Trust Models for Cloud Applications and Identity Access Management - Review of Challenges and Opportunities

M. Kiruthika[1], M.S. Saravanan[2]
[1] Research Scholar, CSE Department, Saveetha School of Engineering Chennai
[2] Professor, CSE Department, Saveetha School of Engineering, Chennai
.

Article Info
Volume 83
Page Number: 6365 - 6374
Publication Issue:
May- June 2020

Abstract:
In recent years, many organizations as well as individuals have made it a common practice to use different service providers to maintain their accounts and access various range of services for different purposes. The service can be Grid, Cloud or Mobile. IAM with sophisticated Identity management systems can provide central administration, self-services, user management, role-based access controls for and using multiple technologies. IAM ensures that human or software agents get properly authenticated and authorized while accessing the cloud or grid network through multiple technologies or web services. Successful IAM can increase the Usability, Availability, Accuracy, Relevance and Cost Effectiveness. If the attributes to the identities are not verified accurately, then the users and usage become vulnerable which may result in either data or financial loss. In some cases, the reputation of the organizations can be greatly affected if there is no IAM or proper security management is in place. Therefore, it is important to realize the gaps with the valuation of the trust models, policies, frameworks and associated service providers, to arrive at proper improvements and recommendations. This paper provides a comprehensive comparative analysis for various trust models, frameworks and related tools. Based on the extended literature reviews and recommendations, this article also provides future directions for improving the effectiveness of the trust models and the related policies using multi-dimensional and multi-variate factor analysis.

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *18 May 2020*

Keywords*: Evaluation, Metrics, Trust Models, IAM, Identity, Access, Management, Effectiveness, Availability, Usability, Relevance, Accuracy, Cost, Effectiveness, Multi-Dimensional Security Demand, Trust Index,, CIA, IAAA,, CIA_IAAA_CER*

Introduction:

The important constituents of verification and trust relationship has compliance management, security procedures/processes for data management, access control and events managements. The three categories that comprise the cloud security principles are identity, information and infrastructure. There are several aspects to data security and it can be dealt like “data in transit”, “data at rest, “data processing”, “data lineage”, “data extraction and “data continuance”. One of such principal security models we will be looking at today that is dedicated to keeping the integrity of information is the Biba integrity model. Usually Trusted computing system includes the mixture of controls, hardware and software for ensuring security as well data integrity. The Security Perimeter acts in between the Trusted Computing Base and the other related systems. The security parameter establishes a secure trusted path between the source and the object. Trust can be defined as a firm belief which is considered as competence of an entity that should behave as expected.

It is also dynamic and mostly associated with the entity and usually applies to a specific context for a point in time. The value of trust can be either continuous or dynamic, usually in the range of 0 and 1. The value 1 indicates very trustworthy and the value 0 indicates very untrustworthy. It is usually built on the past experience and varies based on the context. The value associated with trust may vary based on different contexts or environments. Reputation is usually built on the behavior of the entities which is usually retrieved using past performance and observations.

IAM provides the right mechanisms for authenticating users based on the privileges the user has. Using IAM users can get successful authentication only for resources they have been granted access as it it predominantly deals with role-based access to services. The entities correspond to identities which in turn correspond to Attributes. Based on these attributes access can be granted. The mobile applications like OneLogin allow IAM for mobile devices where they have to login one time from the device for authentication. The Identity providers such as Directories are used to match the user's identity. Single Sign On (SSO) is one of the most popular authentication mechanism which uses authentication server and enables cookies stored in the users client machine. Depending upon this cookie the session for the user is authenticated and continued. If the token is expired, the session gets terminated.[1, 31].

One of the major challenges of Cloud Computing is the procedures and technologies for establishing trust between the consumers and service providers of the cloud. There are various trust models with different parameters which could make selecting the right trust model for a Cloud Consumer quite challenging [1].

