Seminar Report

on

“Cloud Security: Challenges and Solutions”

Submitted to the

Savitribai Phule Pune University

In partial fulfilment for the award of the Degree of

Bachelor of Engineering

in

Information Technology

by

Prathamesh Dhananjay Kulkarni

(Roll No. 307A042 & Division. TE-1)

Under the guidance of

Prof. R. S. Sonar

Department of Information Technology

Sinhgad College of Engineering

S. No. 44/1, Off. Sinhgad Road, Vadgaon Budruk, Pune, Maharashtra 411041

2021-2022

Sinhgad Institutes

CERTIFICATE

This is to certify that the Seminar Report entitled "Cloud Security: Challenges and Solutions" being submitted by Prathamesh Dhananjay Kulkarni (Roll No. 307A042 & Division. TE-I) is a record of bonafide work carried out by him under the supervision and guidance of Prof. R. S. Sonar in partial fulfillment of the requirement for **TE (Information Technology Engineering)** a 2019 course of Savitribai Phule Pune University, Pune in the academic year 2021- 2022.

Date:

Place:

Prof. R. S. Sonar
Guide

Prof. S. P. Potdar
Head of the Department

Dr. S. D. Lokhande
Principal

This Seminar Report has been examined by us as per the Savitribai Phule Pune University, Pune requirements at Sinhgad College of Engineering, Vadgaon (Bk) Pune on . . . .

Internal Examiner

External Examiner

ACKNOWLEDGEMENT

I feel great pleasure in expressing my deepest sense of gratitude and sincere thanks to my guide **Prof. R. S. Sonar** for their valuable guidance during the Seminar work, without which it would have been very difficult task. I have no words to express my sincere thanks for valuable guidance, extreme assistance and cooperation extended to all the **Staff Members** of my Department.

This acknowledgement would be incomplete without expressing my special thanks to **Prof. S. P. Potdar** Head of the Department (Information Technology) for their support during the work.

I would also like to extend my heartfelt gratitude to my Principal, **Dr. S. D. Lokhande** who provided a lot of valuable support, mostly being behind the veils of college bureaucracy.

Last but not least I would like to thanks all the Teaching, Non- Teaching staff members of my department, my parents and my colleagues those who helped me directly or indirectly for completing of this Seminar successfully.

Prathamesh Dhananjay Kulkarni

ABSTRACT

Cloud computing is the delivery of shared computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. To simplify, Cloud computing is on-demand delivery of IT resources.

Many organizations are stuck in the conundrum of whether to cloudify or not to cloudify, mainly due to concerns related to the security of enterprise sensitive data. Removing this barrier is the pre-requisite to fully unleash the tremendous potential of cloud computing. The revolutionary principle of ‘Shared Resources’ is the cause of concern from Information Security point of view.

Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Security concerns have given rise to an active area of research due to the many security threats that many organizations have faced at present.

This seminar report provides a concise study on data security and privacy protection issues associated with cloud computing. Then this report discusses some current solutions and finally describes some measures for top identified threats in data security and privacy protection issues in cloud.

Contents

CONTENTS

List of Figures

List of Tables

1. INTRODUCTION

Cloud computing is the delivery of shared computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. To simplify, Cloud computing is on-demand delivery of IT resources. Cloud computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud Computing is a virtual pool of computing resources. These resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are three service models of Cloud computing namely Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS). As per NIST’s recommendations, four deployment models of Cloud Computing have been proposed, namely Private Cloud, Public Cloud, Hybrid Cloud and Community Cloud.

However, despite cloud computing being seen as a major business avenue, it can be seen that migration to cloud paradigm is barriered by concerns with information security and privacy protection. For example, with rise of digital banking, the financial institutions are attracted towards the cloud. Owing to the security concerns, they are trading with cautious steps to adopt this technology. Since users’ sensitive data is presented in unencrypted forms to remote machines owned and operated by third party service providers, the risks of unauthorized disclosure of the user’s sensitive data by service providers may be quite high. There have been numerous cases of breaches in security resulting in the leakage or unauthorized access of information worth a fortune.

In order to keep the information system free from threats, analysts employ both network and data security technologies.

There are many techniques for protecting data from outside attackers. For protecting the confidentiality of users’ data from service providers, it is ensured that the service providers do not collect users’ confidential data while data is being processed. Cloud provides various Internet based storages and services. More often than not, the same resource is used by more than one user simultaneously. The storages are virtually split to make up space for multiple users on the same service. This implies that multiple user data exists on the same storages more often than not. This means that the user data needs to be protected from not only the service providers and external attackers, but also from the peer users accessing the same resource on the cloud. The data needs to be strictly differentiated to avoid data exchanges.

