Cloud Computing Security: Threats, Vulnerabilities, And Mitigation Techniques

Prof. Himanshu Tarale[1], Mr. Onkar Kailas Mane[2] ,Miss. Sharayu Konde[3]
Lecturer, Dr. Rajendra Gode Institute of Technology and Research, Amravati.[1]
Master Students[2,] Dr. Vishwanath Karad MIT World Peace University India.[2] Modern college of Engineering, Pune, India.[3]

***Abstract*— Cloud computing has become increasingly popular in recent years because of its scalability, flexibility, and cost-effectiveness. However, the security of cloud computing is still a major concern, as the every now and then migration of sensitive data to the cloud exposes it to a wide range of potential threats and vulnerabilities by third party attackers like hackers. This paper provides an overview of the major security threats and vulnerabilities associated with cloud computing, including unauthorized access, data breaches, denial of service attacks, and insider threats. It also examines the potential risks of data isolation, and data loss in the cloud environment. In addition, this paper presents a comprehensive review of the various security measures and mitigation techniques that can be implemented to protect cloud-based systems and data. These include encryption, access control, monitoring, and auditing, as well as secure software development practices and disaster recovery planning. Overall, this paper highlights the importance of addressing cloud computing security concerns and adopting a comprehensive approach to risk management to ensure the confidentiality, integrity, and availability of cloud-based systems and data.**

Keywords*— *cloud, cloud computing, threats, vulnerabilities, mitigation techniques.

I. INTRODUCTION

Cloud computing has become a key technology for organizations, providing a flexible and scalable infr astructure for storing, processing, and accessing dat a and applications. However, this technology also p oses significant security issues due to the complex a nd distributed nature of cloud systems. Cloud comp uting threats and vulnerabilities can compromise the confidentiality, integrity and availability of data an d applications, resulting in significant financial, lega ,and reputational consequences.[1] This briefing pa per will provide an overview of threats andvulnerab ilities facing cloud computing, including malware, d ata breaches, denial of service attacks, and insider th reats. This article also discusses techniques for dete cting and mitigating these threats, including access control, encryption, intrusion detection and preventi on, and threat intelligence.

The objective of this review paper is to provide a co mprehensive understanding of the securiychallenges facing cloud computing and the techniques used to mitigate them. This document will be an invaluable resource for , researchers, and practitioners intereste d in understanding

the state of the art in cloud computing security and developing effective security strategies forcloud sys tems.

II. LITERATURE REVIEW

2.1 Threats to Cloud Computing:

Cloud computing has transformed the way organizations manage their IT infrastructure, enabling them to access a wide range of services and resources on-demand, and at a significantly lower cost than traditional on-premises solutions. However, this shift towards cloud-based computing has also exposed organizations to a new set of security threats and vulnerabilities. As more sensitive data is stored and processed in the cloud, the potential risks and impact of cyber-attacks have increased.[2]

Threats to cloud computing can come from various sources, including malicious insiders, external attackers, and third-party service providers. These threats can result in data breaches, unauthorized access, data loss, and other security incidents that can severely impact an organization's reputation, finances, and operations.

To address these threats, organizations must adopt a comprehensive and proactive approach to cloud computing security. This requires implementing robust security measures and mitigation techniques, such as encryption, access control, monitoring, and auditing, as well as ensuring that third-party service providers adhere to strict security standards.

Figure 1. Threats to cloud computing.

Cloud computing systems are vulnerable to several types of security threats that can impact data security. These include:

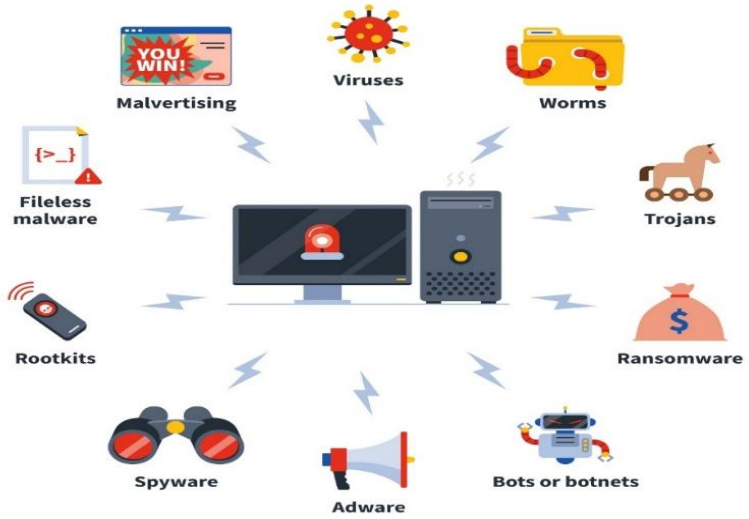

Figure 2. Types of Malwares.

