DATA SECURITY IN CLOUD COMPUTING

Abdul Aman, Adarsh Singh, Shikha Tiwari

[1] *Student , AMITY INSTITUTE OF INFORMATION TECHNOLOGY, Amity University Chhattisgarh, Chhattisgarh, India*
[2] *Student , AMITY INSTITUTE OF INFORMATION TECHNOLOGY, Amity University Chhattisgarh, Chhattisgarh, India*
[3] *Faculty , AMITY INSTITUTE OF INFORMATION TECHNOLOGY, Amity University Chhattisgarh, Chhattisgarh, India*

ABSTRACT

Data security in cloud computing is essential for protecting sensitive information in cloud environments. Encryption is crucial for securing data during transmission and at rest, making it unintelligible to unauthorized individuals. Risks associated with cloud computing include noncompliance, data loss and leaks, trust and reputation damage, business interruption, and financial losses. To mitigate these risks, organizations should implement robust security measures like identity governance, encryption, data backup, IAM, password management, and MFA. Best practices include advanced encryption, DLP tools, unified visibility, security posture, IAM strengthening, and cloud workload protection. These practices address challenges like misconfiguration, unauthorized access, lack of visibility, and compliance. Protecting data confidentiality, integrity, availability, and compliance is crucial, and cloud data security can be enhanced through appropriate measures and practices. This ensures risk mitigation and protection of critical information in the cloud.

Keyword : - *Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats*

1. Introduction

Encryption is a crucial technique for protecting sensitive data in cloud computing. It involves converting data into an unreadable format using encryption algorithms, ensuring that only authorized individuals with the proper encryption key can decipher and access the information. Encryption can be applied to data in transit and data at rest. When data is transmitted over the internet, encryption is used to protect it from interception by unauthorized individuals. The HTTPS protocol, which adds a security layer called SSL, encrypts the data being transmitted between devices and websites. This encryption ensures that even if someone intercepts the data, they cannot understand its contents without the encryption key. Data at rest, or data stored on cloud networks or other storage systems, is also vulnerable to unauthorized access. Encryption is used to transform the stored data into an unreadable code, making it meaningless without the encryption key. This ensures that even if someone gains access to the stored data, they cannot decipher its contents without the proper key. By encrypting data in transit and data at rest, organizations can add an extra layer of security to protect sensitive data in the cloud. Encryption helps maintain confidentiality, integrity, and availability of the data, ensuring that only authorized individuals can access and understand the information.[1,2,3]

1.1 Common cloud data security risks:

In the realm of data management, utilizing the cloud brings with it a host of risks that organizations must confront as an integral part of their comprehensive security strategy. As reliance on the cloud for collecting, storing, and processing critical data continues to grow, two of the most significant risks that emerge are cyberattacks and data breaches. A survey conducted by SailPoint revealed that 45% of companies implementing Infrastructure-as-a-Service (IaaS) have fallen victim to cyberattacks, while 25% have experienced the damaging consequences of a data breach. Furthermore, research indicates that IT security professionals perceive the expanding array of cloud services as the second-largest obstacle hindering their ability to respond effectively to a data breach, and this challenge has only intensified in recent years.[4,5]

Some common risks associated with cloud computing that organizations must contend with are:

1.1.1. Regulatory noncompliance: Compliance requirements, such as those outlined in the General Data Protection Regulation (GDPR) or the Healthcare Insurance Portability and Accountability Act (HIPAA), are made more Complex by the incorporation of cloud computing into the data management landscape.

1.1.2. Data loss and leaks: Inadequate security practices, such as misconfigurations of cloud systems, or threats arising from insiders, can result in data loss or leaks, potentially compromising sensitive information.

1.1.3. Loss of customer trust and brand reputation: Customers place their trust in organizations to safeguard their personally identifiable information (PII). When a security incident leads to the compromise of data, companies invariably suffer a loss of customer goodwill and a tarnished brand reputation.

1.1.4. Business interruption: The failure of cloud technology or platforms, as well as disruptions in supply chains, can cause significant business interruption. Risk professionals worldwide have identified this as one of their top concerns regarding cyber exposure.

