Cloud Computing- Trust Issues, Challenges and Solutions

Sanchika Gupta, Padam Kumar and Ajith Abraham*

Indian Institute of Technology, Roorkee
Department of CSE, Uttarakhand, India
dr.sanchikagupta@gmail.com, padamfec@iitr.ernet.in

*Machine Intelligence Research Labs (MIR Labs)
Scientific Network for Innovation and Research Excellence (SNIRE)
WA, USA
ajith.abraham@ieee.org

Abstract

Cloud computing is now a hot research topic in Computer Science. Cloud is used as a metaphor for the *Internet*, so computing means a type of Internet-based computing. But what actually is? Cloud computing according to National Institute of Standards and Technology (NIST) is a service that provides computing and data storage facilities remotely over network on a pay per usage model [1]. The resources are provided on demand and can be released on demand as well with minimal efforts required for allocation, reallocation and release. There are three parties involved in cloud computing: Cloud Service provider, Cloud users and third parties [2]. Third parties can be cloud certification agencies or computing service providers with which cloud service provider can interact to complete the request of a user.

As cloud places users data in physically remote location with minimal control of users on its storage, customers lacks trust in placing their data on cloud[3]. Also when user submits any of their mission critical data to remote cloud servers as input they want that cloud service provider should ensure that their data will not be stored by the

remote servers [4]. As cloud computing is a distributed form of service it causes a lack of trust. The questions are how much cloud service provider keeps the data of the user safe and secure from others when it is stored in same physical storage with virtual boundaries for individual users.

This Chapter is organized to describe the fundamentals of trust and cloud computing and then illustrate the various issues and challenges in implementing and following the solutions. The article also lists down various solutions available in market and a critical analysis of their approach, advantages and current status of availability for deployment. We hope that the contents would help researchers and industry professionals to get an insight into cloud computing and trust requirements for it with critically analyzed solutions that can help them to get a clear and concise conclusion of need of trust in cloud computing and what they can do from their side to ensure it.

1. What is Trust?

1.1 Defining Trust

However there are many definitions of trust, but we have listed down some of the important ones which are as follows:

> *Trust defines the percentage in which one party meets the behavior as expected by the other. Or*
>
> *It can be defined as the degree in which first party behaves exactly as it was expected from the second party. If the degree is high it represents a higher trust on first party by the second one. In security domain trust acts as an important parameter to determine the threat model of a system. Or*
>
> *To define trust of a system it is represented in the form of a trust model. Trust can also be referred to as confidence. Or*
>
> *It is generally a binary relationship between two entities. Trust is established between two entities based on certain common attributes over which the confidence is analyzed and measured.*

Figure 1.1 shows trust is a relationship between two entities.

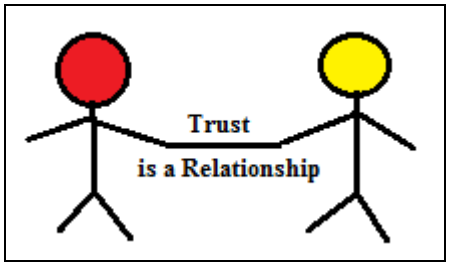

Figure 1.1 Trust is a Relationship

1.2 Trust Modeling

> *Trust modeling is the technique used for evaluating trust of a system. Trust modeling identifies the issues that can affect trust of a system and help in identifying points where a low degree of trust can degrade the system usability. It helps to identify measures that can be applied on the system for making it more trustworthy for end users.*

An Example:

We can generalize the concept of trust modeling by taking an example into consideration. Let' us take an example of a university transferring final examination papers to a college affiliated to it. University had established a new scheme in which they transfer the examination papers to colleges through normal email communication system. The paper of a particular subject is sent with proper ID's, which are then collected at the other end and are printed one day before the day of final examination. Two parties communicate with each other through an underlying email delivery system.

The university and colleges have enough security techniques to ensure that the college will take print out of only those exam papers, which are sent from university without any information leakage. The whole system is dependent on the trust over the email delivery system (Email Service provider). An email communication system that behaves in the expected way as university thinks (timely delivery of message, no tampering spoofing and information leakage) will have higher trust as compared to other email delivery systems that cannot assure expected services. Hence in this case the attributes over which the trust of an email service provider can be analyzed are as follows:

a) Information leakage
b) Timely delivery of message
c) Spoofing and fraud detection schemes availability
d) Message Integrity

If some email delivery system can assure the university on these expected behavioral attributes of service, university will have more trust on the provider and hence will have more confidence on services provided by it. But the question is how the assurance of expected services is fulfilled by the provider? How the provider will make sure that the examination papers will reach to college properly as expected? How he will stand ahead of all other competing mail delivery systems for getting the bid from the university?

This is achieved by understanding the trust requirements for the system. By fulfilling the necessary attributes of the systems in a known and standard way and with the use of advanced technologies and architectural designs, will make the system obtain valuable trust of its customer. For example now in this case if a mail delivery system can show to the university that it uses a 256bit SSL secure connection for encrypted communication of the message and does not store any part of the message in plain text in its servers, the university can make sure that there will be no information leakage as data is strongly encrypted.

The email system can also show that they append a message hash and check it at other end and hence it is impossible to tamper the data and hence they have mechanisms for providing message integrity. Also it is possible to show that they use SMTP authentication and can identify any spoofed communication going from other ends. Timely delivery can be assured by sending a mail failure message in few minutes after trying to send the message fails, so that university can take proper action to deliver the exam papers in timely manner instead of thinking they are reached safely to other end.

Trust is defined hierarchically on any system. However the trust over external entity, which is email communication medium is less, but even having a high amount of trust with external entity does not mean that the whole system is totally secured. For example it is the responsibility of university that the correct examination papers will be sent with the trusted email communication medium by the persons who are responsible for it. As the persons who are responsible for sending correct exam papers are internal to the university, they have more trust level compared to an entity whose services are availed externally for completing the service. Hence trust level of a system over various entities varies according to the entity, its type and on evaluation of their expected behavior.

The next question which comes into the mind is why we are caring about trust? What is the role of trust and trust model that we are discussing. Why we are evaluating trust and what it will give to us that is helpful in determining security aspects of a system.

Trust evaluation helps in development of trust model that represents the hierarchical trust over various entities of a system. This trust model identifies various areas of the system and the trust an entity expects from other entities. Evaluating this trust model helps in determining confidence over entities of the system. Trust model represents major areas of the system where if trust falls will let the system vulnerable to a number of threats. For example the trust model of the above system discussed will describe the external entity Email service provider to provide a higher trust level for the whole system to sustain and behave in the way it is meant for. If entities have a higher trust over each other and if they abide to it a system is expected to work in the best possible way.

The example we discussed is for a quick description of trust and what it means. By entities we will be referring to providers, users or computational systems and subsystems based on the context. Our main focus will be considering the aspects of cloud computing and identifying the need of trust in it. What has been done and what is left will also be discussed.

