DATA SECURITY MANAGEMENT IN CLOUD COMPUTING

CHAPTER-01

Introduction:

1.1 Introductory overview of the topic

Cloud Computing is a collection of various internet services like servers, storage, databases, networking, software, analytics and intelligence and by employing Cryptographic algorithms in cloud computing the user can store and access data in a secure and protective way so that no third part can access and make changes to the user's data. Cryptography handles protection of critical data where the data is no longer under the control of user. In this paper we use AES algorithm to assure that the data is ciphered and is kept safeguarded. This would counteract undesirable interruption into individual information and absence of institutionalization, for example one specialist co-op may have start to finish encryption while others don't.

Data security management in cloud computing involves implementing measures to protect sensitive information stored, processed, or transmitted within cloud environments. Here's a brief introduction:

Understanding Cloud Computing: Cloud computing involves using a network of remote servers hosted on the Internet to store, manage, and process data instead of using local servers or personal computers.

Importance of Data Security: Data is a valuable asset, and ensuring its security is crucial to maintain privacy, comply with regulations, and protect against unauthorized access, breaches, and data loss.

Key Security Considerations:

- Access Control: Limiting access to authorized users and employing strong authentication mechanisms.
- Encryption: Encrypting data both at rest and in transit to protect it from unauthorized access.
- Identity and Access Management (IAM): Managing and controlling access to cloud resources based on roles and responsibilities.
- Compliance and Regulations: Adhering to legal and industry-specific requirements related to data security and privacy.

Security Measures in Cloud Computing:

- Firewalls and Intrusion Detection Systems (IDS): Implementing firewalls to monitor and control traffic, along with IDS to detect and respond to potential threats.
- Data Loss Prevention (DLP): Employing DLP solutions to monitor and prevent unauthorized sharing or leakage of sensitive data.
- Regular Audits and Monitoring: Conducting frequent security audits and monitoring activities to identify vulnerabilities and potential security breaches.

Data Classification and Handling:

- Classifying Data: Categorizing data based on its sensitivity and importance.
- Data Masking and Anonymization: Applying techniques to obscure or anonymize sensitive data, reducing the risk of exposure.

Incident Response and Disaster Recovery:

- Creating Response Plans: Developing strategies to respond to security incidents effectively and minimize damage.
- Disaster Recovery (DR): Establishing measures to ensure data availability and integrity in the event of a disaster.
- Educating Personnel: Educating employees about security best practices, threats, and protocols to enhance overall security posture.

By implementing a comprehensive approach that encompasses these key aspects, organizations can enhance data security in cloud computing environments and safeguard their valuable information.

1.2 Data Security Management in Cloud Computing using Cryptography

Data security management in cloud computing heavily relies on cryptography, a fundamental tool for securing sensitive data. Here's an introduction to data security management in the cloud using cryptography:

Cryptography Fundamentals: Cryptography involves techniques for secure communication, protecting information from unauthorized access or alterations. It uses algorithms to encrypt data (convert into a secure, unreadable form) and decrypt it back to its original state.

Encryption and Decryption:

- Encryption: Converting plaintext (readable data) into ciphertext (unreadable data) using encryption algorithms and a secret key.
- Decryption: Converting ciphertext back into plaintext using decryption algorithms and the corresponding key.

Key Components of Data Security in Cloud using Cryptography:

- Confidentiality: Cryptography helps maintain data confidentiality by encrypting sensitive data, ensuring only authorized parties can decrypt and access it.
- Integrity: Cryptographic hash functions ensure data integrity by generating fixed-size hash values unique to each input. Even a minor change in data results in a significantly different hash.
- Authentication: Cryptographic algorithms authenticate users by verifying their identity through digital signatures or authentication protocols.

Types of Cryptography in Cloud Security:

- Symmetric Key Cryptography: Uses a single key for both encryption and decryption. It's fast and efficient for bulk data encryption.