IAM relates to providing an Identity to the user who is wanting to access a particular system and once on granting entry next step would be to decide on the Applications, Physical Devices and Databases that can accessed by the Individual. The IAM takes care of the CIA Traid – Confidentiality, Integrity and Availability which is the most three key things for an Information asset that belongs any Organization.

I-A-M works on the concept of I-A-A-A(**I**dentification, **A**uthorization, **A**ccess control and **A**vailability). IAM also solves the issue of various system ids for different systems; it works on the concept of one Single Digital id per customer that can be used across trusted systems. This solves a lot of the System administration overheads with regards to maintenance of several users across systems. IAM is critical to the success of any IT Security Governance plans and it also helps a company to stay complaint with SOX and other country specific data security acts. Compliance with regards to Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA and The General Data Protection Regulation (GDPR) (EU Regulation).

IAM plays a major role in Cyber Security preventing system compromise based on Social Engineering, Back Door Trojan or Ransomware Attacks. Some of the benefits of Identity Access management not limiting to the below include providing Internal system access to external partners such as Vendors, Suppliers, Contractors, and Internal users on the Cloud using SaaS applications. IAM management today would typically involve 2 or 3 multifactor Authentication to safe guard the CIA traid and protect the company's Information Asset using what you have, what you know and what you are. These three questions combines the Login Id, Password, a Smart card and a biometric (Face, Retina or Finger Print) multifactor Authentication process to avoid illegal access to outsiders or Cyber Criminals.

IAM aims to improve regulatory compliance management and operational efficiency as well as enabling organizations to obtain access control and operational security. Organizations which employees or uses SaaS service, PaaS or IaaS from cloud may allow end users to access storage in a cloud or application residing in any virtualized platform. So, there exists a need to adopt IAM.

IAM process has the following best practices which are followed for proper implementation.

- ✓ Authentication, Authorization & Access Management
- ✓ User & Data Management
- ✓ Provisioning, Monitoring & Auditing
- ✓ Management of Attributes, Credentials & Entitles
- ✓ Management of Compliance and Association or Alliance
- ✓ Centralized management of authorization and authentication

Enterprise-IAM requires Provisioning of cloud service accounts to users, services for integration, SSO, support as well as user activity monitoring and other mechanisms to support regulatory policies.

I. FACTORS AND METRICS

Measurability, independency, accountability and precision are the main characteristics of a useful metric. Wherever possible, the IAM measures should be the same as or related to existing measures in the organization that monitor the success of security. The basic IAMS can have multiple primary and supporting factors. The factor is usually a controlled variable which is independent and its level is set during the measurement or evaluation. It is also a category or type of evaluation which can be useful to assess the effectiveness of the trust models, frameworks and supporting technologies.

When choosing or defining IAM performance metric, the most important characteristic to consider is whether it indicates if trust is maintained, relevance and services are cost effective apart from other non-functional requirements. Initially, the resource site is demanded by a user job for providing security assistance which is usually denoted as Security Demand (SD). Users usually care about certain typical attributes when determining the security demand. The attributes & associated values may change dynamically which primarily depend on the things like Security Policies, Trust Model, Self Defense Capabilities, History of attacks, vulnerabilities to the sites. The major issues related to trust in cloud, grid and mobile applications discussed by most of the authors are the following:

- Authentic Identification Of both users and providers and evaluation of Credibility
- Protection of integrity of trust management data
- Privacy policies for preventing the accidental leakage of user personal data
- Personalization to have a control over all aspects of trust feedback system
- Integration for the ability to use multiple trust systems together
- Security mechanisms for Protection against attacks and malicious users
- Scalability to increase the number of users, tools services and authentication mechanisms

The process of data encoding named encryption is usually required to avoid any sort of undesirable changes at the Cloud by any unauthorized and malicious [16, 17]. Certification is The process of confirming is usually referred as certification which deals with behavior, property or characteristic of a cloud entities through a proper agencies or authorities for accreditation [18, 19]. The agreement with negotiations recorded as SLA between cloud service provider and consumer, which usually contain multiple performance measures [20]. Data Availability is usually relates to continuous accessibility of the required data at required levels irrespective of time and situations. The situation can be normal or disaster, but the service and servers should be available for the users to consume the services [21]. Data replication is the process of copying and sharing information at various distributed locations to ensure data availability [22].

