A Detailed Study on Security Threats and Issues In Cloud Computing and Its Reduction Techniques

[1]G. RAMESH KUMAR
[1]*Assistant Professor*
Dept. of Computer Science & Applications
Adhiparasakthi College of Arts & Science
G.B.Nagar, Kalavai – 632 506, Vellore District
Tamil Nadu, INDIA

[2]S.HARIKUMAR
[2]*Research Scholar*
Dept. of Computer Science & Applications
Adhiparasakthi College of Arts & Science
G.B.Nagar, Kalavai – 632 506, Vellore District
Tamil Nadu, INDIA

ABSTRACT
Cloud computing is a new technology model for facilitating suitable, on-demand access to a public computing systems. These shared resources may be a network, a group of networks, servers and storage appliances and services that eliminates the requirements of implementing high-cost system architecture for all information technology services a sector requires. It gives an elastic and a non-standard architecture yet easily accessible through internet from any computing device. Cloud allows multifold increase of storage capacity and capable of accessing any kind and any source of data from the existing or new software. It is one of its state of the art architecture that the whole record presides over a group of associated systems. These network enabled resources enables the data accessing throughout virtual machines. Hence, the data centers might locate in any part of the world away from customer location. But, one has to understand that various issues need to be understood before getting into a new technology of architectural framework. There needs to be addressed a variety of sensitive security issues along with the seclusion in a cloud architecture. This widespread paper aspires in elaborating and analyzing the abundant non-resolved problems which are threatening the overall architecture of cloud computing acceptance and disseminations that affects the people associated.

Keywords: ***Cloud Computing, Network Level Security, Application Level Security, Multilayer Security***.

I. INTRODUCTION
Cloud is a visible gathering of a huge amount of information at a particular place. Recently, many new technologies have been arising everyday for the access of data over the internet from a specific location. Perhaps, Cloud Computing is the most discussed among all of them. In the last few years of technological era, the cloud computing protocol has witnessed a massive shift to its adaption. This comes as a new style in IT as its guarantee the overall cost reduction and new business potential for all users and providers.

Cloud computing has its own specific characteristics that distinguish it from traditional resource management and service provisioning environments: i) it is more scalable, ii) it provides an infrastructure for platform for application, iv) cost effective, v) major cloud service providers already invested in large scale to exploit it, vi) non-agreed interfaces, vii) provides data centers for outsourcing, viii) has security as a major concern if a business shifts its expensive data, information or knowledge for its outsourcing, ix) has huge risks in terms of business continuity depending on cloud – where there are many examples of failures of industry giant companies, x) limitations in data shipping over the speed allocated or availability

There are plenty of definitions given explaining about cloud computing as it is a form for permitting omnipresent, more suitable and accessible which may easily preconditioned and upgraded by minimum manageable attempts that provides interactions needed. If this is the point of architecture, the users need not have to be worried about the infrastructure. This integrated aspect supports high scalability and enhanced flexibility when compared to early existed computing methodologies. Cloud can be easily able to allocate, reallocate or deploy resources with dynamism with an increased ability to monitor continuously their speedy performance.

II. TAXONOMY OF CLOUD, ITS DISTINCTIVENESS AND ADVANTAGES

A. CLOUD TAXONOMY
Cloud computing has been broadly categorized on the services available. Cloud computing may be organized into three different layers as per the service type depends.

i) Infrastructure as a Service (IaaS) : The low level layer which endow with the basic network platform
ii) Platform as a Service (PaaS) : The middle layer present platform tilting services for application hosting
iii) Software as a Service (SaaS) : The top layer of the overall model that offers on demand services.

i. Software as a Service (SaaS) ensures whether overall application is hosted on the internet for users use. This application model payment can be utilized as we go, pay peruse model. SaaS eliminated the installation need and running an application on a desktop or a users system which can be also be a desktop. And so, it alleviates the users trouble for maintaining an application locally.

