Trust Evaluation Models For Cloud Computing

Vijay Kumar Damera, A Nagesh, M Nagaratna

Abstract: There is a big race for processing technology and storage and resource sharing capacity on interconnected servers around the world. This race defines what we call “Cloud Computing”. In recent years, cloud computing has developed rapidly in the context of the rise of the global Internet, and more and more services and products based on cloud computing have become more and more. As an emerging information service model, cloud computing has brought about tremendous and profound changes for computing services in the Internet era. However, due to the dynamic and complex nature of the cloud environment, users are faced with various data security and personal privacy risks when using cloud services. These problems have become an important factor hindering the development of cloud computing. In this context, Trust plays a crucial role in cloud environment to offer reliable services to the cloud customers. It is the main reason for the popularity of services among the cloud consumers. To achieve this, trust should be established between cloud service provider and cloud consumer. In this paper, An attempt is made to present different trust evaluation models proposed in the literature for cloud computing environment.

Index Terms: Trust, Trust Model, Cloud Computing,Security and Reputation.

1 INTRODUCTION

Digital transformation already reached the entire market, regardless of whether the business is digital or not and more than anything,this transformation aims to use technology for the benefit of people, employees and consumers. Consumers are increasingly connected and expect organizations to be part of this world as well - not just through marketing, but throughout the journey. The best consumer experience is through digital processes. Organizations looking to move fast, preserve flexibility and keep data safe have chosen the cloud[1,2]. When As a product of the convergence of computer technology and communication technology, the Internet is evolving from a traditional computer communication platform to a ubiquitous distributed network computing platform. In the past, people tried to make computers have networking capabilities, but now they emphasize the network's computing power[3,4]. Especially with the wide deployment and application of various mobile personal computing PCs (Personal Computing) devices, the Internet has become an indispensable tool and carrier for people's lives and work. People put more personal information with privacy and security requirements on the Internet for storage or processing, such as public mail systems and various social networking platforms (Facebook, intranet, etc.); originally served by a single organization, government or scientific research institution. Application systems are rapidly transforming into open systems for the Internet. E-commerce, e-government, and e-science have emerged to better handle and share services[5,6]. New generation information technology and service-oriented system frameworks such as cloud computing provide opportunities for enterprises to improve production and operation efficiency, integrate resources and synergistic value innovation from a wider scope, and establish more efficient and low-carbon operation systems and service models.

- *Vijay Kumar Damera is currently pursuing PhD degree program in Computer Science and Enineering in JNTU Hyderabad, Telangana, INDIA, E-mail: dameravijaykumar@mail.com*
- *Dr. A. NAgesh is currently working as professor in Dept. Of CSE, MGIT, Hyderabad, Telangana, INDIA. E-mail: akknagesh@rediffmail.com*
- *Dr. M. Nagaratna is currently working as professor in Dept. Of CSE, JNTUCEH, Hyderabad, Telangana, INDIA. E-mail: mratnajntu@gmail.com*

However, the new cloud service model has also brought new security risks in the process of re-integrating the industrial chain and the collaborative value chain. The virtualized remote service model and multi-agent collaborative service features have continuously broadened the traditional information security boundary, bringing more security risks[8,9]. Traditional information security technology can't solve this problem very well, and the trust-based system management method provides a new idea. The trust model can help enterprise users to effectively identify the credibility of cloud service resources, so that enterprise users can choose the appropriate service resources to deploy their tasks in accordance with the needs of their own business processes. On the basis of low cost and high efficiency of cloud services, the security and credibility of services are guaranteed, which provides an important guarantee for enterprises to improve production efficiency and gain competitiveness under the wave of new generation information technology. Trustworthiness, as a basic requirement of Internet-based application systems, faces many new challenges in new computing environments and application models. How to effectively manage trust in the Internet environment to adapt to the needs of the development of computing environment and application mode has become a hot issue[10]. Under the background of a variety of trust problems in Cloud Computing environment, in this paper, An attempt is made to present different trust evaluation models proposed in the literature for cloud computing environment[11,12].

2 INTRODUCTION TO CLOUD COMPUTING

Cloud computing is a generic term applied to anything that involves obtaining services hosted on the Internet. We can ask this interesting question: why not implement Internet services or resources under a scheme similar to the payment for drinking water service, or for renting an apartment, where the provider provides what is required and the user only pays for the use that makes? If this happens, the user would not have to worry about acquiring computer equipment and its respective maintenance, updating the applications or operating system, as it would be the responsibility of the supplier. This will lead the company to optimize costs and improve its productivity[2,3,4]. It is for this reason that organizations are turning their attention to this technology known as cloud computing, which is capable of minimizing the time spent in activities of lower value and allowing staff working in technology areas of information, focus your

attention on strategic activities that have a real impact on the business processes of the organization[1,2]. Many researchers in the industrial and academic fields have tried to define exactly what "Cloud Computing" is and what unique features it presents. Buyya [1] has defined it as follows: "Cloud computing is a parallel and distributed computing system consisting of a set of interconnected and virtualized computers. These computers are dynamically provisioned and presented as unified IT resources, based on SLA agreements established through negotiations between service providers and consumers"[4,5]. Other definitions have been proposed to define cloud computing. For example, Gartner's definition is as follows: "A cloud is a computing model in which which scalable and massive computing resources are provided as a service to several external users, using Internet technologies. IDC[2] definition is expressed as: "an emerging IT development and deployment model, enabling the distribution of products, services and solutions in real time across the Internet[3]." The most used and prominent definition of cloud computing is introduced by the American National Institute of Standards and Technology (NIST)[7].