Malware and Viruses: Malware and viruses are major security threats to cloud computing systems. These malicious programs can infect cloud systems and cause significant damage to data, applications, and infrastructure. The impact of malware and viruses on cloud systems can be severe, resulting in data loss, reputational damage, and financial loss.

Malware and viruses can enter cloud systems through various means, including phishing attacks, malicious downloads, and vulnerabilities in software and hardware components.[3] Once inside cloud systems, malware and viruses can spread quickly, infect other systems, and compromise the security of the entire infrastructure. To protect cloud systems from malware and viruses, effective security measures such as firewalls, intrusion detection and prevention systems, and anti-virus software must be implemented. Regularly updating and repairing software and hardware components also help prevent malware and viruses from exploiting vulnerabilities. Data Breaches: They pose a significant threat to clo ud computing as they can lead to unauthorized acce ss to sensitive data stored in the cloud. One of the main causes of data breaches is weak access control s, which allow attackers to gain unauthorized access to cloudbased services.[4] Access controls should b e designed to limit user privileges and provide acces s only to authorized users

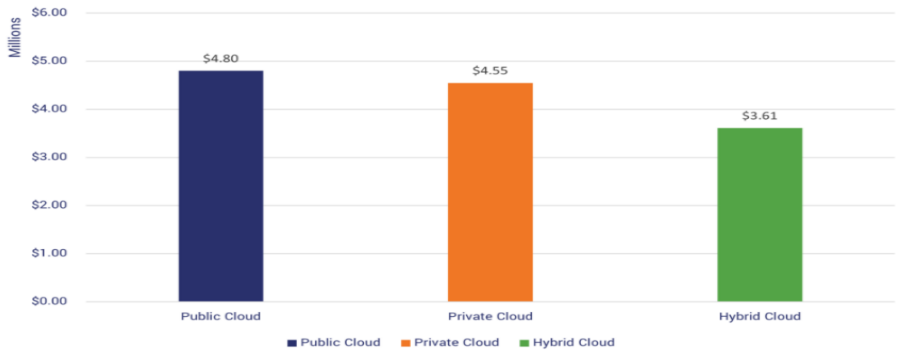

Figure 3. Cloud-Based breaches average total costs.

Additionally, data encryption helps protect sensitive data in the cloud from unauthorized access. Encryption involves converting data into a form that cannot be easily understood without a decryption key, ensuring that even if an attacker accesses the encrypted data, they cannot read it without the decryption key.[5] Effective data encryption technology and strong access control can greatly reduce the risk of data leakage in cloud computing.

Insider threats: Insider threats are another major security challenge in cloud computing. These threats occur when employees or contractors with access to sensitive data misuse cloud resources for personal or malicious gain. Insider threats can be intentional or unintentional, and can include things like stealing data, deleting, or modifying data, or simply accessing data they shouldn't.

The risk of insider threats can be reduced through careful management and monitoring of user access control, as well as employee training and awareness programs. It's important to have strong access controls in place to ensure that users only have access to the data and applications necessary for their job functions. Regular monitoring and auditing of user activity can also help detect and prevent insider threats.[6] Additionally, employee training and awareness programs can help prevent unintended insider threats by educating employees on the importance of security best practices and the potential consequences of security breaches. By taking proactive steps to mitigate insider threats, businesses can better protect sensitive data stored in the cloud.

Denial Of Service (DoS): This attack is a cyberattack designed to disrupt the normal operation of a cloud system by overwhelming it with a flood of traffic. In a DoS attack, the attacker sends a large number of requests to the cloud system, causing the cloud system to crash or become unavailable, resulting in service disruption for legitimate users. This attacks can have serious consequences for cloud computing, especially for mission critical systems that depend on cloud resources.[7] To mitigate the similar risk of DoS attacks, it's important to implement strong security measures, such as firewalls and intrusion detection systems, to identify and block malicious traffic. Additionally, cloud providers must have robust backup and recovery systems to ensure rapid recovery of critical systems in the event of a DoS attack. In recent years, a new type of DoS attack known as Distributed Denial of Service (DDoS) has emerged, in which attackers use networks of infected devices to overwhelm cloud systems. DDoS attacks are particularly difficult to mitigate because they can involve a large number of attackers and devices.

