A Review on Various Applications of Reputation Based Trust Management

https://doi.org/10.3991/ijim.v15i10.21645

Ramya Govindaraj, Priya Govindaraj
Vellore Institute of Technology, Vellore, India

Subrata Chowdhury
SVCET, Chitoor, India

Dohyeun Kim
Jeju National University, Jeju, Republic of Korea

Duc-Tan Tran
Phenikaa University, Hanoi, Vietnam

Anh Ngoc Le (✉)
Electric Power University, Hanoi, Vietnam
anhngoc@epu.edu.vn

Abstract—The extremely vibrant, scattered, and non–transparent nature of cloud computing formulate trust management a significant challenge. According to scholars the trust and security are the two issues that are in the topmost obstacles for adopting cloud computing. Also, SLA (Service Level Agreement) alone is not necessary to build trust between cloud because of vague and unpredictable clauses. Getting feedback from the consumers is the best way to know the trustworthiness of the cloud services, which will help them improve in the future. Several researchers have stated the necessity of building a robust management system and suggested many ideas to manage trust based on consumers' feedback. This paper has reviewed various reputation-based trust management systems, including trust management in cloud computing, peer-to-peer system, and Adhoc system.

Keywords—Reputation, Trust management, Recommendation

1 Introduction

Cloud computing is emerging as great trusted technology, but lack of trust management makes it difficult for its market growth. A secured framework for trust management that can provide solutions to challenges such as identification, security, privacy, integration, personalization, and scalability can help cloud service providers to improve their business and increase trusted customers [3]. Cloud computing is said to the 5th necessary thing after water, gas, electricity, telephone. The reason is that it has

changed the way of storing and accessing the data. Until cloud computing was developed, the computer resources were purchased directly or used as the lease. But cloud computing has changed the method of purchasing resources. This system provides the customers with the facilities of using the service from the Internet, and they have to pay only for what they have utilized. This technology attracts both academic and industrial researchers' attention since it offers organizations opportunities by providing various cloud services. But several problems have to be solved in cloud computing so that people can widely accept it without any reluctance. A significant issue that requires special attention is cloud security, and trust management is the best answer for this issue [5].

In this paper [5], the authors share that the distributed systems are becoming more popular in recent years. Distributed system includes cloud computing, peer-to-peer, cluster and grid computing. People use distributed systems for various purposes like downloading, searching information, online purchase, internet services, or accessing the application from a remote place. Due to the popularity of the distributed system, cloud service providers introduce new services to attract customers. But we cannot persuade that all the providers will conserve high-quality level. Sometimes some disreputable providers may swing to cheat their clients. Thus, it is essential to identify trustworthy providers. In this paper [5], the authors have reviewed the trust management systems and the trust models designed for distributed systems. In specific more concentration is given for the trust models of cloud computing with advantages and disadvantages of each proposal.

Cloud providers have resources on the virtual machine and share them with multiple clients. Many virtual machines can be hosted on a single computer, sharing storage, CPU, and memory, making the customer feel like they work on their physical system. This process is called virtualization, which allows the providers to sell the same physical system to multiple clients. This process reduces the cost of customers and increases the providers [5]. There are three types of services provided by cloud computing as infrastructure as a service, Platform as service, and Software as service. Using the hardware from the virtual computers are said to be infrastructure as service (IaaS). If the consumer has signed for infrastructure type of service from the provider, he can install any type of operating system, applications on the virtual computer. Example: Amazon's Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3). In the platform as a service (PaaS), the development platform is made available to the customers to configure their environment as per their requirements and install their tools. Example: Google App. In software as a service (SaaS), the software or the application is made available to the customers over the Internet. As in other services, the user need not install the application on their system but can use the applications directly from the providers. SaaS has many advantages, like the user can access the application anywhere, they need not install, they need not have to pay the license fee, reliable and scalable. Example: "Google-Docs"-2011 and "Windows Live Mesh" - Microsoft 2011.

While discussing the different distributed systems, the authors of paper [3] vocalize that multiple business organizations group their hardware resources to achieve high performance at low grid computing cost. In service-oriented computing, only software

is provided as a service. Only in cloud computing, both the hardware and software are provided as a service in the form of virtualization. For example, in the business process automation system, the network storage and the virtual instances for the operating system are created. Cloud computing assures several benefits such as low cost, expansion of resources, and easy maintenance. However, on the other hand, the features like non-transparent, highly dynamic, and distributed make it very challenging among the service providers. A recent study shows that inefficient trust management is one of the main reasons that acts as an obstacle for cloud computing.

A lot of research is taking place for trust management in web services. In the paper [3], the authors have discussed the trust classes, the purpose of the trust, and the relationship between trust and reputation. They classified reputation systems into centralized and decentralized, Person/agent and resources, global and personalized. While discussing cloud computing at the corporate level, the authors of paper [1] state that privileged and secret data is stored and accessed through cloud computing. Organizing a large amount of data in the local systems is challenging for the industries as it is very costly and requires an efficient storage system. Hence the big organizations merge from the local storage system to cloud storage. Here the storage will be offered by the providers. This type of service is called storage as service. As the customers allow sensitive data to be stored in a remote place, specific issues regarding confidentiality, access control, and integrity have to be solved. To achieve the data's confidentiality, the owner can encrypt the data before outsourcing the data to the remote server. To achieve integrity on the cloud server, specific techniques have been proposed which validates that the data remain uninjured.