SaaS exploit two types of servers:

a. Main Consistence Server (MCS)
b. Domain Consistence Server (DCS)

The coherence can be achieved by the mutual aid of these two servers. If MCS gets damaged, the overall users control over the cloud will be lost. Hence, huge security has been given of much importance for this main consistence server.

ii. Platform as a Service (PaaS) is a software executing application environment. In this server, the programmer can set up the online web model software. The user doesn't need to buy the actual server(s) for setting them. PaaS aims to secure the data on its server only if it acts as a stored service. Thus, in jamming, here always a difficulty which has to given of much importance to ensure balanced service. Every time, the data has to be encrypted during hosting for security reasons. Hence, cloud uses multiple cryptographic techniques and our paper proposed cryptographic cloud storage.

iii. Infrastructure as a Service (IaaS) is allocation all hardware parts for executions. Especially, by means of virtual technics. Prospectively, in this model, several customer access obtainable data on the cloud. Thus, it assist in achieving abandoned right of entry to data.

B. DEPLOYMENT TYPES

Clouds may be hosted and employed into different styles according to the use, but especially depend on the kind of business model. The major deployed categories are as follows:

i. Public Cloud: A third party will be managing the cloud infrastructure consists of many customers. Accessing data dynamically providing resources over the internet from a remote service provider. Users need not have to pay for the data which was not used or wasted.

ii. Private Cloud: This type of is only available to a precise user administered by the enterprise. Private cloud applies on virtualization machine conception.

iii. Community cloud: This type of architecture will be collective of multiple enterprises for a grouped task.

iv. Hybrid Cloud: Hybrid cloud is a composition of two or more cloud deployment models. The data transferring will takes place between the multiple users without affecting each other.

As the technological advancement keeps growing, the cloud deployment models emerge everyday to support and compete with the emerging need and demand, depending upon the users requirements. Cloud computing is getting a turn-around to its new faces of interfaces in its environment. This in order, coined to the term 'Mobile Cloud Computing (MCC)'. And, to the interest, it is becoming a trend nowadays that many MNC's and major organizations are likely providing their data accessing through employees mobile devices when they are at office through office network.

The earlier computing technology paradigms such as Internet computing and Grid Computing had now been put apart in front of Cloud Computing, is a distinguished feature of itself for its on demand service.

II. TECHNIQUES

A few techniques that add privilege to cloud computing are:

i. Virtualization: The underlying concept for the base for emergence of Cloud Computing in this technology era is the Virtualization. The key term refers to an environment that provides all the services supported by hardware's that local computers encompass with it.

Virtualization can be categorized into three forms which are under existence:

- Server virtualization
- Storage virtualization and
- Network virtualization

ii. Web Service and SOA: The web technologies such as XML, WSDL, SOAP, etc., are used to grant service over the web. The cloud is managed internally by a service oriented architecture (SAS). Hence, we call SOA as the controller over a managed multiple server.

iii. Web 2.0 / Mash-up: The technology Web 2.0 acts as a collaborative platform on the World Wide Web technology. The new web application called the Mash-up combines data from multiple source to a single online integrated storage area.

These are the major technologies that made many multi-national corporations to let them avail free from storing and accessing data and entered into a bother free world of virtualization.

Few prominent clouds are:

- Salesforce.com
- Right Scale
- Google
- Microsoft Windows-Azure
- SimpleDB
- Sun Microsystems
- S3 (Simple Storage Service)
- CF (Cloud Front)
- Amazon's Elastic Compute Cloud – EC2
- Workday

Each of the above are categorized either under one of the three main categorization of cloud structure: private, public and hybrid. Each has its own limitations and delimitations.

It is well understood the changes that keeps changing and it is witnessed in the IT sector. However, the issues that still exist are becoming more complex. The on-demand application usage has been increasing is directly proportional to its cyber attacks. The individuals have to provide their identifications and keep updating and this may reduce the use of attackers by identified theft. In order to overcome the security threats, attacks and privacy issues like integrity, confidentiality, etc.

To maintain high security standards against known threats to data security,

- An encryption scheme has to be made-up.
- Limiting access to the data to their users and to manage it.
- Strict access controls will prevent from illicit and illegal access to the servers over the network.
- Regular back-up of data and redundant data storage will help in case of network failure. For example, the recent failure issues held with Amazon.

One of the major aspects of this model of accessing data leads to a huge rise in number of security attacks in data storage security for few concerns. The data which is stored in a cloud is accessed several times and all are subjected to different kinds of changes applied to it.

This paper aims at increasing and considering diverse issues hampering user confidentiality.