Trust models performance can be measured using parameters to ensure accepted level of response irrespective of the situations and could also include detection of malicions behavior. The QoS parameters can be used to define the levels of performance and transparency. It is measured and analyzed with respect to two different parameters that mainly include the detection of malicious behavior in the Cloud and QoS transparency offered by the service provider to its customers [23, 13].

A trust model that provides QoS transparency gives an in-depth analysis of the Cloud services. The QoS attributes can be evaluated by directly measuring different attributes like the response time, throughput and network bandwidth provided to the customers [24].

A trust model capable of detecting most of the malicious entities in the Cloud environment is more reliable for the customers and is considered to have better performance [25, 26].

Data ownership and process execution control are the crucial assessment features for this category. Trust models provide data ownership by defining the capability lists for various users accessing the data stored on the Cloud [27].

II.REVIEW OF MODELS AND FRAMEWORKS

The authors reviewed different many trust models through a comprehensive study on the available cloud Trust models. The analysis and association from Functional and Non-Functional parameters associated with each of the Trust Model is very much required for effective comparison. They have provided Taxonomies highlighting the features that can be used for evaluating the trust parameters. They have also applied the proposed Taxonomy as a case study for Health Information System [1].

Negotiation of data security and quality of service (QoS) parameters are required and can be given through service level agreements (SLAs) [2, 3]. Multiple definitions are given for trust and associated terms in the literature review [4]. The importance of Trust model is to provide the main feature or requirement as essential core functionality and non-functional features should include security, QoS and performance requirements, which are worth considering for each trust model [5].

There are four key areas addressed in the standard IAM framework, which are Authentication, Authorization, Users Management and Central Repository for Users. IAM framework areas are listed below:

1. Authentication
   a. SSO (Single Sign on)
   b. Session Management process
   c. Strong Authenticated Password Service
2. Authorization
   a. Role based
   b. Department based
   c. Rule based
   d. Authorization for Remote Access
3. Management of Users
   a. User Management
   b. Role Management
   c. Password Management
   d. Self Service
4. User Repository based Centrally
   a. Meta Data
   b. Virtual User Directory
   c. Synchronization of Data

The popular and mostly used security models for IAM are the following:

- ✓ Brewer Nash model / China wall
- ✓ Biba model
- ✓ Bell-Lapadula model
- ✓ Clark Wilson model
- ✓ Graham-Denning model
- ✓ Sutherland model

Reference Monitor which is a part of the Transaction Computing base and oversees making sure that it enforces the access controls on the system resources. The main role of the reference monitor is to make sure that every requesting subject credential matches the object access requirements before any requests are allowed to proceed.

The State Machine model bases most of the Security models. In the State Machine model, at a specific time, a shot of the system is taken and if all features of the system meets the required security policy, the system transition is allowed resulting in a new system. Once the system enters the Secured state then it maintains this across all system transitions and only allows subjects to access resources adhering to the said Security policy in a secure manner.

Bell-LaPadula and Biba models are Information flow models that are based on the prevention of information flow from higher security level to a lower security level, these models deal with direction of the information flow and also the type of information flow. Bell-LaPadula model is a multilevel security policy and using which the resources at or below its security clearance level can be accessed by users. Access for higher clearance level is granted only to specific work task. Bell-LaPadula model handles security and integrity of classified information by blocking lower-classified subjects from accessing higher-classified objects. Bell-LaPadula does not address the availability and integrity of objects. Bell-LaPadula is the first mathematical model of a multilevel security policy and built on a state machine concept and the information flow model. It also employs mandatory access controls and the lattice concept.