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

2.1 Cloud Service Models

There are three fundamental services offered by cloud providers: IaaS (Infrastructure as a Service), SaaS (Software as a Service) and PaaS (Platform as a Service) as shown in figure 1.

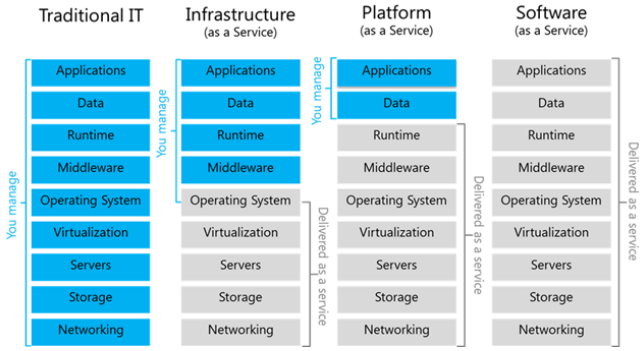

***Fig. 1**. Cloud Service Models*

- Infrastructure as a Service (IaaS): The concept of Infrastructure as a Service (IaaS, Infrastructure as a Service) is one of the three fundamental models in the field of cloud computing. Like all cloud services, IaaS provides access to computer resources located in the virtualized environment that constitutes the cloud through a public connection: Internet. In IaaS the computer resources offered consist of virtualized hardware, in other words, processing infrastructure (virtual server space, network connections, bandwidth, IP addresses, load balancers etc.,). In short, a company can avoid the acquisition of servers, space in a data center or network equipment and buy all these infrastructures from a cloud provider. This resource provisioning is done through the web. Physically, the hardware on which IaaS is based comes from a multitude of servers and networks, generally distributed among numerous data centers, whose maintenance is provided by the cloud provider. The client obtains access to the virtualized components to build their own computing platform with them.
- Platform as Service (Paas): The concept of Platform as a Service (PaaS, Platform as a Service) is one more step with respect to Infrastructure as a Service. The cloud provider, in addition to the Infrastructure as a Service, offers a solution that includes all the software resources necessary to support the complete life cycle of the development and implementation of applications (design, development, testing, distribution, hosting etc.). It is the type of solution normally used by software developers and, with respect to traditional solutions, it means a reduction in costs in both hardware and software infrastructure. An example of using PaaS would be that of a company that develops web applications in an ASP.Net environment and using SQL Server databases. Traditionally, it would be necessary to acquire the Visual Studio .Net and SQL Server licenses for the use of these environments by each member of the development team. If you choose to hire a PaaS, the cloud provider offers the developer all the necessary platform that is accessed through a web browser without high initial investments and without complicated installations.
- Software as a Service (SaaS): Software as a Service is a software distribution model . A single instance of the software application and the data it manages, are hosted in the infrastructure of the cloud provider, being accessible, via the Internet, from anywhere and at any time. That is, the client does not need to install the application on their own computers, avoiding the costs of software support, operation and maintenance of hardware and software, with the cloud provider being solely responsible for these tasks. It is not necessary to purchase any license to use the software, but to pay a rent or rent for the use of the software. A good example of SaaS is Microsoft Office 365 , which offers an online version of MS Office Suite (Office Web Apps) along with SharePoint Server, Exchange Server and Skype for Business Server.

2.2 Cloud Deployment Models

There are four typical deployment modes for cloud computing as shown in figure.2: "public cloud", "private cloud", "community cloud" and "hybrid cloud". The specific description is as follows:

- Public Cloud: Cloud infrastructure provides cloud services to the public or a large industry group. Public cloud services can be opened to customers through the network and third-party service providers. The term "public" does not necessarily mean "free", but it may also represent free or fairly cheap. Public cloud does not mean that user data is available for any. As a result, public cloud providers typically implement access control mechanisms for users, and public clouds are a solution that is both resilient and cost effective. Public clouds are owned and operated by third-party cloud service providers who provide their computing resources (such as servers and storage) over the Internet. In the public

cloud, all hardware, software, and other supporting infrastructure are owned and managed by cloud providers. Use a web browser to access these services and manage your account.

- Private Cloud: The cloud infrastructure specifically runs services for an organization, which may be managed by the organization or a third party, and may be on-premises or off-site (off- Premises). Private clouds have the advantages of many public cloud environments, such as resiliency and service delivery. The difference between the two is in private cloud services. Data and programs are managed within the organization. Unlike public cloud services, they are not subject to network bandwidth and security concerns. In addition, private cloud services allow providers and users to better control the cloud infrastructure, improve security and resiliency, because users and networks are subject to special restrictions. A private cloud is a cloud computing resource that is used exclusively by a business or organization. The private cloud can actually be located on the company's on-site data center. Some companies also pay to third-party service providers to host their private clouds. In a private cloud, maintain services and infrastructure on a private network.
- Community Cloud: Cloud infrastructure is shared by several organizations to support a particular community. A community is a group that has a common appeal and pursuit (such as mission, security requirements, policy or compliance considerations, etc.). Similar to a private cloud, a community cloud can be managed by the organization or a third party, either on-site or off-site. The community cloud is controlled and used by many organizations with similar interests, such as specific security requirements and common purposes. Community members use cloud data and applications together.

