Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 5,May-2018

Key Challenges/Concerns in Cloud Security

G. Kishore Kumar[1], Dr.M.Gobi[2]

[1]*Research Scholar*
[2]*Assistant Professor*
[1, 2]*Department of Computer Science, Chikkanna Government Arts College, Tiruppur-641 602, India*

Abstract —***Security is the primary & major concern in all areas of applications in the modern age. Cloud is a boon to new generation technology and various security issues, such as data protection, network security, virtualization security, application integrity, and identity management, block its various areas of applications. Among all these areas, the data protection is the most critical/important as this must create trust/confidence for the users & organization whom do data transfer to cloud. This paper enlightens various key challenges, which affects cloud security in wherein our research would be focusing to ensure high-level security using cryptography.***

Keywords-***Cloud, Cloud Security, Attacks, Key Challenges, Security Concerns.***

I. INTRODUCTION

a. Cloud Computing[8]

Cloud Computing refers to the exercise of using a network, which comprises remote servers, hosted on the Internet to process, manage and store data, as opposed to a personal computer or a local server. It is a type of Internet-based computing, which offers shared computer handling resources and data to computers and/or other devices required on demand. It is a pattern for enabling a shared pool of configurable computing resources as on when requested and global access such as computer networks, servers, storage, applications and services. [1][2]

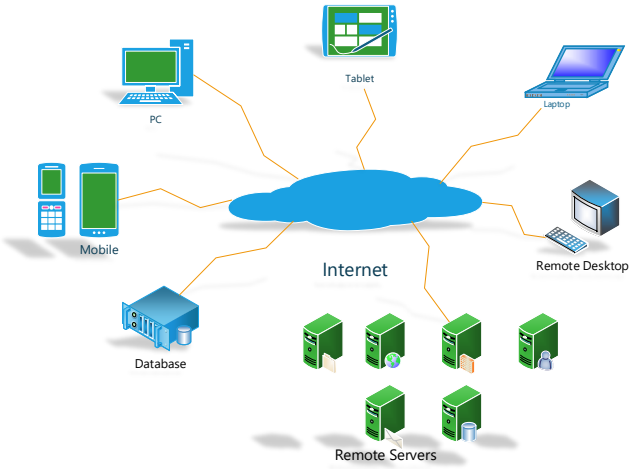

*Figure 1*Cloud Computing Overview

Cloud characteristics are given below:

- On-Demand self-service
- Ubiquitous network access
- Location-independent resource pooling
- Rapid elasticity
- Measured service

Cloud delivery models are given below:

- Application/Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

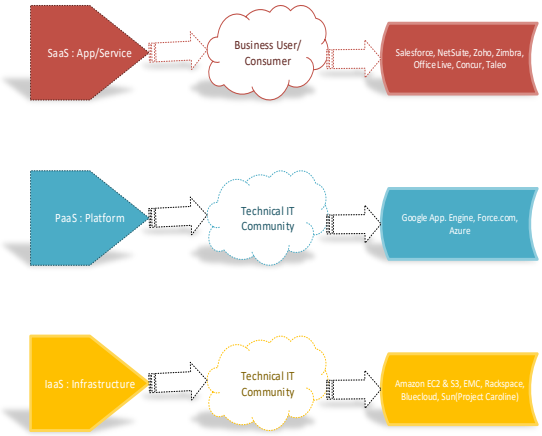

*Figure 2*Cloud Delivery Models

Cloud deployment models are as given below:

- Private
- Public
- Community
- Hybrid
- Virtual Private Cloud [3] - A virtual private cloud (VPC) will reside or within a public cloud environment which contains set of configurable group of computing resources on demand and allocated within a public cloud environment. They will provide a certain level of isolation between the different organizations, which are nothing but users

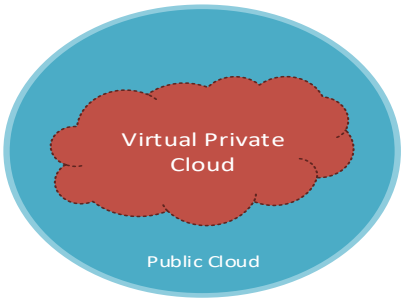

Figure 3 Virtual Private Cloud

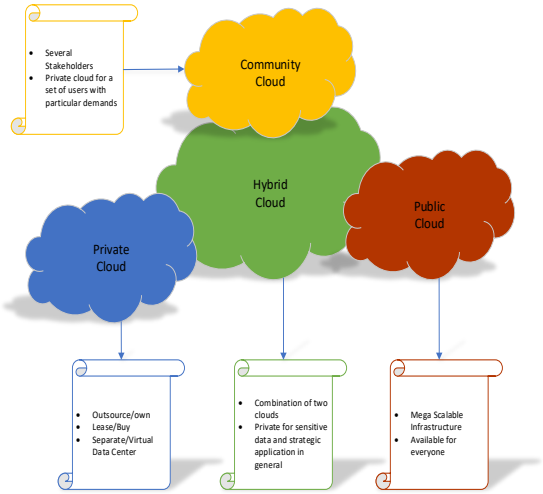

Figure 4Cloud Deployment Models & Properties

b. Cloud Computing Security[8]

