Cloud Computing Security – A Review

Siddhant Bhosle 16010420009
Rohan Chavan 16010420010
Dhruv Daftary 16010420013
Anuskha Bodke 16010420014

Cloud security issues and challenges: A survey

***Abstract*— The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large-scale computation and data storage, virtualization, high expansibility, high reliability and low-price service. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. This paper introduces some cloud computing systems and analyzes cloud computing security problems and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problems. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system.**

Keywords- cloud computing; cloud security; strategy I.

INTRODUCTION

Cloud computing is a new computing model that provides invariant access to wide area distributed coffers on demand. The emergence of cloud computing has made a tremendous impact on the Information Technology(IT) assiduity over the once many times, where large companies similar as Google, Amazon and Microsoft strive to give more important, dependable and cost-effective cloud platforms, and business enterprises seek to reshape their business models to gain benefit from this new paradigm. Still, there are still numerous problems in cloud computing at the moment. A recent check by Cloud Security Alliance(CSA) shows that security has become the primary concern for people to shift to cloud computing. In this paper, we probe the security enterprises of current Cloud Computing systems. As Cloud Computing refers to both the operations delivered as services over the Internet and the architectures(i.e., the tackle and systems software in the data centers) that give those services, we present the security enterprises in terms of the different operations and architectures. further enterprises on security issues, similar as vacuity, confidentiality, integrity control, authorization and so on, should be taken into account.

II. Overview/ Summary

The issues faced in cloud computing are distributed into 2 corridors, security issues faced by cloud providers and security issues faced by guests. Some of the issues are Privileged access, Data position, Data isolation, Data vacuity, Regulatory compliance, Recovery, Investigative Support, Long- term viability. In the SaaS model the providers are more responsible for security As public cloud is less secure than private shadows, the stronger security measures are needed in public cloud. Also in SaaS, it becomes delicate for the stoner to ensure that proper security is maintained or not. Private shadows could also demand further extensibility to accommodate tailored conditions. The following crucial security rudiments should be precisely considered as an integral part of the SaaS operation development and deployment process i) Data security ii) Data position iii) Data integrity iv) Data isolation v) Data access vi) Data confidentiality vii) Network security viii)

Authentication and authorization ix) Vacuity x) Identity operation and subscribe- on process.

In PaaS, guests are suitable to make their own operations on top of the platforms. Therefore it's the responsibility of the guests to cover their operations as providers are only responsible for segregating the guests ' operations and workspaces from one another. So, maintaining the integrity of operations and administering the authentication checks are the abecedarian security conditions in PaaS.

IaaS is substantially used as a delivery model. The major security concern in IaaS is to maintain the control over the client's data that's stored in the provider's tackle. The consumers are responsible for securing the operating systems, operations, and content. The cloud provider must give low- position data protection capabilities. Grounded upon the deployment model, public shadows are less secure.

There are various security issues for cloud computing as it comprises numerous advancements including systems, databases, working frameworks, virtualization, asset planning, exchange administration, stack adjusting, simultaneousness control and memory administration. Similarly, security issues for a greater number of these frameworks and technology are pertinent to Cloud computing. According to the RSA conference which was conducted in March 2016, the CSA (Cloud Security Alliance) has released the list known as Treacherous 12, which includes the top 12 Cloud Computing threats in 2016. The following are the 12 threats in cloud computing.

Data Breaches Due to the improved technology, a large amount of data is stored in cloud servers, which becomes a target for the hackers. More the amount of data exposed, greater will be the damage to the society and users

Compromised credentials and broken authentication

Data breaches and other attacks frequently result from slack authentications, weak passwords, poor key or certificate
than the other cloud models as it allows druggies to pierce the data across a wide area network.

A Service level agreement (SLA) is a part of a service contract between the consumer and provider that formally defines the level of service. It is used to identify and define the customer's needs and to reduce areas of conflict like Services to be delivered Performance, Tracking and Reporting Problem Management Legal Compliance and Resolution of Disputes, Customer Duties and Responsibilities, Security IPR and Confidential Information Termination.