2. What is Cloud Computing?

2.1 Cloud Computing

Since past we are using various technologies for computing including distributed computing, grid computing etc. One of the recent technologies, which is providing computing resources in a more scalable, user friendly and on a pay per usage model is in the market and is known as cloud computing. This new service is available in the market as the next generation architecture for IT enterprises. Cloud computing services are attracting its customers because of the enormous advantages it provides. It is a scalable, efficient and economical solution for storage and computing where the users store their data at cloud storage servers dispersed across the geographies and managed centrally by cloud service provider. Concretely:

> *NIST defines cloud computing as a model that provide on demand network access to shared resources that can be configured, allocated, managed, release with minimal efforts and interaction*

Users can use well-known or specialized software and web applications, can demand for platforms for execution of their own programs and IT infrastructure in whole for handling whole set of IT operations by their own. The concept of cloud computing where the IT resources can be obtained on rent also helps in increasing the resource utilization of IT

infrastructure which are spare with Big IT firms and are going underutilized. This sharing of resources increases efficiency of physical infrastructure with use of virtualization technologies and hence cloud computing provides a low cost solution computing and data storage solution to its users. It provides many other facilities to its users and providers including remote and on demand access, easier management, maintenance and allocation with scalability of resources on demand.

2.2 Current Trends in Cloud Computing

Cloud computing based services are getting a great amount of success both in the market for individual users and small business organizations which don't want to spent money in buying and managing physical computing resources. Examples of cloud computing services that we one or other day uses includes, online data storage facilities, email service provider facilities where they provide handling of customized email services for small business organizations. Others include usage of online web applications such as word processing software's, online management software's etc. and platforms for running users own programs, which includes web and remote code execution platforms.

Due to the alarming need of cloud computing services a large number of highly reputed and well known firms such as Amazon, Google, and Microsoft have already started to come forward in the market. Well known clouds by these firms include Amazon EC2, Google Cloud and App engines and Microsoft Azure. However the concept of Cloud computing is named and popularized now as a service but it was known since past [5]. The usage of free services that resembles the way cloud computing behaves was there in form of free email services, virtual guest operating systems services and online file storage services. But the proper management and involvement of virtualization technologies have made this form of computing more advantageous which is the key difference between cloud computing and other computing services. Figure 2.1 shows an abstracted view of cloud computing environment with the interacting parties.

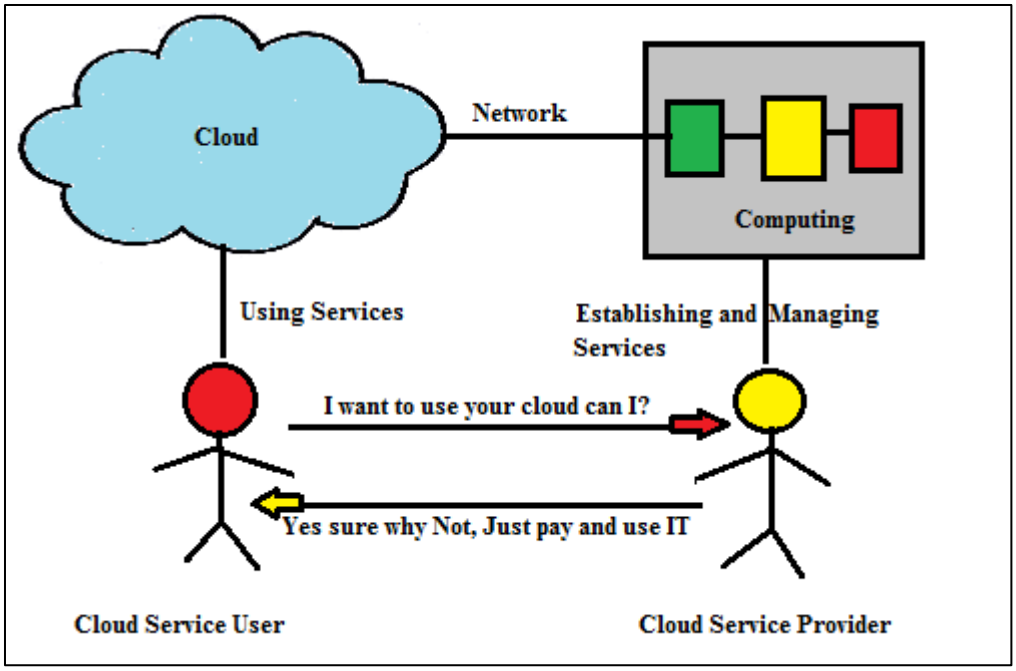

Figure 2.1 Cloud Computing

Cloud concept of having a pool of IT infrastructure, resources, allocating, managing and releasing them on demand with pay as you go model resembles with telecommunication market where big telecommunication companies with spare and large amount of operational resources rent them to a group of startup telecommunication companies that cannot establish their own physical operational resources for their functioning. The concept of renting the resources that are additional and of no use for the telecommunication provider helps them to gain more money from their spare hardware resources with their efficient utilization. Cloud computing is a combination of concepts from technologies including distributed computing, virtualization that increases resource usage by diving physical resources virtually, and high performance computing. The new paradigm of renting the resources and model of using it on pay as u go is something that makes cloud computing new and ahead in market. It's a new era of computing in the internet world and its future looks bright.

2.3 Cloud Services

Cloud can provide two types of resources either computing resources or storage resources. On the basis of the type of service cloud provides it is broadly classified as: Storage Cloud or

Compute Cloud. The service hence varies from data storage to online platforms for remote code executions and known software's in the form of easily accessible web applications.

Some of the essential characteristic that a Cloud should provide according to NIST [1] includes:

1. On demand Self Service
2. Ubiquitous Network Access
3. Resource Pooling
4. Rapid Elasticity
5. Measured Service

Cloud provides its offerings in three well known forms of service:
Software as a service (SaaS) in which cloud user can access applications running over cloud servers with the use of web browser or other customized interfaces. In this service, clients don't have to worry for management or maintenance of software's and has no control over how the software behaves. The user can have some level of privileges to perform configuration changes to his/her view of software or application running over cloud.

Next service is known as Platform as a service (PaaS) where a user can deploy his own created applications over internet with the use of platform from cloud service provider including programming platforms and libraries etc. However users have little control over infrastructure but have enough control over their own software's configuration and working. In Infrastructure as a service (IaaS) user have control over the infrastructure including data storage and network and computing platforms. The user can run the platform they wish and install software accordingly on the rented infrastructure. However the maintenance, allocation, management, scaling and release still remain in control with cloud service providers.