Using cloud computing, large-scale applications can pile services and flexible resources as they require without considerable investment and low operational cost. Although there is a lot of research being carried out to solve various cloud computing problems, service discovery issues remain an unsolved problem. In the case of cloud computing, it is essential to talk about the challenges of service discovery. The first reason is that cloud services are offered at three different levels – software as service, infrastructure as service, platform as service. The second reason is that there is no specific standard for describing and broadcasting the cloud services, making the discovery process harder for the customers. There are particular standards in web services-- WSDL (A language for describing web services) and UDDI (A language for publishing web services). But the majority of the existing cloud services do not follow any standard description, which makes the discovering of the cloud service arduous. For example, some cloud service providers don't mention the word "CloudCloud, "which makes customers' judge that they may not be a cloud provider. Example: Dropbox. Some businesses do not have anything to do with the cloud but have a cloud in their name. Example: Cloud9carwash [8].

CSA-STAR [4] is a publicly available database that maintains security documents given by the cloud service providers while signing the agreement. It is a trusted program that guarantees security in the cloud computing environment. CSA- STAR helps the users in the following ways:

- The users get to know about the security policies of the cloud service providers.
- To identify which providers can go together pleasingly with the offered infrastructure.
- To increase the long term profit.
- Get experience by learning about different cloud providers.

CSA-STAR also helps the providers as follows:

- To find the appropriate tools to set up and organize the security program.
- To maintain their security level.
- To attract wealthy users with better policies.
- To get additional certification and prove their maturity in cloud computing.
- To show themselves as trusted service providers.

In paper [7], others proclaimed the five significant benefits of cloud computing. They are service-on-demand, wide network access, resource pooling, rapid elasticity, and measured service. The interaction between the service providers and the customers can be classified into two categories. 1. Business to business and 2.Business to the client [40,41]. Based on this interaction, the clouds are classified into four types.

- **Private Cloud**: Here, the resources are used by a particular organization. This organization contains many customers. The interactions in this type of cloud will be business to business interaction where all the resources will be maintained by the same organization or a third party, or both.
- **Community Cloud**: Here, the resources are owned by a group of organizations to achieve a specified goal like high performance, reduced cost, or security.
- **Public Cloud**: Here, the resources are made available to the public. This model's interaction will be business to the client where the resources are owned by government or business organization or both.
- **Hybrid Cloud**: Here, the resources are allocated based on two or more models. For example, private and public clouds can be combined. Here the interaction between the client and the provider will be both businesses to business and business to the client as different clouds as involved in this. Probability techniques are used to combine other clouds. It includes cloud bursting to achieve load balancing.

2 Trust Management System

In an information system, trust management is a conceptual system that operates on a symbolic representation of trust for making decisions. The trust value is in the form of cryptographic value, or it can link the trust management system with trust assessment result. Trust management is essential for information security, and in specific, it is necessary to maintain control policies. As we mentioned earlier, the development of cloud computing has increased immensely in the past two decades. Even though there are many useful features, there are undoubtedly serious issues like security, privacy,

etc. The authors of the paper [4] reveal that the consumers are not actually aware of their data's security. Then how will the customers trust the providers? Who will take care of monitoring, validating policy attributes? Trust management is the best answer for all the above questions. Blaze M first introduced trust management in 1996 to solve many problems regarding trust. The authors of paper [7] have classified the tasks of trust management into three categories. They are: Setting up a trust relationship, observing their behavior, taking further steps based on the experience with them. Trust management is the best approach to form a trust relationship. There are several approaches for managing trust-based issues, but all the methods can be categorized into one of the following categories. They are 1. Perspective from provider side 2. Perspective from requester side.

From the provider's perspective, the provider is the most important driver for managing the trust management system where the consumer's trustworthiness is measured in Fig 1.a. In the requester's perspective, the consumers measure the provider's reliability given in Fig 1.b.

