. and J. Wu, 2011; Wang, Y. and M.P. Singh, 2010)</td>
<td>Trust computation with multi-dimensional evidence at each node in a trust network and defines a primary dimensions.</td>
<td></td>
</tr>
<tr>
<td>It establishes the bijection between evidence and trust. It also provides an efficient algorithm for computing the bijection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Shared link in trust evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Cross link in trust evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Trust success ratio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bayesian Network based Trust Management (BNBTM) (Wang, Y., 2006; Wang, Y. and J. Vassileva, 2003)</td>
<td>It shows the system, which communicates with their experience outperforms the other system.</td>
<td></td>
</tr>
<tr>
<td>A trust value is calculated as the expectation value of beta probability density function.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Number of interactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Successful recommendation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Summary:**
In this paper, an overview of various trust based mechanisms in cloud computing platform are presented. Generally, cloud services are less trusted services due to their dynamic nature. The existing trust evaluation schemes lacks in security and privacy in cloud computing environment. Evidence based trust has low fault detection and high conflicting rate. From the survey, it is proven that the SLA based ontology technique effectively computes the trust for cloud user and server. This technique predict the trusted and privileged services for all users.

**REFERENCES**


Goncalves da Silva, E., L. Ferreira Pires and M. van Sinderen, 2009."Supporting dynamic service composition at runtime based on end-user requirements.