2.4 Advantages of Cloud Computing Services

Cloud computing provide to its users the choice to avail services without having to purchase any physical resources, infrastructure or storage etc. Also users do not have to worry about

establishment and management of services. He can just obtain the service by paying for its usage. The solution or services the user is purchasing can be customized to fit their particular needs. After some time when the user thinks that the resources are no more needed they can stop paying for the services and the resources he left can be used by other user in a fresh manner. The important thing is user just see the service without clearly knowing how the service is provided or how and where the data is stored etc. The user merely sees a virtual copy of actual physical resource customized by the service provider. Cloud computing is totally flexible and customized form of computing.

3. Why we Need Trust in Cloud?

3.1 Trust Requirement in Cloud

As cloud computing is a service which is packaged and provided to a user it requires some service level agreements and understanding between the user and the provider of service. Today we use cloud services in our day to day life. From email services to free storage services are all a part of cloud computing environment. We can refer to them as free cloud computing services but are not much different from the services provided by cloud to user on a pay per usage model. Figure 3.1 is a self-descriptive example of why we need trust in cloud computing environment as client has questions regarding trust on cloud service provider as it can bypass client data to other third parties.

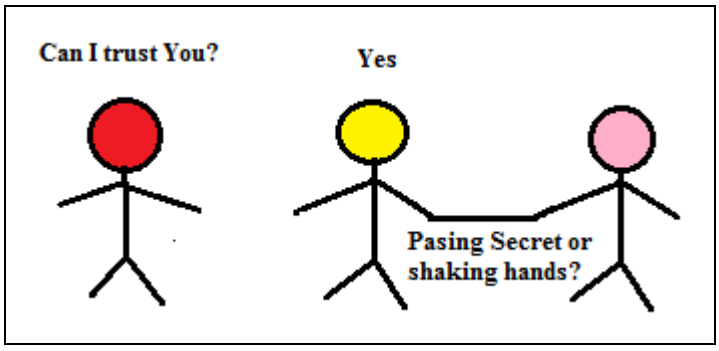

Figure 3.1 Need of Trust in Cloud Services

Trust is required in the cloud computing environment [6] because of the service model it provides. It provides a distributed model of service where user or the customer of the service has generally a low level of control over the service it takes. However the cloud service

provider can have distributed or centralized control over the service it provides to its customers. As a user is placing its secret data in case of storage cloud he has certain questions that he need answered from cloud service provider:

As a cloud is providing data storage services, a user wants the data to be kept to his reach only even if it is stored in a shared manner on physical disks. Hence customer requires trust over cloud in providing data security for the data stored by them in cloud [7].

It's not only data security user also expects that when the data is accessed from the remote location the data cannot be sniffed and converted to information. User also expects that the data can't be seen by the cloud service provider itself and should be kept in encrypted form. Also a user trusts that the data should not be tampered when it lies inside the cloud storage.

In case of Computing as a service a user wants that the application it is using works with user authentication. The application or software that a user is using as a service should be trustable and follow standards and must be compliant to certain guidelines that are governed by trusted third parties.

Also when a customer uses certain platforms (platform as a service) for executing their own software's and applications a user expects that the platforms will not open or use any vulnerabilities present in the application for any unwanted usage. The platform should be secured and must be standards compliant. Similar trust requirements are expected by a user using infrastructure as a service.

A stakeholder or a customer using the distributed services provided by cloud may want assurance that the business critical data must be secured and the processes which are involved in securing it that includes process for accessing the data, for storing it and securing it must follow standards that are well governed by a trusted third party. This assurance is for increasing the trust that the cloud service provider is keeping the business critical data safe and away from reach of insiders and from other users availing the services from the cloud service provider.

In cloud computing service, either data storage or computing a user expects certain trust based attributes to get fulfilled by the cloud service provider, and those are required for proper functioning of cloud computing services [8]. Establishing trust on cloud is a major task that needs to be addressed. It is requirement for the usage of the services provided by cloud that they explore both hard trust and the soft trust to their customer. This means that they should provide hard trust features such as encryption of storage, security of online transactions but at the same place must provide soft trust parameters including user friendliness, theoretical trust etc. It is a requirement that the persistent trust should be provided by cloud service provider to its users. By persistent trust we mean a trust that is permanent and can be proven to the other entity with implementation of technological mechanisms [9]. For example any implementation that can help user to increase his trust on the provider will generate a persistent trust for the cloud service user.

3.2 Trust and Cloud : Current Trends

If we see the recent trends and the customer experience in using online cloud services it has been identified in the surveys that users are insecure about the services provided by them. If you talk about online mail services and free storage accounts provided by well-known service providers users are not sure of whether their data is safe or not. Many think that the data which is stored on such service provider ends is generally compromised and is used for other means. This is one of the reason people generally have started encrypting data at their end while storing it for sharing with other using help from free storage providers.

This lack of trust affects the soft trust of the user over services. This previously had happened with the usage of online transaction services when lack of trust causes many of the users in using the services. The lack of trust is because of the unavailability of persistent trust mechanism system that can make the customer sure that his information will not get revealed to any third party or to the service provider with which he is doing the transaction with. The technological deployments of trust such as encryption of the data (credit card information) and standards compliant transaction processing system which are approved by trusted third party have changed the trust level of the user drastically. The similar deployments are necessary in cloud to assure the cloud service user for placing their data or for usage of computing service in cloud.

4. Proposed Solutions for Ensuring Trust in Cloud

Various research works are going on in the field of providing trust solutions in cloud computing environment. This Section briefs the past works with a critical review on what they did and how it can help ensuring better trust in cloud computing environment. This critical description of current trends in the area of ensuring cloud trust will help industry professionals and researchers to get better understanding of current issues and needs for trust in cloud.

Rashidi [10] focused upon the fact that trust is one of the major concerns to be handled in cloud environment. They have taken the statistics and data from reports such as Gartner, Cloud security alliance to identify what are the questions related to trust in cloud computing in mind of end users. Author listed down the main concerns of users trust in cloud environment which are: Data location, Investigation, Data Segregation, Availability, Long term Viability, Regulatory Compliance, Backup and Recovery, Privileged user Access. With these eight concerns their hypothesis is also provided. Authors have provided a model of user's trust in cloud computing. They also performed a user survey with questionnaire and have done the statistical analysis of their results with SPSS 19 and fit was measured with AMOS 18. The model was examined for maximum likelihood. Research results show that backup and recovery provides strongest impact on the user's trust in cloud computing with recorded value of 0.91 from AMOS analysis. Analysis illustrate that Data Segregation and Investigation have weak impact on user's trust on cloud computing. The findings include determination of eight parameters that can be looked upon for ensuring better trust to the user. Also the model proposed with the findings, can help industry to look upon the concern's that mostly affect the trust and find appropriate solutions for ensuring them.