In order for cloud computing to be seen as a viable alternative, it must provide (at least) the same level of security as traditional IT systems. In this seminar report, we explore through the recognized challenges and threats experienced by cloud computing and also, we discuss some recognized solutions and some measures for top identified threats to cloud computing.

2. LITERATURE SURVEY

2.1 Brief Idea

Cloud computing opens up an active and emerging area of research owing to the security concern surrounded by it. In the literature, there are many works proposing surveys of defence mechanisms implemented in cloud infrastructures. Most of the research has been conducted to derive accurate problem statements and precisely identify the existing problems. Due to its nature, cloud computing provides a vast spectrum of potential problems. Hence, the research into identifying the problems worth looking into is of utmost importance.

2.2 Detailed Analysis

F. Sabahi. [1] and Garfinkel, Tal & Rosenblum, Mendel [2] provides a thorough study of reliability, availability, and security issues for cloud computing (RAS issues). An analysis of Availability management, Access control management, Vulnerability and problem management in cloud services, especially Hybrid cloud service is discussed with length. This paper basically emphasis on using VMM (Virtual Machine Monitors). The VMM also provides the ability to directly inspect the hardware state of the virtual machine that a monitored host is running on. Consequently, we can retain the visibility benefits provided by a host-based intrusion detection system.

The paper [3] by Coppolino, L. & D'Antonio, Salvatore & Mazzeo, Giovanni surveyed the most widely used mechanisms that are currently available for protecting the different layers of a cloud stack. The study was conducted analysing one by one three distinct attack vectors. The paper also reviewed examples of features provided by commercial products and measures taken by Cloud Providers. The analysis shows that Amazon AWS and VMWare vCloud provide a number of products and mechanisms, that are offered either directly by the CPs or by third-parties.

In [4] Akinbi et al. define a classification of the security in PaaS cloud architectures. They use the Cloud Security Alliance (CSA) security guidance to define the areas on which to focus the study. These are: operational domain, which highlights guidance with application security, identity and access management, encryption and key management as well as virtualization security of a PaaS public cloud environment. Based on the areas of interest, they evaluate the Windows Azure cloud analysing the security mechanisms offered and highlight lack of controls.

In [5] Ristov et al. provide a systematic security evaluation of open-source cloud infrastructures, namely: OpenStack, CloudStack, OpenNebula, and Eucalyptus. They evaluate 11 assets of the cloud architecture, giving a score (from –1 to 2) that depend on how much a control objective is met. by summing up the scores, they define which CP has the best final score. The hardware-based attacks remained unaddressed.

2.3 Summarized Analysis

Publication	Author	Title of the paper	Seed Idea
IEEE Xplore 2013	F. Sabahi	Cloud computing security threats and responses [1]	Study of reliability, availability, and security issues for cloud computing (RAS issues). Analysis of Availability management, Access control management, Vulnerability and problem management in cloud services.
International Journal of Engineering Research and General Science, Volume 2, Issue 5, August – September 2014	Divisha Manral, Jasmine Dalal, Kavya Goel	Information Security in Cloud [14]	The paper proposes to develop a secure system by encryption mechanisms that allow a client's data to be transformed into unintelligible data for transmission. The concept of symmetric key is being used where only the data owner, the data retriever and the third-party auditor will be having the access to the keys.

Publication	Author	Title of the paper	Seed Idea
IEEE Xplore 2016 Journal entry: - Computers & Electrical Engineering (Vol. 59)	Coppolino, L. & D'Antonio, Salvatore & Mazzeo, Giovanni	Cloud security: Emerging threats and current solutions [3]	The paper surveyed the most widely used mechanisms that are currently available for protecting the different layers of a cloud stack. reviewed examples of features provided by commercial products and measures taken by CPs.
8th International Conference for Internet Technology and Secured Transactions (ICITST IEEE-2013)	A. Akinbi, E. Pereira and C. Beaumont	Evaluating security mechanisms implemented on public Platform-as-a-Service cloud environments case study: Windows Azure [4]	They use the Cloud Security Alliance (CSA) security guidance to define the areas on which to focus the study. they evaluate the Windows Azure cloud analysing the security mechanisms offered and highlight lack of controls.
IEEE Xplore 2013	Ristov S, Gusev M.	Security evaluation of open-source clouds [5]	The paper provides a systematic security evaluation of open-source cloud infrastructures, namely: OpenStack, CloudStack, OpenNebula, and Eucalyptus.