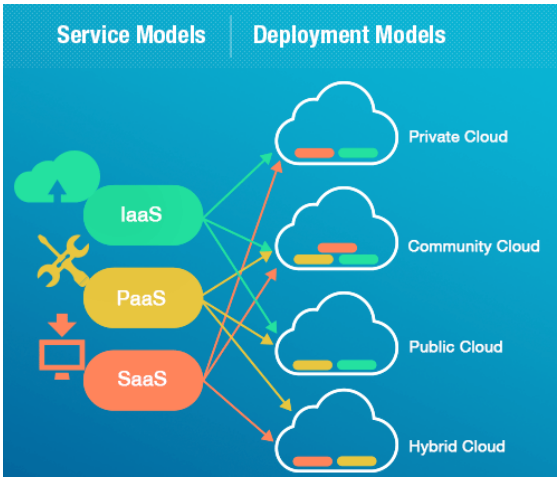

***Fig. 2**. Cloud Deployment Models*

- Hybrid Cloud: A cloud infrastructure consists of two or more clouds (private, community, or public) that exist independently, but are bundled together by standard or proprietary technologies that facilitate data generation. And application portability (such as cloud bursting technology for load sharing between clouds). In this model, users typically outsource non-enterprise critical information and process it on the public cloud, while at the same time controlling key business services and data. Hybrid clouds bind them together by technologies that allow data and applications to be shared between public and private clouds. By allowing data and applications to move between private and public clouds, hybrid clouds provide enterprises with greater flexibility and more deployment options.

3 TRUST

3.1 Definition of Trust

As a basic factor in human society, trust plays a decisive role in social organization. For example, at a traffic intersection, we always believe that cars in the other direction will follow the instructions of the signal lights to make our decisions and travel smoothly. It is precisely because of the importance of trust that trust research has received attention in various fields, including psychology, sociology, philosophy, etc[9,18,24]. With the development of the times, it has been integrated into business management, economic theory, engineering, computer science and other application fields. Knowledge. Due to the complexity and multi-faceted nature of trust, there is currently no precise and widely accepted definition of trust in academia and industry, which is often understood as an intuitive concept. There are various definitions around trust. Trust in the Oxford Dictionary is defined as “a belief in the reliability, authenticity, ability, and strength of someone or something.” Mayer [] defines trust as “based on the prediction of a certain behavior of the believer, the relying party is willing to accept the risk of believing the other party, regardless of whether it can monitor or control the trusted party”. This definition emphasizes the risk of trust, indicating that trust is essentially an assessment of the risk of acceptance. As shown in Figure 3, Huang [32] et al. define "trust is a state of mind, which includes three aspects: (1) expectation: the service that the trustee wants to obtain from the trusted person; and (2) the belief: Based on the judgment of the ability and will of the trusted person, the trustee believes that the expectation is correct; (3) the risk willingness: the trustee is willing to bear the possible failure of the belief."

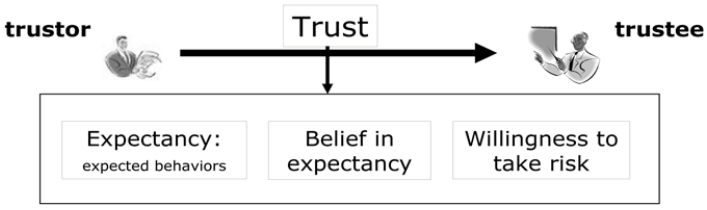

***Fig. 3**. Trust Elements*

3.2 Nature of Trust

The dynamics of trust are the biggest challenge of trust evaluation and trustworthiness prediction. It is determined by the natural attributes of the entities in the trust relationship.This section summarizes the nature of trust as follows:

- Subjective uncertainty: Refers to the fact that the trustee cannot clearly judge the dynamic change of the trustee as the context and time change. The trust can only be evaluated according to the previous interaction history; trust is credit. The party has a subjective judgment on the

recipient, and different entities will have different criteria. Even for the same trusted party, the same context, the same time period and the same behavior, the difference of the creditors, the given quantitative judgment is likely to be different.

- Context-dependent: The specific state of trust is closely related to the context. It is meaningless to discuss the trust issue from the specific context.
- Asymmetry: That is, the trust relationship is one-way, A trusts B, and does not mean that B also trusts A.
- Incomplete transitivity: Trust relationships are generally not fully transitive, that is, A trusts B, B trusts C, and may not conclude that A trusts C. Only under certain specific constraints, trust has a certain degree of transitivity. Recommendation is a typical way of trust communication, and it is an embodiment of trust transfer. The literature [2] shows that the trust of ability is not transitive through formal description, while the trust based on concept is transitive.
- Time Asynchrony: It means that the evaluation result of trust relationship between entities has time asynchrony. The solution to the problem is to average the time slot; trust will decay with time, and the most direct performance is: The longer the trust evaluation, the worse its persuasiveness.
- Multi-objectivity: Trust is often associated with multiple attributes of the trusted party, and is influenced by multiple attributes. It is a concept of multi-attribute interaction. Taking online shopping as an example, customer evaluation of the seller may include evaluations of the quality, price, service attitude, and speed of the delivery.