Firdhous and Hassan [11] focused on various existing trust models for distributed systems and cloud computing environment. They have discussed the cloud computing paradigm with explanation of services provided by it at various layers of computing. Authors have focused on defining trust in terms of human behavior "and how it is taken into consideration by computer science researchers to ensure trust to end users. They have identified some of the common

factors of trust such as “it plays a role only when the environment is ascertain and risky, and is built up by prior knowledge and experience”. They also identified previous researches where characteristics of trust are divided into groups. One of the examples is of McKnight and chervany who divided 16 characteristics of trust into five groups: Competence, Predictability, Benevolence, Integrity and others. Also author refers to some other classification of trust such as given by Zhang et.al who classified trust on the basis of four dimensions which are: Subjective vs. Objective Trust, Transaction Based vs. Opinion based trust, complete information vs. Localized information, Rank-based vs. Threshold-based trust. Authors also describes about various trust models that are developed for distributed systems including, Cuboid Trust, Eigen Trust, Bayesian Network based Trust Management (BNBTM), AntRep, Semantic Web, Global Trust, Peer Trust, PATROL-F, Trust Evolution, Time-based Dynamic Trust Model (TDTM), Trust Ant Colony System (TACS), TRUMMAR (TRUst Model for Mobile Agent systems based on Reputation), PATROL (comPrehensive reputation-based TRust mOdeL), META-TACS, CATRAC (Context-Aware Trust- and Role-Based Access Control for composite web services), Bayesian Network -based Trust Model. Author critically analyzes over the existing research work and come up with some findings that most of the models which are proposed remain short of implementation and a very few of them have been simulated to prove the concept. Authors have critically commented the research work did in past according to their capability and applicability in cloud environment and focused on the fact that there are no complete solution for trust management exists in cloud and hence there is a need of solutions that can be implemented and which resides on strong base.

Jagadpramana et al. [12] focused on how important is the requirement of trust in cloud computing and have discussed key issues in and challenges in achieving a trusted cloud with the use of detective controls. They have also proposed a trusted framework that addresses the issue of accountability with the use policy based approaches. They have referred to one of the research that fujitsu research institute did in 2010 and reported that 88 % of the cloud users are worried about who all can access their data on physical servers also a report by European Network and Information Security Agency states that the loss of governance is major risk to cloud services now a days. They also include findings from cloud security alliance report Ver1.0 which states that increasing the accountability and auditability will increase the trust of the user on the cloud

services and will decrease the probability of the enlisted threats. According to analysis of [13] they cited in their research the important components that affect the trust of cloud includes: Security, Privacy, Accountability, Auditability. They also suggest that usage of detective and preventive controls for ensuring trust in cloud will be a best combination for ensuring trust in cloud in both physiological and technical manner. Authors list down some of the complexities which are introduced because of elasticity in cloud. These include Challenges introduced by virtualization such as: Tracking of Virtual to Physical mapping and vice versa Scale cope and size of logging, Live and Dynamic systems etc. For solving the issues of trust in cloud computing In their research they tried solving the problem by including five abstraction layers in their trust cloud framework. The layers include Trust Cloud Accounting abstraction layer, System Layer, Data layer, Workflow layer and Policy law and regulation layer. They have described how accountability and logging can be achieved with the help of the defined layers. They have described that file centric logging can be performed at Operating system end or in File system or on Cloud's internal network. Data centric logging can also be performed by consistency logger or provenance logger. With workflow layer they have focused on audit trail logs found in software services in cloud. Their focus is on issues related to governance in cloud, automated continuous auditing, patch management auditing, and accountability of services. The research also includes some of the related work done in the area including the work done by CSA, HP Labs, Max Plank Institute etc. Authors are however working on Trust Cloud framework that is capable of providing user a view of accountability in cloud and the research is under progress.

Wang [14] illustrated the fact that there is unavailability of trust evaluation models in cloud computing environment. Author proposed an extensible trust evaluation model named ETEC. The article provided the definition of various trust measures including Trust, Trust Degree, Trust Relation, Trust Service Trust Model, Trust Chain, recommendation trust, Experience or Knowledge, Direct Trust and Time based forgetting function. On the study on properties of trust the article proposed ETEC model that works upon Recommendation Trust and Direct trust. ETEC algorithm with its component algorithms including direct trust, Recommendation trust and dynamic trust are explained. ETEC is actually a time variant and space variant method for evaluating direct and recommendation trust.

Khaled and Khan [15] illustrated the issue of how a cloud service provider can gain its customer's need of trust when a third party is processing important data of the user in various countries. According to their using new emerging technologies can help cloud service provider obtain hard trust from its effective users. They have identified two of the challenges while describing hybrid cloud architecture with the example of a SoftCom Image pro software application running on the Private cloud end of the hybrid cloud architecture. The two challenges include Diminishing control and Lack of transparency. Authors explained how the assurances from public cloud and the software running on private cloud to each other can help provide better trust to the end user. Authors have provided an overview of some of the emerging technologies that can be used for ensuring trust which includes:

a) Remote Access Control: Where a user can have remote access facilities and more jurisdictions over their data.
b) Reflection: Through this the cloud service provider informs the user about its strength and weakness and how the security policies are addressed. This will help user to choose the trusted service and also to ensure the trust from his end if the degree of trust required by him was not provided by service provider.
c) Certification: where a trusted third party will provide trusted certification to the cloud service provider by judging the services according to global standards and based on the trust assurance measures that are implemented by them.
d) Private Enclaves where a set of secured enclaves can be made for users demanding more trust with enhanced logging, auditing, incident response and intrusion detection capabilities with global standards.

Zhexuan et.al. [16] provided their focus into the security issue where unrestricted access to user data from remotely installed software's can cause security risk to SaaS. They have taken this issue into consideration and provided an approach where software can be separated from the data. Authors proposed a mechanism where there are four parties namely, resource provider, software provider, data provider, and coordinator. The responsibility of resource provider is to implement data and software also it should provide the platform for the execution of software. In the proposed scheme the data providers are those who are having control and ownership of data and software provider have control and ownership of software that runs on data. The last party in

the team called coordinator is responsible for connecting software, data and resource provider together and providing interface between data and applications. While any of the software or data providers submit the resources to resource provider they will be encrypted and then stored the resource provider. A coordinator helps the data provider in identifying the software to run on the data on the resource provider. The reference id generated during execution is stored by data provider and after execution a data provider can download and do other operations on the results obtained. Software and resource provider charge the data provider for usage of services. For software provider to understand what software was operated on data and without knowing the identity or content of data provider, the operational logs created are used. This is a new approach towards the development of a more trusted cloud. However authors may have to look upon like how they can assure it to the data provider that software provider is not running some algorithm in the background that can read the contents of the data provided to it for execution.

Manuel et.al. [17] proposed a new trust model that is based on CARE resource broker The technique proposed by researchers focuses on evaluation of trust on grid and cloud systems on the basis of three evaluator components that includes Security level evaluator, Feedback evaluator, reputation trust evaluator. There are various measures that are utilized by each of these trust evaluators. The security level trust evaluator uses these parameters for evaluating the trust: Authentication type, authorization type, mechanism used for self-security, multiple authentications, and authorization mechanisms. The degree of trust is based on the grade that is provided to each of the security parameter based on the strength of their implementation in the system. There are three steps while calculating the evaluation during feedback evaluation. These include feedback collection, feedback verification and feedback update. Finally the reputation evaluator uses the grid and cloud resources parameters such as computing power and network capabilities to calculate the trust value. At last all the values obtained from the three trust evaluators are then used to arithmetically calculating the final sum value which will be the final trust of the cloud of the grid system. The value of final trust can then be used for accessing the cloud services and is applicable on heterogeneous cloud. However the concept is not implemented and is in progress but an initial prototype has tested by the authors in simulation.