International Journal of Computer Science and Information Technologies, Volume 3, 2012	Juhi Sharma, Kshitiz Saxena	Cloud Security Challenges [6]	The paper discusses security concerns with cloud and potential solutions in the form of Securing Hypervisor, use of solid-state devices for memory access and deploying Intrusion Detection Systems (IDS).
International Journal of Computer Science & Engineering Survey (IJCSES) Vol.5, No.2, April 2014	Siddeeq Y. Ameen, Shayma Wail Nourildean	Firewall and VPN Investigation on Cloud Computing Performance [7]	The paper investigates the impact of using Virtual Private Network VPN together with firewall on cloud computing performance. They prove that there is impact in throughput and delay through the use of VPN and firewall. The impact on throughput is higher than that on the delay.

Table 2.1: Summarized Analysis of Literature Survey

3. CLOUD ARCHITECTURE

The architecture of cloud involves multiple cloud components communicating with each other over the application programming interfaces (APIs), usually web services. The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e., the customer. This includes the client’s network or computer, and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the cloud itself, which comprises of various computers, servers and data storage devices.

The general architecture of cloud (cloud stack) is given in figure 3.1 [8]. There are 2 types of models in the cloud—Service models and Deployment models. The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, and provides users with basic computer infrastructure capabilities like data storage, servers, and hardware; all of the resources are present in the cloud (e.g., Amazon EC2). The middle layer delivers Platform-as a-Service (PaaS), is made up of a programming language execution environment, an operating system, a web server & a database (e.g., Google App Engine). Software- as-a Service (SaaS) locates in the top layer, in which a cloud provider further confines client flexibility by merely offering software applications as a service (e.g., Gmail).

Cloud deployment models include public, private, community, and hybrid clouds which is shown in figure 3.2. Public clouds are external or publicly available cloud environments that are accessible to multiple tenants, whereas private clouds are typically tailored environments with dedicated virtualized resources for particular organizations. Similarly, community clouds are tailored for particular groups of customers.

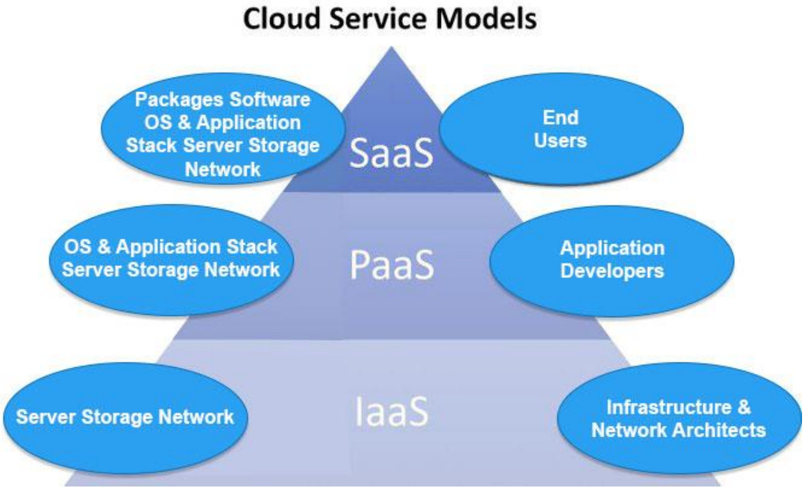
Cloud Service Models
Packages Software OS & Application Stack Server Storage Network
SaaS
End Users
OS & Application Stack Server Storage Network
PaaS
Application Developers
Server Storage Network
IaaS
Infrastructure & Network Architects

