INJRI
International Journal of Research Instinct
(Peer-reviewed Journal)

ISSN ONLINE 2348-2095
Research Article

An Overview and A Study of Security Issues & Challenges in Cloud Computing

[1.] **J. Rajeshwari [2.],Dr. P. Srivaramangai**
[1.]*M.Phil – Research Scholar – Department of Computer Science,* [2].*Asst Professor* - *Department of Computer Science*
Srimad Andavan Arts and Science College (Autonomous)
Trichy -5 Tamil Nadu
srivara.padma@gmail.com

INTRODUCTION

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Its advantages are few including scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud Computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome whereas the consumers need to be vigilant in understanding the risks of data breaches in this new environment. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in thirdparty data centers.[1] Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community).[2] There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software, platform, or infrastructure as a service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).

1. ARCHITECTURE

In this technology we ensure cloud storage security with the help of Kerberos authentication service. That is by implementing the Kerberos; security would be achieved for users. We define the Kerberos for create the ticket and granting ticket for each user. So to make the more focus on user we made more secure. Kerberos operation Kerberos use strong encryption method and complex ticket granting algorithm so that user can be authenticated on network. It also uses session key which allow encrypted data stream over an IP network for each user. If new user wants to use the cloud then he should make profile on network by providing information then attributes like user ID, hashed password will save in the large Data Base. All user are registered with the Kerberos server have user ID and passwords. Following steps must be taken by each user for using cloud data: Log on to workstation. Send the request for ticket granting ticket to the AS. AS verifies user’s access right in database, create ticket-granting ticket and session key. Results are encrypted using key derived from user password. User will send the request cloud service granting ticket to TGS. TGS will send the Ticket+session key to the user (it execute one per type of service). Workstation sends ticket and authenticator to cloud server provider. Server verifies ticket and authenticator match, then grant access to service. Here assumption is that each user, who connects and utilizes the cloud server, must create the profile and provide some private information for more security of his data at cloud servers.

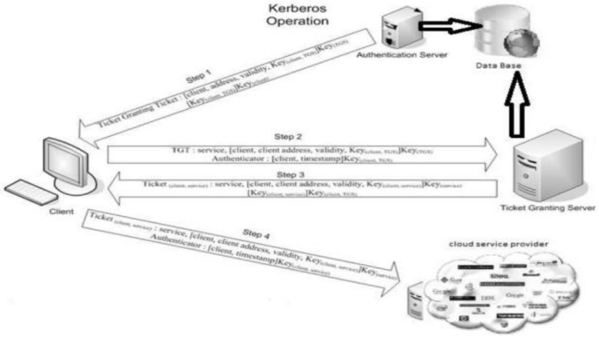
Kerberos Operation
Authentication Server
Data Base
Step 1
Ticket Granting Ticket : [client, address, validity, Key(client, TGS)]Key(TGS)
[Key(client, TGS)]Key(client)
Step 2
TGT : service, [client, client address, validity, Key(client, TGS)]Key(TGS)
Authenticator : [client, timestamp]Key(client, TGS)
Step 3
Ticket(client, service) : service, [client, client address, validity, Key(client, service)]Key(service)
[Key(client, service)]Key(client, TGS)
Client
Ticket Granting Server
Step 4
Ticket(client, service) : service, [client, client address, validity, Key(client, service)]Key(service)
Authenticator : [client, timestamp]Key(client, service)
cloud service provider

Fig:1 Cloud Data Storage Architecture

2. CHARACTERISTICS

Cloud computing can be classified based on the services offered and deployment models. According to the different types of services offered, cloud computing can be considered to consist of three layers. Infrastructure as a Service (*IaaS)* is the lowest layer that provides basic infrastructure support service.

Platform as a Service (*PaaS)* layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. Software as a Service *(SaaS)* is the topmost layer which features a complete application offered as service on demand [5]. SaaS ensures that complete applications are hosted on the internet and users use them. The payment is made on a payper-use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock" [7]. Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS [8]. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance. In the *Platform as a Service approach (PaaS)*, the offering also includes a software execution environment. For example, there could be a PaaS application server that enables the lone developer to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons. Cloud computing architectures making use of multiple cryptographic techniques towards providing cryptographic cloud storage have been proposed in [9]. *Infrastructure as a Service (IaaS)* refers to the sharing of hardware resources for executing services, typically using virtualization technology. Potentially, with IaaS approach, multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged on a pay-per-use basis [10]. They are all virtual machines, which need to be managed. Thus a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user's sensitive information. Irrespective of the above mentioned service models, cloud services can be deployed in four ways depending upon the customers' requirements:

Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party [11]. Multiple enterprises can work on the infrastructure provided, at the same time. Users can dynamically provision resources through the internet from an off-site service provider. Wastage of resources is checked as the users pay for whatever they use.