Shen et al. [18] discussed the trust aspects of cloud. Concretely they have talked about the trusted computing platform in cloud computing. Authors have proposed a method to improve the security and dependability of cloud computing environment. The application of trusted computing platform will be used in ensuring authentication, confidentiality and integrity in cloud computing environment. Authors have provided this model as Trusted Platform software stack as software middleware in the environment. The proposed model however provides identify management and authentication also it is applicable to heterogeneous cloud..

Alhamad and Chang [19] proposed a trust model based on SLA. SLA agents, cloud consumer module and cloud services directory are the components of this trust model. Various task that are performed by the SLA agents includes: Grouping the consumers to classes on the basis of the needs, designing of SLA metrics, negotiation with cloud service providers, selection of provider based on nonfunctional requirements such as quality of service, monitoring the consumer activities etc. The responsibility of cloud consumer module is in requesting the services externally in cloud environment. The information of cloud service provider who is meeting functional requirements for getting chosen by consumers is present in cloud service directory. The requirements that user needs to view using cloud service directory includes database provider, hardware provider, application provider. Also service providers advertise the services provided to cloud users through cloud service directory. The model looks a quite novel one for ensuring trust in cloud computing environment but there is no implementation by authors till present. Hence the effectiveness of the solution is yet to be determined when it will come as implementation.

Sato and Tanimoto [20] identified a new issue of social security trust. They approached the social security problem by dividing into three subareas including multiple stakeholder problems, open space security problem and mission critical data handling problem. They have addressed the multiple stakeholder problems, which happen because of the interaction of third parties. The parties that generally involve in cloud communications include, cloud service provider, client and the stakeholders and rival of business. A service level agreement between cloud service provider and client is provided by client that contains the administration and operational information. SLA plays a specific role in defining the policies between the three interacting

parties to ensure a greater trust on each other. Open space security problem tries to address the issue of the loss of control over users on data when it is transferred to a cloud service provider end. They proposed solving this problem by data encryption, which requires a key management infrastructure. Mission critical data handling problems looks for the issues that are of concern when a mission critical data is stored on cloud servers. They have proposed that if the mission critical data is stored in a private cloud the problem can be easily addressed but with a drawback of increased cost of setting up the private cloud. Authors proposed and developed trust model called "cloud trust model". Trusts layers namely internal trust layer and contracted trust layer have been added as additional layer in cloud environment. The work of internal trust layer is to handle ID and key management operation. Mission critical data can also be stored in the internal trust layer for better trust and security needs. Cloud service providers also provide the trust to its clients in the form of three documents which are known as Service Policy/ Service Practice, ID Policy/ID Practice Statement and the contract. The parties can ensure a higher level of trust based on their needs to each other and hence can implement a more trustable cloud infrastructure. However the authors have only discussed the issues and the work exists as proposals without implementation.

Yang et al. [21] proposed a non-traditional trust management module and a security framework for ensuring trust in cloud. Some of the security measures based on trust are also provided by the authors. A family gene technology based trust model is also proposed by Zhu et al. [22] [3]on authentication, authorization management and access control mechanisms. We have presented taxonomy of cloud trust solutions in Figure 4.1. The taxonomy describes various proposed techniques on the basis of the kind of approach utilized for ensuring trust in Cloud computing environment.

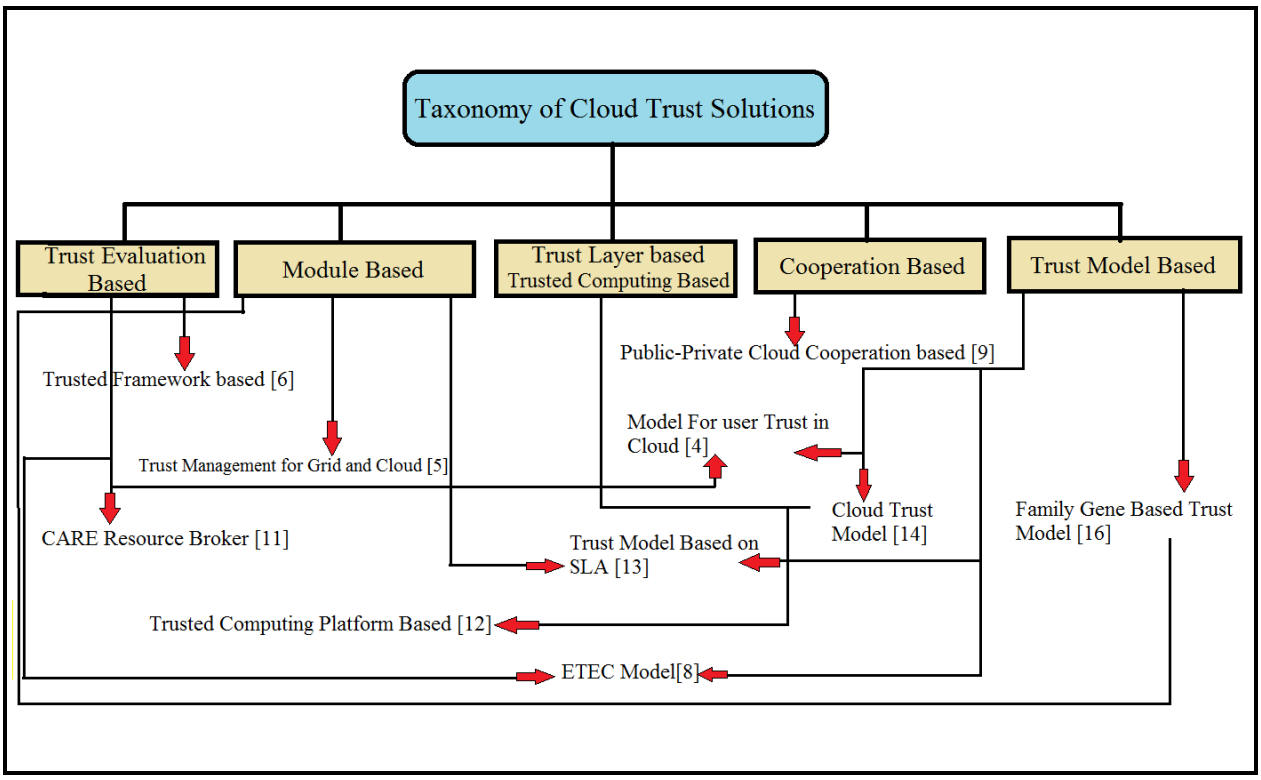

Figure 4.1 Taxonomy of Cloud Trust Solution

The proposed solutions are categorized on the basis of five different overlapping approaches for ensuring trusted cloud computing environment.