1.1.5. Financial losses: The aftermath of cloud security incidents can result in substantial financial losses. The costs associated with incident mitigation, data breaches, business disruption, and other related consequences can accumulate to staggering amounts, potentially reaching hundreds of millions of dollars. To mitigate these risks effectively, organizations must implement robust security measures, including rigorous access controls, encryption protocols, regular security audits, and comprehensive employee training programs. Moreover, fostering a culture of security awareness and promoting proactive incident response strategies are crucial for safeguarding sensitive data and preserving the integrity of cloud-based operations[6,7].

1.2 Cloud computing threats to data security:

When using cloud computing, there are certain threats to the security of your data that you should be aware of. These threats are in addition to the cybersecurity risks that exist for traditional on-site infrastructure.

Here are some common cloud computing threats explained in simple terms:

1.2.1. Unsecure application programming interfaces (APIs): Cloud services and applications often use APIs to provide certain functions, such as user authentication and access. However, these APIs can have security vulnerabilities, like misconfigurations, which can be exploited by attackers to gain unauthorized access to your data.

1.2.2. Account hijacking or takeover: Many people use weak passwords or reuse passwords across multiple accounts, including their cloud accounts. This makes it easier for cyber attackers to gain control of your cloud account and access your sensitive data.

1.2.3. Insider threats: Insider threats involve individuals who have authorized access to your cloud environment but misuse it for malicious purposes or accidentally expose sensitive data. In the cloud, the lack of visibility into the ecosystem increases the risk of insider threats. This could include someone intentionally accessing and stealing data or inadvertently sharing or storing sensitive information in an insecure manner through the cloud. It's important to be aware of these threats and take appropriate measures to protect your data when utilizing cloud services. This may include implementing strong passwords, regularly monitoring, and reviewing access logs, and implementing security controls to safeguard against potential vulnerabilities.

1.3 Safeguards for data security in cloud computing:

To safeguard data security in cloud computing, there are several recommended measures that organizations can take:

1.3.1. Identity governance: Establish a comprehensive view of data access across on-premises and cloud platforms, ensuring visibility, federated access, and monitoring to maintain authorized and appropriate access.

1.3.2. Encryption: Protect sensitive data by encrypting it both during transit and while at rest. Consider implementing a third-party encryption solution for enhanced protection if the cloud vendor does not provide encryption.

1.3.3. Data backup: Back up cloud data locally in addition to the vendor's backup procedures. Follow the 3-2-1 rule: maintain at least three copies of the data, store them on two different media, and keep at least one backup offsite.

1.3.4. Identity and access management (IAM): Implement IAM technology and policies to control access to data, including components such as single sign-on (SSO) and privileged access management.

1.3.5. Password management: Enforce strong password policies and provide employees and end users with password management solutions to promote secure password practices.

1.3.6. Multi-Factor Authentication (MFA): Use MFA to add an extra layer of security beyond passwords, making it harder for attackers to gain unauthorized access to cloud accounts.

By following these safeguards, organizations can enhance the security of their data in the cloud and mitigate potential risks and threats

1.4 Cloud Data Security Best Practices:

To enhance cloud data security, organizations should implement the following best practices:

1.4.1. Leverage advanced encryption capabilities: Encryption is a crucial technique to protect data in the cloud. It involves converting data into an unreadable format using encryption algorithms. Data should be encrypted both when it's stored in the cloud and when it's being transferred. Cloud service providers offer encryption capabilities for data stored in block and object storage services. Additionally, using encrypted connections like HTTPS/TLS ensures the security of data during transit.

1.4.2. Implement a data loss prevention (DLP) tool: DLP tools help detect and prevent data loss, leakage, and unauthorized access in cloud repositories. These tools monitor and analyze data flow, identify sensitive information, and apply appropriate security controls to prevent data breaches.

1.4.3. Enable unified visibility across cloud environments: Having unified visibility allows organizations to monitor and manage their cloud resources effectively. It involves continuous monitoring and detection of misconfigurations, vulnerabilities, and data security threats. This visibility provides actionable insights and guidance for remediation.