Effective DDoS attack mitigation strategies include a combination of traffic filtering and redirection, as well as the use of distributed infrastructure to absorb attack traffic. By implementing these policies, cloud providers can better protect their systems from the risk of DoS attacks.

Advanced Persistent Threats (APTs): They are a particularly difficult type of cyberattack to detect and prevent in cloud computing. APTs are sophisticated attacks that use multiple methods to gain access to cloud systems and go undetected for long periods of time. These attacks often involve a combination of social engineering, malware, and other advanced techniques to evade detection and gain access to sensitive data.

APTs are particularly dangerous in cloud computing because they can have a significant impact on multiple organizations sharing the same cloud infrastructure. To reduce the risk of APT, it's important to implement a multi-

layered security approach that includes strong acces s controls, ongoing monitoring and analysis of user activity, and security testing and auditing. regular se curity.

Additionally, organizations should invest in employ ee training and awareness programs to educate empl oyees about the risks of APTs and how to recognize and prevent them. By implementing effective secur ity measures and staying alert to signs of APT activi ty, organizations can better protect their cloud syste ms from the risk of advanced persistent threats. It is important to understand the latest threats and trends in APT attacks, as attackers areconstantly improvin g their tactics and techniques.

2.2 Vulnerabilities in Cloud Computing:

The cloud provides many benefits such as scalability, cost savings and flexibility, but it also creates new security challenges. Due to the nature of cloud computing, resources and data are shared across multiple users and locations, opening the door to multiple vulnerabilities. Cloud computing security is critical to protecting sensitive data and systems, and any vulnerability can result in significant data breaches or financial losses. Therefore, understanding the vulnerabilities of cloud computing is essential to implement effective security measures to protect against these risks. In this context, this paper explores some of the vulnerabilities in cloud computing and how to mitigate them.

Table 1. Network related cloud threats

Threat	Vulnerability	C	I	A
T1. Malicious probes or scans	▪ Open ports ▪ Unavailable or misconfigured IDS	✓		
T2. Cross - VM attack via side channels	▪ Multi-tenancy	✓	✓	✓
T3. Data leakage on up/download, intra-cloud T4. Man-in-the-Middle	▪ Communication encryption vulnerabilities ▪ Weak authentication mechanism ▪ Poor patch management	✓	✓	✓
T5. Denial of Service	▪ Poor system configuration ▪ Inadequate resource filtering ▪ Weak policies for resource capping			✓
T6. Flooding attack via bandwidth starvation T7. Fraudulent resource consumption attack	▪ Bandwidth Under-provisioning ▪ Exploitation of the Cloud Pricing Model			✓
T8. Cross-site scripting	▪ Insertion of unchecked data in restricted system locations ▪ Lack of monitoring mechanism	✓	✓	✓
T9. Cross-site request forgery	▪ Weak authentication or monitoring mechanism ▪ Insertion of unauthorized commands in the browser	✓	✓	✓
T10. Cookie manipulation	▪ Lack of hashes to protect the cookie ▪ Weak encryption mechanism	✓	✓	✓
T11. Cookie replay attack	▪ Insecure system databases ▪ Lack of timestamp	✓	✓	

Table 2. System or Data-oriented cloud threats.

Threat	Vulnerability	C	I	A
T12. Brute force attacks T13. Dictionary attacks T14. Privilege escalation	▪ Weak password policy ▪ Weak encryption or authentication	✓	✓	✓
T15. Buffer overflows	▪ Application vulnerabilities	✓	✓	✓
T16. Management interface compromise	▪ Remote access ▪ System or OS vulnerabilities ▪ Application vulnerabilities or poor patch management	✓	✓	✓
T17. File system or registry tampering	▪ Poor management of privilege distribution ▪ Weak protection mechanism	✓	✓	✓
T18. Service engine compromise	▪ Hypervisor vulnerabilities ▪ Lack of resource isolation	✓	✓	✓
T19. Dishonest computation in remote servers	▪ Loss of physical control of data and applications		✓	
T20. Connection pooling	▪ Weak authentication	✓	✓	✓
T21. Physical threats (theft, vandalism, etc.)	▪ Unreachable data storage location ▪ Weak physical security measures ▪ Unknown risk profile	✓	✓	✓
T22. Data disclosure/Leakage/Insider threat	▪ Weak encryption or authentication ▪ Insiders on the provider side	✓		
T23. Data loss/Manipulation	▪ Loss of physical control of the data ▪ Poor integrity or backup controls		✓	✓