1. Trust Evaluation Based: The solutions lying in this approach are those which have used trust evaluation components that evaluate trust on the basis of predefined features. After evaluation of trust by individual components the final trust value is calculated by their combination. The solution includes Trusted Framework based [6], CARE resource broker based [11], Model for user Trust in Cloud [15], ETEC Model [8].
2. Module Based: Module based solutions are those where the system is divided into specific modules with their predefined task and responsibilities to ensure the trust in cloud environment. Example includes: Trust Management for grid and cloud[15], Trust Model based on SLA [13].
3. Layer Based and Trusted Computing Based: Techniques in this approach are those in which the system is divided into multiple trust layers which have specific trust ensuring responsibilities. In trusted Computing based solutions a layer of software stack generally

referred to as Trusted computing platform is used for ensuring trust on certain operation that can vary from authentication authorization etc. Proposed techniques include Cloud Trust Model [14] and Trusted Computing Platform based [12].

4. Cooperation based: Certain trust solutions are based on cooperation between operational entities. One of the examples is the cooperation and trust between public and private cloud in a hybrid cloud environment can help both the entities to create a higher overall trust. Techniques include: Public Private Cloud Cooperation based [9].
5. Trust Model Based: There are various overlapping solutions in this category. However the model based solutions are those who either creates a Trust model for evaluation of trust based on features, layers or modules etc. These solutions may also follow well defined mathematical and analytical models for calculating trust in Cloud. Techniques include: Model for User Trust in Cloud [15], Cloud Trust Model [14], Family Gene Based Trust Model [16], Trust Model based on SLA [13] and ETEC model [8].

5. Challenges in Deploying Trust based Solutions in Cloud

We list the questions regarding trust that a cloud user has in their mind and how a cloud service provider can answer them with challenges that needs to be tackled.

5.1 Trust: A user's perspective

If you look into the characteristics or the qualities that a customer of cloud service user expects the cumulative assertion from the surveys gives the information. The user generally calculates the belief or trust or confidence on the services a provider provides on the basis of these soft trust parameters:

What is the brand it is having a service with? You can say that what is the overall online reputation of the brand whose cloud services a person is using?

Recommendation is the second parameters a service is assessed with. If any service is recommended by a trusted third party a user find it easier to generate a trust and get used to a service with a higher level of confidence.

The third is with use of the service they wants to generate trust with. Many users use the free or paid cloud service and give a trial to them. They look for some time for any breaches that they can detect and from knowledge of their own they rank the service and create a trust with the service they are using.

Many users create trust relationship on a contractual manner with the service provider.

Other reasons may also exist but we want to have a cleat description of a cloud user thinking over assessing a cloud service with no technological aspects involved. These characteristics are generally found with customer who use free cloud services and users with having low risk with the data stored on a cloud service provider end. However they play role for assessing the services with a small business organization thinking to use the service with some other technological or hard trust aspects taken into consideration. The hard trust concerns for assessing any cloud service with respect to a cloud service user are as follows:

How the data is getting stored in the service provider end and what are the mechanisms which are going to access it? Are they standards compliant and approved by trusted third parties.

Is the data stored in meaningful form or as garbage value (encrypted data to others)? How strong is the scheme used? Can cloud provider have privileges to obtain data as meaningful information?

How data integrity is assured when data is stored at cloud service provider end?

Is the Network access to storage systems secured and encrypted? How the authentication to access is done and is it secured?

What are the availability aspects of using the storage service of cloud?

Figure 5.1 depicts how a cloud user can assess the trust from cloud service provider by getting answer in both technical and physcological form from cloud service provider end.

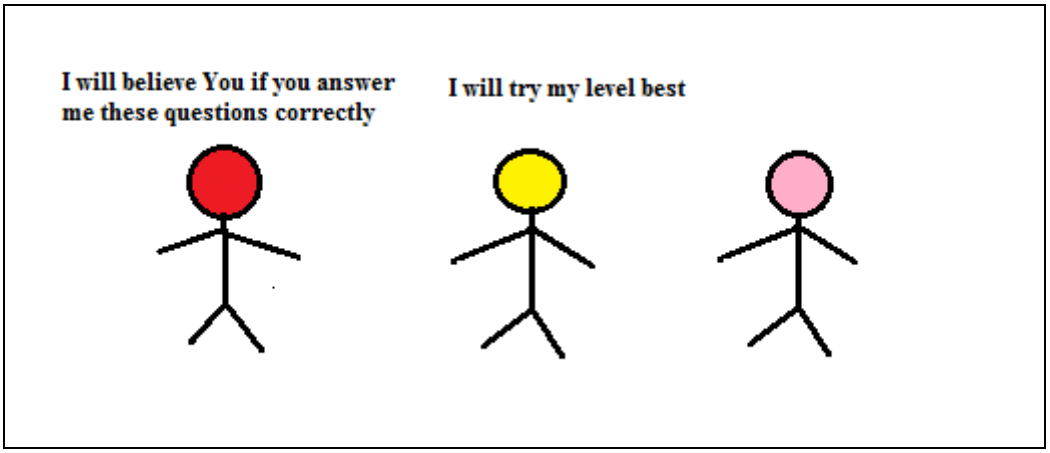

Figure 5.1 Assessing Trust in Cloud

In case of using computing services of cloud user is concerned about asking the following question from a cloud service provider:

Are the software standard compliant and secure to be used? Will their usage cause any vulnerability exploitation to their end systems?

Does the platform provided by cloud service provider secured for the software to run? Does the platform is transparent and will not do something for his interest in case of platform, as a service?

How much I can believe over the infrastructure provided by the cloud service provider?

A cloud service provider must be ready to answer these questions for providing a trusted service to its users. A healthy trust relationship between the cloud service provider and a cloud service user can be built if these questions can be answered with both technological and non-technological manner to the stakeholders.

In conclusion, a cloud user assess a cloud service security on the basis of data security mechanisms available, transparency measures in both execution and storage in both computing and storage cloud services, availability of the services and their reliability. A cloud service user also looks for good authentication mechanisms including two factor authentications with proper mechanism for ensuring the auditing and logging.

In conclusion answer to these questions may help user establishing trust (both security and availability) on cloud services:

Are the services standards compliant and follow the government regulations in which they are running.

Are the cloud services globally accepted?

Will they provide audit logging monitoring and reporting?

Do they provide access to customer data and if then in what situations?

Is the data can be seen at cloud service provider end or not. How the data is stored encrypted or unencrypted. Does integrity of data maintained.

If a user deletes his data what is the surety that cloud service provider will permanently delete it and does not use for his own means.

What happen in events of crash or failures? Are there any backup or recovery mechanisms that keep data safe?

