BVG Trust

J. Sci. Trans. Environ. Technov. 2018, 11(3) : 129-136

Scientific Transactions in Environment and Technovation

Survey based on different trust models in Cloud Computing

https://doi.org/10.56343/STET.116.011.003.003
http://stetjournals.com

Mahesh Kalyanaraman and ThilagarajRamasubbu*

Corporate Security Team, Tata Communications Limited, Chennai, Tamilnadu, India.
*Center of Excellence in Digital Forensics, Chennai, Tamilnadu, India.

Abstract

Cloud computing is the most discussed research area now-a-days which helps to provide flexibility and elasticity in using the computing properties and services to fulfill the condition of current companies. Cloud computingdeals dynamic, shared services, scalable and cost-effective for enterprises from distant data center. However, the problem of trusting the cloud computing is a supreme concern for enterprises as trust is widely regarded as one of the top problems for the approval and development of cloud computing. It deals with many obstacles in the path of its growth, that are security issues, data privacy issues and distrust on Cloud Service Providers (CSP). To achieve this, trust should be established between CSP and Cloud Consumer (CC). There are a lot of methods proposed to help the consumers identify the cloud service provider who seems to be more reliable. Authentication based trust models use encryption and key management technologies to establish trust between CCs and CSPs. This category includes trust models that ensure the availability, integrity and confidentiality of data on cloud by using certificates from standardized body, trust tickets, private and public keys, Tested Platform Module (TPM) endorsement keys and etc. This paper addresses the existing trust models for trust establishment in cloud services and also tries to find out the shortcomings of these models. Trust models are measured as a methodology that aids to estimate trust on the CSP's or the third party suppliers that are providing the cloud services.

Key words: Cloud computing, Trust Models, Cloud Consumer(CC),cloud service providers (CSP)

Received : November 2017 Revised and Accepted : February 2018

INTRODUCTION

The last few years, almost every kind of associations cloud computing has been generally adopted, for giving on-demand infrastructures that are ûexible, software as a service and platformsas a service. In daily life Customers beneût from cloud services, most of the time without even being aware that they are using services developed on a cloud computing infrastructure. In addition to the well-known beneûts resulting from cloud computing adoption, several issues have emerged during its evolution, most of them relate to trust management, privacy and security. Specifically, trust management by its explosion have placed even more attention, key challenges representing one of the cloud computing technologies adoption. cloud computing paradigm are understanding their correct motivated vendor offering adjustment of the speed and ûexibility but, at the same time the data privacy and the security from higher risk are introduced (Pearson and Benameur, 2010) From the cloud customer point of view, who may be citizens, businesses or organizations, this represents a crucial concern, especially when entrusting Cloud Service Providers (CSPs) for private or sensitive information, like ûnancial or health data or business-conûdential information. The resulting lack of trust is a key inhibitor to cloud adoption in domains where conûdential or sensitive information is involved. To establish the Cloud computing adoption is one of the major challenges to prevent the distrust that comes out of the majority or the consumers through their extensive use, because a consumer does not have a direct control in excess of their data lying on the cloud. Trust is a social problem, NOT A PURELY TECHNICAL ISSUE (Kai Hwang and Li,2010). It is viewed as a measurable belief that utilizes experience to make trustworthy decision(Dawei Sun *et al.*, 2011); The CSP offers to the Cloud Service Users (CSU) for all time include to remain trust and cloud services are established strongly in the CSUs from the CSPs include keeping trust. Each security factor almost control direct, if the hold CSPs and the CSPs handles the digital resources that provide all their cloud computing scenarios. CC's trust on the cloud computing systems that vary based on the scope and context of applications in cloud computing. For example, CCs

*Corresponding Author :
email: rthilagaraj@gmail.com

who are using data storage applications for storing their aware information on the cloud, have different requirements than those who use cloud for online gaming service. CSPs should offer a secure and controllable environment for those CCs who use data storage applications to get CCs' trust, while, for those who use gaming services, CSPs should just offer a high performanceenvironment.Therefore, there are different trust models available for evaluating the trustworthiness on cloud services and CCs can choose one based on the service they want to use. Therefore, it becomes difficult to select a trust model that best satisfies the user's requirements. There is a need for assessment criteria that can evaluate the trust models and helps the users in selection of most suitable model in line with their preferences.This paper has categorized trust models into five categories namely trust mechanisms which are

Reputation based trust models Authentication based trust models SLA based trust models Domain based trust models Platform based trust models (Maryam Rodaki, 2016)

Trust Mechanisms in Cloud Computing

The system security is improved in good way by through trust mechanism. It gives access control, security states, policies and reliability for resolution creation by identifying and distributing security mechanisms in different systems the malevolent being based on extracting the detected results. The aims of trust model are to assign high quality computing resources to users and reconfigure servers dynamically. Trust evaluation factors include availability, scalability, usability and security. Some of the trust mechanisms are reputation based trust, authentication based trust models, Evidence trust, domain based trust models and platform based trust models.