In general, security is extremely tough to define. The objectives of information security are Integrity, Confidentiality, and Availability. Wide set of policies, controls and technologies are installed in Cloud Computing to protect data, applications and its infrastructure, which is a sub-domain of computer security, network security, and information security as well.

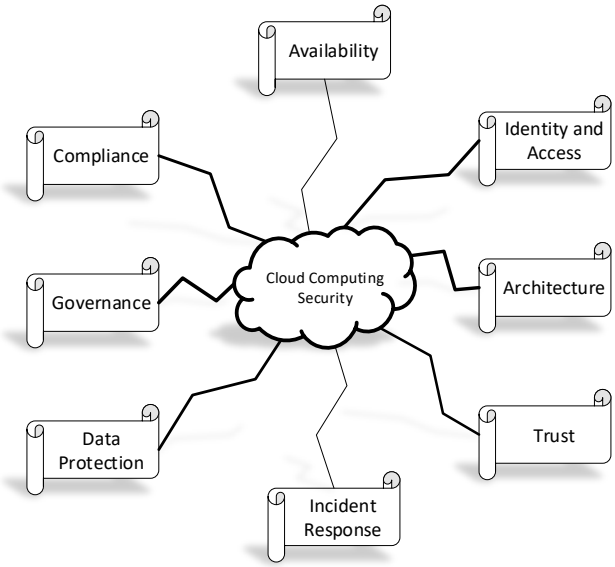

Figure 5 Cloud Computing Security

The below diagram illustrates about various parameters that affect cloud security:

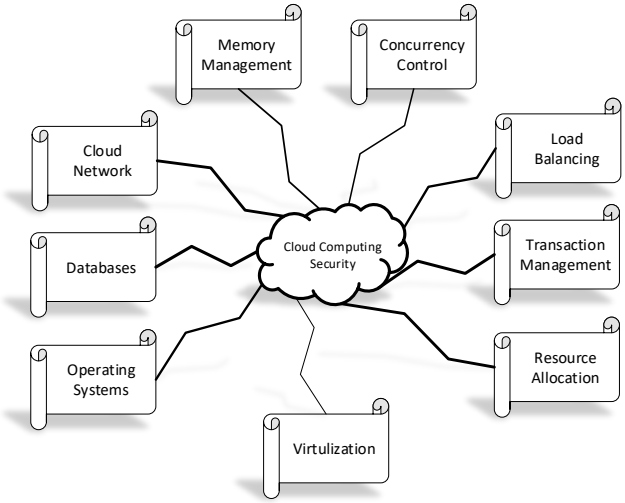

Figure 6Parameters that affect Cloud Security

II. CLOUD SECURITY CHALLENGES

a. Introduction

The need for today's business is secured data/applications that are available/accessible anywhere from any kind of device. The cloud technology helps in attaining this, but the associated inherent challenges makes this complicated. When the enterprise businesses do to reap, the benefits of cloud technology for providing a secured environment, they first concentrate on the challenges in finding the solutions that actually work. The next step would be selecting right tools and vendors to mitigate those challenges.

The below given are the few key challenges in cloud security:

1. DDoS attacks

The cloud providers are being targetted nowadays for malicious attacks as more & more businesses and operations are mvoing to the cloud. This attack has become more common nowadays. This attack is intended to overwhelm the web servers so that it will not respond to the authentic user requests. If this attack becomes successful, the concerned website becomes useless for hours, sometime even for days, which results in revenue loss, customer trust and brand authority. As per Verisign reports, SaaS is the most frequetnly targeted industry in Q1-2015. DDoS protection complemented to cloud services is not a good idea for the interprise, instead must be necessity wherein the websites and web-based applications are the core components for busines which requires state-of-the-art security in the 21st century.