Thus, a trust framework should be developed to allow for efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements.

Cloud Computing: Security Issues and Research Challenges

.

Hacked Interfaces and APIs

At present, every cloud service provides APIs. They are used to manage the cloud services, management, orchestration, monitoring. The interfaces and APIs which are weak would expose the authorizations to security issues like confidentiality, integrity, availability and accountability

Exploited system vulnerabilities

We have been facing the problem of bugs for a very long time. One can say that they are always observed in one or the form. As the usage of technology has increased in a wide range, these vulnerabilities have become a bigger issue. The sharing of memory, databases and other data among the organizations would lead to data crash or reports larger bugs and later on even may be affected by virus too

Account Hijacking

One of the most common and daily heard issues in the society at present is account hijacking. There may be various reasons for hijacking such as sharing our credentials to others, sharing of our data to third-party vendors during online transactions and so-on. The attackers who would hijack our account may probably even

Malicious Insiders

These threats generally appear from the people who work in the organizations as employees, business associates and have valuable information regarding the organizations which are to be maintained securely and secretly. By limiting the assessing needs in the computer systems during working

hours and by encrypting the routine job such as malicious we can avoid these insider threats to certain extent.

The APT parasite

The APT is a continuous hacking process, synthesized by a person or group of persons targeting a specific organization. It is well known for attacking private organizations for business motives. This advanced process uses malware to cause vulnerabilities (virus, bugs, installations) in the system.

Inadequate diligence

Associations that grasp the cloud without completely understanding nature and its related dangers may experience a horde of business, money related, specialized, legitimate, and consistent chances. Due to constancy applied, whether the association is attempting to relocate to the cloud or combining (or working) with another organization in the cloud

Cloud services abuses

The main concept of cloud service abuse is that the hackers use the social media services to understand and extract different codes so that they can disturb the cloud environment. Once this occurs, the organizations may face problems like shut down of computers, erase of the necessary data.

Security Issues, Security Problem and Strategy, Threats And Respective Mitigation In Cloud Computing –A Systematic Review

I. CLOUD SECURITY PROBLEM

Dos attacks

They critically affect the performance of the system. The system may run out of time and even become lower than the normal condition. The DOS attacks consume more power due to which our billing expenses also increase. The clue for this is, anticipating the threats before itself and access to the necessary resources.

Share technology and Share dangers

Cloud service provides shared infrastructure, platforms and applications. If a bug arises in any of the mentioned layers, it affects the secured data which directly affects the users. A defense-in-depth technique is suggested by CSA including the multi-factor authentication on all hosts, host based and network based systems

RESEARCH CHALLENGES IN CLOUD COMPUTING

Although cloud computing has quickly come into existence. The research of cloud computing is still in an early stage. Many issues have not been resolved and new challenges have been emerging in every industry day-by-day. The following are a few research challenges in cloud computing.

- Service level agreement (SLA)
- Cloud data management and security
- Data Encryption
- Virtual machines migration
- Access controls
- Multi-tenancy
- Reliability and availability of services

PC and it can meet other special and new security problems. The biggest concerns about cloud computing are security and privacy. The traditional security problems such as security vulnerabilities, virus and hack attacks can also make threats to the cloud system and can lead to more serious results because of the properties of cloud computing. Hackers and malicious intruders may hack into cloud accounts and steal sensitive data stored in cloud systems. The data and business applications are stored in the cloud center and the cloud system must protect the resource carefully. Cloud computing is a technology evolution of the widespread adoption of virtualization, service-oriented architecture and utility computing. over the Internet and it includes the applications, platform and services.