Reputation Based Trusts

Reputation based trust models, an entity's reputation is usually evaluated based on opinion they have about direct connections with the agreement. Therefore, this category includes the trust models that collect CC's feedback to estimate trust from cloud services. In this section, we categorize to estimate reputation based trust models and some of the recent trust models are studied. Character and trust are different where trust is between two entities. But the aggregated opinion of a community towards the agreement is the character of an agreement (Wang and Singh, 2010); An entity with high reputation is trusted by lots of unity in the community. Trust ruling on an entity is made by trustee and the reputations are used to compute the trust stage from the trustee. The reputation of cloud users provides an impact on cloud users. Reputation is represented by a complete score reflecting the general opinion. Reputation is more useful for the cloud users in choosing a cloud service from many options without particular requirement. A huge number of raters are needed for meaningful and objective ratings. The advantage of the data used for assessment covers more situation and wider time-window of observations. It also maintains overall credibility level of the system. It affects the reliability of the system and misuses the resource providers to gain popularity.

Service Level Agreement (SLA) Based Trust

A Service Level Agreement (SLA) is a legal contract between a cloud user and a CSP. It is one of the approaches and trust on CSPs. The entities that are providing services are necessary to follow consistent SLA, e.g., from proposed cases community are used by cloud computing (Wang *et al*, 2013); SLA validation (Haq *et al*., 2010); and monitoring (Applogic, 2015); methods are used to verify the quality of CSPs and CCs which are dependable for monitoring SLA violations. Since SLA compensation clauses are developed by the CSPs, CCs do not have enough chance to apply for compensation if SLA violation happens and this is a problem as cloud computing because of lack of standardized SLAs that are not analyzed for the stakeholders. However industry driven initiative (Dustin Amrhein *et al*., 2009); have addressed this problem but still it is not fully implemented.There are a number of extra issues with SLA based trust. First, SLA focuses the "visible" element of cloud service performance, and does not address "invisible" elements namely privacy and security. Second, many cloud users does not have sufficient capability to perform SLA verification on their own and they need a professional third party help to provide these services. In a hybrid cloud, private cloud trust ability may still rely in the private cloud user and SLA verification, however the individual users in a public cloud and some small organizations without technical capability may use a commercial professional cloud entity as trust broker. Trust organization below this category is based on agreement signed and contracts by CSPs for the delivery of different services to CCs. SLA provide the basis for trust establishment. Various security concerns and quality of service attributes are incorporated in agreements and contracts to start trust on CSP (Kanwal *et al*., 2013);

Domain Based

Fundamental plan in domain based trust model cloud is divided into number of autonomous domain and it differentiates two types of domain they are Within-

domain Inter-domain trust relationship Within-domain trust principles depend on the transactions between the unities that are in the same domain. If an entity needs to compute the trust value for some other entity, it checks the direct trust table but if the direct trust value is not found then it looks for the suggested trust values from other entities (Kanwal *et al*.,2013); The inter-domain trust relationship is using the trust relationship between domains. There is a validation mechanism for every domain which trusts the authentication mechanisms of other domains. If a unity is authenticated by one domain, then its authentication is acceptable by all other domains.

Platform Based

Platform based trust models consists of policies that ensure applications are executing on platforms that meet a specified trust assurance level and evaluate the confidence of CCs on using cloud services lunch on a specific platform. Therefore, by using this trust model, CCs can trust a CSP to use the offered platform (Kanwal *et al*.,2013).

Authentication Based Trust Models

Authentication based trust models use encryption and key management technologies to found trust between CCs and CSPs. This category includes trust models that ensure the availability, integrity and confidentiality of data on cloud by using certificates from standardized body, trust tickets, private and public keys, TPM endorsement keys etc. and evaluates the confidence of CCs regarding the expected behavior of cloud services.