2. Data breaches

The primary objective of a targetted attack is the security breach such as application vulnerabalities, poor security practices or result of human error as per CSA. This might involve any kind of information that was not intended for public release, including personal health information, financial information, personally identifiable information, trade secrets, and intellectual property.The cloud-based data value will vary from customer to customer for different reasons in an organization. The data breach risk consistently on top concern which is not unique in cloud computing. Hacking was in number one in the known data breach causes in US, which highlighted the growing challenge in securing the sensitive data. For securing proprietary data, the IT professionals have had great control over the physical hardware like firewalls etc and network infrastructure, but wherein in terms of cloud [irrespective of private/public or hybrid], some of these controls are relinqished/handed-over to third-party/trusted partners. This has become a great challenge as vital in choosing a right vendor with a strong record of security. [7]

3. Data loss

It's obvious that there would be concerns in the security when any business critical information is moved into the cloud. The data loss is disastrous for an enterprise business by loosing data from the cloud either through malicious tampering like DDoS/accidental deletion or an act of nature brings down a cloud service provider. The DDoS attack is a greater threat as an attempt to delete/steal data.To overcome this challenge, it's imperative to ensure a disaster recovery process in place and an integrated system as well to mitigate malicious attacks. Moreover, a cloud security solution needs to be build-in for the protection of every network layer which included the application layer (Layer 7).There is a possibility that the data stored in cloud can be loft various reasons other than malicious attacks as per CSA. The following facts will lead to a permanent last of customer data such as accidental deletion by the cloud service provider or a physical catastrophe such as fire / earthquake unless the user has adequate measures to back up the data using best practices in business continuity and disaster recovery.

4. Insecure access points

The main/major advantage of the cloud is it's accessibility wherein it can be accessed from anywhere and using any device. But the issue will occur when the interfaces and API's are not secure which makes path to the hackers to exploit them. The web applications can be protected from security breaches using the always-on device which examines the HTTP requestes to a website to ensure it is legitimate traffic.

5. Notifications and alerts

Awareness and proper communication about security threats is a keystone of network security and cloud security as well. Whenever any threat is identified, the alerting of the relevant website or application managgers must be part of a through security plan.The swift mitigation of a threat relies on clear and/or prompt communication, hence the required steps can be taken by proper entities and the threat impact is minimized.

6. User Authentication - Insufficient identity, credential, and access management

The data that resides in the cloud must be accessible by the authorized personnel only. The restriction and monitoring on who will be accessing the company's data through the cloud is critical. The organizations must have the facility to view data access logs and audit trails to cross-check whether only the authorized users accessing the data. In addition, these logs and audit trails need to be securely maintained as long as the company requires otherwise for legal purpose. With respect to the cloud computing security challenges, the whole responsibility lies with the customer to ensure that the necessary secuirity measures are taken to protect the customer data and data access by the cloud provider. The users impersonating as operators or developers or authentic users are called as bad actors who can reach/modify/delete data; controlling management functions; spy on data in transit; releasing malicious software which appears as originating from legitimate source. Finally, there is a possibility of treadful damage to organizations/users would be caused by an inadequate key/credential management/identity by unauthorized/malicious access.

7. System vulnerabilities

In general the bugs and vulnerabilities are not unique to cloud, but still they can be an issue with specific to shared cloud environments. For example, thousands of open source databases in MongoBD were encountered in a ransomware incident due to the default configuration settings were left open. It's also important that the regular monitoring on sytem activity and logs to consider risk. The system vulnerabilities are the exploitable program bugs that can be used by attackers to infiltrate a system for data steal/taking control/distrupting service operations. The vulnerabilities lies within the operating system components put the all security services and data into the risk.

8. Account hijacking

As per CSA, Account/Service hijacking is not a new, but the cloud services adds a new threat to this. If the attackers gain access to any user's credentials, they can do spy on activities and transactions, data manipulation, return falsified infomration and redirection to illegitimate sites. The new base for attackers is the account or service instances wherein the attackers often access the critical areas of cloud services with the stolen credentials which compromise the confidentiality, integrity, and availability of those services.

9. Malicious insiders

As per CSA, the insider threat is a real adversary or not, while the level of threat is open for debate. A malicious insider can access the potential sensitive information and increased access level to more important systems and/or data as well such as an system administrator.