1.4.4. Ensure security posture and governance: Establishing proper security policies and governance ensures adherence to industry and government regulations. Cloud security posture management (CSPM) solutions help detect and prevent misconfigurations and control plane threats, reducing security blind spots and ensuring compliance across various cloud environments, applications, and workloads.

1.4.5. Strengthen identity and access management (IAM): IAM solutions streamline identity and access management tasks, enabling organizations to enforce granular access controls and privileges. IAM automates processes such as assigning access controls, monitoring privileges, and deprovisioning accounts. Implementing single sign-on (SSO) allows users to authenticate their identity once and access multiple applications and websites with one set of credentials. Following the principle of least privilege ensures that users only have access to the necessary data and cloud resources.

1.4.6. Enable cloud workload protection: Protecting cloud workloads is critical due to the increased attack surface. Cloud workload protection (CWP) involves securing the entire cloud-native stack, including workloads, containers, Kubernetes, and serverless applications. This protection includes vulnerability scanning, breach prevention, and monitoring to ensure the security of cloud applications throughout their development and production stages.

By implementing these best practices, organizations can enhance the security of their data in the cloud, mitigate risks, and maintain compliance with regulatory requirements.

1.5 Why Is Sensitive Data Protection Important in Cloud Computing?

Protecting sensitive data in cloud computing is crucial for several reasons:

1.5.1. Confidentiality: Sensitive data, such as personal information, financial records, or intellectual property, must remain confidential to prevent unauthorized access or data breaches. Cloud computing introduces additional complexities due to the shared nature of infrastructure and potential exposure to vulnerabilities. By implementing strong security measures and encryption techniques, organizations can safeguard sensitive data and maintain its confidentiality, ensuring that only authorized individuals can access and view the information.

1.5.2. Integrity: Data integrity ensures that information remains accurate, consistent, and trustworthy throughout its lifecycle. In cloud computing, where data is often shared and processed across multiple systems and applications, maintaining data integrity becomes challenging. Organizations need to protect sensitive data from unauthorized modifications, tampering, or corruption. Implementing measures such as access controls, data validation techniques, and secure data transfer protocols helps maintain the integrity of sensitive data, ensuring its reliability for decision-making processes and analytics.

1.5.3. Availability: Data availability is crucial for organizations to operate efficiently and make informed decisions. Cloud computing offers scalability and flexibility, enabling collaboration and access to data from anywhere. However, organizations must ensure that sensitive data remains available and accessible to authorized users while protecting it from accidental or intentional loss or destruction. Implementing backup and disaster recovery mechanisms, redundancy strategies, and access controls helps maintain data availability and minimize disruptions in case of incidents or system failures.

1.5.4. Compliance: Many industries have regulatory requirements and data protection laws that organizations must adhere to, such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act). Failure to protect sensitive data in accordance with these regulations can result in legal and financial consequences. By implementing robust security measures, encryption, access controls, and audit trails, organizations can demonstrate compliance with regulatory requirements and protect sensitive data from unauthorized access or disclosure.

Overall, protecting sensitive data in cloud computing is essential to maintain trust, mitigate risks, comply with regulations, and safeguard the confidentiality, integrity, and availability of critical information. It allows organizations to leverage the benefits of cloud computing while ensuring that sensitive data remains secure throughout its lifecycle.

1.6What are the top cloud computing security challenges?

Cloud security threats can arise due to various factors, and it's crucial to address them to protect sensitive data in cloud computing. [8,9,10]

Here are some of the key challenges and corresponding security measures to consider:

1.6.1. Misconfiguration:
- Implement proper configuration management practices for cloud resources.
- Use cloud storage services with built-in security features such as encryption and access control.
- Regularly review and update security configurations to align with best practices and industry standards.

1.6.2. Unauthorized Access:
- Implement strong authentication mechanisms like multi-factor authentication (MFA).
- Use robust access controls to ensure that only authorized users can access data and applications.
- Regularly monitor and audit access logs to detect and respond to any unauthorized access attempts.