Figure 3.1: Cloud Delivery Model

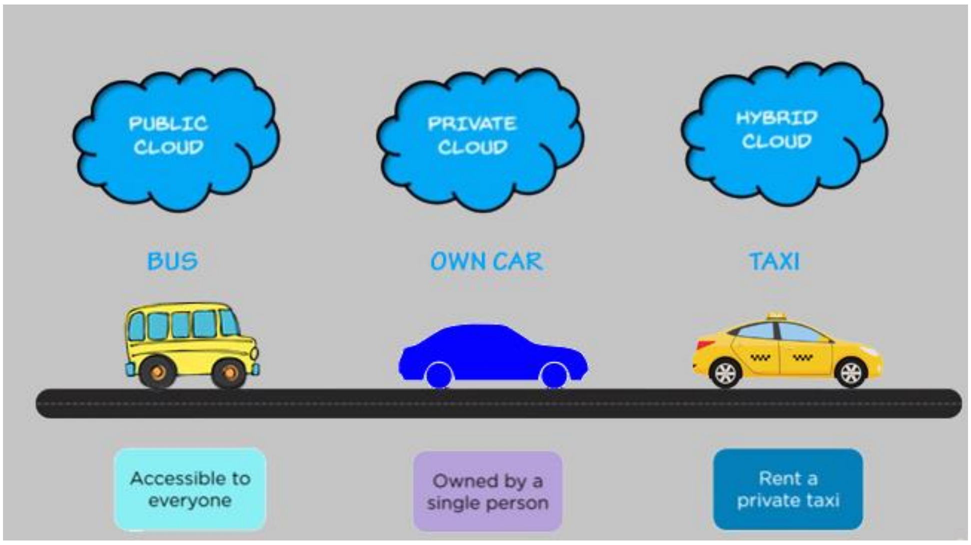

Figure 3.2: Cloud Deployment Model

3.1 Characteristics of Cloud Computing

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches [8]:

- **On-demand self-service -** A consumer can provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.

- **Resource pooling -** The providers computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned according to consumer demand. The consumer has no control or knowledge over exact location of provided resources and with whom they are being shared with.

- **Broad network access -** The Computing services are generally provided over standard networks and heterogeneous devices.

- **Rapid elasticity** – Computing services can be rapidly and elastically provisioned in some cases automatically to quickly scale out; and rapidly released to quickly scale in.

- **Measured service -** The resource utilization is tracked for each application and occupant; it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.

4. CLOUD SECURITY CHALLENGES

4.1 Security Overview

Location of data and processes makes the difference in the realm of computation. In cloud computing, the service and data maintenance are provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it nor do they have the knowledge about its whereabouts. The cloud computing uses the internet as the communication media. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues.

Traditional security issues are still present in cloud computing environments. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer suitable for applications and data in cloud. Traditional concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Due to the openness and multitenant characteristic of the cloud, cloud computing is bringing tremendous impact on information security field [9].

Well-publicized incidents of cloud outages include Gmail. As with the Traditional Security concerns, cloud providers argue that their server uptime compares well with the availability of the cloud users own data centres. Cloud services are thought of as providing more availability, but perhaps not there are more single points of failure and attack. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality, regulatory compliance requires transparency into the cloud [8].

4.2 Five Main Challenges

- **Massive data and intense computation -** Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected [8].

- **Multi-tenancy -** Multi-tenancy means that the cloud platform is shared and utilized by multiple customers. Moreover, in a virtualized environment, data belonging to different customers may be placed on the same physical machine by certain resource allocation policy. Adversaries who may also be legitimate cloud customers may exploit the co-residence issue. A series of security issues such as data breach, computation breach, flooding attack etc., are incurred. Although Multi-tenancy is a definite choice of cloud venders due to its economic efficiency, it provides new vulnerabilities to the cloud platform [8]. From a customer's perspective, the notion of using a shared infrastructure could be a huge concern. However, the level of resource sharing and available protection mechanisms can make a big difference.

- **Outsourcing -** Outsourcing brings down both capital expenditure (Capex) and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become root cause of cloud insecurity.

Outsourcing will potentially incur privacy violations, due to the fact that sensitive/classified data is out of the owners’ control [8].

- **Data Storage Risk -** Some valued data and resources, related programs and applications of users are stored in the cloud using cloud storage service. Current cloud storage service providers take measures of centralised storage, unified management, real-time monitoring of users’ data, to ensure system and data security. However, the cloud storage system is a huge and complex system with a structure of four layers, which involves the integrity, confidentiality and availability issues of data. Different cloud service providers have their security policies and technical solutions to ensure the safety of the user's data [10].

- **Data Transmission Risk -** Data transmission depends absolutely on the network in cloud storage mode. Therefore, the threat of network attacks on data security is badly big. Hackers may intercept information, modify access rights, obtain or modify data, to compromise the benefits of cloud storage providers and users. In the Data Link, Network and Transport Layer, in the case of improper use of Technology, data will be at risk even though there are SSL, SSH, IPSEC and other VPN technology for data transmission to establish a trusted secure connection. In the Application layer, the DDoS and other network attacks will take up most of the network bandwidth, resulting in network equipment downtime. Service can’t respond to user requests, resulting in user data in the transmission process damaged or lost, affecting the availability and Integrity of data [11].

5. NEED FOR SECURITY IN CLOUD

A user’s dependence on cloud is analogous to a person’s dependence on public transportation as it forces one to trust over which one have no control, limits what one can transport, and subjects us to rules and schedules that wouldn’t apply if one had their own vehicles. On the other hand, it is so economical that one doesn’t realistically have any alternative. Users of the cloud aren’t aware about the location of the data and ultimately have to rely on the cloud service provider for exercising appropriate security measures. Therefore, cloud security issue is the most important and elicited topic among the IT professionals.