II. STRATEGY

The data stored in the cloud system can meet the problem of being stolen and modified unlawfully. The data can be encrypted before stored in the cloud system. But if the data size is very large, it will need more time and computing resources. The confidential data will be treated by the outside people of the company and the other people can access the data. Traditional techniques can protect user data privacy and security in the cloud environment to some extent. These technologies include encryption mechanisms, security

authentication mechanisms and access control policy. Encryption mechanism depends on the reliability of the difficulty of decryption. Encryption methods include symmetric key encryption systems and asymmetric key encryption systems. Asymmetric keys can get high security but encryption and decryption are slow. Security authentication mechanism currently has a complete set of technical solutions.

The cloud provider can transmit the customer data from the server to another server and the user can not know the data storage place. The data storage and manipulation are related to the resources of the cloud center in a cloud computing environment. The cloud provider is responsible for security but the monitoring and auditing for them become an important problem. The cloud computing services provided for customers are difficult to achieve full transparency. Customers do not understand internal processes of cloud computing and data storage location information. The customers do not know what kind of situation data will meet if an accident occurs. Customers should have the right of the supervision and audit of cloud computing services in order to fully ensure the security of customer data. The communication of worms, virus and Trojan in cloud computing platforms within the network of internal and external systems must be controlled. Malicious programs must be isolated promptly. Damage to the system must be repaired immediately. The data traffic in the cloud system and cloud computing system running status should be monitored in real time. The abnormal action of the network and system must be detected and fixed timely. The network attack detection and defense system must be deployed in the cloud network. The service interruption and system failures because of hackers must be amended. The disaster recovery mechanism of the cloud computing platform must be realized which includes important system backup and data disaster recovery. The emergency response mechanism and the emergency response capabilities for emergency cases must be established and improved. The user information availability, privacy and integrity must be protected.

III. Research Questions

RQ1. What are the major security challenges encountered by Cloud Computing?

RQ2. What are the security hurdles encountered by cloud computing adoption?

RQ3. Which security threat mitigation techniques are available to ensure the acceptable security of Cloud Computing services?

The purpose of RQ1 is to identify the security issues that arise in cloud computing when the user makes use of cloud services and of RQ2 is to identify the security attacks. The RQ3 presents up to date mitigation techniques that are implemented in cloud Computing environments to ensure reliable and secure services. When the data is in transit state the main security risk associated with technology used to transfer the data among the networks.

The Impact of Cloud Computing on Network Security and the Risk for Organization Behaviors

Systematic Analysis of the Cloud Security

Issues Related Systematic Review

Question Validation

In this step, the question is focused on identifying the main issues in cloud computing security related to threats, risks, vulnerabilities, solutions and requirements of the network security of cloud computing.

Sources Selection

The selection of sources are defined in this research based on the following: Scholar Google, ACM digital Library, ScienceDirect, DBLP, and IEEE digital library.

Results and Discussion

Table II shows that virtualization and data storage are the most important, and any attack on these will cause harm. These solutions also affect the cloud, and it might have a significant impact.

T04 (VM scape) to take control of the infrastructure SPI

Table II Vulnerabilities in cloud computing

Vulnerabilities	Description	level
V01(resources)	Inaccurate modeling usage	SPI
V02 (data related)	Unrestricted allocation	SPI
V03 (Insecure Appl.) interfaces	Weak credential	SPI

To summarize the current existing vulnerabilities and threats related to cloud computing security, a literature systematic review is carried out. In order to analyze the major security issues related to vulnerabilities and threats in these related existing literature for identifying the cloud computing security levels.

Attacks on lower levels have a far greater impact on the higher levels. Table III provides an overview of the hazards associated with Cloud Computing. Table III, like Table II, discusses the dangers connected with the science used in cloud settings, as well as which cloud service providers are vulnerable to these threats. Table IV describes the connection between risks in addition to vulnerabilities and how the threat is able to make use of vulnerability to compromise the product.