1.6.3. Hijacking of Accounts:
- Encourage users to create strong, unique passwords and enable password complexity requirements.
- Implement additional security measures like security questions or biometric authentication.
- Regularly educate users about phishing and social engineering techniques to prevent credential theft.

1.6.4. Lack of Visibility:
- Implement comprehensive monitoring and logging solutions to gain visibility into cloud environments.
- Utilize security information and event management (SIEM) tools to detect and respond to security incidents.
- Regularly conduct security assessments and audits to identify vulnerabilities and gaps in visibility.

1.6.5. Data Privacy/Confidentiality:
- Encrypt sensitive data at rest and in transit to protect confidentiality.
- Implement robust access controls to restrict data access based on user roles and permissions.
- Comply with relevant data protection regulations and industry standards.

1.6.6. External Sharing of Data:
- Establish strict policies and procedures for external data sharing.
- Vet and approve third-party providers based on their security practices.
- Use encryption and secure data transfer protocols when sharing sensitive information externally.

1.6.7. Legal and Regulatory Compliance:
- Stay informed about applicable legal and regulatory requirements related to data protection.
- Implement security measures and controls to ensure compliance with relevant regulations.
- Conduct regular audits and assessments to validate compliance and address any gaps.

1.6.8. Unsecure Third-party Resources:
- Carefully evaluate and select trusted third-party resources for cloud computing.
- Regularly assess the security posture of third-party resources and ensure they meet security standards.
- Implement strong authentication and access controls when interacting with third-party resources.[11,12,13]

By addressing these challenges and implementing appropriate security measures, organizations can enhance the protection of sensitive data in cloud computing environments and mitigate potential security risks.

1.7 Protecting Data Using Encryption:

Encryption techniques for data at rest and data in transit can be different.
For examples, encryption keys for data in transit can be short-lived, whereas for data at rest, keys can be retained for longer periods of time.

1.7.1 Encrypting Data in transit:
When data is transmitted over the internet, it can be vulnerable to interception by unauthorized individuals. To protect this data, encryption is used. Encryption is a process of converting information into a code that can only be read by authorized users. One way to encrypt data in transit is through the HTTPS protocol. When you visit a website that uses HTTPS, it adds a security layer called SSL (Secure Sockets Layer) to the standard IP (Internet Protocol). This SSL encrypts all the information being transmitted between your device and the website's server. Think of it as sending a secret message. The SSL acts as a special code that scrambles the message, making it unreadable to anyone who intercepts it. Only the authorized recipient, who has the digital key to unlock the code, can decipher the message and understand its content. This encryption ensures that even if someone manages to intercept the data being transmitted, they won't be able to make any sense of it. The decoding process can only happen at the user-level with the proper key, providing a secure and private communication channel between your device and the website you're accessing.[14]

In simple terms, encrypting data in transit means converting the information into a secret code that can only be understood by authorized users. This protects your data from unauthorized access while it travels across the internet.

1.7.2 Encrypting Data at Rest:
When data is stored on a cloud network or any other storage system, there is a risk that it could be accessed by unauthorized individuals. To protect this data, encryption is used even when it's not actively being transmitted.
When data is encrypted at rest, it means that the information is transformed into a code that is unreadable without a special key. This encryption ensures that even if someone gains access to the stored data, they won't be able to understand its contents without the encryption key. Imagine you have a secret diary that you want to keep safe. You write your entries in a secret code that only you understand. This way, if someone finds your diary, they won't be able to read what you've written without knowing the secret code. The encryption key is like the secret code that allows you to decipher and read your own diary. Similarly, when data is encrypted at rest, it is like putting your information into a digital safe. The data is scrambled into a code that is meaningless without the encryption key. Only authorized users with the proper key can unlock and access the data. So, if the stored data is lost, stolen, or

accidentally shared, it remains secure because the encrypted content is essentially useless without the encryption key. The encryption and decryption processes are managed by the software application or system in charge of storing and accessing the data.