III. BARRIERS AND OPPORTUNITIES IN CLOUD COMPUTING

Regardless the changing trend in IT world, there are certain things which are associated with Cloud Computing which resulted in organizations that are not sure in adopting cloud. There are certain things which have made cloud computing more susceptible to a variety of security threats. We study a few issues that limit the restrictions of this revolutionary concept.

A. Privacy and Security

It is a predefined factor that the success and failure is determined by the protection it gives to its users. It is easy to access our personal computers hard drives whenever we wish. But, in a cloud computing architecture, if there evolves an internet slowdown or limited connection we were denied accessing to our own data. Though, over the cloud architecture, the data is distributed over many individual systems regardless of their base location. There are many instances where the security has been overrun many a times which are down for many hours.

In a public cloud, there are many security issues that need to be addressed as the cloud acts with a number of virtual computers, monitors and supporting components. The security of the cloud depends on these objects and their behavior and object interaction between them. The security risks get increased when the number of users increased in a public cloud. Thus, adapting to a private cloud has become an innate solution for moving from a public cloud.

Materialization of cloud computing has obliged to mash up. A mashup is a new kind of function that merges data from multiple sources and develops new services out of it. As this involves usage of many sub-elements for a specific task, the security risks become more extensive. Upon these, different security architectures have evolved. Such as, a model based on entropy framework using service mashups. But also, the security in privacy needs to be retained at every stage since there are chances for an outsider to enter inside.

B. Performance Unpredictability, Latency and Consistency

A VM allocates CPU in a good way when compared with network and disk input output. EC2 may vary in i/o operation performance than the main memory. So, we need to enhance the i/o performance by improving the base structure of the cloud. Another way is to make use of a semiconductor memory that preserves data even when there is no power and it is much faster in accessing data which consistently consuming less energy.

When traffic goes high congestion comes up and there may be many requests of same priority and needs to be executed at same degree. Another method is windowing where the receiver needs to send a message to the sender. Whatever the fact, the presentation of the system which is used to operate is a major factor and need to be considered. This adds to system latency and affects the performance.

C. Portability and Interoperability

Many organizations wants to change their existing cloud service providers but there have been many cases where companies are unable to shift their data from one platform to other. Such migration impossibility is called as Lock-in.

In case of SaaS, during migration, there may not be applicable data format available with the new service provider and as it requires a new application to be developed by them. This requires an additional effort and needs to ensure any data loss during the process. Additionally, performing regular data backup and extraction is usable without SaaS application. The platform needs to be taken care during integration between the major interfaces.

In case of PaaS lock-in, the language may not support the other cloud service provider and that becomes a major issue. Different API's need to be developed for data view ability. Lock-in in this platform could be avoided if we address the following:

- PaaS cloud should be made as non-closed model and typical structure supporting ought to be developed.
- Performing on understanding the various application components and modules which are more specific to PaaS service providers along with the basic services such as logging, scrutinizing, etc.,
- Understanding the control functionality specific to Paas service providers.

Common lock-in is data lock-in. One option is, identifying the hardware dependencies may minimize such issues during migration. The companies have to be clear in choosing right choice that matches their business operations and technical requirements.

D. Breaching Data through Fibre Optic Cables

The data transit is increasing in last few years in favor of its security risks involved. Transitioning of data is an usual activity today and so it may include many data centers. Data centers have breaches many times now-a-days. The data are transferred through fibre-optic cables over a network and it was considerably a safe mode. But recently, in a US based firm named Telco Verizon, a mutual fund company, an illegal fibre snoop the data flew through it. Many devices have come in the market that taps the data flow without disturbing the cable. Hence, ensuring data security over transition network has given much importance.

E. Storage of Data over IP

Data stored over internet protocol is becoming quite popular now-a-days. It is to be accepted by all of us that almost all the enterprises will network their operations in the future since it allows huge amount of data. This exist more security threats where new threats are evolving day by day despite of it mass advantage. These network devices are classified into SAN (Storage Area Network) and NAS (Network Attached Storage) based on their level of operations and storage capability. This storage resides at various server at various locations along with it various security threats and vulnerability of data storage over a network is big.

Apart from normal cloud, in a mobile cloud computing, more challenges have to be considered.