Security in Cloud is of two types:

- **Data Security -** It focuses on protecting the software and hardware associated with the cloud. It deals with choosing an apt location for data centres so as to protect it from internal threats, different types of weather conditions, fire and even physical attacks that might destroy the centre physically and external threats avoiding unauthorized access and break ins.

- **Network Security -** Protecting the network over which cloud is running from various attacks DOS, DDOS, IP Spoofing, ARP Spoofing and any novel attacks that intruders may device. Attack on data affects a single user whereas a successful attack on Network has the potential to affect multiple users. Therefore, network security is of foremost importance.

5.1 Security Framework

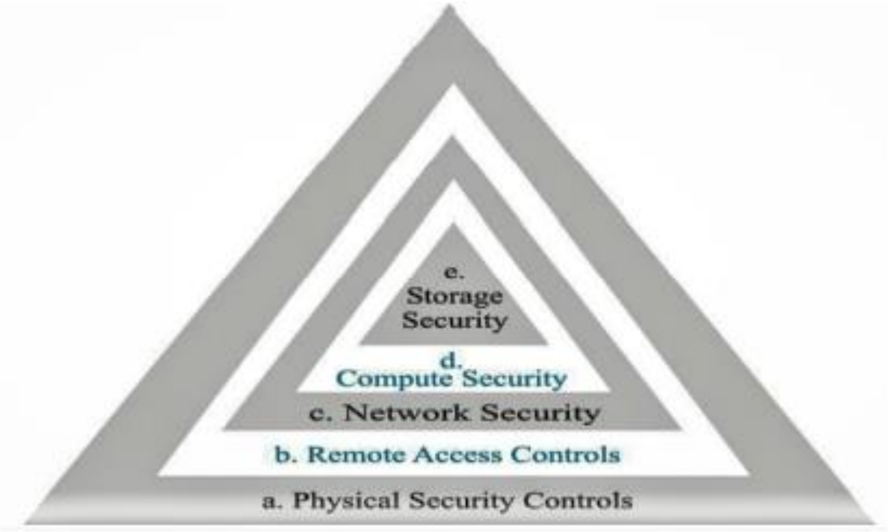

Figure 5.1: Security Framework for Cloud Computing

The five important layers of Data security frameworks are shown in figure 5.1 [11]:

- **Physical Security (Perimeter Security):** Physical devices should be secured.
- **Authentication (Access Control):** Identification of User should be done with access control.
- **Network Security (Firewall):** Going to observe inbound and outbound traffic.
- **Computer Security (Antivirus):** The software antivirus is used to protect from malicious content.
- **Storage Security (Encryption):** The data should be encrypting with some algorithm.

5.2 Security and Privacy Attributes

Five most representative security and privacy attributes are confidentiality, integrity, availability, accountability, and privacy-preservability, which is shown in figure 5.2 [8]. For data transmission across enterprise boundaries, both data confidentiality and integrity should be ensured in order to prevent data from being tapped and tampered with by unauthorized users. In other words, only the data encryption is not enough. Data integrity is also needed to be ensured. Therefore, it should ensure that transport protocols provide both confidentiality and integrity.

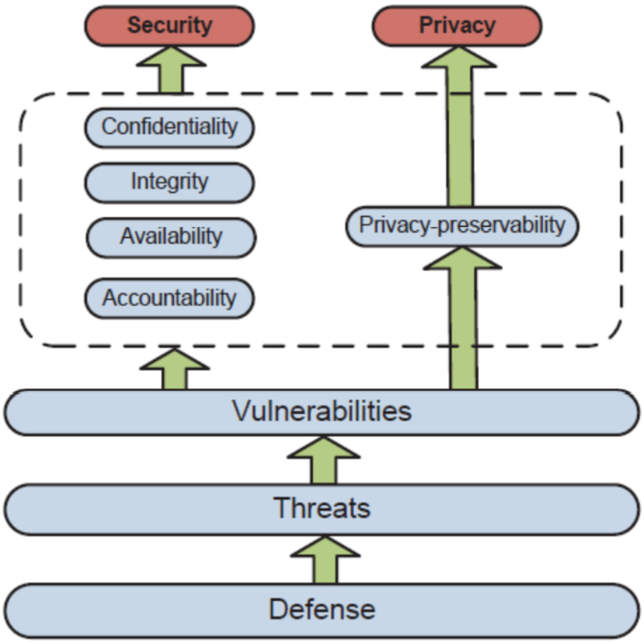

Figure 5.2: Security and privacy attributes

Threats to these attributes and Defence strategies are discussed in next section.