3.3 Principles of trust

To guarantee a maximum level of confidence certain principles must be followed:

- Trust transitivity, if entity A trusts entity B and entity B trusts entity C, then we can come to the conclusion that A can trust entity C by referring to the trust of entity B;
- Trust is a function of perception of risk, it represents a belief in a person for his correct actions. Thus, trust must also assess the uncertainty that the other party is acting properly and incorporate the associated risks;
- Trust is determined by time, it is built over time based on past experiences;
- The trust can be measured, it is measurable by a numerical value, generally in the interval [0 – 1];
- Formal and social tools are necessary for the evolution of trust, trust can be modeled according to various formal models.

3.4 Trust in Cloud Computing

Trust is originally a concept that emerges in sociology, and concepts in sociology are often vague. Trusted computing leads the concept of trust to the field of computer science. Trusted Computing Group (TCG) defines Trust as: An entity that can always achieve the desired goal in the expected way, then the entity is trustable. That is, trust emphasizes the expectation of the entity's behavior, while also paying attention to the security and reliability of the system[11,12]. Trust is a corresponding binary relationship. This relationship can be one-to-one, one-to-many, or many-to-one, many-to-many. There are several ways to gain trust: Direct trust, Recommended trust, Multi-level recommendation trust and Hybrid trust[12]. In online transactions (such as e-commerce transactions), trust is one party who believes the other is reliable and able to fulfill its promise. Only when the two parties trust each other the transaction proceed smoothly, so trust is the premise and customs of trading activities. In a complex network environment like cloud, trust between entities can be divided into direct trust and Indirect trust. Direct trust is a relationship established by two entities based on past experience. Indirect trust refers to relationship established by the recommendation of other entities. Therefore, trust has the following characteristics: asymmetry (if entity A trusts entity B but does not neccessary that B truts A, subjectivity (trust is the subjective judgment of the evaluator on the evaluation object), dynamic (trust may follow Change in time, environment or other factors) Multidimensionality (trust between entities is related to multiple attributes, such as historical trust value, social status, income level, etc.) Fuzziness and incomplete transferability (Entity A trust entity B, and entity B trusts entity C, but does not necessarily have A trust C).

4 TRUST EVALUATION MODELS FOR CLOUD

Cloud computing is an emerging computing model with the advantages of large scale, high reliability and extremely low cost. At present, there have been a large number of public cloud service providers at home and abroad, such as Google's GFS (GoogleFileSystem), IBM's blue cloud computing platform. On the one hand, different cloud service providers may provide some of the same basic services, and also provide some unique services; on the other hand, the service quality of different cloud computing vendors also differs greatly. With the further popularization and development of cloud computing, users will face an increasingly important issue called How to choose a service provider that best suits users' needs from many cloud service providers? In order to solve this problem, trust evaluation models for cloud computing must be used. The credibility of the service quality of the business is evaluated. The trust evaluation in the existing cloud computing environment can be used for service quality transactions [1,3], secure storage [4], resource allocation [5,6], access control [8],cloud environment security [8,9] and other aspects. Service quality is an important factor affecting the development of cloud computing. Before opting any cloud service consumer always depends on trust evaluation model to select the services of a CSP and outsources its critical data to the Cloud platform. Trust is highly subjective and context-sensitive.Due to this nature the service selection from a cloud provider becomes most challenging task. Furthe trust value may change with time based on the experiences of user with provider. This trust level may also vary with feedback from other cloud users availing the services from same the CSP[14,15]. Whenever an organisation wants to migrate its critical data on to the Cloud, it prefers to evaluate the trustworthiness of the CSP. The trust level of that CSP is evaluated using a trust model. The mechanisms, techniques and protocols that help in evaluating the trust level are commonly known as trust models. A trust model can be defined as a coded implementation that relies on concepts of trust in order to assign a trust value for a CSP, based on which the interactions with that specific cloud provider are restricted and controlled [18,20]. There is need to categorize existing trust models presented in the literature

[21,23] in a precise way in order to identify and analyze the current state of the art. In this regard, we have systematically categorized the trust evaluation models for cloud environment into four main classes on the basis of their diverse approaches for calculating the trust score, as shown in Figure 4. These classes include Agreement based, Certificate based, Feedback based, and Domain based, which we describe briefly in the following subsections.

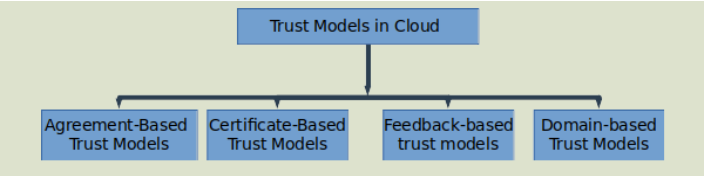

***Fig. 4**. Trust Models in Cloud*

4.1 Agreement-based trust models

In this category Trust models are created on contracts and agreement between the CSP and Cloud Users. The most frequently used contracts are SLAs (service level agreements) and service policy reports. It contains several security documents and QoS parameters to establish the trust between two parties.Trust evaluation under this category is depicted in Fig. 5. In the first step, cloud user gives his security and QoS requirements to the trust evaluation module. This module is is capable of creating and negotiating the agreement with the Cloud Service Provider. Generally such agreement is called either an SLA or service practice statement. Trust evaluation module in its next step, forwards an agreement negotiation request to the Cloud provider along with the cloud user required parameters. Finally, the contract parameters monitoring module exchanges the agreement with the consumer for establishment of trust between both entities [24,25].