The following are the three basic properties of state machine model:

- The Simple Security Property (no read up) - Subject may not read information at a higher sensitivity level.
- The Star Security Property / Confinement Property (no write down) - Subject may not write information to an object at a lower Sensitivity level.
- The Discretionary Security Property - Discretionary access controls are enforced using access matrix.

The Bell La-Padula model had its flaws such as not being able to deal with the integrity of data. A lower level subject could write to a higher classified object as seen above and has always been possible. Because of this the Biba model was created which has deep roots of Bell La-Padula model. Biba created a model made sure integrity is enforced in a computer system. A group of integrity policies were proposed that can be used with different conditions to ensure information integrity. Biba model uses both discretionary and nondiscretionary policies. The Biba model has two types of policies, mandatory and discretionary. Within these two there are a number of policies based on the security needs. The following has the details of these two types:

Mandatory Policies:
1. Strict Integrity Policy
2. Low-Water-Mark Policy for Subjects
3. Low-Water-Mark Policy for Objects
4. Low-Water-Mark Integrity Audit Policy
5. Ring Policy
Discretionary Policies:
1. Access Control Lists
2. Object Hierarchy
3. Ring

Biba model consists of family policies with strict integrity policy which are too strict to meet the flexibility of the system. The low-water-mark policy enhances its flexibility by allowing the “read down.” Operation The monotonous decline of the subject tags reduces its practical and system life cycle which lower the availability of system. There are three major challenges when try to establish trust among grid sites.

The first one is integration with existing tools technologies and systems. The second challenge is interoperability with different hosting environments. The third challenge relies in the construction of trust relationships among multiple hosting environment or services. There are two types of trust models are often used in grid, one is the PKI based model and another one is reputation based model. The general trust model used in grid system is given in Figure 1. There are multiple techniques can be considered for trust management. Some may consider policy as a trust management technique, some many use recommendation as trust management technique, a few consider reputation as a trust management technique and others consider prediction as trust management technique.

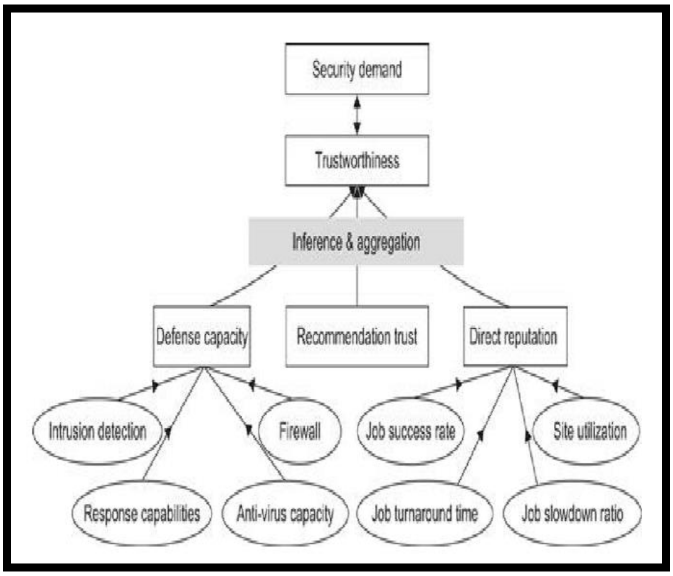

Fig. 1. General Trust Model

There are many trust models which were applied and adopted for grid and cloud environment. Network Sniffing, Out Of Control Access, Faulty and Malicious Operations are some of the issues might occur in distributed systems if there are no trust models followed. Trust Models can be viewed from Service Providers perspective as well as Service Requestors or Consumers perspective which are shown in Figure 2 and Figure 3. Various trust models for Cloud is given in Figure 4.