Table 3. Organizational cloud threats.

Threat	Vulnerability	C	I	A
T24. Loss of governance	▪ Unclear roles and responsibilities ▪ SLA clauses with conflicting promises to stakeholders ▪ Audit or certification not available to customers ▪ No control on vulnerability assessment process ▪ Certification schemes not adapted to the cloud ▪ Lack of information on jurisdictions ▪ Lack of completeness and transparency in terms of use	✓	✓	✓
T25. Lock-in	▪ Poor provider selection ▪ Lack of supplier redundancy ▪ Lack of completeness and transparency in terms of use			✓
T26. Non-compliance	▪ Audit or certification not available to customers ▪ Lack of standard technologies and solutions ▪ Certification schemes not adapted to the cloud ▪ Lack of information on jurisdictions ▪ Lack of completeness and transparency in terms of use	✓	✓	
T27. Service termination or failure	▪ Poor provider selection ▪ Lack of supplier redundancy			✓
T28. Supply chain failure	▪ Cross-cloud applications creating hidden dependency ▪ Poor provider selection ▪ Lack of supplier redundancy	✓		✓
T29. Conflicts between customer hardening procedures and cloud environment	▪ Lack of completeness and transparency in terms of use ▪ SLA clauses with conflicting promises to stakeholders ▪ Unclear roles and responsibilities	✓		✓

In addition to threats, cloud computing systems are vulnerable to several types of vulnerabilities that can be exploited by attackers. These include:

Weak authentication and access control: Weak authentication and access control are the most common security concerns in cloud computing. If access controls are not configured or managed properly, attackers can exploit this vulnerability to gain unauthorized access to sensitive data stored in the cloud. This may include stealing login credentials or using other methods to authenticate and access cloud systems. To reduce the risk of weak authentication and access control,[8] it is important to implement strong security measures, including multi-factor authentication, role-based access control, and regular monitoring and auditing of user activity. Cloud providers should conduct regular security testing and vulnerability assessments to identify and address potential weaknesses in access controls.

In addition, organizations should provide regular training and awareness programs to employees and users, educating them about the importance of strong authentication and access control and the dangers of not following these best practices. By implementing these measures, organizations can better protect their sensitive data stored in the cloud from the risk of weak authentication and access control.

An application programming interface (API): It is a key component of cloud computing, which allows users to access cloud services and applications through a standard interface. However, if APIs are not properly secured, they can be used by attackers to gain unauthorized access to cloud systems and steal sensitive data. Insecure APIs are a common security problem in cloud computing because they are vulnerable to various attacks, including injection attacks, buffer overflows, and cross-site scripting (XSS) attacks. To reduce the risk of insecure APIs, it is important to implement strong security measures, including strong coding practices, regular vulnerability testing and analysis, encryption, and other security protocols to protect sensitive data.

Cloud providers must implement strict security controls to ensure that only authorized users and applications can access their APIs and must regularly monitor and analyse user activity to detect potential security breaches. In addition, organizations should provide regular training and awareness programs to employees and users to educate them about the potential risks of insecure APIs and how to identify and prevent them.

Shared Infrastructure: It is a key aspect of cloud computing that allows multiple users to share computing resources and reduce costs. However,

shared infrastructure also presents security issues, as a single compromised system can affect multiple users and put sensitive data at risk.[9] When multiple users share the same infrastructure, it is important to implement strong security measures that isolate each user's resources and protect them from threats. It can use virtualization and other technologies to create a unique environment for each user, as well as implement strict access control and monitoring to prevent unauthorized access.

In addition, cloud providers must conduct regular security tests and vulnerability assessments to identify potential vulnerabilities in shared infrastructure and take steps to address them. Organizations using cloud computing services must implement their own security measures, such as strong authentication and access control, data encryption, and regular monitoring and control of user activity.