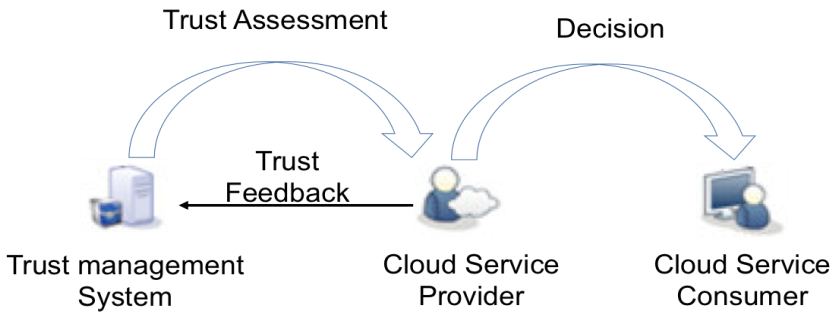

Fig 1 a) Service providers' perspective

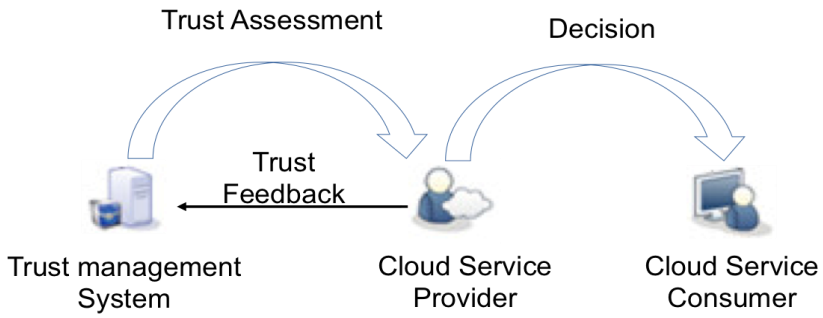

Fig 1 b) Service requesters' perspective

Fig. 1. a) Service providers' perspective & b). Service requesters' perspective

There are some common factors of trust [5]. They are as follows:

- Trust is essential for a risky environment.
- Trust is used to make decisions.
- Trust is made based on experience.
- Trust is an opinion of an individual
- Trust is dependent on context

Trust management is based on the following factors: Policies, prediction, recommendations, and reputation. An admired technique to set up a trust in the midst of independent entities is to manage end-user approval through the policy. End users are approved access if they are met with the policy's threshold, followed by trust results. The SLA monitors the violation of services or judges a service's credibility concerning the parameters like security, availability, and latency. The latter is based on X.509v3.9 [a plain public-key], infrastructure (SPKI), ten or the Security Assertions Mark-up Language. The consumers who are known as the inquiring entity will sign up individual policies with providers who are known as an unknown entity to reveal their credentials for controlling their access. If the consumers satisfy the providers' minimum threshold, they are permitted to consume the service.

The third-party giving the recommendations will have prior knowledge about the trusted parties; particularly, they know the trust feedback source in the TMS (Trust Management System). The theory of social psychology says that an unknown person to a particular person will believe the recommendation of a person who knows them before. The researchers tell that the entities with like-minded trust each another. Based on the similarity, the consumer trusts the provider.

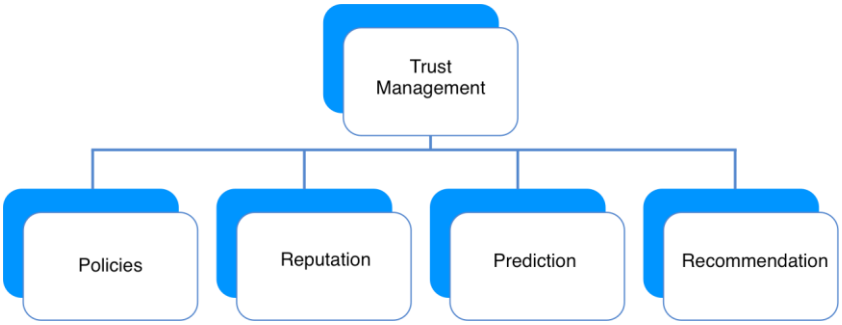

Fig. 2. Trust management techniques

The taste of an individual may vary from others. So we cannot come to a conclusion based on individual feedback. To rectify this opinion of the individual is calculated against a universal standard called "objective trust." If the trust is only based on one individual's taste, then it is called "Subjective taste" If the trust is given based on the transaction, it is called "transaction-based trust." If the trust is created by collecting opinions from every node, it is called "complete trust." But if the trust is created by collecting opinion from the neighbors alone, it is called "localized trust." [5].

A reputation system helps to build trust through social networks by collecting feedbacks from community-based sites. The user gives feedback about a particular entity from their experience. This feedback helps recommend and judge the specific transaction quality and the particular service provider [25]. Reputation has a significant impact on the trust management system. Various customers give a different opinion on a particular entity, which impacts that entity's overall trust—the reputation influences either positively or negatively. In the case of a recommendation system, there are no trusted relations. An entity may not know about the source of the feedback. An entity may have many trusted relations (network members) who provide feedback about that entity. If the feedback is more positive, the inquiring entity will be more trusted by the other entities [3].

The feedback is collected on various parameters. The customers choose the provider who gives assurance about the quality of service. In paper [4], the authors deliver that the entity's reputation is the overall opinion of the community over that entity. The provider with a high reputation will be trusted the most by that community member. We can't predict that all the collected feedback is trusted, but there may also be much untruth feedback. The feedback filtering algorithm has to be used to filter the trust feedback. The agent-based system is created to protect against malicious attacks. A lightweight system has been proposed to discover the feedback rate for the service. It has two phases. The first phase is the trust vector, which eliminates the wrong feedback. The second phase is reputation calculation, where the reputation value is calculated based on fuzzy logic.

3 Reputation Management in Adhoc

In the [14] paper, the authors used an efficient TCG (Trusted Computing Group) to get the trusted knowledge about the software coupled with devices. They assume that the TCG can securely inform the integrity value by calculating it from all the particular node software components.