Trusted Virtual Environment Module (TVEM*)*

Trusted Virtual Environment Module (TVEM) is also known as trust model (Krautheim *et al*.,2010); and it is obtained as a software use. Trusted Platform Module (TPM) virtualization methods are already given from the cloud environments. Cryptographic algorithm flexibility, enhanced Application Program Interface (API), and a modular architecture are better features of TVEM. It also introduces a unique Trusted Environment Key, information owner to the combining trust, and creates trust dual root from the CSP for the TVEM every virtual environment is distinct and platforms trust separate (Krautheim *et al*.,2010); The configuration of a Host Platform (HP) with multiple virtual environments requires a TVEM. The virtual environment may be an entire virtualized OS that supports many applications or a special purpose virtual environment that performs a single application. The hypervisor and its related VM are lies between the TVEM. TVEMs on the aware hyper visor and give sustain via a TVEM manager. Each TVEM to the TPM services gives the TVEM manager mediation and it requires other process in TVM services. TVEMs are allowing access and the TVEM manager must gives from the host platform. In HP TVEM's private information are secure the RTS which is used for the host platform. TPM during the hypervisor to build the transitive trust chain and TVEM ensuring trust from the TVEM manager of the hardware trust platform TVEM is rooted (Krautheim *et al*.,2010);

Mutual Trust Based Access Control (MTBAC)

Mutual Trust Based Access Control (MTBAC) is also known as trust model which not only considers user's performance trust and make sure that cloud server from user's access request poses no malicious threat, and also takes cloud service node's authority into account. To established a mutual trust mechanism by trust dealings between users and cloud service nodes and only trusted users have access to the Cloud, and simultaneously users can select the most credible cloud service nodes (Guoyuan *et al*.,2014); The physical structure of MTBAC consists of users, Authentication and Authorization Center (AAC), cloud service nodes, user's behavior trust database and cloud service node's trust database. User represents individuals or organization who appeals access to cloud services or resources. A cloud services node are entities that provide services or resources to users in cloud computing platform. User's behavior trust database and cloud service node's trust database store interact history, behavior information, trust values, cloud service nodes and user trust models correspondingly. According to user's behavior in user's trust database, AAC will detect user's behavior in the primary place in order to prove user's identical legitimacy, behavior trustworthy and then sort nodes according to trust levels and recommend the finest service node for the user. AAC verifies user's legitimacy primarily include which identity legitimacy and behavior trust. AAC ensures that only when user's trust degree is higher than the trust threshold, user's access request can be accepted by cloud server. Afterwards, the majority appropriate cloud node will be selected to provide services according to user's request and node's credibility (Guoyuan *et al*.,2014); The access control policy of MTBAC can not only guarantee that access request of users could get response, but also ensure that all cloud service nodes can't be attacked or illegally occupied by malicious users.

Grid and Cloud Trust Model

This trust model named Grid and Cloud Trust Model which is a trust model CARE resource broker are integrated (Manuel *et al*.,2009 and Apologic, 2015); Both cloud systems and grid are supported for the proposed trust model. The resource broker has been implemented with Kerberos Based Authentication

Module and PERMIS Role Based Authorization Module to improve the security measure of the broker compared to the conventional security mechanism incorporated in it. Network substantiation protocols are Kerberos. A non-secure network belongs to permit nodes communicate to establish their characteristics to one another in a secure approach. A client-server model aimed firstly in Kerberos, and it gives mutual substantiation between the server and the user to verify all other identity. Policy controlled role of PERMIS based on the authorization system that uses digitally signed X.509 attribute certificates or Kerberos tickets to hold user's roles / attributes. The PERMIS based authorization makes the decision for the user's access to be granted or without based on the policy for the target domain (Manuel *et al*.,2009);

Hierarchical Attribute Set Based Encryption (HASBE)

This trust model named Hierarchical Attribute Set Based Encryption (HASBE) (Wan *et al*.,2011); which is an undeniable access control conspire for cloud computing. A delegation algorithm to ASBE is applying a hierarchical structure of system users are effortlessly incorporates in the HASBE method. HASBE due to flexible characteristic set combinations are not only supports compound attributes, efficient user revocation are also achieves because of various value attributes assignments (Wan *et al*.,2011); A system user is the hierarchical structure. HASBE representation consists of a numerous users, trusted authority, and multiple domain authorities' consequent to data consumers and data owners. The trusted ability is dependable for distributing system and generating system parameters and the top-level domain establishment are approved as well as root master keys. After that level or users in its domain subordinate, domain authorities are delegating keys for responsible domain authority. The user's decryption keys are associated attributes specifically key structures are assigned on the each user system (Wan *et al*.,2011);

Trusted Platform Software Stack (TSS)