Data Loss: It is a common security concern in cloud computing, as sensitive data stored in the cloud can be lost due to various factors, including human error, hardware failure, or malicious attacks. Human error can occur when users delete or modify data, or when they fail to back up important data regularly. Physical devices that store data in the cloud can fail due to mechanical or electrical problems, or due to natural disasters such as floods or fires.

Malicious attacks such as ransomware or hacking can cause data loss in the cloud. Attackers can use various methods to access cloud systems and exploit vulnerabilities in software or hardware to steal or destroy sensitive information, such as social engineering attacks or phishing emails. To reduce the risk of data loss in the cloud, it is important to implement strong security measures, including regular backups, disaster recovery planning, and encryption and other security protocols to protect sensitive data. In addition, organizations must implement strict access controls and controls to prevent unauthorized access, and regularly train and educate employees and users about the risk of data loss and how to prevent it.

By implementing these measures, organizations can better protect sensitive data from the risk of data loss in the cloud and ensure the availability, integrity, and confidentiality of their data.

Lack of Transparency: It is a common problem in cloud computing, as cloud providers may not provide full visibility or transparency into their security practices. This can make it difficult for customers to assess their security risks and determine whether a particular cloud provider is suitable for their needs. Cloud providers may not include concerns about exposing proprietary information or vulnerabilities that could be used by attackers for various reasons regarding their security practices.[10] Additionally, providers may lack a standardized approach to security, making it difficult to compare security practices across providers.

To answer this challenge, it is important for cloud providers to be more transparent about their security practices and provide customers with clear and comprehensive information about security measures. This may include details of encryption and access control, routine security testing and assessments, and incident response and disaster recovery plans.

In addition, organizations using cloud computing services should perform due diligence on potential cloud providers, including asking for detailed information about their security practices and certifications. By taking these steps, organizations can better assess their security risks and choose the cloud provider that best suits their specific security needs.

2.3 Mitigation Techniques:

Mitigation techniques play an important role in securing cloud infrastructure and reducing the impact of vulnerabilities. Cloud computing presents unique challenges for security professionals due to its distributed nature and shared responsibility model between cloud providers and customers. Effective mitigation techniques include a combination of proactive planning for emerging threats, continuous monitoring, and rapid incident response. [11] This article will explore the most effective ways to secure your cloud infrastructure, including access control, encryption, network security, and disaster recovery planning. By understanding these techniques, organizations can better protect cloud resources and reduce the risk of security breaches.

To address the various security concerns in cloud computing, several mitigation techniques are used. These include:

Encryption Techniques: Encryption is a key security measure used in cloud computing to protect sensitive data stored in the cloud. Encryption involves the use of algorithms to convert plaintext data into ciphertext, readable only by authorized users with encryption keys. By encrypting sensitive data in the cloud, organizations can ensure that even if attackers can access the data, they cannot read it without the right keys. This helps protect against data theft and other malicious activities that may compromise the confidentiality, integrity, and availability of data. Encryption can be applied to data in transit and data in the cloud. Data in transit encryption involves encrypting data as it travels between the user and the cloud provider, while data in transit encryption involves encrypting data stored in the cloud.

To ensure the effectiveness of encryption, it is important to implement strong encryption protocols and regularly update encryption keys and algorithms to protect against new and emerging threats. In addition, organizations must implement strict access controls and controls to prevent unauthorized access to encryption keys and sensitive data.