Cloud computing makes use of a variety of current technologies such as virtualization, online browsers, and web services, accelerating the growth of cloud locations. As a result, any vulnerability connected to

V04 (virtual machine)	Possible covert channel	SPI
V05 (virtual image)	Uncontrolled virtual machine	SPI
V06 (hypervisors)	Complex code	SPI
V07 (virtual network)	Sharing of virtual networks	SPI

Table III Threats in cloud computing

Threats	Description	Level
T01 (account risk)	Attacker access user profiles	SPI
T02 (data leakage)	Attacker recover data	SPI
T03 (denial of service)	the system cannot satisfy any request	SPI
T05 (VM hopping)	VM is able to gain access to another VM	SPI
T06 (VM creation)	Malicious VM creation	SPI
T07 (VM migration)	Insecure VM migration	SPI

		resources	scanners
V05	T05	command injection	Web application scanners
V06	T06	most virtual machines monitors	Mirage
V07	T07	Sniffing and spoofing virtual networks	network modes: “bridged” and “routed

Table IV threats and vulnerabilities relationship

Vulne.	Threats	Description	Possible solutions
V01	T01	Use user profile account	Identity and Access Managem ent Guidance
V02	T02	Data cannot be removed	Dynamic credential
V03	T03	Side channel	Digital Signatures
V04	T04	An attacker can request more computational	limited computatio nal resources

Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study

Cloud Computing and Blockchain

Blockchain overcomes the key challenge of cost in cloud computing, enabling its decentralization to eliminate the risk of data violations. Although cloud computing tends to be cheaper than blockchain technology, it is quite expensive when used with a variety of objects. Blockchain enables the direct connection to massive GPU mining companies to gain their computing power. Moreover, blockchain
storage accounts cannot easily be targeted or hacked, and thus it is difficult for a hacker to access large

Table 1: Survey on cloud security concerns

Reference Number	Solved problems	Blockchain techniques
[21]	Transparency issues related to TTPs	Ethereum and white list policy
[22]	Forgery attacks	SMS and Ethereum
[23]	Tenant and service accounts	Smart contract and quorum
[24]	Data privacy	Demand response management, and public key infrastructure
[25]	Data traceability	DataProv, ProvChain and CoPS
[26]	Integrity verification	Two-layer blockchain network

amounts of data through blockchain, whose data are stretched out as a chain and not together in one place.

Challenges and Privacy Aspects of Cloud Computing and Possible Solutions

The cloud computing environment faces various challenges and privacy concerns. Hence, effective security measures should be implemented. Tab. 2 identifies these challenges, their nature, and possible solutions.

Table 2: Challenges and privacy aspects of cloud computing, and their possible solutions

Table 2: Challenges and privacy aspects of cloud computing, and their possible solutions

Cloud security challenges/concerns	Nature of problem	suggested solutions
Data Security and confidentiality issues [27]	Data confidentiality	Hashing and encryption
Browser security [27]	Web Service Security	SSL/TSL for client authentication
Data availability and reliability issues [27]	Uncertainty in service of reliability	Authorization and authentication
Data loss or leakage prevention	Unauthorized access to infrastructural components	Fragmentation redundancy and scattering techniques [28]
Access control [29]	Illegitimate access	Enforcement of access policies
Eavesdropping and confidentiality [30]	Eavesdropping and alteration	Proper integration and confidentiality mechanism
Data Authentication [31]	Unauthorized access	Application of one-way hash function [32]
Data privacy and integrity	Unauthorized access	Native and integrity mechanisms
DoS attack	Malicious attacks	Cryptographic techniques
Malicious insiders	Loss of data integrity and confidentiality	Standard cryptographic algorithms
Spoofing, phishing [33]	Data forgery	IPS and IDS
Distributed denial of service (DDoS) [34]	DDoS	Fuzzy logic-based mechanisms