- **Network accessibility:** Online accessing over the secure Internet Protocol is the reason of evolution of cloud computing and without it nothing is possible in a mobile cloud.
- **Data Latency:** It is more reliable transferring data through a wired LAN than accessing over a wireless network. The interval may be longer time and is responsible for it because of its intermediate networking mechanism.
- **Confidentiality in data sharing:** MCC may become public when its root level access hacked. There is a much possibility for data accessibility from a stolen device where it becomes even more critical when the stolen device was an administrator that contains many confidential data.
- **Better access control and identity management:** The user authentication and access control is high on mobile cloud since it involves virtualization concept. The existing models cannot handle multiple users since multiple user's data will be stored on a single hypervisor of the cloud.

IV. DATA SECURITY AND STORAGE IN A CLOUD

Most service providers offer SaaS. Many service providers adopt themselves many new technologies in order to guarantee security on the cloud. But, is the data actually secure over the cloud architecture? The old method for handling security issues on virtualized cloud system is of no more a security protector. A parallel modus operandi that utilizes homomorphism token with a distributed erasure-coding method could

be applied to ensure such security. There are several other models such as Trust Based Model that will be useful in establishing relationships in a networked and distributed environment and Domain Based Trust-Model is used to hold security and interoperability.

The following needs to be taken care before shifting to a new cloud service provider:

i. Data-in-transit
ii. Data-at-rest
iii. Data Lineage
iv. Data Remanence
v. Data Provenance

In data-in-transit, encryption technology is uses that is associated with a huge risk for it non enhancement in updated protocol. Just using the technology will not put an end to the security. Additionally, an encryption-decryption algorithm should be applied for secure data transferring. When we apply, the data will be broken into packets and then transferred.

Data provenance is maintaining integrity of the data in a cloud. And, this is at a higher risk in security providence. Data remanence is yet another that keep neglected by the service providers. This is the data left out after data removed or transferred and it is minimal in a private cloud.

In the recent past, many security threats and issues have been seen by major organizations.
Some are: Epsilon, an email marketing company, suffered by a huge data of its customers was exposed to the attackers. Customers including JP Morgan Chase, Marriott Hilton, Best Buy, Citi Bank, Barclays Bank, etc. The data accessed also included customer email ids and bank details.

Similarly, with Amazon, the EC2 was disrupted by hackers. Quora and Four-Square are the major sufferers out of it. These portray the susceptibility of the cloud services.

V. SECURITY THREATS IN A CLOUD COMPUTING MODEL

"Trust us" is the word or idea for cloud business. Proving their customers an multi-level security and multi-tenancy besides more comfort. Security needs a holistic approach. This has been classified based on the nature of the service provided. Network Level Security and Application Level Security are the main classifications on how the service provider serves for an enterprise. Based on these different levels, diverse security breaches may evolve every day.

A. Essential Security

Web 2.0 is a major technology in SaaS that relieves users from maintenance and installation of specific software. The community is adding its users countless by leaps and bounds. Such a environment needs to be addressed much and given of more importance.

SQL injection attacks is a breach where a malicious code is introduced in standard SQL code. So, the hackers can gain accessing the data. Perhaps, the introduced code may be misunderstood by the cloud and allows accessing the SQL server and attackers get to know the functionalities of the cloud application. Many techniques such as i. Avoiding dynamic SQL code generated for usage, ii. Using filtration techniques that cleans the user input and checks the injection attacks. So, a proxy based architecture prevents such attacks and that dynamically detects and extracts user inputs.

XSS attacks also known as Cross Site Scripting where malicious scripts are injected in the web content. This has become more familiar after the emergence of Web 2.0. Injections can be done using two methods, one is Stored XSS and the other one is RXSS. In Reflected XSS, the attack is not stored permanently.
Dynamic websites victim by XSS attacks. These attacks enters when users either knowingly or unknowingly. Technologies such as Active Content Filtering, Web Application Vulnerability Detection, and Content-Based Data Leakage Prevention can be adopted and various methodologies detects security issues and fixes them accordingly.

Man in the Middle attacks shortly known as MITM is popular in SaaS, is an attack where a new entity tries to break-in during a conversion going on between the client and the sender. These type of attacks injects false information. Dsniff, Wsniff, Airjack, etc., are some of the few developed encryption technologies to prevent data in a cloud.