6. THREATS AND DEFENCE STRATEGIES

6.1 Cloud Confidentiality

Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or Devices. i.e., customers data and computation tasks are to be kept confidential from both the cloud provider and other customers. Confidentiality remains as one of the greatest concerns with regards to cloud computing. This is largely due to the fact that customers outsource their data and computation tasks on cloud servers, which are controlled and managed by potentially untrustworthy cloud providers [8].

Threats:

- *Cross-Virtual Machine (VM) attack via Side Channels* - A Cross-VM attack exploits the nature of multi-tenancy, which enables that VMs belonging to different customers may co-reside on the same physical machine. Timing side-channels as an insidious threat to cloud computing security due to the fact that a) the timing channels pervasively exist and are hard to control due to the nature of massive parallelism and shared infrastructure; b) malicious customers are able to steal information from other ones without leaving a trail or raising alarms.

- *Malicious sysadmin* - The Cross-VM attack discusses how others may violate confidentiality cloud customers that co-residing with the victim, although it is not the only threat. Privileged sysadmin of the cloud provider can perform attacks by accessing the memory of a customer's VMs.

Defence Strategies:

- *Placement prevention* - In order to reduce the risk caused by shared infrastructure, a few suggestions to defend the attack in each step are given in. For instance, cloud providers may obfuscate co-residence by having Dom0 not respond in traceroute, and/or by randomly assigning internal IP addresses to launched VMs. To reduce the success rate of placement, cloud providers might let the users decide where to put their VMs; however, this method does not prevent a brute-force strategy.

- *NoHype* - It attempts to minimize the degree of shared infrastructure by removing the hypervisor while still retaining the key features of virtualization. The NoHype architecture provides a few features: i) the one core per VM feature prevents interference between VMs, eliminates side channels and retains multi-tenancy, since each chip has multiple cores; ii) memory partition restricts each VMs memory access on an assigned range; iii) dedicated virtual I/O devices enables each VM to be granted direct access to a dedicated virtual I/O device. NoHype has significantly reduced the hypervisor attack surface, and increased the level of VM isolation.

- *Trusted cloud computing platform (TCCP)* - It offers a closed box execution environment for IaaS services. TCCP guarantees confidential execution of guest virtual machines. It also enables customers to attest to the IaaS provider and to determine if the service is secure before their VMs are launched into the cloud. The design goals of TCCP are: 1) to confine the VM execution inside the secure perimeter; 2) that a sysadmin with root privileges is unable to access the memory of a VM hosted in a physical node.

6.2 Cloud Integrity

Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

Threats:

- *Data loss/manipulation* - In cloud storage, applications deliver storage as a service. Servers keep large amounts of data that have the capability of being accessed on rare occasions. The cloud servers are distrusted in terms of both security and reliability, which means that data may be lost or modified maliciously or accidentally. Administration errors may cause data loss (e.g., backup and restore, data migration, and changing memberships in P2P systems). Additionally, adversaries may initiate attacks by taking advantage of data owners' loss of control over their own data.

- *Dishonest computation in remote servers* - With outsourced computation, it is difficult to judge whether the computation is executed with high integrity. Since the computation details are not transparent enough to cloud customers, cloud servers may behave unfaithfully and return incorrect computing results; they may not follow the semi-honest model. For example, for computations that require large amount of computing resources, there are incentives for the cloud to be lazy. Even in semi-honest model, problems may arise when a cloud server uses outdated, vulnerable code, has misconfigured policies or service, or has been previously attacked with a rootkit, triggered by malicious code or data.

Defence Strategies:

- *Provable data possession (PDP)* - The main challenge of integrity checking is that tremendous amounts of data are remotely stored on untrustworthy cloud servers; as a result, methods that require hashing for the entire file become prohibitive. In addition, it is not feasible to download the file from the server and perform an integrity check due to the fact that it is computationally expensive as well as bandwidth consuming. Each of the former notions is not acceptable in cloud environments.

- *Third party auditor (TPA)* - Instead of letting customers verify data integrity, it is also possible to offload task of integrity checking to a third party which can be trusted by both cloud provider and customers. It is proposed to adopt a TPA to check the integrity of outsourced data in cloud environments. TPA ensures the following: 1) cloud data can be efficiently audited without a local data copy, and cloud clients suffer no on-line overhead for auditing; 2) no new vulnerabilities will be introduced to jeopardize data privacy.

