A Survey on Trust Management in Cloud Computing

T. Judgi and Dr. P. Varalakshmi

Abstract

Cloud computing is the buzz word where server, storage, CPU etc., are provided as service to organizations and individual users over the internet. Since cloud computing is of non-transparent nature, there could be some issues that are to be dealt with. In this, trust management becomes an essential ingredient since services interact over the online. Many trust models were suggested to provide efficient management of trust. These approaches aim to enhance the overall performance of the cloud and to provide the user more satisfying and efficient services. In this paper, we investigate the latest trust models proposed and discussed the unsolved issues of trust in future research aspect in cloud computing.

Introduction

Cloud computing has emerged as a popular paradigm to provide cloud services to the cloud users for their successful execution of a submitted task. As most entities will not have any direct experience of other entities in cloud computing, trustworthiness gains importance to develop the credibility between the communicating entities. Further, expectations from users are high in terms of a secured system, requiring right provisioning at right time, with pay as you go model. Hence building a trustworthy system in cloud computing brings the confidence to the users which becomes very essential for cloud provider. Blaze et al. (2010) differentiated the terms trust and security. Trust is related to security, reliability, availability and not limited to other characteristics of node. A trust or node evaluates the trustworthiness of a trustee node. Generally there are two methods of trust evaluation. They are 1) Direct Trust Evaluation 2) Indirect Trust Evaluation. Direct trust evaluation implies the trust level of a person who has the past experience for a certain service. In indirect Trust evaluation, one person might not have prior experience of interacting with the provider or any services, but he knows a cloud customer who has a direct trust value for a service. The salient features of this survey paper are as follows:

1. A comprehensive review of recent research papers on trust management models in cloud computing.
2. A summary of research issues in trust management based on in-depth literature study and analysis.
3. One can have an overall idea on trust management in cloud computing by going through our survey.

The rest of the paper is structured as follows. In section 2, we have surveyed the recent research paper and have discussed some of the schemes, proposed for solving the issues of the trust management. In section 3, we have discussed on the challenges and future research trends of trust management. In section 4, we have indicated our plan of improving trust management scheme and have concluded the paper.

2. Trust Management models Review:

We have reviewed the recent research papers on trust management based on Scheduling, Cloud service provider, File Sharing, Storage System, Trust Evaluation, Trust Framework, etc. Some of the trust management frameworks have been highlighted as follows:

Trust in storage system:

Trust mechanism in storage system helps the customer to know about the location of the stored data.
Saravana kumar et al. (2013) presented a deployment model for location awareness of the cloud storage. There are two types of backups: 1) Local backup, 2) Remote backup. In the first type, the data are backed up in the same location either in different part of the same disk or in the next disk. In the second type, the data are backed up in the remote location. The customer can identify the current location of the CSU’s data with the help of the tag sent to the CSU’s. On the basis of File size, Maximum transfer rate, Buffer size, Memory availability, Memory allotment, free memory etc trust is evaluated. When the size of the file is small the trust value also will be low. In the same way, the trust value becomes high as the file is large in size. Advantage: 1) Data becomes reliable. 2) Maximum user satisfaction. 3) User can have control over their data. 4) It provides inter-operable storage access. Disadvantage: Lack of process in data processing & Database handling.

**Integrating workflow to scheduling:**

Scheduling is the method of utilizing the system resources effectively for the submitted task. To improve the efficiency of the virtual resources trust mechanism in scheduling is needed.

Hemant Kumar Mehta et al. (2010) Proposed the reliability & reputation based trust management scheduling algorithm. Here the trust management is achieved by using reputation points that are assigned to both the providers and consumers. The execution of process decides the evaluation of reputation point for the resource provider. When it successfully completes the process, the trust value is added to existing reputation point. When QoS is not achieved, the resource provider faces the penalty. The fair information, provided by the consumer, is considered as higher reputation point for calculation of the reputation point for resource consumer. The reputation point is decremented by one for the mismatch of information otherwise it will be incremented by one. Advantage: 1) This method reduces the number of failure rate, 2) This provides successful completion of task execution. Disadvantage: When the provider does not have sufficient instances of the resource, the reliability of the scheme is decreased.

Wenjuan Li et al. (2012) has brought out a novel customizable cloud workload scheduling model. This model divides the workflow scheduling into two stages: 1) Macro Multi – Workflow Scheduling, 2) Micro Single Workflow Scheduling. In the first stage, cloud user sends the service request to the User Scheduling Center (USC) which helps to understand the need of the users to providers on the basis of current status of user, resource and load of the system and then send the result to the corresponding users and providers. This module is used to identify the trustworthiness of suitable providers by the integration of both direct and recommended chain of trust. In the second stage, the provider analyses the priority of the workflows for the request received from the users and classify the workflows based on fuzzy clustering. Advantage: 1) This improves the efficiency and satisfaction of the user 2) This reduces the problem scale of workflow scheduling. Disadvantage: It is not evaluated in real cloud platform.