Private Cloud*:* Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider [11]. This uses the concept of virtualization of machines, and is a proprietary network.

Community cloud*:* Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider.

Hybrid Cloud*:* A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other.

3. OPPORTUNITIES

In spite of being a buzzword, there are certain aspects associated with Cloud Computing as a result of which many organizations are still not confident about moving into the cloud. Certain loopholes in its architecture have made cloud computing vulnerable to various security and privacy threats [27]. A few issues limiting the boundaries of this transformational concept are:

Privacy and Security

The fundamental factor defining the success of any new computing technology is the level of security it provides [28, 29, 30]. Whether the data residing in the cloud is secure to a level so as to avoid any sort of security breach or is it more secure to store the data away from cloud in our own personal computers or hard drives? At-least we can access our hard drives and systems whenever we wish to, but cloud servers could potentially reside anywhere in the world and any sort of internet breakdown can deny us access to the data stored in the cloud. The cloud service providers insist that their servers and the data stored in them is sufficiently protected from any sort of invasion and theft. Such companies argue that the data on their servers is inherently more secure than data residing on a myriad of personal computers and laptops. However, it is also a part of cloud architecture, that the client data will be distributed over these individual computers regardless of where the base repository of data is ultimately located. There have been instances when their security has been invaded and the whole system has been down for hours. At-least half a dozen of security breaches occurred last year bringing out the fundamental limitations of the security model of major Cloud Service Providers (CSP). With respect to cloud computing environment, privacy is defined as “the ability of an entity to control what information it reveals about itself to the cloud/cloud SP, and the ability to control who can access that information”. R. Gellman discusses the standards for collection, maintenance and disclosure of *personality identifiable information* in [24]. Information requiring privacy and the various privacy challenges need the specific steps to be taken in order to ensure privacy in the cloud

Performance Unpredictability, Latency and Reliability

It has been observed that virtual machines can share CPUs and main memory in a much better way in comparison to the network and disk I/O. Different EC2 instances vary more in their I/O performance than main memory performance [37]. One of the ways to improve I/O performance is to improve architecture and operating systems to efficiently virtualize interrupts and I/O channels. Another possibility is to make use of flash memory which is a type of semiconductor memory that preserves information even when powered off and since it has no moving parts, it is much faster to access and uses comparatively less energy. Flash memory can sustain many more I/O operations than disks, so multiple virtual machines with large number of I/O operations would coexist better on the same physical computer

4. THREATS IN CLOUD COMPUTING

In this section the major threats for cloud computing are explored. These are: i) data threats including data breaches and data loss, ii) network threats including account or service hijacking, and denial of service, and iii) cloud environment specific threats including insecure interfaces and APIs, malicious insiders, abuse of cloud services, insufficient due diligence, and shared technology vulnerabilities.

A. Data Threats

Data is considered to be one the most important valuable resource of any organization and the number of customers shifting their data to cloud is increasing every day. Data life cycle in cloud comprises of data creation, transit, execution, storage and destruction. Data may be created in client or server in cloud, transferred in cloud through network and stored in cloud storage. When required data is shifted to execution environment where it can be processed. Data can be deleted by its owner to complete its destruction. The biggest challenge in achieving cloud computing security is to keep data secure. The major issues that arise with the transfer of data to cloud are that the customers don’t have the visibility of their data and neither do they know its location. They need to depend on the service provider to ensure that the platform is secure, and it implements necessary security properties to keep their data safe. The data security properties that must be maintained in cloud are confidentiality, integrity, authorization, availability and privacy. However, many data issues arise due to improper handling of data by the cloud provider. The major data security threats include data breaches, data loss, unauthorized access, and integrity violations. All of these issues occur frequently on cloud data. In this paper, we focus on data breaches and data loss that are described as the two most severe threats to cloud computing by CSA [1].