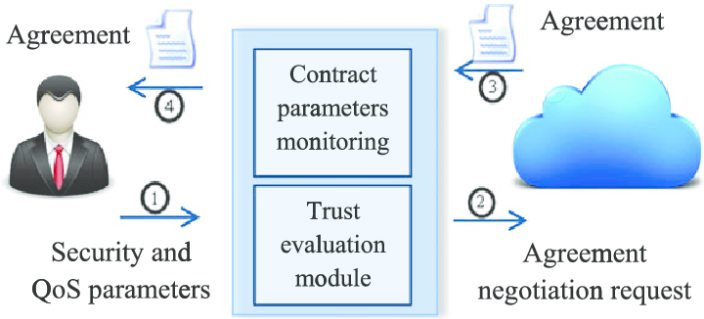

***Fig. 5**. Agreement-based trust model*

In the SLA-based trust model, it is necessary to monitor the service level, and the monitoring results will be used as the basis for objective trust calculation. There are many related studies on SLA monitoring. The traditional SLA monitoring methods and tools mainly monitor the performance parameters of the network element layer and the network layer. For example, Netlogger [33] can effectively Monitor and collect information about network information and application calls, but it cannot monitor other information related to host operations, such as memory and CPU information, which cannot meet the needs of users to monitor various low-level resources in the cloud environment. Alhamad et al. [34] pointed out that SLA's service level requirements can well meet cloud computing. For the environment with strict requirements for services, the conceptual framework structure of SLA in cloud computing environment is introduced, and different SLA parameter standards for different services (IaaS, PaaS, SaaS, etc.) in cloud computing are given. After that, they proposed an SLA-based trust management model for the cloud computing environment in the literature [34]. Gao Yunqi et al [35] A trust model based on SLA and user evaluation is proposed. Two static and dynamic subsystems of SLA subsystem are designed. The two trust evaluation results are combined to obtain the most trusted cloud service provider. The model only relies on static evaluation system and user. The subjective scoring method does not use the actual service process to monitor, so it is difficult to objectively and accurately assess the credibility of the service. Wang et al. [36] proposed A reputation-based third-party SLA auto-negotiation platform. The reputation system in the platform is used to record the reputation of users and service providers, and to determine the most credible service providers through reputation; At the same time, SLATemplatePool is also introduced. When the user requests the service, the SLATemplate can be selected as a reference and a new SLA can be developed to improve the efficiency and credibility of the protocol negotiation. There is lot of research is going on in this area. Currently,local Reputation trust mechanism can no longer meet the needs of users in the cloud computing environment for node selection that has not been traded; Studies made in EigenRep[14], SGM[15], MGM[16], presents, there are many related researches on SLA monitoring.

4.2 Certificate-based trust models

In this category Trust establishment happens through certificates, trust tickets (TTs) and endorsement keys issued by certificate authority(CA). For trust establishment under this category Security certificates for software, platform and infrastructure services palys an important role.Trust Tickets are issued in order to comply with integrity and confidentiality of data on the Cloud and to improve the trust of customers [26]. Control over data which is being shifted to cloud environment[27,28] to the cloud customers is being ensured using various certificates and secret keys used in trust model. As shown in Fig.6 this class additionally includes the trust models based on trusted platform module (TPM) endorsement keys which are responsible for calculating the configurations and measurements of the Cloud for trust establishment.

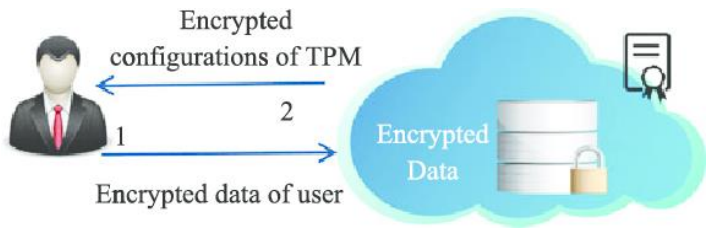

***Fig. 6**. Certificate-based trust model*

Certification-based solutions give the power of priori analysis of cloud behavior and verification of non-functional properties of cloud application services. Initially, certification approaches are designed for static and monolithic package, and applied at

preparation and installation time [4]. Later, certification approaches are designed to manage the peculiarities and to address the wants introduced by service-based systems(e.g., [3], [5], [7], [11], [24]). Recently, these approaches began to be tailored to deal with the dynamic, flexible, multi-layer, and hybrid nature of the cloud. Spanoudakis[26]gave a summary of the EU FP7 Project CUMULUS [6],aimed at manufacturing a security certification theme for the cloud. Sunyaev and Scheneider [27] mentioned the potential blessings introduced by a certification approach once integrated in an exceedingly cloud system. Bertholon[28] and Munoz and Mana [29] given certification approaches that accept trustworthy computing platforms. Krotsiani[30] planned an answer supporting progressive certification of cloud applications, where as Cimato[31] a abstract framework and a meta model for certification management within the cloud.