Yuli YANG et al. (2013) proposed a trust-based scheduling strategy for workflow applications. The author focuses on scheduling workflow applications which comprise a number of independent tasks. This strategy proposes that the scheduling problem for the workflow application is formulated first before evaluating the algorithm. There are four phases: 1) Initialization phase, 2) Replica selection phase, 3) Resource set selection phase, 4) Termination. In this strategy firstly the initialization is executed for each task. The data host forms the rows and the data sets form the columns, creating the adjacency matrix. Then, in the replica selection phase, the data host and the data set are added, starting from the smallest index. When all the data are completed it should be stored and the incomplete solution set should be deleted. Then, in the resource set selection phase, the lower value is replaced by the best resource. Finally, execution time of each task is evaluated in the termination phase. Advantage: 1) It decreases the failure rate and improves the efficiency of executing the task 2) Reliability is higher against the traditional schemes. Disadvantage: The different scheduling methods are not considered.

Wei Wang et al. (2012) proposed a new trust evaluation method. In this method, with the view of the experiences of previous customers, a new customer can determine the trust level of the cloud service. An adaptive method is introduced in this with which malicious and reliable customer feedbacks can be identified. Then the reliability weight is assigned to each customer feedback. The evaluation of a new service should be given a higher weightage when the users who have shared the cloud service before and rated it in the same way. When no users have shared any cloud service before, the feedback of the existing customer is more reliable and a higher weightage is given for their opinion. Advantage: 1) It decreases the failure rate and successful completion of the execution. 2) Proposed algorithm is scalable. Disadvantage: This proposed system does not consider the infrastructure properties.

ImadM. Abbadi et al. (2013) proposed a novel cloud scheduler which can automatically manage the cloud infrastructure based on requirements of the user and infrastructure properties. The proposed framework uses an open stack Controller node and an Open stack Nova-compute with updation in some of the functions of the components. Chains of Trust (CoT) are used for trust calculation. There are two ways of chains of trust 1) Single resource CoT 2) Compositional resource CoT. The compositional resource CoT is considered as more reliable. Also the authors used the concept of remote attestation and secure scheduling for improving the
trustworthiness of a proposed system. Advantage: Assuring users to match with their requirements. Disadvantage: Bootstrapping Delay.

Zohre Raghebi et al. (2014) proposed the trust scheduling, based on the proposed system framework. First of all the tasks are submitted to the task queue and scheduler communicates this to the schedule advisor. The same is communicating to the trust model by the schedule advisor. Then the trust model communicates to the trust middleware and obtains the detailed trust information of task and they are transferred to the task scheduler. Finally, the task is executed on the trustworthy resource node by the task scheduler in the Cloud. There are two methods: 1) Similarity in common services. 2) Closeness to majority feedbacks. Advantage: 1) It minimizes the malicious feedback. 2) The proposed scheme having a faster response time. Disadvantage: Lack of experimental Evaluation.

Selection of cloud service provider:

Cloud service provider provides services to user. Some of the reasons for selecting trustworthy service provider are: 1) In a cloud marketplace, emergence of new service provider provides the cloud services with similar offering. 2) A customer does not have control over its data, deployed in cloud. 3) Cloud service providers are selfish towards increasing their own revenues. 4) Because of pay – as - you - use model, user expectation is high in terms of quality service from the trustworthy provider.

Nirnay Ghosh et al. (2013) proposed SeICSP, a framework which enables the users to evaluate the trustworthiness and to know the competent SPs. The trustworthiness can be evaluated in terms of context-specific, dynamic trust and reputation feedbacks. The competence of a service provider can be evaluated by this method. This model, comprising these two entities, provides the amount of risk level involved in an interaction. This enables a customer for choosing a service provider. There are two types of risk estimation. They are: 1) Relational risk, 2) Performance risk. Where there is lack of trust among interacting entities there arises the relational risk and when the communicating parties’ do not achieve satisfaction, there arises the performance risk. Advantage: This method considers the issue of selecting trustworthy service provider in cloud marketplace. Disadvantage: The proposed method does not check the credibility of the feedback.

Obed Jules et al. (2014) proposed a framework called Bayesian network and probabilistic ontology driven trust model. In this model, Bayesian network is used to select a trusted provider on the basis of its reputation. Bayesian network is updated with the violations via cloud directory. The author has introduced a SLA management scheme to detect violations of SLAs parameters with the help of probabilistic ontology. Apart from this, alerts are used to understand about the triggered SLA violations. There are three modules: 1) Reputation-based trust module, 2) Intelligence Module and 3) Control Module. In the first module, Bayesian model is used to assess the provider’s trust level and the trust values are stored in a cloud directory. Well before the SLA negotiations, the customer is aware of the provider’s credibility. In the second module, the knowledge about available resources is estimated and determines the risk involved. In the third module, the resources are monitored for proper management. Alerts are used to inform the providers. Advantage: 1) Customer will have an idea about the providers before starting SLA negotiation. 2) Probabilistic ontology is used to detect SLA violations and alerts the service provider. 3) Accurate prediction of trust value of the provider, using Bayesian network. Disadvantage: The proposed scheme is not implemented in a real environment to show the accuracy of the scheme.