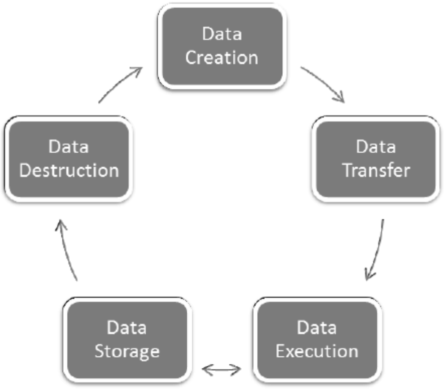

Fig.2: Data Transaction in Cloud Computing

1) Data Breaches: Data breach is defined as the leakage of sensitive customer or organization data to unauthorized user. Data breach from organization can have a huge impact on its business regarding finance, trust and loss of customers. This may happen accidently due to flaws in infrastructure, application designing, operational issues, insufficiency of authentication, authorization, and audit controls [2]. Moreover, it can also occur due to other reasons such as the attacks by malicious users who have a virtual machine (VM) on the same physical system as the one they want to access in unauthorized way. Apple's iCloud users faced a data leakage attack recently in which an attempt was made to gain access to their private data. Such attacks have also been done at other companies cloud such as Microsoft, Yahoo and Google. An example of data breach is cross VM side channel attack introduced by Y. Zhang et al.,that extracts cryptographic keys of other VMs on the same system and can access their data [3].

2) Data Loss: Data loss is the second most important issue related to cloud security. Like data breach, data loss is a sensitive matter for any organization and can have a devastating effect on its business. Data loss mostly occurs due to malicious attackers, data deletion, data corruption, loss of data encryption key, faults in storage system, or natural disasters. 44 percent of cloud service providers have faced brute force attacks in 2013 that resulted in data loss and data leakage [4]. Similarly, malware attacks have also been targeted at cloud applications resulting in data destruction.

B. Network Threats

Network plays an important part in deciding how efficiently the cloud services operate and communicate with users. In developing most cloud solutions, network security is not considered as an important factor by some organizations. Not having enough network security creates attacks vectors for the malicious users and outsiders resulting in different network threats. Most critical network threats in cloud are account or service hijacking, and denial of service attacks.

1) Account or Service Hijacking: Account hijacking involves the stealing of user credentials to get an access to his account, data or other computing services. These stolen credentials can be used to access and compromise cloud services. The network attacks including phishing, fraud, Cross Site Scripting (XSS), botnets, and software vulnerabilities such as buffer overflow result in account or service hijacking. This can lead to the compromise of user privacy as the attacker can

eavesdrop on all his operations, modify data, and redirect his network traffic. 1n 2009 a legitimate service was purchased from Amazon's EC2, and compromised to act as Zeus botnet [5].

2) Denial of Service: Denial of Service (DOS) attacks are done to prevent the legitimate users from accessing cloud network, storage, data, and other services. DOS attacks have been on rise in cloud computing in past 5 years and 81 percent customers consider it as a significant threat in cloud [1]. They are usually done by compromising a service that can be used to consume most cloud resources such as computation power, memory, and network bandwidth. This causes a delay in cloud operations, and sometimes cloud is unable to respond to other users and services. Distributed Denial of Service (DDOS) attack is a form of DOS attacks in which multiple network sources are used by the attacker to send a large number of requests to the cloud for consuming its resources. It can be launched by exploiting the vulnerabilities in web server, databases, and applications resulting in unavailability of resources.

C. Cloud environment specific threats

Cloud service providers are largely responsible for controlling the cloud environment. However, a survey report by Alert Logic [4] shows that almost 50 percent of the cloud users consider service provider issues as a major threat in cloud computing. Apart from service provider threats, some threats are specific to cloud computing such as providing insecure interfaces and APIs to users, malicious cloud users, shared technology vulnerabilities, misuse of cloud services, and insufficient due diligence by companies before moving to cloud.

1) Insecure Interfaces and APIs: Application Programming Interface (API) is a set of protocols and standards that define the communication between software applications through internet. Cloud APIs are used at all the infrastructure, platform and software service levels to communicate with other services. Infrastructure as a Service (IaaS) APIs are used to access and manage infrastructure resources including network and VMs, Platform as a Service (PaaS) APIs provide access to the cloud services such as storage and Software as a Service (SaaS) APIs connect software applications with the cloud infrastructure. The security of various cloud services depends on the APIs security. Weak set of APIs and interfaces can result in many security issues in cloud. Cloud providers generally offer their APIs to third party to give services to customers. However, weak APIs can lead to the third party having access to security keys and critical information in cloud. With the security keys, the encrypted customer data in cloud can be read resulting in loss of data integrity, confidentiality and availability. Moreover, authentication and access control principles can also be violated through insecure APIs.

2) Malicious Insiders: A malicious insider is someone who is an employee in the cloud organization, or a business partner with an access to cloud network, applications, services, or data, and misuses his access to do unprivileged activities. Cloud administrators are responsible for managing, governing, and maintaining the complete environment. They have access to most data and resources, and might end up using their access to leak that data. Other categories of malicious insiders involve hobbyist hackers who are administrators that want to get unauthorized sensitive information just for fun, and corporate espionage that involves stealing secret information of business for corporate purposes that might be sponsored by national governments.