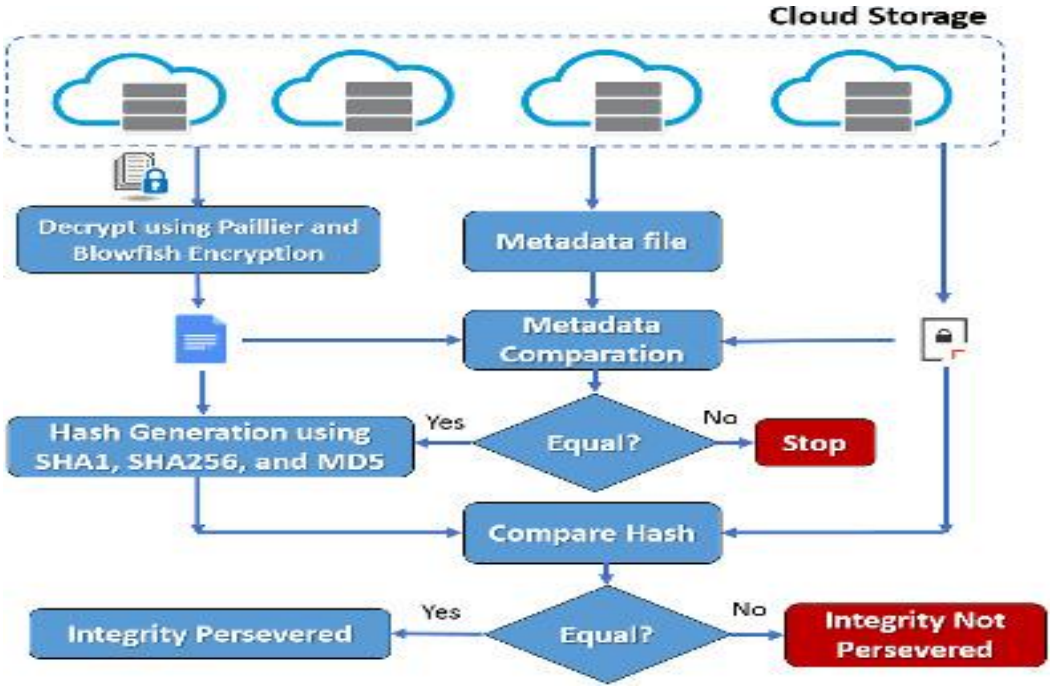

Figure 4. Integrating encryption techniques for securing data storage in cloud.

Access Control: Access controls are security measures implemented to restrict access to sensitive data, systems, and resources to only authorized users. These controls are used to ensure that confidential information is accessible only to those who need it, and that unauthorized persons cannot access it. Access controls can take many forms, including passwords, biometric authentication, access cards, and other methods. These controls can be implemented at multiple levels, including physical, logical, and administrative levels.

Physical access controls can include security guards, locked doors, and surveillance systems that limit access to specific buildings or areas. Logical access controls may include usernames and passwords, digital certificates, or other forms of authentication that allow access to computer systems or networks. Administrative access controls may include policies and procedures, such as background checks and security training, implemented to monitor access and user behaviour.

Security Monitoring: Security monitoring refers to the process of monitoring and analysing an organization's digital environment to detect and respond to security threats in real time. This is necessary to ensure the security of the organization's sensitive data and systems. Continuous security monitoring involves the use of a variety of tools and techniques to collect information from systems and daily systems, including logs, alerts, and other compliance indicators. This data is then analysed to identify potential threats, such as malware infections, unauthorized access attempts, or suspicious network activity.[12]

Once a potential threat is identified, security teams can quickly diagnose and respond to mitigate the impact of an attack. This can include blocking the source of the threat, isolating affected systems, and restoring data from backups.

Effective security controls require a combination of technical expertise, advanced tools, and robust processes and procedures. By implementing regular security controls, organizations can significantly reduce the risk of data breaches and other security incidents and ensure the security and privacy of their sensitive data.

Regular Audits: Regular security audits are an important part of any organization's security program. These inspections help identify vulnerabilities in the organization's systems and operations and help ensure that security controls are working effectively.

A security audit typically includes a comprehensive review of the organization's security policies and procedures, as well as a technical assessment of existing security controls. This may include penetration testing, vulnerability assessments, and other technical assessments to identify weaknesses in the organization's security defences.

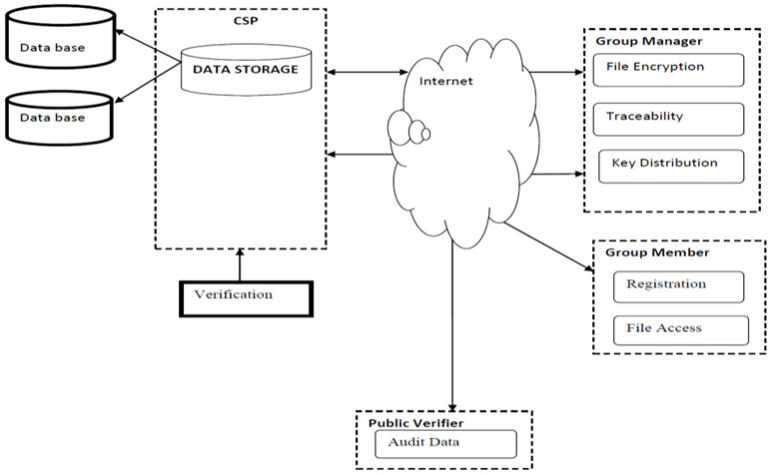

Figure 5. Public auditing in cloud.