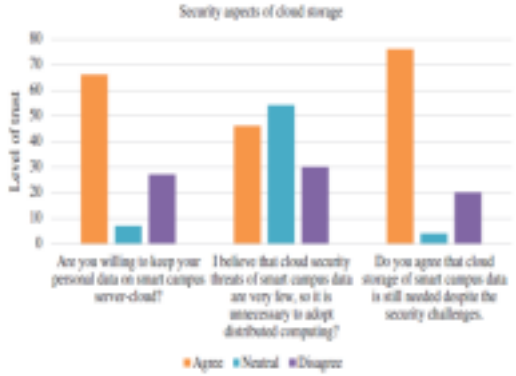

Figure 2: Security aspects of cloud storage

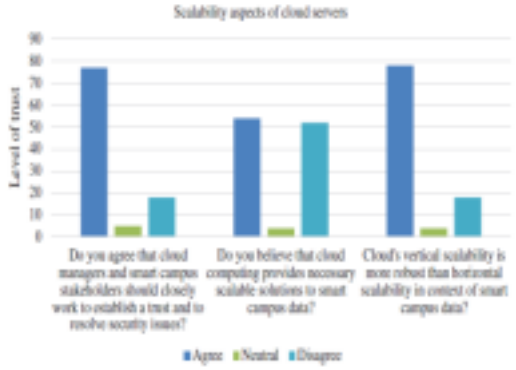

Figure 3: Scalability aspects of cloud storage

Fig. 2 addresses the security aspects of cloud storage. We can see that 76% of stakeholders were willing to keep their data on the cloud, and 46% believed that cloud storage comes with security issues. Many participants provided a neutral response, which indicates uncertainty. Furthermore, 76% of respondents believed that cloud storage for a smart campus is important despite security challenges. Here, we observe that people mostly trust cloud servers for smart campus data management irrespective of security issues.

Fig. 3 shows the scalability concerns for cloud storage. We can see that 78% of stakeholders believed that cloud managers and smart campus stakeholders should coordinate on the policies for smart campus data management on cloud servers so as to maximize data protection. Similarly, 56% of people believed that cloud storage provides scalable solutions. A small number of participants gave a neutral response, which indicates uncertainty related to the scalability of the cloud. Moreover, 78% of respondents believed that vertical scalability is more appealing than horizontal scalability. small number of respondents did not provide feedback, while another small number of respondents thought

horizontal scalability is better than vertical scalability.

Cloud computing is an evolving, internet-based technology that tends to dominate in computer science and information technology applications that involve large scale network computing. Cloud computing is a shared pool of resources that is gaining popularity because of its affordability, performance, and availability. Cloud computing faces challenges including data privacy, intellectual property rights, data security, and authenticated access. We studied its security and privacy through a case study in a smart campus scenario. We seek to highlight the major security vulnerabilities in cloud computing since it has become the most commonly used method of virtualization in large and modern data centers and cloud infrastructures. The major threats and open security issues are a breach of data, IP spoofing, ARP spoofing, DNS poisoning, injection with SQL, injection with OS, LDAP injection, orchestration of the cloud, and zombies or DDos.

Cloud Computing and Security Issues

Deployment Model Security Issues

Security Problems with Platform-as-a-Service (PaaS)

PaaS enables the deployment of cloud-based applications without incurring additional costs for the purchase and upkeep of the supporting hardware and software layers. A safe and dependable network is necessary for PaaS. Two software layers make up PaaS application security: security of the PaaS platform itself and security of customer apps installed on a PaaS platform.Interactions with Third Parties Due to the fact that PaaS (Platform as a service) models provide third-party web service components, such as mashups, they pose security vulnerabilities. Users of PaaS are reliant on the security of both third-party services and web hosted development tools.

Construction Life Cycle

The complexity of creating safe applications that might be hosted on the cloud may provide a challenge for developers. The System Development Life Cycle and security will be impacted by how quickly cloud-based applications change. Software developers must be aware.

Infrastructure Security from Below Software providers are

responsible for protecting the underlying infrastructure and the application services in PaaS because software developers typically do not have access to the lower levels. Developers do not have the certainty that the development environment tools given by a PaaS provider are secure, even if they are in charge of security.