In simple terms, encrypting data at rest means converting the stored information into a secret code that can only be understood with a specific key. This ensures that even if someone gets hold of the encrypted data, they can't make any sense of it without the key. It adds an extra layer of security to protect your data from unauthorized access. Different cryptographic techniques are used for encrypting the data these days. Cryptography has increased the level of data protection for assuring content integrity, authentication,and availability. In the basic form of cryptography, plaintext is encrypted into cipher text using an encryption key, and the resulting cipher text is then decrypted using a decryption key as illustrated in Fig.1.

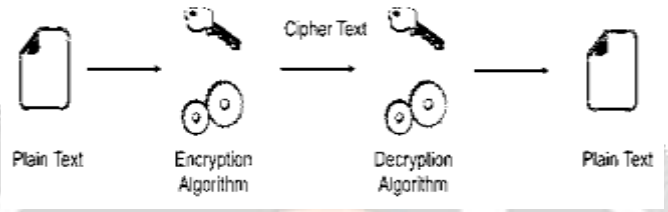

Fig.1 Encrypting data[17]

1.7.3 Normally there are three basic uses of cryptography:

1.7.3.1 Block Ciphers: A block cipher is a method used for encrypting data by applying a cryptographic key and algorithm to a block of data instead of encrypting it bit by bit. It ensures that similar blocks of text do not get encrypted in the same way within a message. To understand how a block cipher works, let's imagine a scenario where we want to encrypt a message. The message is divided into blocks of data, typically 64 bits in size. Each block is then encrypted using an encryption key, which is a specific value used to perform the encryption process. When encrypting the blocks, the output of the encryption process, called the cipher text, is generated. This cipher text is the encrypted version of the original data block. To enhance security and avoid patterns, the cipher text from the previous encrypted block is often applied to the encryption of the next block in the series. This process continues until all the blocks in the message have been encrypted, resulting in a series of cipher text blocks. The order and arrangement of the blocks in the original message are preserved during encryption.[15]

The main idea behind using block ciphers is to divide the data into manageable chunks (blocks) and encrypt each block individually. This approach allows for more efficient encryption and decryption operations, as the algorithm can process larger chunks of data at once.

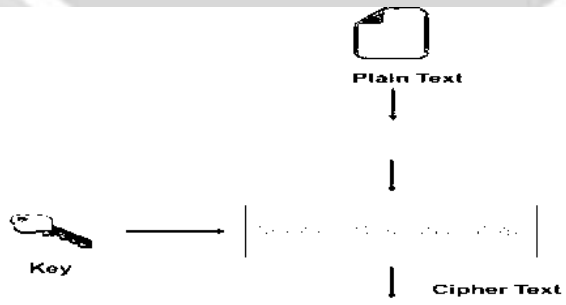

Fig.2 Block Cipher Mechanism[17]

1.7.3.2 Stream Ciphers: A stream cipher is a method used to encrypt data by encrypting each individual bit instead of dividing it into blocks. It relies on the current state of the cipher to determine how each bit is encrypted. In this technique, an encryption key and algorithm are applied to each bit of the data, one at a time. Unlike block ciphers that encrypt data in chunks, stream ciphers encrypt data bit by bit. This approach often results in faster encryption

performance because it has lower hardware complexity. However, it's important to note that stream ciphers can be vulnerable to security issues if not used correctly. If an attacker gains access to the encryption key or the encryption process is flawed, it could lead to serious security problems. When a stream cipher encrypts data, it produces a stream of encrypted bits, which is called the cipher text. To decrypt the cipher text and recover the original plain text, a decryption key is used. The decryption key reverses the encryption process and converts the encrypted bits back into the original data.[16]

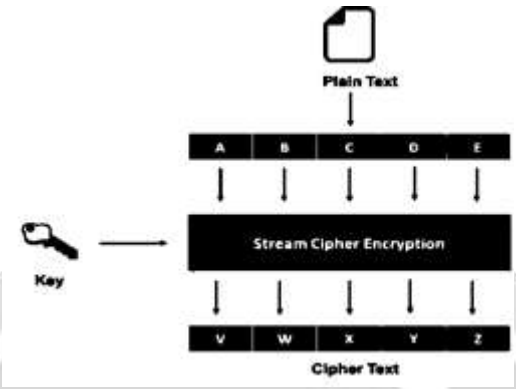

Fig.3 Stream Cipher mechanism[17]