This approach is used to evaluate the probability of malicious behavior of a peer-based on the software composition. The process of finding the probability of malicious behavior of software composition is a cumulative function of probabilities of malicious behavior of all its software components. Based on this assumption, the majority of the peers do not involve in malicious behavior. This approach can detect a trusted peer that is recently attacked by malicious software. Since this approach can detect the attacks very fast, the recovery can be made easily. The integrity measurement measured by TCG will be very useful since the Ad-Hoc network peers are highly mobile. The result of their simulation shows that their simple approach can detect malicious attacks efficiently. This approach is used for basic Ad-Hoc network; this can be further extended to complicated networks where the humans cannot involve in node behavior.

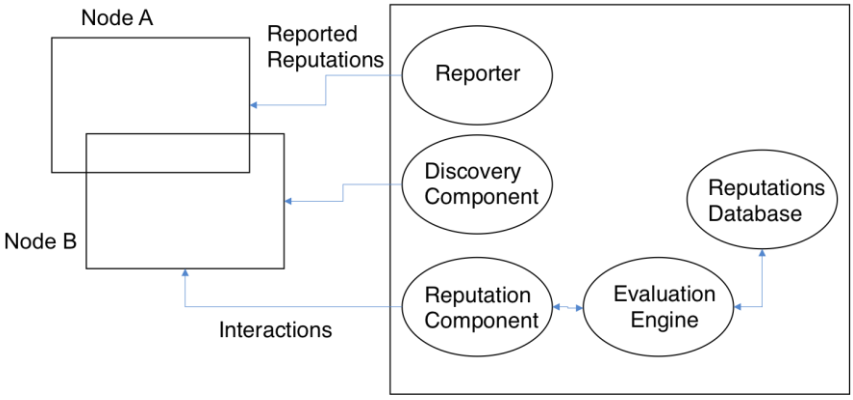

Fig. 3. Reputation management in Adhoc.

In the paper [15], the authors have proposed a strategy to get necessary details about the unfamiliar node and reduce memory space. In this solution, they have first gathered all the neighbor nodes to form the cluster, and one node will be acting as the cluster head. The cluster head will issue a trusted certificate to all cluster members. The trust ratings are combined with modified Bayesian in information exchange and while judging the reputation. This network is said to be not easily attacked by malicious nodes.

4 Reputation Management in Peer to Peer Network

In unstructured peer to peer networks, the possibility of wicked codes and fake transactions. It produces fake identities to perform fake transactions. In the paper [27], the authors have used a method with the concept of DHT along with a reputation system, which includes well-organized file searching facilities. The self-certifications techniques such as RSA and MD5 are used to ensure the data's security and availability from one peer to another. The peer's reputation measure determines the peer's trust, i.e., whether to decide if the peer is good or malicious. Once the peer is found to be malicious, then the transaction is canceled. The reputation of the peer is integrated with its identity. Every peer will maintain its certification authority, which gives the certificate and digital signature to themselves.

In the reputation management of the peer-to-peer network, the file searching method is proficient, but during the transformation of files, there may chance of viruses and other malicious attacks. Self-certification algorithms such as RSA, Naive Bayes, and MD5 are used for authentication. These algorithms can able detect malicious peers quickly and stop the transaction.

So the communication between the peers will be more secure. Usually, the transferred files face the problem in compression. But this system provides DSS (Digital Signatures Standard), which does the compression efficiency. It also transmits the short messages resourcefully.

In the paper [18], another reputation model in peer to peer system has been proposed. Using the feedback given by the other entities, the central entity calculates the trust of a particular peer. They have used three approaches: 1. Perron Trust, 2.Cred Trust, and 3.Cred Trust-trust. These approaches have been compared under various parameters, and finally, the third approach Cred Trust-trust is proved to be efficient. This model uses the combined concept of trust and credibility. This approach avoids malicious behaviors and also helps in selecting the reliable entity in the cloud. The framework has three modules: Reputation collector [to collect local trust], trust manager [to collect global trust], decision-maker [to deciding for present and future]. A peer can behave in one of the following:

1. The peer works accurately as per the protocol [Altruistic].
2. The peer is interested only in the optimization of its resources. It deviates from the protocol, so its performances get reduced [Rational].
3. The peer does not follow the protocol. This may be because it uses optimization of its resources [Byzantine].

The reputation of the peers is decided based on how it behaves With the local nodes. So, the peers interacting with each other will give reputation value to the other peers. In the evaluation process, the factors considered are: The time taken by the peer will be considered to measure its performance, the accuracrvy of the results, and collisions. The error can occur in the cloud peer, or peer can be byzantine or rational. When every peer makes sure that they return the correct value on time, then the errors are reduced. If they do not return the correct value, they are considered to be cheating, and the task is transferred to another peer. It makes unsatisfactory about the quality of execution.