- *Combating dishonest computing* - Conventional strategies to check external computation integrity fall into four categories:

  a. **Re-computation** requires the local machine to re-do the computation, and then compare the results. Re-computation guarantees 100% accuracy of mistake detection, and does not require trusting the cloud vendor. However, the cost is usually unbearable due to the fact that each of the verifications require at least the equal time as the original computation.

b. **Replication** assigns one computation task to multiple machines, and then compares the results. Majority voting may be employed to determine correctness. Replication assumes semi-trust to cloud vender because both computation and verification are conducted remotely. Intelligent adversaries that control certain amounts of machines may bypass replication checking by returning the same incorrect results.

c. **Auditing** usually works together with logging. During the execution of a computation, a logging component records all critical events into a log file, which is subsequently sent to one or multiple auditors for review. Auditing is a typical approach to do forensics investigation. One drawback of auditing is that if the attacker understands the computation better than the auditor, it is possible for the attacker to manipulate data bits without being detected.

d. **Trusted computing** enforces the computer to behave consistently in expected ways with hardware and software support. The key technique of integrity checking is known as remote attestation, which works by having the hardware generate a certificate stating that what software is running. The certificate can then be sent to the verifier to show that the software is unaltered. One assumption of trusted computing is that some component like the hardware and the hypervisor is not physically altered.

6.3 Cloud Availability

Availability is crucial since the core function of cloud computing is to provide on demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system. In this section, we have studied two kinds of threats that impair cloud availability.

Threats:

- *Flooding attack via Bandwidth Starvation* - In a flooding attack, which can cause Deny of Service (DoS), a huge number of nonsensical requests are sent to a particular service to hinder it from working properly. In cloud computing, there are two basic types of flooding attacks:

  Direct DOS the attacking target is determined, and the availability of the targeting cloud service will be fully lost.

  Indirect DOS the meaning is twofold: 1) all services hosted in the same physical machine with the target victim will be affected; 2) the attack is initiated without a specific target.

- *Fraudulent Resource Consumption (FRC) attack* - A representative Economic Denial of Sustainability (EDoS) attack is FRC, which is a subtle attack that may be carried out over a long period (usually lasts for weeks) in order to take effect. The attackers, who act as legal cloud service clients, continuously send requests to website hosting in cloud servers to consume bandwidth, which bills to the cloud customer owning the website; seems to the web server, those traffic does not reach the level of service denial, and it is difficult to distinguish FRC traffic from other legitimate traffic. A FRC attack succeeds when it causes financial burden on the victim.

Defence strategies:

- *Defending the new DOS attack* - This new type of DOS attack differs from the traditional DOS or DDOS attacks in that traditional DOS sends traffic to the targeting application/host directly while the new DOS attack does not. A DOS avoidance strategy called service migration has been developed to deal with the new flooding attack. A monitoring agent located outside the cloud is set up to detect whether there may be bandwidth starvation by constantly probing the cloud applications. When bandwidth degradation is detected, the monitoring agent will perform application migration, which may stop the service temporarily, with it resuming later.

- *FRC attack detection* - The key of FRC detection is to distinguish FRC traffic from normal activity traffic. Idziorek et al. [12] propose to exploit the consistency and self-similarity of aggregate web activity. To achieve this goal, three detection metrics are used: i) Zipf 's law [97] are adopted to measure relative frequency and self-similarity of web page popularity; ii) Spearman's footrule is used to find the proximity between two ranked lists, which determines the similarity score; iii) overlap between the reference list and the comparator list measures the similarity between the training data and the test data. Combining the three metrics yields a reliable way of FRC detection.

7. MEASURES FOR TOP IDENTIFIED THREATS

Category wise proposed measures are as follows [13]:

For ***Abuse and Nefarious use of cloud computing***

- Care must be taken in Initial registration and Validation process.
- To use credit card in Cloud computing an Enhanced fraud monitoring system must be implemented.
- Monitoring public blacklists for one’s own network blocks.

For ***Insecure Interfaces and APIs***

- Cloud providers interfaces security model must be analysed properly.
- Strong authentication and access controls must be implemented.
- Understand the dependency chain associated with the APIs.

For ***Malicious Insiders***

- Identify the human resources requirements as a part of legal contracts.
- Information security, management practices require transparency.
- Decide Security breaches.
- Conduct survey on comprehensive supplier assessment and implement strict supply chain management.

In case of ***Shared Technology issues***

- Best Security practices must be implemented for installation or System configuration.
- Unauthorized activities must be monitored.
- Service level agreements must be enforced.
- Configuration audits and vulnerability scanning must be conducted.
- Strong authentication and access control administrative access.