How the data will get protected in case of network based attacks what preventive or defense measures are in place to thwart such attacks. What is the network model? How does data flows in encrypted or unencrypted format.

As cloud service provider uses various well known hypervisors to provide virtualized sharing of physical resources. Then how the user will handle the well-known hypervisor vulnerabilities existing and exploited. Does the user have any such defense measures?

How the user will ensure security of his data in an environment where other are also viewing the same resources virtually. The assurance of security in a multitenant environment

Does cloud service provider have a threat model for the service he provides and hence can identify threats to the system before they are exploited? How secure security policies are there and are they implemented.

How the access control will be provided to the user and how the access control parameters (user name and passwords or any two factor authentication technique parameters) will be kept safe in the environment.

Does the cloud service provider provide software's and web applications which are secured and up to date with patched known vulnerabilities?

Does cloud service provider updates the applications used with patches released so that they will not cause harm to cloud user and if yes then how frequently?

Will cloud service provider ensure any investigatory services through his audit logs and monitoring in case any breach to user data is reported?

The answer to these questions will surely help cloud service user and provider to create a healthy trust relationship between them.

5.2 Challenges in Establishing Trust to Cloud Computing

It not the case that the cloud service providers does not know about the aspects that they need to look into for providing trust to their users and can hence increase the growth to their business. Many researchers have addressed the issue and they know them well. The deployment and implementation of such schemes is delayed or not taken into consideration because of some of the challenge's that needs to be faced for providing trust to cloud computing environment user and these are as follows:

Many of the cloud service providers are ready to establish a higher and more better trust based mechanisms in terms of technological aspects also referred to as hard trust but are scared of the degradation in the performance of cloud services. As the cloud is a pay per usage model hence the resources are limited and shared and if the cloud resources are utilized for ensuring the conditions that a user expects for trust then he may need to pay more for the services he is availing and with a degraded performance in some cases. Some solutions may also make the system user unfriendly and complex to use. The cloud service provider based on various measures needs to identify and answer that how such a change for increasing trust level among his customers will be increased with minimal changes and degradation to the service.

The second question which comes in how such measures will be provided in a standards compliant way. How the services should be provided by vendors in a transparent and globalized manner so as to gain confidence of the users.

As there is no complete model for ensuring the trust that can be implemented in cloud. And if such solutions exists then which solution or trust model to use with maximum benefit in assuring trust to its users.

There are many more challenges which include the implementation difficulties in deploying the models in cloud because of its complexity. These and many more challenges that need to be addressed for deploying a trust cloud environment for users. Figure 5.2 is a representation of how cloud service provider thinks while implementing and assuring it to the cloud users.

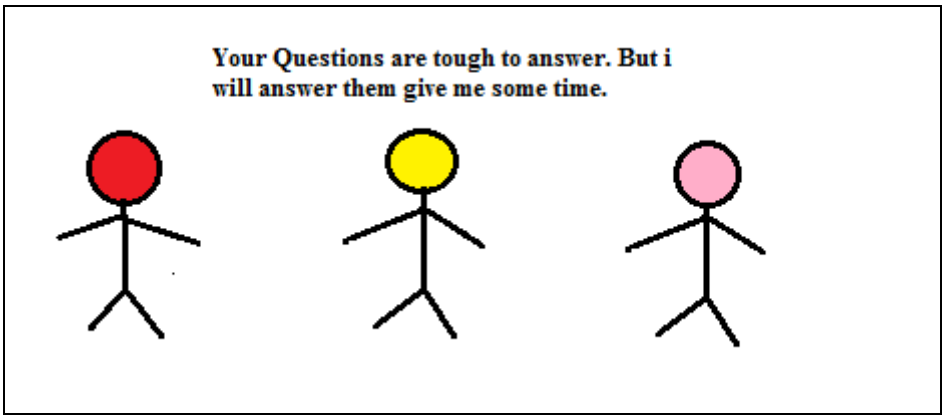

Figure5.2 Challenges in establishing Trust

6. Ensuring Trust in Cloud Environment

To provide trust in cloud computing many technological implementation are used and deployed [4]. To ensure data integrity and security data encryption and message digest schemes can be used over the data stored on cloud servers. Better authentication and access control systems are also a requirement. There are certain techniques that can be used by the cloud service provider which allows them to take encrypted data from a cloud service user and process it. With these many other implementations and measures can be utilized that will allow the cloud service provide to ensure data security that will eventually increase user trust over cloud computing

services. Many can be taken from cloud user end to ensure security of its data at providers end. These are as follows:

A cloud service provider can provide a cloud service user privileges to dynamically check the status of the services availed by him. For example he may remote login to cloud server and can provide restriction for what a cloud service provider can see and what it cannot. By having such access to its data through resources of cloud service provider he will remain confident of his data secured at cloud service provider end. In case of computing as a service a cloud user may fire rules that will delete his personnel data when a cloud service provider or any cloud service user other than he himself logins somehow to his account. He may also set alerts that will get raised when unauthorized access happens with proper auditing and logging mechanisms of such access. This kind of technology can be provided as a single customized service to a cloud service user for increasing his trust level on a cloud service provider with larger benefits with a little increased cost for managing and maintaining such customer controlled facility. In this technique even if the data of the owner lies at various different location he can have full control over who can see the data and which part of it.

When a cloud provider provide transparency of the services it uses for accessing and storing the data with other technological aspects of how the data is stored in its repository a cloud service user can determine the weak and vulnerable areas which can create threats to its data or services in cloud. A deeper analysis of the security provided by a clouds service provider will help the customer's identify the weak areas over which they need to establish security on their own. Such transparency will help customer provide better security at their end and have an increased trust on the services it uses from a cloud service provider. For example if it is known that the data can be seen as plaintext to an employee of cloud service provider the customer will then store his data in encrypted formats instead of plaintext.

Third party certification techniques can help increase user trust over cloud services. As each cloud service provider has their own security mechanisms that can't be accessed globally in general and many or many be compliant to a given standards a cloud service user may find it difficult to access the security and hence the trust over a cloud service e provider. However if techniques are implemented where a trusted party can assess the security mechanisms provided by a cloud service provider and can rank them on the basis of confidence they are

providing in the security services a cloud user may obtain the same confidence which will help him in selecting the cloud service provider for a particular service meeting his expectation's. In such a mechanism there is a need of trusted third party that can transparently judge security of a cloud service provider for various services it provides and a set of well-known security parameters over which security of the system can be judged. Many of such techniques in which a third party gives rating such in the form of trust cards are available now days. Trust measures in these techniques generally collect a large amount of behavioral aspects of the system with its reputation and historical evidences of its working to define trust a stakeholder can expect from a cloud service provider.