3) Abuse of Cloud Services: The term abuse of cloud services refers to the misuse of cloud services by the consumers. It is mostly used to describe the actions of cloud users that are illegal, unethical, or violate their contract with the service provider. Abusing of cloud services was considered to be the most critical cloud threat in 2010 [2], and different measures were taken to prevent it. However, 84 percent of cloud users still consider it as a relevant threat [1]. Research has shown that some cloud providers are unable to detect attacks launched from their networks, due to which they are unable to generate alerts or block any attacks. The abuse of cloud services is a more serious threat to the service provider than service users.For instance, the use of cloud network addresses for spam by malicious users has resulted in blacklisting of all network addresses, thus the service provider must ensure all possible measures for preventing these threats. Over the years, different attacks have been launched through cloud by the malicious users. For example, Amazon’s EC2 services were used as a command and control servers to launch Zeus botnet in 2009 [6]. Famous cloud services such as Twitter, Google and Facebook as a command and control servers for launching Trojans and botnets. Other attacks that have been launched using cloud are brute force for password cracking of encryption, phishing, performing DOS attack against a web service at specific host, Cross Site Scripting and SQL injection attacks.

4) Insufficient Due Diligence: The term due diligence refers to individuals or customers having the complete information for assessments of risks associate with a business prior to using its services. Cloud computing offers exciting opportunities of unlimited computing resources, and fast access due which number of businesses shift to cloud without assessing the risks associated with it. Due to the complex architecture of cloud, some of organization security policies cannot be applied using cloud. Moreover, the cloud customers have no idea about the internal security procedures, auditing, logging, data storage, data access which results in creating unknown risk profiles in cloud. In some cases, the developers and designers of applications maybe unaware of their effects from deployment on cloud that can result in operational and architectural issues.

5) Shared Technology Vulnerabilities: Cloud computing offers the provisioning of services by sharing of infrastructure, platform and software. However, different components such as CPUs, and GPUs may not offer cloud security requirements such as perfect isolation. Moreover, some applications may be designed without using trusted computing practices due to which threats of shared technology arise that can be exploited in multiple ways. In recent years, shared technology vulnerabilities have been used by attackers to launch attacks on cloud. One such attack is gaining access to the hypervisor to run malicious code, get unauthorized access to the cloud resources, VMs, and customers data.Xen platform is an open source solution used to offer cloud services. Xen hypervisors code creates local privilege escalation (in which a user can have rights of another user) vulnerability that can be launch guest to host VM escape attack. Later, Xen updated the code base of its hypervisor to fix that vulnerability. Other companies such as Microsoft,Oracle and SUSE Linux that were based on Xen also released updates of their software to fix the local privilege escalation vulnerability. Similarly, a report released in 2009 [7] showed the usage of VMware to run code from guests to hosts showing the possible ways to launch attacks.

5. SOLUTIONS AND TIPS TO CLOUD SECURITY ISSUES

There are several groups interested in developing standards and security for clouds and cloud security. The Cloud Security Alliance (CSA) is gathering solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud (Cloud Security Alliance (CSA) – security best practices for cloud computing, 2009). The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups (Clouds Standards, 2010). There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud. For this a layered framework is available that assured security in cloud computing environment.

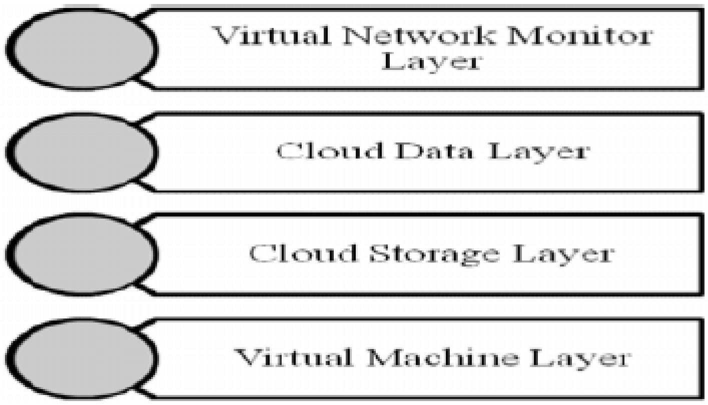

Fig.3: Layered framework in Cloud Computing Environment

First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer. This layer combining both hardware and software solutions in virtual machines to handle problems such as key logger examining XEN. However, there are several groups working and interested in developing standards and security for clouds. The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups. The Cloud Security Alliance (CSA) is one of them. CSA gathers solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. Another group is Open Web Application Security Project (OWASP). OWASP maintains a list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes. The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers. There are some tips and tricks that cloud security solution providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution. Verify the access controls: Set up data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer. To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumer’s data. Control the consumer access devices: Be sure the consumer’s access devices or points such as Personal Computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. The loss of an endpoint access device or access to the device by an unauthorized user can cancel even the best security protocols in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features.