Trusted Platform Software Stack (TSS) is also known as trust model to evaluate the security and dependability of cloud computing integrating the cloud computing system to the Trusted Computing Platform (TCP). In cloud computing environment TCP has been used in integrity, confidentiality and authentication (Shen *et al*.,2010); (Shen and Tong,2010);

Improved Trusted Cloud Computing Platform (Improved TCCP)

Improved Trusted Cloud Computing Platform (Improved TCCP) Model is also known as trust model which is used Privacy CA and scheme Direct Anonymous Attestation (DAA) to evaluate the anonymity and availability of the TC1'CP model. This model ensures the confidentially and the integrity of a CC's VM, and is able to solve the dependence issue on the Trusted Coordinator (TC) (Zhang and Sheng,2010);

Security and Trust Management Mechanism

Many organizations including government and private sectors employ cloud computing technology to satisfy the demands of data storage, computing, and maintenance. Security is a significant concern for those organizations, apart from the advantages of cloud computing. Trust is a vital component in cloud computing to assure security to the services being delivered to the clients. The lack of trust and security in cloud computing limits the cloud usage among the users. The cloud services are offered through virtual machines available in the Internet, which makes it possible to be accessed by multiple users at the same time. The multi-agent access reduces the cost, but increases the risks and vulnerabilities to resources in the cloud. As the services are hosted on the datacenter space of the third party service providers, it is impossible for the data owner to have direct control over the data.There are a lot of methods proposedby researchers to help the consumers identify the cloud service provider who seems to be more reliable. These trust-aided unified evaluation framework help in measuring the trustworthiness of cloud service providers.

SUMMARY

The cloud computing is the state of art technology for sharing the computational or storage resources among several users. It uses the information technology as a service over the network and provides the trust mechanisms for end users with strong computational capability and huge memory space at a low cost. In this paper, various papers regarding cloud computing, its security mechanisms and trust mechanisms are surveyed. The existing papers regarding trust and recommendations have many drawbacks with respect to trust and security. In order to overcome the drawbacks of the existing systems, a Trusted Cloud Certifying Authority approach to ensure security in cloud computing use encryption and key management technologies are important technologies that can help secure applications and data in cloud to establish trust between CCs and CSPs.

Proposed Work

The Cloud Trust Authority will seek data input from the above listed authoritative sources (at present restricted to India) on a regular basis, run the algorithm and arrive at the Trust scope for the Cloud Service Provider as well as the Consumers. The Trust Score

Table.1. Information about Various Trust Mechanisms in Cloud Platform

S. No.	Name of the Authors	Technology used	Purpose	Merits and Demerits
1.	Lin *et al.,* (2014)	A Mutual Trust based Access Control (MTBAC) model	To provide access control in the cloud environment	**MERITS** 1.Efficient security 2.Reliability **DEMERITS** Lack of Privacy 1.Transferability 2.Heterogeneity
2	Noor *et al*., (2015)	Trust as a Service (TaaS)	For the design and implementation of Cloud Armor	**MERITS** 1. Availability 2.Credibility **DEMERITS** 1.Although credibility model is present, there are chances of Sybil attack and collision attack occurring. 2.Needs improvement in trust accuracy
3	Wang *et al*., (2015)	A lightweight reputation measurement approach	To solve the trust evaluation of cloud services	**MERITS** 1.Cost-efficient opportunities for enterprises by offering a variety of dynamic, scalable and shared services. **DEMERITS** 1.Need to address the demand of high reputation cloud services, when mass unstable feedback ratings exist 2.Dynamic computation is required
4	Li *et al.,* (2012)	Trust Multi-Dimensional Vector	For representing the credibility of providers and also apply the fuzzy comprehensive evaluation method to classify the services	**MERITS** 1. High trust accuracy. 2. Fast and safe trust relationship among the customer and the provider. **DEMERITS** To extend the exchange of reputation to the case where contracts are not homogeneous. 2.That is, not all agents observe the same contract dimensions.
5	Banyaljain and jain (2014)	Access Control Framework	To address the security and privacy issues for the cloud	**MERITS** 1.Multi-layer security standard 2.High user friendly **DEMERITS** 1. Reusability is not mentioned 2. Based on the security issue the performance may vary.
6	Banirostam *et al.*, (2013)	User Trusted Entity (UTE)	To make the cloud computing infrastructures reliable for ordering developers to provide closed execution environment	**MERITS** 1.It protects the confidentiality and integrity of the information exchanged between a Trusted Application and the user **DEMERITS** 1.Privacy regulation complaint