10. Advanced persistent threats (APTs)

An advance persistent threat (APT) is the aceess stays undetected when someone gain access to the system. The APTs move sideways and blend with normal traffic through the network. The advantage of APTs is the combination of techniques used for network penetration. The common entry points such as spear phising, USB drive with prelaoded malware, direct attacks and third party networks can be managed by maintaining a vulnerability management system, regular patches, incident response plan and security hygiene training for the user, which is otherwise called as multiple layers of security. The other recommendations would be monitoring user behavior and capabilities which in turn will be compared with normal patterns to find-out whether any anomolies in the normal traffic and usage. The potential risks in the cloud organization can be mitigated by monitoring and analyzing the network along with sensitive data security by using the best practices as the nature of cloud computing will always present the unique challenges.APTs are a scrounging form of a cyber attack. The attackers target the companies by infiltrating the systems which will establish a grip in the IT infrastructure from which the data will be stolen. The APTs initially adapting to the intended defend security measures against them, and they laterally move and blend with normal network traffic to achieve their objectives, as per CSA.

11. Insufficient due diligence

As per CSA, the cloud technologies and service providers must be considered, when the business strategies are created by the executives. While evaluating the technologies and providers it's essential that good roadmap development is required with due diligence. The risk will occur to the organizations that are rush in adapting the cloud technologies and choosing providers without due diligence.

12. Abuse and nefarious use of cloud services

As per CSA, cloud computing models are prone to malicious attacks due the various factors such as poorly secured cloud service deployments, free service trials, fraudulent account sign-ups etc. The attackers/bad users will target the users, organizations and/or other cloud providers so that the initiation of denial-of-service attacks, spam mails and phising campaigns happens.

13. Denial of service (DoS)

DoS attacks works in such a way that the users will be prevented from services by which they would be able to access their data or applications. The attackers makes the system shutdown/slowdown along with service users prevented from the access to services such as memory, disk space, network bandwidth, processor power etc.

14. Shared technology vulnerabilities

The various services of cloud are delivered by the service providers by infrastructure sharing, platforms or applications. Cloud technology divides the service offerings without extensively changing the off-the-shelf hardware/software. The underlying components that consists of the infrastructure which supports the cloud service deployment by which the strong isolation properties cannot be offered for a multi-tenant architecture or multi-customer applications. This leads to the shared technology vulnerabilities that impacts all the delivery models.

15. Risky App Usage - Insecure interfaces and APIs

The extensive use of cloud applications makes the user's life easier. But in parallel the organizations face risk due to volume of data exchanged across the applications and security loopholes within each of them. The organization's applications can be protected various threats like SQL Injection, DDoS etc uses application level security solutions such as firewalls to define the boundaries on data access. In general, the applications code and APIs define the security based on the data exchange. Most of the applications are designed for usability alone and not for security, hence the functional application will have inborn vulnerabilities. In addition, the risks would increase when any third party rely on & build upon APIs and interfaces that are easily accessible. Hence all the vendor applications must be tested and reviewed for security.As per CSA, the API security need to be designed to safe-guard against accidental and malicious attempts in the services such as provisioning, management and monitoring.

16. Spectre and Meltdown[6]

This is a new and recent threat got in the year 2018, which is relevant to microprocessor. There is a common design feature in common which allows content encompasses encrypted data that can be read from memory using a malicious JavaScript code. In this, two variations are available Spectre and Meltdown that affect all devices from smartphones to servers. These threats permit the side-channel attacks as the isolation breaks-down between applications. An attacker who

would be able to access a system using unprivileged log in by which he/she can read information from the kernel or a root user on a virtual machine.

III. CLOUD SECURITY ARCHITECTURE

There are many types of cloud security architecture controls and the categories are as shown below:

1. **Detective Control**: To detect and react instantly & appropriately to any incident.
2. **Preventive Control**: To strengthen the system against any incident or attack by actually eliminating the vulnerabilities.
3. **Deterrent Control**: To reduce attack on cloud system; it reduces the threat level by giving a warning sign.
4. **Corrective Control**: To reduce the consequences of an incident by controlling/limiting the damage. Restoring system backup is an example of such type.

IV. CLOUD SECURITY CONCERNS

The below given diagram illustrates on the top 3 data security concerns :

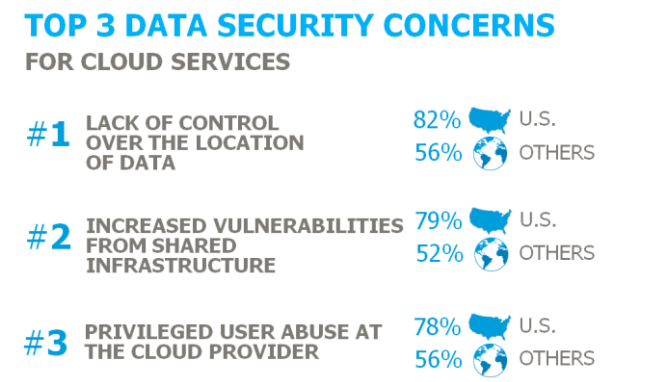

Figure 7 Top Security Concerns

1. Data Protection

Placing a critical data in the hands of a third-party along with ensuring the data remains secure both at rest in storage media when in transit as well is used in implementing a cloud computing strategy. The data must be encrypted always with clearly defined roles with encryption key management. The confidentiality of this data lies on the cloud service provider's server with the management of data encryption keys. The major concerns in the data security are access control, auditing, authorization and authentication.