Hence, we study that security is at required at different levels to ensure suitable cloud computing infrastructure. Security in Server Access, Database Access, Internet Access, Data Privacy, and Program Access are the critical levels of security where we need to provide an appropriate solution.

B. Network Level Security

There are many classifications in networking. Such as public and private, shared and non-shared, small or large area networks, etc., where each one has its kind of security threats that harms the overall system. There occurs always a less vulnerability in a private when compared with a public cloud. Most of the organizations prefer private cloud service rather than

public even though private is costlier yet secured to some extent. This is because, in a public cloud, to implement advanced new features advanced network topology must be adopted. The following shows some of the points to be addressed in a public cloud.

- Ensuring confidentiality and integrity in data-in transit in the architecture
- We must ensure proper access to cloud using specific controls for each operation.
  - The entire cloud system works on the basis of internet accessibility that has a big chance for data leakage or security breach. This must be handled very specifically.
  - Security policies over a cloud have to be updated every time to prevent our own resources when new threats evolve. There is always a problem of accessing others data in a public cloud.
- Checking and updating the trusted encryption schemes and as well as tokenization models must be taken care of by the security alert team.

Some of the network level security issues are in round are DNS attacks, issuing re-used IP addresses, DoS attacks and DDoS attacks, BGP Prefix Hijacking and Sniffer attacks.

C. Application Level Security

The outdated network level security policies provide access to attackers even though the data is allowed to access by the authorized user from a specific IP. This has become obsolete since the technological advancements has reached to its high and attackers use many new methodologies to hijack any system.

With advanced technology, anything is possible in an application level security. It is very easy to imitate like a trusted user that too without even notifying to the user who is accessing the data and collapses and corrupts the entire data.

The task oriented and traditional method of ASIC provides better security with higher performance. Even though, since application level threats are dynamic, it needs to be clearly watched every time and should prevent it by adopting various security checks.

Adopting open ended system along with the capabilities of a closed system can be used to develop a Check Pont System will be one of the good security platform. In VMware, they use Intel virtualization technology in their virtual infrastructure for better security and performance. It is to be understood that, whatever the technology we use, the websites are more often the main object for the hijackers that has many loopholes to access information by an unauthorized user. Some of the application level securities are SQL injection attack, Hidden Field Manipulation, XSS attacks, Cookie Poisoning, DoS attacks, Debug option attacks, Captcha breaking, Google Hacking, Dictionary attack, etc.,

VI. SECURITY ISSUES IN THE CLOUD DEPLOYMENT MODELS

All the major cloud deployment models have its own advantages and disadvantages. Each one of the deployment models have certain areas that needs to be addressed to avoid security breaches that occurs.

A. Security issues in a public cloud

Since the security provided is shared one on a public cloud, we see some of the key issues on a public cloud.

1. Confidentiality, Integrity and Availability are the three key points to be addressed to protect data throughout the cloud life. At each stage of creation, updating, sharing, processing, etc., data must be protected by implementing various security practices. Situations in a public cloud are becoming more complicated where we don't have any control on the security protections provided by the service providers.
2. There are many chances for data leakage in a public cloud since, the resources are shared between multiple clients over the same infrastructure. To avoid such security risks, proper study about the provider needs to be made.
3. The cloud user must ensure what are the service level agreements between the service provider and the third party vendor since most of the service providers uses these third party vendors. Appropriate contingency tactics to be known before signing an ink-pact. Otherwise, it will be a higher risk if there occurs any disputed between the service provider and the third party vendor.
4. Service Level Agreements (SLA) must be defined properly for how the encrypted data send over the web and what the penalties for such happenings are.

Although it is understood what the security over a cloud is, we could not deny the possibilities of getting insiders accessing illegally. This clearly shows that the cloud expands the base by providing an access to any number of users at the same time. An access control policy should be shared between both the sides for prevention. Implementing policy enforcement at the data centers and nodes may prevent from such harms.

To achieve these, we must do the following:

a. Define a policy
b. Propagate the policy by dissemination element
c. Implementing the dissemination element

B. Security issues in a private cloud

Providing security on a private cloud is easier when compared to a public cloud over the network. In a private cloud, the users have the overall control and there is a flexibility to implement any security practice by the user itself. Although private cloud is easily accessible and reliable, there are issues to be addressed in its architecture.