The results of security audits are used to prioritize security improvements, allocate resources to address identified vulnerabilities, and ensure that the organization's security program meets best practices and industry standards. Regular security audits can help organizations meet regulatory requirements and demonstrate due diligence in protecting sensitive data. They can also provide valuable feedback that enables senior management to make informed decisions about security investments and priorities.

Backup and recovery: Data backup and recovery processes are an important component of any organization's data protection strategy. This procedure is designed to ensure data recovery in the event of data loss due to equipment failure, natural disasters, or malicious attacks. Backing up data involves creating two copies of an organization's data that can be stored on-premises or in the cloud. This backup data can be used to restore lost or corrupted data in the event of an unexpected connection or attack.

The recovery process is designed to ensure fast and efficient data recovery in the event of an incident. This may include restoring data from backups, repairing damaged hardware, or using other methods to recover lost or damaged data.

An effective data backup and recovery process requires careful planning, implementation, and testing. This may include developing backup and recovery policies and procedures, selecting appropriate backup solutions, and regularly testing the effectiveness of those solutions.

III. CONCLUSION

In summary, cloud computing offers many benefits to individuals and businesses, but it also comes with its own security risks. The distributed nature of cloud infrastructure and the shared responsibility model between cloud providers and customers means that security must be a priority. Threats and vulnerabilities such as data breaches, DDoS attacks,

and insider threats pose significant risks to cloud infrastructure, resulting in data loss, financial loss, and damage to an organization's reputation. However, effective practices such as access control, encryption, network security, and disaster recovery planning can help mitigate these risks. By applying these techniques, organizations can better protect their cloud infrastructure and protect sensitive data and systems from cyber-attacks. Cloud computing security is an ongoing process that requires continuous monitoring, testing, and updates to stay ahead of emerging threats. That's why it's important for organizations to be aware of the latest threats, vulnerabilities, and mitigations to ensure the safety of their cloud infrastructure.

REFERENCES

[1] Buyya, R., Broberg, J., Goscinski, A.M.: Cloud computing: Principles and paradigms, vol. 87. John Wiley & Sons,2010.

[2] Top-Threats-Working-Group: The notorious nine: Cloud computing top threats in 2013. Cloud Security Alliance , 2013.

[3] Goyal, M., & Singh, S. (2012). Security Issues in Cloud Computing: A Survey. International Journal of Advanced Research in Computer Science and Software Engineering, 2(10), 210-217.

[4] Chong, F., Carraro, G., Wolter, R.: Multi-tenant data architecture. MSDN Library, Microsoft Corporation, 2006.

[5] Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T.: Cross-vm side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security, pp. 305–316. ACM, 2012.

[6] Chong, F., Carraro, G., Wolter, R.: Multi-tenant data architecture. MSDN Library, Microsoft Corporation, 2006.

[7] Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T.: Cross-vm side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security, pp. 305–316. ACM, 2012.

[8] Kumar, N., Sharma, S.: Study of intrusion detection system for ddos attacks in cloud computing. In: Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on, pp. 1–5. IEEE, 2013.

[9] Rajput, S., & Singh, A. K. (2016). A Review of Cloud Computing Security Threats and Mitigation Techniques. International Journal of Advanced Research in Computer Science, 7(5), 1-5.

[10] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud Computing: State-of-the-Art and Research Challenges. Journal of Internet Services and Applications, 1(1), 7-18.

[11] Varshney, U. (2014). Information Security in the Cloud Computing Era: New Challenges and Opportunities. IEEE Security & Privacy, 12(4), 61-64.

[12] M.A. Shah, M. Baker, J.C. Mogul, R. Swamina than, Auditing to Keep Online Storage Services Honest Proc. 11th USENIX Workshop Ho t Topics in Operating Systems (HotOS'07) (2007), pp. 1-6.

[13] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.