For ***Data loss or Leakage***

- Implement strong API access control.
- Specify backup and retention mechanisms
- Analyse data protection at both design and run time.
- Necessary measures must be taken for strong key generation, storage, and destruction practices.

With respect to ***Account or Service Hijacking***

- Strong monitory system implementation for to detect unauthorized activity.
- Sharing of account details between users and services must be avoided.
- Read and understand properly cloud security policies.

8. CONCLUSION

Every new technology has its pros and cons, similar is the case with cloud computing. Although cloud computing provides easy data storage and access. But there are several issues related to storing and managing data, that is not controlled by owner of the data. This paper discussed security challenges for cloud along with some defence strategies. The issues include cloud integrity, cloud confidentiality, cloud availability, cloud privacy. There are several threats to cloud confidentiality including cross-VM attack and Malicious sysadmin. As discussed, defence strategies include Placement prevention, NoHype architecture and Trusted cloud computing platform (TCCP). On the other hand, integrity of cloud is compromised due to data loss and dishonest computation in remote servers. To tackle this, use of Provable data possession (PDP), Third party auditor (TPA), Combating dishonest computing was studied. Denial of Service attack (Dos) is the most common attack which is also possible in cloud computing network. This attack attempts to prevent the data from being available to its intended users. The paper concludes with measures to be taken for the top threats identified in the Cloud Computing.

9. REFERENCES

[1] F. Sabahi, "Cloud computing security threats and responses," 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 245-249, doi: 10.1109/ICCSN.2011.6014715.

[2] Garfinkel, Tal & Rosenblum, Mendel. (2003). A Virtual Machine Introspection Based Architecture for Intrusion Detection. NDSS. 3.

[3] Coppolino, L. & D'Antonio, Salvatore & Mazzeo, Giovanni. (2016). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering. 10.1016/j.compeleceng.2016.03.004.

[4] A. Akinbi, E. Pereira and C. Beaumont, "Evaluating security mechanisms implemented on public Platform-as-a-Service cloud environments case study: Windows Azure," 8th International Conference for Internet Technology and Secured Transactions (ICITST IEEE-2013), 2013, pp. 162-167, doi: 10.1109/ICITST.2013.6750183.

[5] Ristov S, Gusev M. Security evaluation of open-source clouds. EUROCON, 2013. Zagreb: IEEE; 2013. p. 73–80. doi:101109/EUROCON20136624968.

[6] Juhi Sharma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012,4514-4515

[7] Ameen, Siddeeq & Nourildean, Shayma. (2014). Firewall and VPN Investigation on Cloud Computing Performance. International Journal of Computer Science & Engineering Survey. 5. 15-25. 10.5121/ijcses.2014.5202.

[8] Xiao, Zhifeng & Xiao, Yang. (2013). Security and Privacy in Cloud Computing. Communications Surveys & Tutorials, IEEE. 15. 843-859. 10.1109/SURV.2012.060912.00182.

[9] Chen, Deyan & Zhao, Hong. (2012). Data Security and Privacy Protection Issues in Cloud Computing. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012. 1. 10.1109/ICCSEE.2012.193.

[10] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), 2017, pp. 145-149, doi: 10.1109/BigDataSecurity.2017.12.

[11] B. S. Shirole and L. K. Vishwamitra, "Review Paper on Data Security in Cloud Computing Environment," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 79-84, doi: 10.1109/SMART50582.2020.9337115.

[12] Joseph Idziorek, Mark Tannian, and Doug Jacobson. 2011. Detecting fraudulent use of cloud resources. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop (CCSW '11). Association for Computing Machinery, New York, NY, USA, 61–72. DOI:https://doi.org/10.1145/2046660.2046676

[13] Kalluri, Ramakrishna & Rao, Chakunta. (2014). Addressing the Security, Privacy and Trust Challenges of Cloud Computing. Journal of Computer Science and Technology. 5. 6094-6097.

[14] Divisha manral, Jasmine Dalal, Kavya Goel, “Information Security in Cloud”, International Journal of Engineering Research and General Science, Volume 2, Issue 5, August – September 2014, pp. 122-128.

[15] J. Jang-Jaccard, S. Nepal, “A survey of emerging threats in cybersecurity”, Journal of Computer and System Sciences 80 (2014) 973–993

[16] H. Takabi, J. B. D. Joshi and G. J. Ahn,” Security and Privacy Challenges in Cloud Computing Environments”, Security and Privacy, IEEE, vol.8, no.6, pp.24-31, Nov/Dec 2010.