4.3 Feedback-based trust models

This category includes trust models that collect feedback and opinions from other consumers to evaluate the trust on the CSPs. As an initial step of trust evaluation, various CSPs are registered with the trust model via service registry module [29,31]. Later on, the feedback module collects and manages the feedback from consumers regarding different QoS and security parameters offered by the registered Cloud providers. As shown in Fig.7, The trust evaluation module calculates CSPs trust score for CSPs on the basis of the collected feedback. Further, the Cloud Users can send request for trust score of the required Cloud Service Provider to the trust evaluation module and the same is returned to the cloud user.

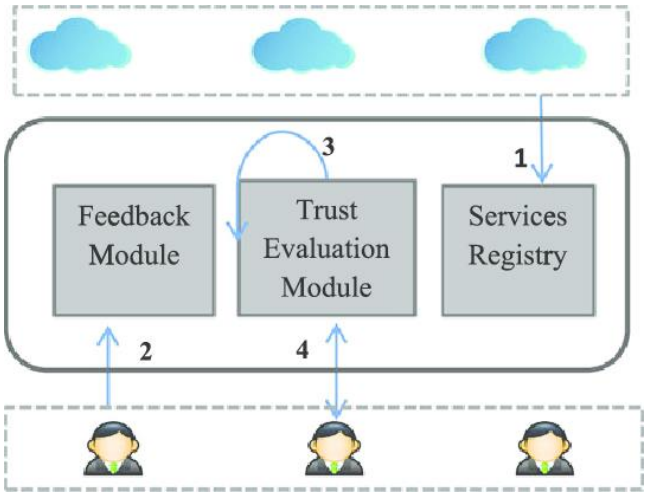

Fig. 7. *Feedback-based trust model*

In this classification, trust models evaluates CSPs trust score based on CSPs reputation and feedback. In this model, it collects the feedbacks and an opinion of cloud consumers to measure the trust on the cloud resources provided by the CSP. Different parameters offered by CSPs like QoS parameters and Security parameters are used by trust model to evaluate trust score. This trust score is useful for the cloud customers to choose the particulat CSP who guarantee the QoS to its customers. Jingwei Huang[] in their work concluded that "Reputation of an entity is the collective opinion of a community towards an entity". It is the value reflecting the overall belief. CSPs with high trust value will be the most trusted among the community [21]. Abawajy J[] in his work presented an honesty ranking factor that states an attitude on how reliable is a service provider of used information. It is difficult to find out an inactive rates and malicious rates. They enhance a mechanism to know the trustworthiness of opinions and filter out opinions that are not true. In[37] a feedback filtering algorithm is proposed to identify and eliminate the dishonest feedbacks by computing the trustworthiness of feedback ratings using a threshold value and their own experience. Borowski, J.F [38] have developed a mechanism in which it collaborates a reputation trust mechanism with agent-based safety system to safeguard against wicked failure ratings. Reputation based trust score is calculated depending on the direct interactions between the agents. Agents will relay on the interval status requests to the peers in their cluster. Whenever the peer receives the query they have to reply immediately with their present status. If the reply is not acknowledged then the agent is faulty. Each interaction result is either 0 or 1. The ultimate Reputation based trust rating is calculated by an average of all interactions [6]. H. Abawajy and A.M. Goscinski[39] in their work stated that "Reputation is a measure that is derived from direct or indirect knowledge of previous communications of peers and is used to access the level of trust a peer puts into another". The trust evaluation models used in distributed and grid computing have depended on the feedback about a service given by the customers. There is a chance that a malicious users who can give negative feedback about a service purposely and this may lead to a wrong opinion about a service among the cloud users. All existing trust evaluation models simply based on feedback values and calculates the trustworthiness of a service instead of verifying whether the feedback given by the customer is genuine, unbiased, reliable and trustworthy. The latest trust evaluation models used in cloud identify the malicious users and fake feedbacks. P.D. Manuel [40] have proposed the cloud trust management model which calculates trust value based on identity, capability and behaviour. TAAS framework was proposed by Talal H Noor and Quan Z Sheng [41] in which they have proposed adaptive reliability model that differentiate genuine feedback by considering customer competency and agreement of their opinion ratings. Talal H Noor[42] have propsed a method to detect the fake ratings from malisious users and provide enhancement on trust group. Talal H Noor [42] have come with an implemented model called a Cloud Armor, a trust management framework based on reputation which is used to deliver the trust as a service. Vijayakumar V[43] in his work proposed an approach for selecting the grid services based on trust and reputation to implement the jobs. Xiaonian Wu [44] introduced a Dempster Shafer theory based trust assessment framework to find the malicious entities. In this model, first hand evidences are nothing but direct interactions and second hand evidences are the recommendation trust values. At the end the cumulative of recommended trust values forms the reputation of entities. Zaki Malik and athman Bouguettaya [45] have proposed a framework for establishing the trust in service oriented environment namely RATE Web. It is composed of a cooperative model in which web services distribute its experiences of the CSPs with their cloud customers through feedbacks. Cloud Service provider's trust value is calculated by aggregating the different ratings. The following reputation evaluation metrics namely rater credibility, majority rating, past rating history, personal experiences for credibility evaluation,

personal experiences are considered for reputation assessment and temporal sensitivity [45].