5 Reputation Model Using Fuzzy Logic

This system is beyond doubt unique and entirely comprehensive, which incorporates fuzzy systems to integrate trust characteristics—initially, the host request for the reputation of the objective host to which it wants to communicate. The host then calculates the overall reputation by gathering a reputation from all other hosts along with the previous experience it had with that particular host. Now, based on the reputation value, the host decides whether to connect with the target host or not. The initiator calculates the target's credibility value by considering the similarity, popularity, activity, and collaboration. The host uses fuzzy logic to decide the importance of the transactions, the result of the transaction, and also to decide whether to communicate with a particular target if the previous decision is not accurate. Hosts consider various dynamic time decay factors depending on the reliability of the communication with other hosts.

6 Parameters for Trust Evaluation

The authors of the paper [19] have considered the essential attributes of trust evaluation to be availability, turnaround efficiency, availability, and data integrity. Ultimately, after much research, it is delivered that these attributes are essential for evaluating the trust result. The authors strongly believe that these attributes have a significant impact on trust.

Availability: is a facility where the services, resources, and data stored in the cloud are accessible and can be used by other authorized entities. Moreover, the services are offered even if many numbers of nodes get a breakdown. Availability is concerned with the time in which a system is active for the entire period, which is essential to predict the function. Therefore it is expressed either as a direct proportion or percentage. It is also expressed in qualitative terms, indicating to which extent a system can work even if another set of component breakdown.

Reliability: is the major part of the trust. It measures the ability of the hardware and software components to constantly do in accordance with the specifications.

Data integrity: An important issue that requires more concentration in the cloud environment is security. Data integrity is the broader term that includes privacy, security, and accuracy of the stored data. The provider's integrity will give the customer trust in that particular provider, and it also provides the customer with confidence about the provider. Security means how safe the data is in the cloud. Loss of data may occur due to low maintenance of data. Accurate loss may happen because of superseded computing infrastructure.

Identity: The different levels of security are:

- Authorization level
- Security level
- Entity Protection level
- Recovery level.

Capability: The present capacity of the resources affects the execution of the application and file or transfer of data. This parameter is based on processor speed and memory speed. It also depends on network parameters – bandwidth and latency.

7 Feedback Collection and Management

Distinctively, TMS [Trust management service] has two main functions: *Data Provisioning*, *Trust Assessment Function*. *The Data Provisioning is* conscientious for collecting information about cloud services and trust information of that service. *Services Crawler* module is based on the Java Open Source, which allows the system to find out cloud services over the Internet involuntarily. They have implemented functionalities to make the crawling process simpler and ended the crawling data more wide-ranging. The functionalities are addseeds(), addcrawling time(), select crawling domain(). Along with this, they also have developed the feedback collector module,

which can collect feedback from the users directly. The feedbacks are collected in the form of records, and they are stored in the database.

Availability Model: is one of the critical requirements of the trust- management service. So, in this model, several nodes manage the feedback provided by the user. The feedbacks are placed in different nodes in a decentralized method. The workloads are shared using load balancing techniques so that the availability level is continuously maintained. The number of nodes is decided by the measure called *the operational power* metric. In order to reduce the clashing of nodes in TMS, replication techniques are subjugated. Another metric called *replication determination* is used in this model, which determines the number of replicas. This metric, in turn, exploits filtering techniques to foretell the availability of each node accurately.

8 Reputation Evaluation

- ***Troll*:** A troll entity is an intentionally aggressive message panel entity. Trolls work up to begin conflict between other candidates and distress them. They interrupt the forum with irrelevant or negative comments, sing their own praises nonstop about them themselves, laugh at others' opinions, or introduce notorious comments to upset conversations. It means trolls play a vital role anywhere in the online world that interact in blog sites, social networks, distributed systems, hobby site cloud, and discussion forums. The hackers could also use a cloud to amplify a troll's role to attain its intention by offending the cloud or given with another consumer in the cloud.
- ***Opinion leader*:** An opinion leader in the powerful candidate of a particular group whose advice will be followed by the other candidates. An opinion- leader in a popular candidate who can persuade public opinion. In other words, we can say that opinion leader is meant for public opinion. Trust is a valuable thing that has to be gained from the consumer, and it cannot be gained that easily. While evaluating the trust, opinion leaders are the candidates who are superiors to others, which makes them trust-worthy. Whereas trolls are the entities, On the other hand, trolls are the candidates who post unreal and irrelevant comments about the provider. In this paper [19], authors have calculated trust by giving more importance to the opinion leaders' comments. They have introduced methods to identify the troll entities and remove their comments. As we mentioned earlier, the authors have calculated trust values using five important parameters like availability, reliability, data integrity, identity, and capability. Also, they proposed methods to identify opinion leaders and troll entities. These metrics have been used by them, including the degree of the input, degree of the output, and reputation. The accuracy of the trust value has been improved much by removing troll entities' comments and taking the comments of an opinion leader.
- ***Credibility Model***: The credibility of the consumers' feedback plays a major part in the trust evaluation. Consequently, in the paper [17], they proposed metrics for the collision detection in feedback. The metrics include including Density of the feedback and Occasional feedback collusions. These metrics differentiate the

misleading feedbacks or the comments given by the malicious consumers. It also detects the strategic and suddenly changed behaviors which lead to collusion attacks. In addition to this, they have also proposed many metrics for detecting Sybil attacks, which includes Multi Identity Recognition and Occasional Sybil Attacks. These metrics permit TMS to spot deceptive feedbacks from Sybil attacks. This function is in charge of managing the assessment of trust requests from the consumers where various cloud services' credibility is compared. The credibility factors of feedback are measured. They developed a calculator for calculating factors regarding attack detection. Furthermore, they developed the Trust Assessor to compare the trustworthiness of services. The trust results are stored in the database for further use.