1. Hypervisor should be analyzed in a private cloud since it is of a virtualization technique. There are many instances when a guest is running a process on other guest's host. It is possible in virtual machines to communicate with everyone.
2. The host system should be kept free to enter any kind of security threats and to be monitored. A physical infrastructure must be developed for this type of communication.
3. Users are facilitated to manage some portions on the cloud by accessing the infrastructure through the web interface. For this, there are two different ways for implementing such interface. One is using a Standard Applicative Stack and the other is developing the whole application.
    - During the screening process, it is found that Eucalyptus interface has a bug that allows any user to perform to scan the internal ports. This must be avoided.
4. In most of the instances, the key vital point will be missed that stress be the mostly seen upon providing the security. When we look for a standard internet security, we should also look for standard security policies to protect our system. There should be maintained a proper guidelines for security in each departments and implemented as per the requirements.

Thus, we found, that the study shows that even though private cloud model seems to be much safer when compared with public cloud model, they still have many issues. If we don't look after it seriously or unattended, this may lead to a huge disaster for our own resources stored over the cloud.

A secured and trusted cloud security model is proposed recently known as "Security Aware Cloud" may be used to deploy. Internal and Contracted Trust Layers are the two additional layers of this trust security cloud model to enhance the security over the cloud infrastructure.

VII. ENSURING SECURITY AGAINST THE DIVERSE ATTACKS

Different cloud service providers use different techniques to secure cloud from multiple security threats and attacks. We studied some of the security threats like XSS attacks and other attacks.

A few techniques that are used to detect these attacks include:

i) Avoiding dynamic SQL codes generated during usage
ii) Meta-structure finding in the code
iii) Validating all parameters entered by the user
iv) Not allowing and removing redundant typeset, etc.,

This framework should act as an interface between the cloud environment and the user. The service provider should be able to detect the personalized security practices. Symantec Message Labs uses the same approach for their web security over the cloud that blocks the new threat entrants and filters before they actually reaches the network system. This web security cloud security system architecture acts with the major two components:

1. **Multilayer Security**
   Multilayer security platform provides data security and block the possible entrants from entering into the network.
2. **URL Filtering**
   An attack mostly enters through web pages and websites. So, filtration of such attacks may protect our web pages and sites from harming which are accessible. And, this URL filtering will blocks contents from unknown websites.

This system provides security for highly conflicting environments and ensures proper protections against emerging malwares.

One of the big and well-known cloud service providers in the market is Amazon where it uses multi-layer and multi-factor authenticating techniques. Thus, Amazon provides an enhanced security model with an control over AWA account settings and subscribed services management.

In Google Hacking, the database has many kinds of data in it. They can be User Logon Details, Login Passwords, Login Gateway logging using these passwords, Usage session Information, etc., A perfect and efficient method to identify and detect such

entrants are Web Vulnerability Scanner be able to be used in case of Google Hacking.

The main issues in attacks of DoS and DDoS are:

i) The speed of the system gets reduced
ii) Programs run more slower than unexpected
iii) Restrictions to use the available resources
iv) Receiving numerous connection requests from illicit users and so on,

Though the DDoS attacks are less harmer over the network, it still needs to be monitored carefully. A new approach based on Game Theory to act against bandwidth which was recently proposed can be applied to overcome from such issues. In this approach, there will be an interaction between the user and the attacker. This will be like a two play non zero with double situations. They are:

i. Single Node Attacking and
ii. Multiple Node Attacking

Based on these nodes, the user can be able to determine the firewall settings so as to block the unauthorized users requests and shall allow the authorized users.

In IP spoofing, the threat will be in accessing the data destination. The attackers spoof the users by creating and impression and try to know the packets coming from the reliable sources. In this way, the attacker may take the full control of a user.
Sales Force implemented a new security method to avoid unauthorized access by sending a secret security code to access from a same IP address or a different one. Every time the registered user needs to provide the secret code to prove his identity.

In data-transit, the security for the data transmission could be accomplished by applying cryptology design. A new practice for this threat ensuring is Steganography.

It is a big problem that in a virtual machine, the traffic passing between two VM's will not travel out of its network. Certain applicable methodologies should be adopted to ensure such security issues.