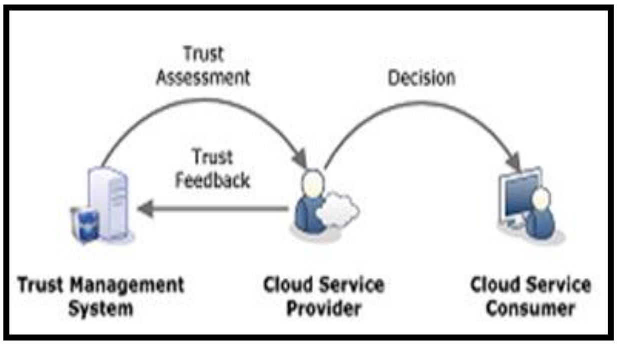

Fig. 2. Trust Model From Service Providers' View

Fig. 3.

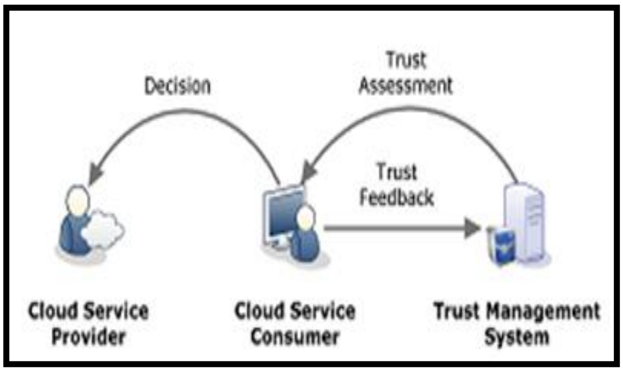

Fig. 4. Trust Model From Service Consumers' View

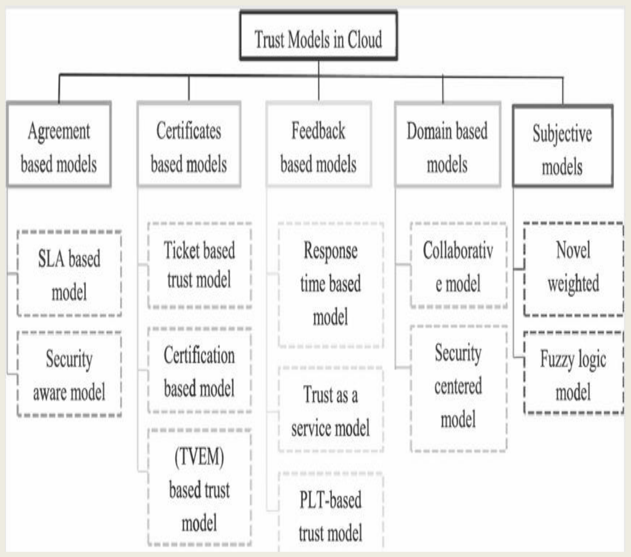

Fig. 5. Trust Models in Cloud

Figure 5 has the typical model framework for trust management. This framework has three major layers which are described in the below section.