Nafisheh Agnelli et al. (2014) proposed trust evaluation model for selecting cloud service provider by evaluating the problem of creating trust in cloud services. Service requestor sends a service request to services’ information layer to know about the details of services and providers. Then it communicates to the trust management system and obtains the trust information of service provider. Trust management system uses the three different information sources: 1) Direct experience, 2) Direct Evaluation satisfaction level module and 3) Indirect experience. Service provider’s different services are categorized based on functional and non-functional requirements by risk assessment module. Finally, user can choose the best service provider according to the user requirements from the categorized list. Advantage: 1) This model increases the user satisfaction level. 2) It helps the user to choose proper provider. Disadvantage: Lack of process in performance analysis and Evaluation.

Sarbatjeet Singh et al. (2014) proposed a trust evaluation framework to calculate trust on service provider. In this framework, consumer sends the service request to service provider and in turn, the service provider response back to the service requestor. Independent third party monitoring the interacting services and the monitoring information helps the consumer to choose the trustworthy service provider. Trust calculation, named final trust, is calculated for service provider based on customer’s self-trust, friend’s recommendations and third party’s recommendations. Advantage: 1) Accurate and more reliable. 2) It is flexible, extensible and robust. Disadvantage: This proposed framework is not implemented in a real time scenario to show the effectiveness in cloud.

Chunsheng Zhu et al. (2014) proposed a novel trust and reputation management system for cloud and sensor networks integration. The proposed scheme helps the user to choose the best cloud service provider and assist the cloud service provider to select sensor network provider by considering the attributes requirement,
Cost, Trust and Reputation. An authorized trusted center entity is used to store the direct and reputation trust value of each service from the both cloud service provider and sensor network provider. Direct trust value and reputation trust value is considered for building a trust of the service provider. Advantage: It provides an integration of cloud and sensor network: 1). The proposed system should consider the infrastructure properties of two different domain for efficient management. 2). System Overhead.

Hasen Nicanfar et al. (2013) proposed the service-oriented and reputation management systems. This includes: 1) Trusted Center Entity (TCE), 2) Cloud Service Provider (CSP), 3) Cloud Service Consumer (CSC). Current trust value and overall reputation is calculated by TCE. On the basis of per service & per trust, CSP is evaluated for its trust. When CSC sends request with a price value to the CSP, it responds back and then CSC chooses the best cloud service provider which has the highest trust value. Advantage: 1) Maximizing the trust and decreasing the cost to the cloud service consumer. 2) This system can be adapted to the CSP service. 3) This method has high reliability and secure. Disadvantage: It does not detect the CSP with low trust value.

Wenjuan Fan et al. (2014) proposed a trust management framework for selecting a cloud service provider in a multi-cloud environment based on a set of trust service providers (TSP). In this, the tasks of eliciting, processing and evaluation of cloud service providers are performed. The trust related information can be collected by TSP whether single user perspective or the whole user aggregated perspective. The trust information is shared by interacting through trust propagation network. TSP response, on getting the required trust information, on the same path in which the requests have been received. Advantage: 1) This provides an effective and robust scheme to identify the trustworthy service provider. 2) Trust evidence is gathered and aggregated from different sources to select the best CSP. Disadvantage: This method does not prevent untrustworthy rating from completely malicious CSUs.

Trust in file sharing:

Edna Dias Canedo et al. (2011) proposed that the trust model ensures secure and reliable exchange of files among cloud users in public cloud. The node allows the file to be shared on the basis of Processing capacity, Storage capacity, Link and checking the trustworthiness of the node. There are two trust tables: 1) Direct Trust Table, 2) The recommended list. The direct trust table is checked when the node wants to know the trust value of another but the recommended list is checked when the value is not available in direct trust table. When no value is found, it sends queries to peers. The node which has greatest storage capacity or processing of better link is assigned to the requesting node. Advantage: This provides secure and reliable file sharing among the users. Disadvantage: Lack of process in performance analysis.

3. Challenges and Future Trends:

The following information gives the challenges of trust management towards the final success of cloud computing.

Power Efficiency:

This research requires lightweight trust mechanism, making trust management algorithms and mechanisms faster and less energy-consuming to support even small things. This is considered as a major issue in cloud computing.

Performance Improvement:

There are major research challenges in this like, how to share trust information effectively and efficiently and how to avoid complicated and energy-consuming trust calculation are examples for such challenges.

Network Congestion:

Researcher should take more attention to solve the issue of network congestion since there could be high volume of trust information passing through the network during peak hours.

Environmental Change:

Environmental changes may affect the trust management since the nature of cloud computing is dynamic. E.g. If A interacts B at present, it is not guaranteed that the same A and B would be able to interact with each other in the future.

Location Awareness:

Cloud service provider may change the location of data storage frequently. User does not know about the current location of the stored data. This could degrade the trust on cloud. So it is better to take necessary steps in this regard.
4. Conclusion:

In this paper, we could survey the different trust management schemes in cloud computing and understood how a trust value could be evaluated to identify the trustworthy one in cloud computing. We could also survey the different solutions proposed over the past few years for the trust management issues. Our future plan is to concentrate on multi-disciplinary trust management models in different subjects and domains.

REFERENCES