2. Contingency Planning

The cloud serving as a single centralized repository for any company's mission-critical data with underlying risks of data breach or temporary data unavailability due to natural disaster. The company's critical operations depend on the data. The liability must be negotiated with the service provider and a complete/full security assessment from a third party is recommended as well. The companies must be aware that how the data is being secured and the actions taken by a service provider for the integrity and availability. In addition, the contingency plan must be in place by the companies.

V. PROPOSED APPROACH / RELATED WORK[5]

Following are the few security measures suggested/identified by few researchers, which can be taken into consideration for warranting the security in a cloud environment:

1. File Encryption

The hackers can very easily steal all the critical information from the machines in a cluster, as the entire data is present & stored in them. Hence, an encryption technique is a must while storing the data, at the same time various different encryption keys/techniques can be used on different machines and the key information can be stored behind a firewall stored centrally. By using these methods, the encryption helps to securely store & manipulate the data.

2. Data Privacy in the Cloud

The privacy in the cloud would have been managed by converting the data into encrypted form and providing the key to the user only in case of just data storage, but cloud serves the user in not only data storage but also various activities like

searching, access control decisions, transformations etc. Hence, the prevailing challenge is to incorporate a strong type of encryption for serving both the above-said activities in the cloud storage.

3. Network Encryption

As per the industry principles, encryption must be applied in all the network communication happen. Whatever be the RPC procedure call, which takes place, should happen over an SSL. Hence, even though the hacker taps into the network communication packets, useful information cannot be extracted or manipulated

4. Mobile – Cloud Server Communication

The encryption is mandatory in another type of communication happen in the cloud between mobile and server located in a cloud environment. As the usage of mobile is also drastically increased nowadays, the encryption is necessary for this area as well.

A. Abbreviations and Acronyms

Abbreviation	Meaning
CSA	Cloud Security Alliance
API	Application Programming Interface
DoS	Denial of Service
SLA	Service Level Agreement
APT	Advanced persistent threats

VI. FUTURE RESEARCH DIRECTIONS

There are actual benefits in the usage of cloud computing which includes few key security advantages as well. This evolving cloud technology is facing many technological challenges in different aspects of data/information handling/storage. The encryption process keeps the data protected in both storage and on transit as well. In addition, this helps in unauthorized access protection and prevention of data loss. This paper has highlighted on the various key challenges in cloud security. Our future research would be focusing on ensuring high-level security in cloud using cryptography & its algorithms.

REFERENCES

[1] US National Institute of Standards and Technology (NIST, http://csrc.nist.gov).
[2] Cloud Security Alliance (CSA)
[3] Mashrufee Alam, Israt Jahan, Liton Jude Rozario, Israt Jerin ,"A Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems",International Journal of Innovative Research in Advanced Engineering(IJIRAE) ISSN: 2349-2763 Issue 03, Volume 3 (March 2016)
[4] G.Kishore Kumar, Dr.M.Gobi,"Role of Cryptography & its Related Techniques in Cloud Computing Security", INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET), Volume 5 Issue VIII (August 2017)
[5] G.Kishore Kumar, Dr.M.Gobi,"Current Trend in Cloud Computing Security & Future Research Challenges", INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY,Volume-7,Issue-6 (June-17)
[6] https://meltdownattack.com
[7] https://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html
[8] G.Kishore Kumar, Dr.M.Gobi,"Secured Big Data Computing in Cloud Environments", GRD Journals- Global Research and Development Journal for Engineering | Volume 2 | Issue 8 | July 2017.

BIOGRAPHY

G. Kishore Kumar – Research scholar in Department of Computer Science, Chikkanna Government Arts College, Tirupur, India. He has completed Master of Computer Applications [MCA] in Alagappa University, Karaikudi, India. His major field of study in Network Security and Cryptography.

Dr. M.Gobi – Assistant Professor in Department of Computer Science in Chikkanna Government Arts College, Tirupur, India. He teaches courses for BSc Computer Science, BCA and Master of Computer Science (MSc). His research areas of interest include Cryptography, Java, Software Engineering and Information Systems Security.