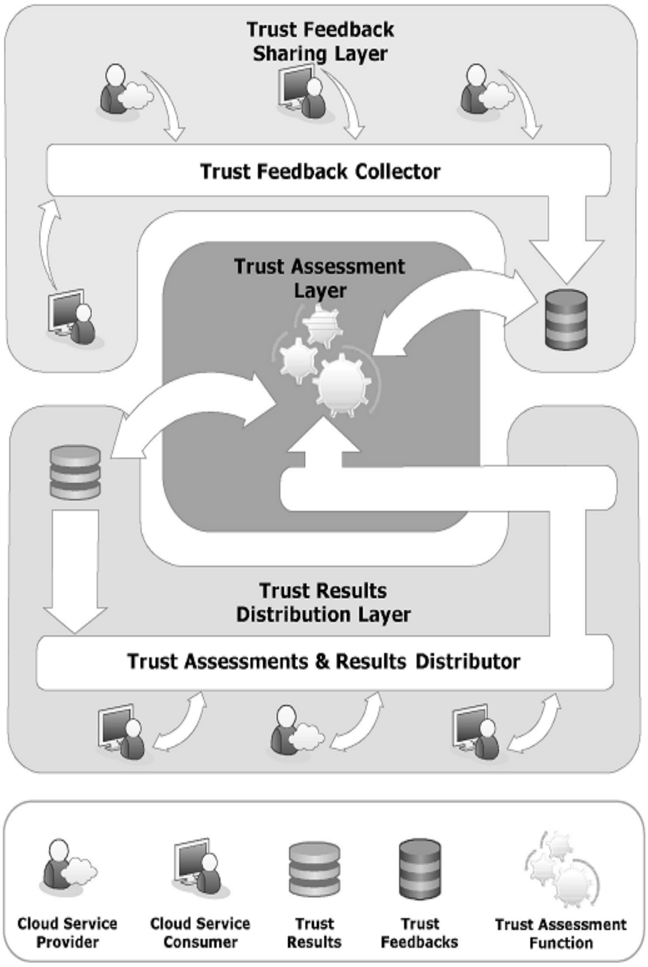
Trust Feedback Sharing Layer
Trust Feedback Collector
Trust Assessment Layer
Trust Results Distribution Layer
Trust Assessments & Results Distributor
Cloud Service Provider
Cloud Service Consumer
Trust Results
Trust Feedbacks
Trust Assessment Function

Fig. 6. Trust Management Framework

Fig. 7.

Fig. 8. Trust Feedback Sharing Layer has three layers namely Credibility, Trust Assessment and Trust Results Distribution Layer. The credibility layer address the following:

- The quality of the information or service that makes people trust the cloud
- The credibility of the cloud as well as that of the feedback
- Privacy
- The degree of potential information exposure that users of the cloud could face when interacting with the cloud
- Personalization
- The degree to which people adhere to the trust management rules
- Users selecting their preferred feedback mechanism
- Integration
- Ability to integrate other trust management principles

Fig. 9.

Fig. 10. The Trust Assessment Layer has the following

- From whose perspective is trust determined? User or provider?
- Technique
- The flexibility of a technique to being adopted
- Adaptability
- Responsiveness of the system to changes from requesting parties
- Security
- Degree of robustness to operate in the face of attack and malicious behaviour
- Scalability
- Amount the system can be scaled
- Applicability
- How useful the system is for cloud trust

Fig. 11.

Fig. 12. The Trust Results Distribution Layer has the following

- Response time
- How long it takes trust system to respond to request
- Redundancy
- How much redundancy is used to handle load
- Accuracy
- The degree of correctness of trust results
- Security
- Protection of trust results have from being tampered with

Cloud Computing has a few trust models. The Cloud Consumer is not sure on which of these models would suit his Business requirements and CIA Triad requirements. This paper enlists the different parameters that can be analyzed to arrive at the correct Trust model to suite the IT Security Governance Policy. Some of the trust models have both Functional features as well as Non-Functional features. The Functional features and non-functional features for the below mentioned Trust models are selected and listed in this paper which will form a set of parameters to be used by the Cloud Consumers to do an evaluation on the exact trust model to choose that will fit their Business needs and IT Security Governance policies. The users will rank or choose the parameters and at the end the proposed system will give them the correct trust model to suit their needs.

The contract parameters monitoring module exchanges the agreement with the consumer for establishment of trust between both entities [6, 7]. So there exists a gaps in the agreement based trust models. Inter domain trust value is a comprehensive value based on direct and recommended trust values from other domains [8, 9]. Domain based trust models do provide competitive advantages when compared with other trust models when it is applied for the specific domain [10].

As part of taxonomy for functional features, various techniques have been proposed in the literature to classify and identify these features for a system, which can be used for categorization of functional features of trust models [11, 12].
Non-functional features of trust model is dependent upon the scope and context of various applications and the services offered and consumed [13, 14, 15].