4.4 Domain-based trust models

Domain-based trust models, as shown in Fig. 8, are primarily developed for grid computing, but some of the selective trust models have been proposed under this category for Cloud Computing environment. The underlying idea of this category is to divide the Cloud into a number of autonomous domains and distinguish two types as intra-domain and inter-domain trust relationships that are extracted from direct and recommended trust tables, respectively. Intra-domain trust values depends upon the transactions between the entities that are in the same domain. If an entity wants to evaluate the trust value for another entity, it first checks the direct trust table, if the direct trust value (DTV) doesnot exists, then it looks for the recommended trust values from the other entities. Inter-domain trust value is a comprehensive value based on direct and recommended trust values from other domains[32,33].

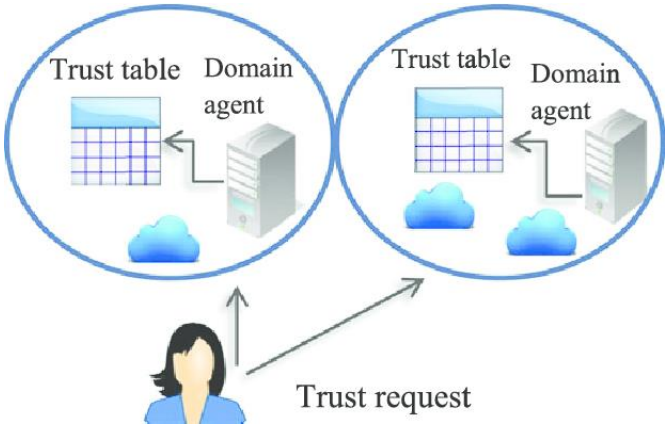

***Fig. 8**. Domain-based trust model*

5 CONCLUSION

In this paper we have presented different trust evaluation models in the literature for cloud computing environment. All these models in the literature are classified into four categories namely: Agreement-based trust models,Certificate/secret keys-based trust models,Feedback-based trust models and Domain-based trust models. Detailed explanation about each category is given along with the research work done so far in each classification. Along with this an overview of Trust management, types of trust and factors effecting trust also discussed. Further we have discussed in detail classification of trust evaluation models for cloud.

6 REFERENCES

[1] Manvi S.S, Krishna Shyam, G., 2014. Resource management for Infrastructure as a Service (IaaS) in cloud computing: a survey. J. Netw. Comput.Appl. 41 (May), 424–440.

[2] Azad P, Navimipour, J.N., 2017. An energy-aware task scheduling in cloud computing using a hybrid cultural and ant colony optimization algorithm.Int. J. Cloud Appl. Comput. 7.

[3] Mohammadi S.Z, Navimipour J.N., 2017. Invalid cloud providers' identification using the support vector machine. Int. J. Next Gener. Comput. 8(1), 82–98, 17p.

[4] Wang Y, Wei J., 2015. Toward protecting control flow confidentiality in cloud-based computation. Comput. Secur. 52, 106–127.

[5] Huang J, Nicol D.M., 2013. Trust mechanisms for cloud computing. J. Cloud Comput. 2, 1–14.

[6] Filali F.Z, Yagoubi B., 2015. Global trust: a trust model for cloud service selection. Computing 3, 19

[7] Mell P. and Grance T., 2011, The NIST definition of cloud computing. National Institute of Standards and Technology, October 7. Available from: http://csrc.nist.gov/groups/SNS/cloudcomputing/cloud-def-v15.doc

[8] Chong S.K, Abawajy J., Ahmad M, Hamid I.R.A., 2014. Enhancing trust management in cloud environment. Procedia Soc. Behav. Sci. 129,314–321.

[9] Keshanchi B, Souri A, Navimipour N.J., 2017. An improved genetic algorithm for task scheduling in the cloud environments using the priorityqueues: formal verification, simulation, and statistical testing. J. Syst. Softw. 124, 1–21.

[10] Chen X, Wang L, Zomaya A.Y, Liu L, Hu S., 2015. Cloud computing for VLSI floorplanning considering peak temperature reduction. IEEETrans. Emerg. Top. Comput. 3, 534–543.

[11] Mei S, Wang Z, Cheng Y, Ren J, Wu J, Zhou J., 2012. Trusted bytecode virtual machine module: a novel method for dynamic remoteattestation in cloud computing. Int. J. Comput. Intell. Syst. 5, 924–932.

[12] Shanmugam U, Tamilselvan L., 2017. Trusted Computing Model with Attestation to Assure Security for Software Services in a Cloud Environment.10 (1).

[13] Mahboob T, Zahid M, Ahmad G., 2016. Adopting information security techniques for cloud computing—a survey. International Conference onInformation Technology, Information Systems and Electrical Engineering (ICITISEE), 7–11.

[14] Shen Z, Tong Q., 2010. The security of cloud computing system enabled by trusted computing technology. 2010 2nd International Conference onSignal Processing Systems (ICSPS), V2-11-V2-15.

[15] Habib, S.M., Ries, S., Mühlhäuser, M., Varikkattu, P., 2014. Towards a trust management system for cloud computing marketplaces: using CAIQas a trust information source. Secur. Commun. Netw. 7, 2185–2200.

[16] Sidhu J, Singh S., 2016. Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers.J. Grid Comput., 1–25.

[17] Lu J, Shao M., 2012. Trust establishment for data integrity checking in cloud computing. Adv. Inf. Sci. Serv. Sci. 4.

[18] Rahi S.B, Bisui S, Misra S.C., 2017. Identifying the moderating effect of trust on the adoption of cloud-based services. Int. J. Commun. Syst. 30(11), e3253.