C. Hash Functions: In this technique, a mathematical function called a hash. function is used to convert an input text into an alphanumeric string. Normally the produced alphanumeric string is fixed in size. This technique makes sure that no two strings can have same alphanumeric string as an output. Even if the input strings are slightly different from each other, there is a possibility of great difference between the output string produced through them. This hash function can be a very simple mathematical.
function like the one shown in equation (1) or very complex.
F(x) = x mod 10 (1)
Fig. 4 below shows the mechanism of hash function.
Cryptography

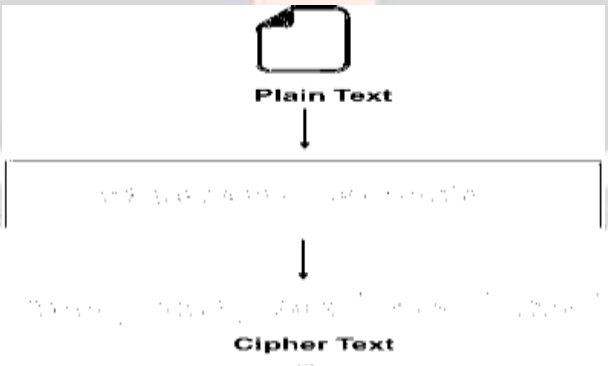

Fig.4 Hash Function Mechanism[17]

1.8 Conclusion:
Data is transformed into an unreadable format and can only be deciphered with the proper encryption key. This ensures that even if someone gains access to the stored data, they won't be able to understand its contents without the encryption key. Encryption at rest is important because it adds an extra layer of security to protect sensitive data from unauthorized access. It ensures that even if the storage system is compromised or the data is stolen, the encrypted data remains meaningless without the encryption key. By encrypting data both in transit and at rest, organizations can maintain the confidentiality, integrity, and availability of their data in cloud computing environments. Encryption helps prevent unauthorized access and protects sensitive information from being exposed or compromised.

REFERENCES:

[1] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," *Build. Infrastruct. Cloud Secur.*, vol. 1, no. September 2011, pp. 3–22, 2014.
[2] M. A. Vouk, "Cloud computing - Issues, research and implementations," *Proc. Int. Conf. Inf. Technol.Interfaces, ITI*, pp. 31–40, 2008.
[3] P. S. Wooley, "Identifying Cloud Computing Security Risks," *Contin. Educ.*, vol. 1277, no. February, 2011.
[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan.2011.
[5] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M.Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *J.*
[6] V. J. Winkler, "Securing the Cloud," *Cloud Comput. Secur. Tech. tactics. Elsevier.*, 2011.
[7] F. Sabahi, "Virtualization-level security in cloud computing," *2011 IEEE 3rd Int. Conf. Commun. Softw. Networks*, pp. 250–254, 2011.
[8] Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM
[9] Ransome, J. F., Rittinghouse, J. W., & Books24x7, I.2009).
[10] Wang, Y., Chandrasekhar, S., Singhal, M., & Ma, J. (2016). A limited-trust capacity model for mitigating threats of internal malicious services. Cluster Computing,19(2), 647-662. doi:10.1007/s10586-016-0560-2
[11] Shah, H. and Anandane, S.S., 2013. Security Issues on Cloud Computing. arXiv preprint arXiv:1308.5996.
[12] Jensen, M., Schwenk, J., Gruschka, N. and Iacono, L.L., 2009, September. On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.
[13] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," *Security*, no.
[14] F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage," pp. 1–6, 2014.
[15] H. Qian, J. He, Y. Zhou, and Z. Li, "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," *Math. Probl. Eng.*, vol. 2010, pp. 7–9, 2010.
[16] T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy," p. 299, 2009.

IMAGE REFERENCES:

[17] 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), IEEE,