9 Conclusion

Given the reality of the increased implementation of cloud computing in the modern years, there is a considerable challenge in overseeing trust within providers, between service providers and service consumers. In this paper, we presented various reputation-based trust management frameworks to handle trust in cloud environments. We discussed the credibility model, which differentiates the true and the malicious feedback. The existing reputation system solves almost all the problems efficiently. Still, they are lack one or more factors—most of the reputation models used to have the weighted mean method as a rating aggregator. Performance optimization is the only area that is unfocused so far. It can be focused on in the future for a further robust reputation system.

10 References

[1] Mr. Anup R. Nimje, Prof. V.T.Gaikwad, Prof. H.N.Datir "A Review of Various Trust Management Models for Cloud Computing Storage Systems" in International Journal Of Engineering And Computer Science, ISSN:2319-7242, Volume 3, Issue 2, February 2014, 3924-3928.

[2] Mr. Uday Nalavade, Prof. Vina M. Lomte "Survey on Various Trust Management Issues in Cloud Environments" in International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 5, Issue: 1, 15 – 18.

[3] Talal H. Noor, Quan Z. Sheng, Zakaria Maamar, Sherali Zeadally, "Managing Trust in the Cloud: State of the Art and Research Challenges", Computer 49.2 (2016): 34-45. https://doi.org/10.1109/mc.2016.57

[4] Priya Govindaraj, N Jaisankar "A Review on Various Trust Models in Cloud Environment" in Journal of Engineering Science and Technology Review 10 (2) (2017) 213- 219

[5] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan "Trust Management in Cloud Computing: A Critical Review" International Journal on Advances in ICT for Emerging Regions (ICT), ·November 2012 source: arXiv. https://doi.org/10.4038/icter.v4i2.4674

[6] Saket Maskara, Mudit Saraf, Priya G "Trust Management in Cloud Computing" International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395 -0056, Volume: 03, Issue: 11, Nov -2016.

[7] Talal H. Noor and Quan Z. Sheng, Sherali Zeadally, Jian Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions" ACM Computing Surveys, Vol. 46, No. 1, Article 12, Publication date: October 2013. https://doi.org/10.1145/2522968.2522980

[8] Talal H. Noor, Quan Z. Sheng, Anne H.H. Ngu, Schahram Dustdar "Analysis of Web-Scale Cloud Services" 1089-7801/14/$31.00 © 2014 IEEE Published by the IEEE Computer Society. https://doi.org/10.1109/mic.2014.64

[9] Noor, Talal H., and Quan Z. Sheng. "Trust as a service: A framework for trust management in cloud environments." International conference on web information systems engineering, Springer, Berlin, Heidelberg, 2011. https://doi.org/10.1007/978-3-642-24434-6_27

[10] Yefeng Ruan, Arjan Durresi "A Trust Management Framework for Cloud Computing Platforms" 2017 IEEE International Conference on Advanced Information Networking and Applications. https://doi.org/10.1109/aina.2017.108

[11] M. Thangapandiyan, P. M. Rubesh Anand" A Secure and Reputation Based Recommendation Framework for Cloud Services" 2016 IEEE International Conference on Computational Intelligence and Computing Research. https://doi.org/10.1109/iccic.2016.7919611

[12] Somaya Aboulwafa, Reem Bahgat "DiReCT: Dirichlet-based Reputation and Credential Trust Management".

[13] N.Sateesh, Yelagandula Mounika "Cloud shield: Backing honor-based trust authority for cloud utility" International Journal of Research 3 (11), 1161-1177, 2016.

[14] Segla Kpodjedo, Samuel Pierre "Reputation-based trust management using TCG in Mobile Ad-Hoc networks (RTA)" 978-1-4244-2413-9/08/$25.00 ©2008 IEEE. https://doi.org/10.1109/lcn.2008.4664218

[15] Li Xu, Yihui Zhang "A New Reputation-based Trust Management Strategy for Clustered Ad Hoc Networks", 2009 International Conference on Networks Security, Wireless Communications and Trusted computing. https://doi.org/10.1109/nswctc.2009.265

[16] Talal H. Noor, Quan Z. Sheng, Abdullah Alfazi "Reputation Attacks Detection for Effective Trust Assessment Among Cloud Services" IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013. https://doi.org/10.1109/trustcom.2013.59

[17] Talal H. Noor, Quan Z. Sheng, Lina Yao, Schahram Dustdar, Anne H.H. Ngu "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services", IEEE transactions on parallel and distributed systems, 27(2), 367-380. https://doi.org/10.1109/tpds.2015.2408613