Monitor the Data Access:

Cloud service providers have to assure about whom, when and what data is being accessed for what purpose. For example many website or server had a security complaint regarding snooping activities by many people such as listening to voice calls, reading emails and personal data etc. Share demanded records and Verify the data deletion: If the user or consumer needs to report its compliance, then the cloud service provider will share diagrams or any other information or provide audit records to the consumer or user. Also verify the proper deletion of data from shared or reused devices. Many providers do not provide for the proper degaussing of data from drives each time the drive space is abandoned. Insist on a secure deletion process and have that process written into the contract [30].

Security check events:

Ensure that the cloud service provider gives enough details about fulfillment of promises, break remediation and reporting contingency. These security events will describe responsibility, promises and actions of the cloud computing service provider [31].

Web Application Solutions:

The best security solution for web applications is to develop a development framework that shows and teaches a respect for security. Tsai, W. et al. put forth a four-tier framework for web-based development that though interesting, only implies a security facet in the process [33]. "Towards best practices in designing for the cloud" by Berre, Roman, Landre, Heuvel, Skår, Udnæs, Lennon, & Zeid (2009) is a road map toward cloud-centric development, and the X10 language is one way to achieve better use of the cloud capabilities of massive parallel processing and concurrency (Saraswat, Vijay, 2010).

Accessibility Solutions:

Krügel, C., Toth, T., & Kirda, E. (2002) point out the value of filtering a packet-sniffer output to specific services as an effective way to address security issues shown by anomalous packets directed to specific ports or services. An often-ignored solution to accessibility vulnerabilities is to shut down unused services, keep patches updated, and reduce permissions and access rights of applications and users.

Authentication Solutions: Halton and Basta , suggest one way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged

Data Verification, Tampering, Loss and Theft Solutions:

Raj, Nathuji, Singh and England (2009) suggest resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache. Hayes points out that there is no way to know if the cloud providers properly deleted a client's purged data, or whether they saved it for some unknown reason.

Privacy and Control Solutions:

Hayes (2008) points out an interesting wrinkle here, "Allowing a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to a document if you fail to pay a bill?". The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.

Physical Access solutions:

One simple solution, which Milne (2010) states to be a widely used solution for UK businesses is to simply use in-house "private clouds".

6. CONCLUSION

Cloud, is prone to manifold security threats varying from network level threats to application level threats. In order to keep the cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like security issues, accessibility issues, confidentiality, integrity of data. Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. In addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning. In this paper various security concerns related to the three basic services provided by a Cloud computing environment are considered and the solutions to prevent them have been discussed.

7. FUTURE WORK

In this survey, we studied several key security concerns for Cloud computing environment from multiple perspective and the solutions were discussed that all users and organizations should be aware of, when deciding whether to use the cloud or not and this paper helps to find out the solution for the drawbacks found in other methods and come up with new solution or method to secure the cloud.

8. REFERENCES

[1]. http://en.wikipedia.org/wiki/Cloud_computing#History

[2]. http://mp3.about.com/od/glossary/g/Cloud-Storage-Definition-What-Is-Cloud-Storage.htm

[3]. Jacob R. Lorch, David Molnar, Helen J. Wang, and Li Zhuang,' Enabling Security in Cloud Storage SLAs with CloudProof', Microsoft Research.

[4]. Enabling Security in Cloud Storage SLAs with CloudProof. Cloud security still the biggest concern/hurdle for google, microsoft,verizon.www.taranfx.com/blog/.

[5]. http://technet.microsoft.com/en-us/library/cc700811.aspx

[6]. http://www.trustedcomputinggroup.org

[7]. http://www.tar.hu/wininternals/ch12lev1sec8.html

[8]. Sushama Karumanchi ,'A TRUSTED STORAGE SYSTEM FOR THE CLOUD',July 08, 2010

[9]. http://www.trustedcomputinggroup.org

[10]. TCG Published,' TPM Main, Part 1, Design Principles', 9 July, 2007.

[11]. Mehdi Hojabri,' Ensuring data storage security in cloud computing with effect of Kerberos'**,**Vol. 1 Issue 5 , July - 2012 ISSN: 2278- 01 8