Pooling resources and cloning
Data replication or duplication is called "cloning." Cloning can result in data leakage issues that make the machine's legitimacy obvious.

REAL LIFE EXAMPLES
These real life examples underline the significance of deploying efficient security measures to safeguard sensitive data. In 2013, Target suffered a security breach that exposed the credit card information of 70 million consumers. Using the monitoring system of an HVAC contractor, hackers were able to enter Target's network, which resulted in the breach. Similar to this, Home Depot's network was compromised for almost six months through the use of a third-party
vendor's username and password, resulting in the loss of 53 million emails and 56 million credit or debit cards. The need for appropriate network security measures was highlighted by the fact that Sony was also a victim of a security breach that resulted in the loss of computers and servers. Google and Microsoft have had data breaches in addition to these incidents.

Users must rely on a variety of protection policies and practices, including data encryption, stringent access control, and efficient backup management systems, to reduce hazards. Contingency measures like Hot Sites and Warm Sites can be used in the event of service availability issues, such as a failure or catastrophe. In the context of cloud computing, user authentication, authorization, and auditing are crucial in order to verify that the people using the services are, in fact, who they say they are. User and password, token or card, as well as retinal or fingerprint analysis are all examples of authentication techniques. Cryptography techniques, including the use of encryption keys and algorithms, should be widely employed to protect data communicated when using cloud computing. It is also advised to utilize a VPN because it offers a higher level of privacy and data integrity due to its usage of encryption and encapsulation techniques.

CONCLUSION

Cloud computing is a relatively new idea, but it has a lot to offer customers in terms of scalability, efficiency, and flexibility. It does, however, also present a number of security issues that might prevent enterprises from using it. As the technology uses many other technologies and inherits their security challenges, it is essential to understand the vulnerabilities that exist in cloud models in order to fully take use of the advantages of cloud computing. Cloud customers have a lot of concerns about

Cloud Computing Security

How to ensure safety?

virtualization, which allows several users to share a single physical server. Due to shared physical resources amongst tenants, this strategy may cause security concerns. The biggest security risks in cloud computing are storage and networks, both of which are targets for some attacks.

Depending on the service model, such as IaaS, PaaS, or SaaS, cloud models vary, and each model has a unique set of security concerns. For instance, the customer is in charge of protecting their operating system, data, and applications when using Infrastructure as a Service (IaaS). In contrast, the provider of Software as a Service (SaaS) is in charge of protecting the application and the data. With Platform as a Service (PaaS), the platform is secured by the provider, while the client is in charge of protecting their application and data.

Multitenancy, which enables multiple users to share the same physical resources, is another essential component of cloud computing. To guarantee the security and privacy of data in the cloud, multi-tenancy creates a number of security risks, including unauthorized access, data leakage, and application vulnerabilities. To maintain the safety and security of their data in the cloud and to help organizations make educated decisions about their cloud adoption strategy, it is crucial that they have a better awareness of the security challenges and vulnerabilities in cloud com

References:-

[1] Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. International Journal of Network Security & Its Applications, 6(1), 25.

[2] Brandao, P. R. (2019). Cloud computing security. IJCST, 10(1).

[3] Ouda, A. J., Yousif, A. N., Hasan, A. S., Ibrahim, H. M., & Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organization behaviors. Webology, 19(1), 195-206.

[4] Ali, M., Malik, S., Khalid, Z., Awan, M. M., & Ahmad, S. (2020, August) Security Issues, Threats And Respective Mitigation In Cloud Computing–A Systematic.

[5] Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., Haq, I. U., Jhanjhi, N. Z., ... & Masud, M. (2022). Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study. Intelligent Automation & Soft Computing, 31(1).

[6] Liu, W. (2012, April). Research on cloud computing security problem and strategy. In 2012 2nd international conference on consumer electronics, communications and networks (CECNet) (pp. 1216-1219). IEEE.

[7] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[8] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. International Journal of Engineering Research and Applications, 7(6), 31-38.