Trust model based on QoS named as Turnaround_Trust with certain standards can be used to build trust more reliable for Grid or Cloud with other methods as QoS can be defined and customized based on the needs. All the performance measures were better with Trust Model based on QoS when compared with other models like FIFO and QoS Trust models. This can be adopted for IAM and can be customized based on the domain needs. [28].

Multi-tenant trusted computing environment model was designed primarily for the Infrastructure as Service for securing reliable infrastructure for the users [29]. The presence of the critical factors like Confidentiality, Availability, location and protection of data can improve the trust levels with the consumers or users [30].

CONCLUSION

This paper provided the basic details of IAM and Trust MODELS. Secondly this paper also describes the gaps in the existing research works related to trust models for IAM and provides future directions and avenues for building hybrid and comprehensive framework with supporting metrics. There exists a need for developing a comprehensive trust model and supporting algorithm to ensure three parameters Effectiveness, Cost and Relevance. The future directions should focus on multi-dimensional trust model which also supports evaluation to see the cost effectiveness and relevance for the specific domain where the trust model is applied.

REFERENCES

1. Ayesha Kanwal, Rahat Massod,Awasis Shibili, Rafia Mumtaz (2014), Taxonomy for Trust Models in Cloud Computing, The Computer Journal, March 2014
2. Abawajy, J. (2011) Establishing Trust in Hybrid Cloud Computing Environments. 10th Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), Australia, November 16–18, pp. 118–125. IEEE, New York,USA.
3. Habib, S.M., Hauke, S., Ries, S. and Mühlhäuser, M. (2012) Trust as a facilitator in cloud computing: a survey. J. Cloud Computing, 1, 1–18.
4. Rimal, B.P., Choi, E. and Lumb, I. (2009) A Taxonomy and Survey of Cloud Computing Systems. 5th Int. Joint Conf. INC, IMS and IDC, NCM'09, Korea, August 25–27, pp. 44–51. IEEE, New York, USA.
5. Sommerville, I. (2007) Software Engineering. John Wiley & Sons, Scotland.
6. Alhamad, M., Dillon, T. and Chang, E. (2010) SLA-Based Trust Model for Cloud Computing. 13th Int. Conf. Network-Based Information Systems (NBiS), Takayama, Japan, September

14–16, pp. 321–324. IEEE Computer Society, Los Vaqueros.