[18] Amira Bradai, Walid Ben-Ameur, Hossam Afifi "Byzantine Resistant Reputation-based Trust Management" IEEE international conference on collaborative computing: networking. Applications and work sharing, 2013, pp. 269-278. https://doi.org/10.4108/icst.collaboratecom.2013.254048

[19] Matin Chiregi, Nima Jafari Navimipour "A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities" Computers in Human Behavior 60 (2016) 280e292. https://doi.org/10.1016/j.chb.2016.02.029

[20] Gennaro Costagliola, Vittorio Fuccella, Fernando A. Pascuccio “Towards a trust, reputation and recommendation meta-model” Journal of Visual Languages and Computing, 25(2014), pp. 850–857. https://doi.org/10.1016/j.jvlc.2014.10.001

[21] Talal H. Noor, Quan Z. Sheng, Abdullah Alfazi, Anne H.H. Ngu and Jeriel Law "CSCE: A Crawler Engine for Cloud Services Discovery on the WorldWideWeb ", IEEE International Conference on Web Services, 2013. https://doi.org/10.1109/icws.2013.66

[22] Ayman Tajeddine, Ayman Kayssi, Ali Chehab, Hassan Retail, "Fuzzy reputation-based trust model", Applied Soft Computing 11 (2011) 345–355. https://doi.org/10.1016/j.asoc.2009.11.025
[23] Tyrone Grandison and Morris Sloman "Trust Management Tools for Internet Applications" Proc 1st Int.Conference on Trust Management, May 2003, Springer LNCS 2692, pp 91-107. https://doi.org/10.1007/3-540-44875-6_7
[24] Arijit Banerjee, Sarmistha Neogy, Chandreyee Chowdhury "Reputation Based Trust Management System for MANET" 2012 Third International Conference on Emerging Applications of Information Technology (EAIT). https://doi.org/10.1109/eait.2012.6407975
[25] Siddharth Maini "A Survey Study on Reputation-Based Trust Management in P2P Networks".
[26] Talal H. Noor, Quan Z. Sheng, Anne H.H. Ngu, Abdullah Alfazi and Jeriel Law "Cloud Armor: A Platform for Credibility-Based Trust Management of Cloud Services" https://doi.org/10.1145/2505515.2508204
[27] M. Sasitharagai, A. Renuga, A. Padmashree, T. Rajendran "Trust-Based Communication In Unstructured P2p Networks Using Reputation Management and Self Certification Mechanism" 2012 IEEE International Conference on Engineering Education: Innovative Practices and Future Trends (AICERA). IEEE, 2012. https://doi.org/10.1109/aicera.2012.6306737
[28] Ali Aydin Selpk Ersin Uzun Mark Regat Pariente "A Reputation-Based Trust Management System for P2P Networks" 2004 IEEE International Symposium on Cluster Computing and the Grid. https://doi.org/10.1109/ccgrid.2004.1336575
[29] Yanzhen Zou, Liang Gu, Ge Li, Bing Xie, Hong Mei "Rectifying Prejudicial Feedback Ratings in Reputation-based Trust Management "2007 IEEE International Conference on Services Computing (SCC 2007). https://doi.org/10.1109/scc.2007.91
[30] Yuqiong Sun, Giuseppe Petracca, Trent Jaeger, Hayawardh Vijayakumar, Joshua Schiffman "CloudArmor: Protecting Cloud Commands from Compromised Cloud Services" 2015 IEEE 8th International Conference on Cloud Computing. https://doi.org/10.1109/cloud.2015.42
[31] Makbule Gulcin Ozsoy and Faruk Polat "Trust-Based Recommendation Systems".
[32] Talal H. Noor and Quan Z. Sheng "Credibility-Based Trust Management for Services in Cloud Environments" printer-Verlag Berlin Heidelberg 2011.
[33] Talal H. Noor1, Quan Z. Sheng1, Abdullah Alfazi,Jeriel Law, and Anne H.H. Ngu" Identifying Fake Feedback for Effective Trust Management in Cloud Environments" Springer-Verlag Berlin Heidelberg, 2013.
[34] Talal H. Noor, Quan Z. Sheng, Sherali Zeadally, Jian Yu "Trust Management of Services in Cloud Environments: Obstacles and Solutions" 2013 ACM 0360-0300/13/00-0001. https://doi.org/10.1145/2522968.2522980
[35] Talal H. Noor, Quan Z. Sheng, and Abdullah Alfazi "Detecting Occasional Reputation Attacks on Cloud Services" Springer-Verlag Berlin Heidelberg, 2013.
[36] Talal H. Noor, Quan Z. Sheng, and Abdullah Alfazi "Reputation Attacks Detection for Effective Trust Assessment Among Cloud Services" 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. https://doi.org/10.1109/trustcom.2013.59
[37] Aldiabat, Khaled, Anwar Al-Gasaymeh, and Ameer K. Rashid. "The effect of mobile banking application on customer interaction in the Jordanian banking industry." (2019): 37-49. https://doi.org/10.3991/ijim.v13i02.9262
[38] Maziriri, Eugine, et al. "Antecedents That Influence the Intention to Use the Uber Mobile Application: Customer Perspectives in South Africa." (2020): 76-96.