[19] Duckett B., 2005. Concise oxford english dictionary. Ref. Rev. 19, 33.

[20] Rajendran V.V, Swamynathan S., 2015. Hybrid model for dynamic evaluation of trust in cloud services. Wirel. Netw., 1–12.

[21] Lynn T, van der Werff L, Hunt G, Healy P., 2016. Development of a cloud trust label: a Delphi approach. J. Comput. Inf. Syst. 56, 185–193.

[22] Manuel P., 2013. A trust model of cloud computing based on quality of service. Ann. Oper. Res., 1–12.

[23] Selvaraj A, Sundararajan S., 2017. Evidence-based trust

evaluation system for cloud services using fuzzy logic. Int. J. Fuzzy Syst., 1–9.
[24] Pathan A.S.K, Mohammed M.M., 2015. Building Customer trust in cloud computing with an ICT-enabled global regulatory body. Wirel. Pers.Commun. 85, 77–99.
[25] Tang M, Dai X, Liu J, Chen J., 2017. Towards a trust evaluation middleware for cloud service selection. Future Gener. Comput. Syst. 74,302–312.
[26] G. Spanoudakis, E. Damiani, and A. Mana., 2012, " Certifying Services in Cloud: The case for a hybrid, incremental and multi-layer approach", in Proc. Of IEEE HASE'12, Omaha,NE,USA. Pp.102-122.
[27] 27. A. Sunyaev and S. Schneider.,2013, Cloud services certification,Communications of the ACM, vol. 56, no. 2, pp. 33–36.
[28] Sunyaev and S. Schneider.,2013,Cloud services certification,Communications of the ACM, vol. 56, no. 2, pp. 33–36.
[29] Munoz and A. Mana., 2013, Bridging the gap between softwarecertification and trusted computing for securing cloud com-puting, inProc. of IEEE SERVICES 2013, pp.Santa Clara, CA, USA.
[30] M. Krotsiani, G. Spanoudakis, and K. Mahbub.,2013, Incrementalcertification of cloud services, inProc. of SECURWARE2013, Barcelona, Spain.
[31] S. Cimato, E. Damiani, F. Zavatarelli, and R. Menicocci.,2013, Towards the certification of cloud services, inProc. of IEEESERVICES 2013, Santa Clara, CA, USA.
[32] Huang, J. and Fox, M.S., 2006, An ontology of trust – formal semantics and transitivity, in Proceedings of the Eighth International Conference on Electronic Commerce, ACM,pp.259–270.
[33] D Gunter, B Tierney, B Crowley, M Holding, J Lee.,2000, Netlogger: A toolkit for distributed system performance analysis, Proceedings 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems,pp.267-273.
[34] Alhamad, M. Alhamad, T. Dillon, E. Chang.,2010,Sla-based trust model for cloud computing, 2010 13th International Conference on Network-based Information Systems, IEEE (2010), pp. 321-324
[35] Yunqi Ye, Liangliang Xiao, I-Ling Yen, and Farokh Bastani. Secure, depend-able, and high performance cloud storage. InProceedings of the 29th Sympo-sium on Reliable Distributed Systems (SRDS), pages 194–203, 2010.
[36] Khalid, O.; Khan, S.U.; Madani, S.A.; Hayat, K.; Khan, M.I.; Allah, N.M.; Kołodziej, J.; Wang, L.; Zeadally, S.;Chen, D. Comparative Study of Trust and Reputation Systems for Wireless Sensor Networks. Secur. Commun. Netw. 2013, 6, 669–688.
[37] D.W. Oard and J. Kim., 1998, Implicit Feedback for Recommender Systems, Proc. 5th DELOS Workshop on Filtering and Collaborative Filtering, pp. 31-36.
[38] Borowski, J.F., et al., 2011, Reputation-Based Trust for a Cooperative Agent-Based Backup Protection Scheme. IEEE Transctions on Smart Grid (2011),pp. 287 – 301.
[39] Jemal H. Abawajy, Andrzej M. Goscinski., 2006, A Reputation-Based Grid Information Service, InProceedings of International Conference on Computational Science (2006), pp 1015-1022.
[40] P. D. Manuel, M. I. Barr, S. T. Selvi., 2011, A novel trust management system for cloud computing - IaaS providers, JCMCC-Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. 79, Issue.3,pp.19-23.
[41] Noor, T. H., \& Sheng, Q. Z., 2014, Web service-based trust management in cloud environments. In A. Advanced web services (pp. 101-120)
[42] 4TH Noor, QZ Sheng, A Alfazi.,2013, Reputation attacks detection for effective trust assessment among cloud services, 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications,pp. 469-476.
[43] V Vijayakumar, RSDW Banu., 2008, Security for resource selection in grid computing based on trust and reputation responsiveness, International Journal of Computer Science and Network Security, pp.107-115.
[44] Xiaonian Wu, Runlian Zhang, Bing Zeng, Shengyuan Zhou., 2013, A Trust Evaluation Model for Cloud Computing, Proceedings of the First International Conference on Information Technology and Quantitative Management, {ITQM} 2013, pp.1170–1177
[45] Zaki Malik, Athman Bouguettaya., 2009, RATEWeb: Reputation Assessment for Trust Establishment among Web services, The VLDB Journal (2009), pp.885–911.