7. Sato, H., Kanai, A. and Tanimoto, S. (2010) A Cloud Trust Model in a Security Aware Cloud. 10th IEEE Int. Symp. Applications and the Internet (SAINT), Korea, July 19–23, pp. 121–124. IEEE, New York, USA.
8. Yang, Z., Qiao, L., Liu, C., Yang, C. and Wan, G. (2010) A Collaborative Trust Model of Firewall-Through Based on Cloud Computing. 14th Int. Conf. Computer Supported Cooperative Work in Design (CSCWD), China, April 14–16, pp. 329–334. IEEE, New York, USA.
9. Li, W. and Ping, L. (2009) Trust Model to Enhance Security and Interoperability of Cloud Environment. 1st Int. Conf. Cloud Computing (CloudCom), China, December 1–4, pp. 69–79. Springer, Berlin.
10. Krautheim, F.J. (2009) Private Virtual Infrastructure for Cloud Computing. Int. Conf. Hot Topics in Cloud Computing, USA, June 14–19, pp. 5–5. USENIX Association, California, USA.
11. Kotonya, G. and Sommerville, I. (1992) Viewpoints for requirements definition. Softw. Eng. J., 7, 375–387.
12. Darke, P. and Shanks, G. (1997) User viewpoint modelling: understanding and representing user viewpoints during requirements definition. Inf. Syst. J., 7, 213–219.
13. Kim, H., Lee, H., Kim, W. and Kim, Y. (2010) A trust evaluation model for QoS guarantee in cloud systems. Int. J. Grid Distrib. Comput., 3, 1–10.
14. Krautheim, F.J. (2009) Private Virtual Infrastructure for Cloud Computing. Int. Conf. Hot Topics in Cloud Computing, USA, June 14–19, pp. 5–5. USENIX Association, California, USA.
15. Xiong, L. and Liu, L. (2004) Peertrust: supporting reputation based trust for peer-to-peer electronic communities. IEEE Trans. Knowl. Data Eng., 16, 843–857.
16. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.,Konwinski, A. and Lee, G. (2010) A view of cloud computing. Commun. ACM, 53, 50–58.
17. Kaufman, L.M. (2009) Data security in the world of cloud computing. Secur. Priv., IEEE, 7, 61–64.
18. Ahmed, M. and Xiang, Y. (2011) Trust Ticket Deployment: A Notion of a Data Owners’ Trust in Cloud Computing. 10th Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), China, November 16–18, pp. 111–117. IEEE.
19. Bezzi, M., Kaluvuri, S.P. and Sabetta, A. (2011) Ensuring Trust in Service Consumption through Security Certification. Proc. Int. Workshop on Quality Assurance for Service-Based Applications, Switzerland, September 14, pp. 40–43. ACM.
20. Alhamad, M., Dillon, T. and Chang, E. (2010) Conceptual SLA Framework for Cloud Computing. 4th IEEE Int. Conf. Digital Ecosystems and Technologies (DEST), Dubai, April 13–16, pp. 606–610. IEEE, New York, USA.
21. Sengupta, S., Kaulgud, V. and Sharma, V.S. (2011) Cloud Computing Security-Trends and Research Directions. IEEE World Congress on Services (SERVICES), Washington, DC, July 4–9, pp. 524–531. IEEE, New York, USA.
22. Park, N. (2011) Secure Data Access Control Scheme Using Type-Based Re-Encryption in Cloud Environment. In Radosaw, K. (ed.), Semantic Methods for Knowledge Management and Communication. Springer, Berlin.
23. Sharma, Deepak & Dhote, Chandrashekhar & M. Potey, Manish. (2016). Identity and Access Management as Security-as-a-Service from Clouds. Procedia Computer Science. 79. 170-174. 10.1016/j.procs.2016.03.117.
24. Schad, J., Dittrich, J. and Quiané-Ruiz, J.-A. (2010) Runtime measurements in the cloud: observing, analyzing, and reducing variance. Proc. VLDB Endowment, 3, 460–471.
25. Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Othmane, L.B. and Lilien, L. (2010) An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing. 29th IEEE Symp. Reliable Distributed Systems, pp. 177–183. IEEE, New York, USA.
26. Pannu, H.S., Liu, J. and Fu, S. (2012) A Self-Evolving Anomaly Detection Framework for Developing Highly Dependable Utility Clouds.

Global Communications Conf. (GLOBECOM), Anaheim, CA, December 3–7, pp. 1605–1610. IEEE, New York, USA.

27. Wang, G., Liu, Q. and Wu, J. (2010) Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services. 17th ACM Conf. Computer and Communications Security, Chicago, October 4–8, pp. 735–737. ACM, New York, USA.
28. Atoosa Gholami and Mostafa Ghobaei Arani. (2015) International Journal of Database Theory and Application. Vol.8, No. 5, pp 161-170.
29. L.X. Yong, L.T. Zhou, Y. Shi and Y. Guo, A trusted computing environment model in cloud architecture. 2010 International Conference on Machine Learning and Cybernetics, Vol 6, pp 2843-2848.
30. Harfoushi, Osama. (2017). Trust Model for Effective Cloud Computing Usage: A Quantitative Study. Journal of Theoretical and Applied Information Technology Vol 95, No 5.
31. Ali M. Al-Khouri (2011), Optimizing Identity and Access Management (IAM) Frameworks, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 3, pp.461-477.
32. Gang Liu Jing Zhang Jinhui Liu Yuan Zhang(2015), Improved Biba model based on trusted computing(2015),
33. Journal Security and Communication Networks archive, Volume 8 Issue 16, November 2015, Pages 2793-2797