Some of the methodologies include:

i) Checking Virtual Machines that are linked to the host system
ii) Constantly monitoring the activities of these virtual machines
iii) Securing these host systems to avoid tampering and updating when these VM's are offline, etc.,

VIII. CONCLUSION

Cloud has been dominating the Information Technology world today. A foremost change to this model might be explored even more in forthcoming years. Many of the organizations have already started to this new trend of storing and accessing their own resource over a virtualized environment in the name of Cloud. Some of the major organizations and their cloud model are: CRM Solutions of SaaS platform from Sales Force by Schneider Electric, Toyota's signing with Microsoft for its automobile delivery network on Azure platform, etc. Apart from these, more number of organizations are moving forward towards cloud with the materialization of NoSQL technology such as Cassandra which are facilitating and attracting more customers for their advantage over collecting and storing a massive amount of data. Cross cloud connectivity and integrations has made cloud as a better environment to adopt it with feasible data migration. With the increase in number of high end mobile users which has accessibility internet technologies and tablet users have made the way for new cloud service deployments along with considering the enhanced security and this has already increased the user's base over the cloud. Technologies such as HTML 5, Ruby on rails will be continuing to improve the experience.

Even though, the cloud system had transformed IT enterprise, it still lying its face down when comes to see a numerous amount of security threat. The security may vary from network level system to application level system. Making the environment safer, the entire infrastructure should be well secured and appropriate deployment schemes should be applied to control these attacks. And also, data accumulated is a flat to multiple issues like confidentiality as well as data integrity. This should be considered before moving to a service provider. Cloud should be audited at regular time of intervals in order to safeguard it against external threats and attacks. The cloud service has a major role in ensuring the security alone and must ensure providing all the security guards provided in the SLA's are met. Service provider should control or minimize human errors. In this paper, we studied about various security apprehensions related to the three major models of cloud services are considered and mitigated solutions are provided to prevent are discussed.

IX. RELATED WORKS

In the paper [1] the author E.Mathisen have studied about major security challenges in cloud computing and also discussed about preamble solutions to overcome these threats.

Wang, Gregor and Marcel discussed about new generation computing and distribution of data in their paper [2].

Ramgovind, Eloff and Smith has clearly talked in their paper [4] about how to manage security in a cloud and researched upcoming evolutionary ways to breach data from a cloud.

In the paper [12], the authors Hendricks, Ganger and Reiter have researched and found a new encryption technology using distributed erasure coding.

The authors of paper [6] have discussed in depth about the security considerations in a cloud.

X. REFERENCES

[1] E. Mathisen, "Security Challenges and Solutions in Cloud Computing", Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 208-212, June, 2011, ISBN: 978-1-4577-0871-8, DOI:10.1109/DEST.2011.5936627.

[2] L. Wang, Gregor Laszewski, Marcel Kunze, Jie Tao, "Cloud Computing: A Perspective Study", New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2,2008.

[3] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology, International Journal of Recent Technology and Engineering (IJRTE) , April ,12- 2011

[4] Ramgovind S, Eloff MM, Smith E ,"The Management of Security in Cloud Computing", School of Computing, University of South Africa, Pretoria, South Africa ©2010

[5] Jianfeng Yang and Zhibin Chen," Cloud Computing Research and Security Issues", IEEE 2010

[6] Alok Tripath and Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur Centre Gorakhpur, India, 2010, IEEE.

[7] IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. http://blogs.idc.com/ie/?p=210.

[8] Security and Privacy policies of sales-force.com, "Secure, Private and Trustworthy: Enterprise Cloud Computing with Force.com".http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf http://trust.salesforce.com/trust/security/best_practices http://trust.salesforce.com/trust/privacy/tools/

[9] S. Sengupta, V. Kaulgud and V. S. Sharma, "Cloud Computing Security - Trends and Research Directions," *IEEE World Congress on Services*, pp. 524 - 531, 2011.

[10] Security Guidance for Critical Areas of Focus in Cloud Computing. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.

[11] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws. amazon.com, 2008

[12] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasurecoded Data," *Proc. 26th ACM Symposium on Principles of Distributed Computing*, pp. 139–146, 2007.

[13] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S.Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11,Issue 11, July 2011.