For user that demand for higher trust levels with the available infrastructure of a cloud service provider, a private enclave can be created that will be externally separated from other cloud user's data and have given added security measures and control mechanisms for incident intrusion detection and response. Such private enclaves will have a higher security defense measures which includes firewalls, network traffic filters and intrusion detection systems and may have better auditing event log management and incident response components. They will have standards compliant implementation of security measures that will be different from the normal security measures. This type of services can be helpful in increasing trust of cloud service users that demand for higher level of trust and also don't want to ensure such mechanisms from their end.

Figure 6.1 describes how cloud service provider can ensure trust to its users by answering to cloud users question with the help of soft trust and hard trust measures.

Figure 6.1 Establishing Trust Measures

7. Conclusions

Trust is a relationship between two entities. Trust is commonly known as the confidence of the second party that the other party will work according to expectations. Trust modeling concepts are used to present trust levels that exists between various entities in a system which will eventually help system designers to identify weak trust areas. This information helps them include better practices to include hard or soft trust as required to make system more trustworthy. Trust modeling is used for identify and demonstrating trust over real time systems. The chapter discusses trust issues and challenges over cloud computing environment. Cloud computing is a new paradigm of network access based computing that can be accessed on a pay per usage model by customers varying from individual users to small business organizations.

The services are provided in the form of cloud storage services and cloud computing services. The Software as a service, Platform as a service and Infrastructure as a service are provided by cloud service providers now days. Cloud distributes physical resources into virtual counterparts with the help of virtualization technologies which can are rented to users on a pay per usage model which eventually increases efficient resource utilization. However cloud is growing at a good pace still a large population of users have questions regarding the trust they can have over cloud computing. There is a need of trust establishment in cloud computing as the clients using the rented resources may not want any risk from the storage service or applications they uses from cloud service provider. As user's data is stored in a distributed manner and the data can be confidential users want to be assured from cloud service provider that the data will remain available and secure with integrity maintained. Also the cloud user wants that if he uses cloud applications or platforms they must not explore vulnerabilities to third parties also will not exploit one to compromise their end systems. They also want assurance that their data will not be shared with any third party and will get deleted completely in case the agreement of services ends.

It is a requirement that these and many other questions will be answered with technical and non-technical aspects because an increase in trust will affect the population of users that will use them. To solve these questions and many others it require added implementation measures such as intrusion detection systems , storage encryption, data anonymity and other can help increasing

the trust but on the same place will utilize cloud resources and hence will increase the maintenance and operational cost. But the requirement is an immediate need and the challenges for ensuring trust needs to be tackled in positive ways that will result in a more trusted cloud environment. The chapter lists some of the known solutions that can be easily implemented over cloud including concept of third party service certification and private enclaves Cloud computing environment requires trust as one of the major topic to look upon for its better growth. An increased trust will attract more and more users to use the services with a more confidence level.

Bibliography

1. E. Brown, "NIST Issues Cloud Computing Guidelines for Managing Security and Privacy," *National Institute of Standards and Technology Special Publication 800-144*, 2012.
2. T. Bradley, *PCI compliance: implementing effective PCI data security standards*, Syngress Media Inc, 2007.
3. Protogenist Info Systems, Technology Research, "Trust challenges of Cloud computing," 2012. http://blog.protogenist.com/?p=1068 (Accessed on February 23, 2013).
4. K.M. Khan, and Q. Malluhi, "Establishing Trust in Cloud Computing," *IEEE IT Professional*, vol. 12, no. 5, 2010, pp. 20-27.
5. R. Buyya, Y. Chee Shin, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," *High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on*, pp. 5-13.
6. S. Pearson, G. Yee "Privacy, Security and Trust in Cloud Computing," 2012, ISBN: 978-1-4471-4188-4, Springer London, pp. 1-306.
7. M.B. Nick Coleman, "Cloud Security Who do you trust? IBM, 2010," 2010.
8. S. Subashini, and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11.
9. Ronald L. Krutz, and R.D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley publishers, 2010.
10. N.M. Ahmad Rashidi, "A Model for User Trust in Cloud Computing," *International Journal on Cloud Computing: Services and Architecture(IJCCSA)*, vol. 2, no. 2, 2012.
11. O.G. Mohamed Firdhous, Suhaidi Hassan, "Trust Management in Cloud Computing: A Critical Review," *International Journal on Advances in ICT for Emerging Regions (ICTer)*, vol. 04, no. 02, 2011, pp. 24-36.
12. P. Jagadpramana, Mowbray, M, Pearson, S, Kirchberg, M, Qianhui Liang, Bu Sung Lee "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," *Services (SERVICES-2011) 2011 IEEE World Congress*, IEEE, pp. 584 - 588.
13. S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," *Book Privacy, Security and Trust Issues Arising from Cloud Computing,* Series Privacy, Security and Trust Issues Arising from Cloud Computing, 2010, pp. 693-702.
14. G. Qiang, S. Dawei, C. Guiran, S. Lina, and W. Xingwei, "Modeling and evaluation of trust in cloud computing environments," *Advanced Computer Control (ICACC), 2011 3rd International Conference on*, IEEE, pp. 112-116.

15. Q.M. Khaled M. Khan, “Establishing Trust in Cloud Computing,” *Book Establishing Trust in Cloud Computing*, Series Establishing Trust in Cloud Computing, 2012, pp. 7-283.
16. M. Zhexuan Song, J.; Strong, C. , “Trusted Anonymous Execution: A Model to Raise Trust in Cloud,” *Book Trusted Anonymous Execution: A Model to Raise Trust in Cloud*, Series Trusted Anonymous Execution: A Model to Raise Trust in Cloud, 2010, pp. 133- 138
17. P.D. Manuel, S. Thamarai Selvi, and M.I.A.E. Barr, “Trust management system for grid and cloud resources,” *Advanced Computing, 2009. ICAC 2009. First International Conference on*, IEEE, pp. 176-181.
18. S. Zhidong, L. Li, Y. Fei, and W. XiaoPing, “Cloud Computing System Based on Trusted Computing Platform,” *Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on*, IEEE, pp. 942-945.
19. M.D. Alhamad, T.; Chang, E., “SLA-Based Trust Model for Cloud Computing,” *Book SLA-Based Trust Model for Cloud Computing*, Series SLA-Based Trust Model for Cloud Computing, IEEE, 2010, pp. 321 - 324.
20. H.K. Sato, A. ; Tanimoto, S. , “A Cloud Trust Model in a Security Aware Cloud,” *Book A Cloud Trust Model in a Security Aware Cloud*, Series A Cloud Trust Model in a Security Aware Cloud, IEEE, 2010, pp. 121 - 124.
21. W. TieFang, Y. BaoSheng, L. YunWen, and Y. Yi, “Family gene based Cloud Trust model,” *Educational and Network Technology (ICENT), 2010 International Conference on*, IEEE, pp. 540-544.
22. W. TieFang, Y. BaoSheng, L. YunWen, and Z. Lishang, “Study on enhancing performance of Cloud Trust model with Family Gene technology,” *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, IEEE, pp. 122-126.