7	Shaikh &SasiKumar (2015)	Cloud Service Alliance (CSA)	To access the security of a service and validity of the model	**MERITS** 1.Protection against DDoS 2.Data security 3.Flexibility **DEMERITS** 1. Authentication factors may vary 2. Less data protection schemes are provided.
8	Sidhu & Singh (2014)	Trust model	Cloud users select the most reliable service providers and services.	**MERITS** Robust, Scalable and flexible. **DEMERITS** The Trust can be expensive to establish and maintain
9	Tang & Sadhu (2013)	The formal Cross Tenant Trust Model (CTTM)	To increase the need of tenants	**MERITS** 1.To increase the need of tenants **DEMERITS** 1. Cannot support the agility of cross-tenant access needs 2. Maintenance of cryptographic credentials is very costly in cloud settings
10	Marudhadevi *et al*., (2014)	Trust Mining Model (TMM)	For identifying trusted cloudservices and negotiating the SLA	**MERITS** Data Integrity, Data Access 2. Availability **DEMERITS** Transparency leads lack of trust.
11	Pavlidis *et al*., (2013)	Trust and control concepts	For the selection of appropriate cloud provider on the basis of security and privacy requirements	**MERITS** Data Non Editable by Cloud Provider, Data Non Readable at Cloud Provider. **DEMERITS** Broken authentication & session management, insecure direct object references, cross-site request forgery, security missed configuration.
12	Qu &Buyya (2014)	Fuzzy Quality of Service (QoS) requirements and services	Evaluation of trust in clouds	**MERITS** Improves cost- efficiency and service stability **DEMERITS** Needs improvement in trust evaluation based selection phases; otherwise, it degrades the performance in selection phase.
13	Gonzales *et al*., (2015)	Cloud architecture reference model	To assess the level of security of the multi- tenant IaaS cloud architecture	**MERITS** Improved manageability and less maintenance **DEMERITS** Rapidly adjust resources to meet fluctuating

will be published by the Cloud Trust Authority which can be accessed by either the Cloud Service Provider or the Consumer.The Cloud Service Provider can also be a consumer for some of its requirements.

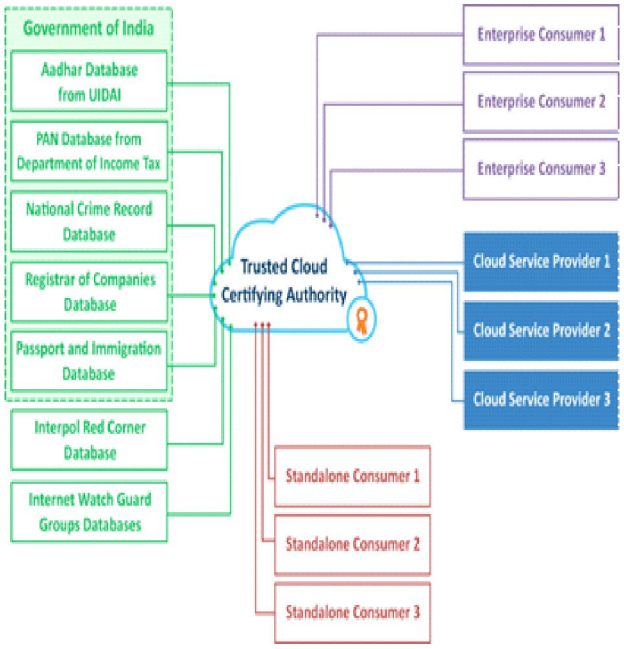

Fig.1. Proposed Trust Model

The Figure - 1 indicates as to how the architecture for the proposed model will work like

The following will be the methodology in which Survey implementedThe second rating will be based on the effectiveness of the implementationThe third rating will be based on sustenance of implementation and effectiveness and the time period which is year on year or on agreed periodicity.The fourth rating will be any security breach or security incidents reported by the CSP or reported by the external parties including regulators.For all positives, the scoring will be on positive scale and for any negatives transactions the rating will undergo a negative adjustment. So, the net off score at any given point in time will be the score of the CSP. This scoring will be dynamic and will be managed by the TCCA

Also TCCA will publish the scoring in its website which can be accessed by either consumers or the cloud service providers at any point in time.The TCCA will be calculating the Trust score on a real time basis without recreating a duplicate data base of its source data. At any point in time, the TCCA will not store any data TCCA will be running only the Algorithm and publishes the score real time using its front-end server accessible by authorised cloud service providers or consumers.