[39] Alshurideh, Muhammad, et al. "Understanding the Quality Determinants that Influence the Intention to Use the Mobile Learning Platforms: A Practical Study." International Journal of Interactive Mobile Technologies 13.11 (2019). https://doi.org/10.3991/ijim.v13i11.10300

[40] Uma Nandhini D, Udhayakumar S, Latha Tamilselvan, Silviya Nancy J, "Client Aware Scalable Cloudlet to Augment Edge Computing with Mobile Cloud Migration Service," International Journal of Interactive Mobile Technologies, Vol 14, No 12, 2020. https://doi.org/10.3991/ijim.v14i12.14407

[41] Osman Ghazali, Chun Yang Leow, Shahzad Qaiser, Nanthini Pattabiraman, Sathiyaroobaa Vasuthevan, Eman Mohamed Abdusalam, Mustafa M. Barakat, "Cloud-Based Global Online Marketplaces Review on Trust and Security," International Journal of Interactive Mobile Technologies,Vol 13, No 04, 2019. https://doi.org/10.3991/ijim.v13i04.10523

11 Authors

Ramya Govindaraj is an Assistant professor in the School of computer science and Engineering, Vellore Institute of Technology, Vellore 632014, Tamilnadu, India. She completed her B. E in Networking at Adhiparasakthi college of engineering, Anna University, Kalavai. She is pursuing her Ph.D. Degree at VIT university-Vellore. She published more than 25+ research papers in reputed journals and conferences. ramya.g@vit.ac.in

Priya Govindaraj is an Associate professor in School of computer science and Engineering, Vellore Institute of Technology, Vellore. She completed her B. E in computer science and Engineering under Madras university, M.Tech Computer science and Engineering and Ph.D in VIT. She published more than 30+ research papers in reputed journals and patent is published on one of her research work. Her area of interest is Trust management, cloud computing, IoT and Deep learning and Blockchain Technology. gpriya@vit.ac.in

Subrata Chowdhury (Computer Science Department, SVCET Chitoor, India) received his BCA from the Punjab Technical University in 2012. He pursued his MCA from the VIT Vellore in the year 2015. Currently, he has been pursuing his Ph.D. research work from the VISTAS pall avaram. He had published papers in international's journals and conferences. He has been the author of books and is the editor for the book series for the reputed International publishers. He has been awarded national and international awards. He is associated with international journals and conferences as the speaker and the reviewer. He has been the guest speaker for many workshops and seminars. He has been the reviewer for many journals. His area of expertise is IoT Healthcare, Blockchain, Machine learning. subrata895@gmail.com

Dohyeun Kim, received the B.S. degree in electronics engineering from the Kyungpook National University, Korea, in 1988, and the M.S. and Ph.D. degrees in information telecommunication the Kyungpook National University, Korea, in 1990 and 2000, respectively. He joined the Agency of Defense Development (ADD), from Match 1990 to April 1995. Since 2004, he has been with the Jeju National University, Korea, where he is currently a Professor of Department of Computer Engineering. From 2008 to 2009, he has been at the Queensland University of Technology, Aus-

tralia, as a visiting researcher. His research interests include sensor networks, M2M/IoT, energy optimization and prediction, intelligent service, and mobile computing. mailto:kimdh@jejunu.ac.kr(D.K.)

Duc-Tan Tran is an Associate professor and Vice Dean of the Faculty of Electrical and Electronic Engineering, Phenikaa University. He has published over 150 research papers. His publications received the "Best Paper Award" at the 9th International Conference on Multimedia and Ubiquitous Engineering (MUE-15) and International Conference on Green and Human Information Technology (ICGHIT-2015). He was the recipient of the award for the excellent young researcher from Vietnam National University in 2008, Hanoi, and the third prize in the contest "Vietnamese Talents" in 2008. His main research interests include the representation, processing, analysis, and communication of information embedded in signals and datasets. He serves as a TP Co-chair, technical committee program member, track chair, session chair, and reviewer of many international conferences and journals. tan.tranduc@phenikaa-uni.edu.vn

Anh Ngoc Le is a Vice Dean of Electronics and Telecommunications Faculty, Electric Power University. He received his B.S in Mathematics and Informatics from Vinh University and VNU University of Science, respectively. He received a Master's degree in Information Technology from Hanoi University of Technology, Vietnam. He obtained a Ph.D. degree in Communication and Information Engineering from the School of Electrical Engineering and Computer Science, Kyungpook National University, South Korea, in 2009. His general research interests are embedded and intelligence systems, communication networks, the Internet of things, AI, and Big data analysis. On these topics, he published more than 30 papers in international journals and conference proceedings. He served as a keynote speaker, TPC member, session chair, and reviewer of international conferences and journals. anhngoc@epu.edu.vn

Article submitted 2021-01-31. Resubmitted 2021-03-28. Final acceptance 2021-03-29. Final version published as submitted by the authors.