CONCLUSION

In this paper, an overview of various trust based mechanisms in cloud computing platform is presented. Generally, cloud services are less trusted services due to their dynamic nature. The existing trust evaluation schemes lacks in security and privacy in cloud computing environment. From the survey authentication based trust models use encryption and key management technologies are important technologies that can help secure applications and data in cloud to establish trust between CCs and CSPs. This category includes trust models that ensure the availability, integrity and confidentiality of data on cloud by using certificates from standardized body, trust tickets, private and public keys, TPM endorsement keys and etc. Thus the data can be securely shared with the authorized users by adopting the cryptographic techniques.

REFERENCES

Applogic, T. 2015. 3tera'sCloud Computing SLA goeslive Internet:http://blog.3tera.com/computing/175/, 2015.

Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang.2011. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments, Advanced in Control Engineering and Information Science, Procedia Engineering 15, P. 2852-2856. https://doi.org/10.1016/j.proeng.2011.08.537

Dustin Amberihein, K.L. 2009. Cloud computing use cases white paper," Cloud Computing Use Cases Discussion Group.

Guoyuan, L., Danru, W., Yuyu, B. and Min, L. 2014. MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing China Communications, vol. 11, no. 4, P. 154-162, April 2014. https://doi.org/10.1109/CC.2014.6827577

Haq, I.U., Brandic, I. and Schikuta, E. 2010. Sla validation in layered cloud infrastructures in Economics of Grids, Clouds, Systems and Services, Springer-Verlag, Berlin, Heidelberg, 2010, Vol. 6296, P.153–164. https://doi.org/10.1007/978-3-642-15681-6_12

Kai, Hwang. and Deyi Li. 2010. Trusted Cloud Computing with Secure Resources and Data Coloring, IEEE Internet Computing. https://doi.org/10.1109/MIC.2010.86

Kanwal, A., Masood, R., Ghazia, U.E., Shibli, M. A. and Abbasi, A.G. 2013. Assessment Criteria for Trust Models in Cloud Computing,in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom),IEEE International Conference on and IEEE Cyber, Physical and Social Computing, P. 254-261. https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.61

Krautheim, F.J., Phatak, D.S. and Sherman, A.T. 2010.Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing, in TRUST'10 Proceedings of the

3rd international conference on Trust and trustworthy computing, P. 211-227.
https://doi.org/10.1007/978-3-642-13869-0_14

Manuel, P.D., Selve, T., Ibrahim and Barr, A.2009. Trust management system for grid and cloud resources," in First International Conference on Advanced Computing (ICAC 2009), 2009, P. 176-181.
https://doi.org/10.1109/ICADVC.2009.5378187

MaryamRoodaki. 2016. A survey on Trust Management in cloud computing March.

Pearson, S. and Benameur, A. 2010. Privacy, security and trust issues arising from cloud computing. In Cloud Computing Technology and Science (Cloud- Com), IEEE Second International Conference on, P.693–702. IEEE.
https://doi.org/10.1109/CloudCom.2010.66

Shen, Z. and Tong, Q.2010. The security of cloud computing system enabled by trusted computing technology," in 2nd International Conference on Signal Processing Systems (ICSPS), P.. 11-15.
https://doi.org/10.1109/ICSPS.2010.5555234

Shen, Z., Li, Yan F. and Wu, X. 2010. Cloud Computing System Based on Trusted Computing Platform," in International Conference on Intelligent Computation Technology and Automation (ICICTA), P. 942 - 945.
https://doi.org/10.1109/ICICTA.2010.724

Wan, Z., Liu J. and Deng, R.H. 2011. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing, Information Forensics andSecurity, IEEE Transactions, vol. 7, no. 2, P. 743-754.
https://doi.org/10.1109/TIFS.2011.2172209

Wang, S.X., Zhang, L., Wang, S. and Qiu, X. 2013. A cloud-based trust model for evaluating quality of web services."Journal of computer science and technology, vol. 25, pp. 1130–1142.
https://doi.org/10.1007/s11390-010-9394-1

Wang,Y. and Singh, M.P., 2010. Evidence- based trust: A mathematical model geared for multiagent systems, ACM Transactions on Autonomous and Adaptive Systems (TAAS).
https://doi.org/10.1145/1867713.1867715

Zhang, W.H. and Sheng, H.L. 2010. An improved trusted cloud computing platform model based on DAA and Privacy CA scheme," in 2010 International Conference on Computer Application and System Modeling (ICCASM 2010),P. V13-33-V13-3