- Asymmetric Key Cryptography (Public-Key Cryptography): Involves a pair of keys - a public key for encryption and a private key for decryption. It's used for secure communication and key exchange.

Use Cases in Cloud Security:

- Data Encryption at Rest: Encrypting stored data to prevent unauthorized access, using encryption algorithms like AES (Advanced Encryption Standard).
- Data Encryption in Transit: Encrypting data during transmission between the user and the cloud server, ensuring data remains secure during transit.

Key Management:

- Key Generation: Securely generating encryption and decryption keys using cryptographic algorithms.
- Key Storage and Distribution: Safely storing and distributing keys to authorized users, ensuring protection against unauthorized access.

Homomorphic Encryption:

Allows computation on encrypted data without decryption, enhancing privacy and security in cloud-based processing.

Secure Multi-Party Computation (SMPC):

Enables parties to jointly compute a function over their inputs while keeping those inputs private, enhancing privacy and security in collaborative cloud computing.

Integrating cryptographic techniques into cloud computing provides a robust layer of security, ensuring data confidentiality, integrity, and authenticity throughout its lifecycle, making cloud services more trustworthy and resilient against potential threats.

CHAPTER-02

HISTORICAL DEVELOPMENT

2.1 Historical evolution of Data Security in Cloud Computing

The historical evolution of data security management in cloud computing can be outlined through key milestones and advancements:

Early Adoption and Trust Concerns (2000s):

- Cloud computing emerged in the early 2000s, offering the potential for cost-effective and flexible IT solutions.
- Early adopters were cautious due to trust and security concerns, especially regarding data residing outside traditional on-premises environments.

Initial Security Measures (Early 2000s):

- Cloud providers introduced basic security measures like firewalls and access controls to address initial concerns.
- Data encryption for transit and at rest was implemented to enhance data protection.

Maturation and Standardization (Mid-2000s):

- Industry groups and standards bodies, like the Cloud Security Alliance (CSA), started to establish best practices and frameworks for cloud security.
- Concepts like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) began to solidify.

Regulatory Frameworks and Compliance (Late 2000s - Early 2010s):

Governments and industry bodies started developing regulations specific to cloud computing, addressing data protection and privacy (e.g., GDPR, HIPAA). Cloud providers began aligning their security practices with these regulatory requirements.

Advanced Encryption and Key Management (2010s):

Enhanced encryption algorithms and stronger key management practices were introduced to bolster data security. Homomorphic encryption and other advanced cryptographic techniques were explored for secure computation on encrypted data.

Focus on Identity and Access Management (IAM) (Mid-2010s):

- IAM gained prominence to manage user identities, access privileges, and authentication mechanisms within the cloud environment.
- Multi-factor authentication (MFA) became a standard to enhance user authentication.

Security Automation and AI (Late 2010s - Early 2020s):

- Machine learning and AI technologies were integrated into security measures, enabling proactive threat detection and automated responses.
- Security Information and Event Management (SIEM) solutions evolved to provide real-time security monitoring and incident response.

Zero Trust Architecture (ZTA) (Mid-2020s):

- Zero Trust gained traction as a security model, assuming that threats may exist both outside and inside the network.
- Emphasizes continuous verification and validation of security posture, with least privilege access principles.

Resilience and Disaster Recovery (2020s):

An increased focus on disaster recovery and business continuity, ensuring data availability and integrity during cyber-attacks or unforeseen events.

The historical evolution demonstrates a shift from early trust concerns to a more matured and proactive approach to data security management in cloud computing. The industry continuously adapts to emerging threats and regulations, incorporating advanced technologies and best practices to enhance cloud security.

2.2 The early Methods of Data Security Management in Cloud Computing

In the early stages of cloud computing, data security management was a growing concern, and foundational methods were implemented to address security risks. Here are some early methods used for data security management in cloud computing:

1. Access Controls: Basic access controls were implemented to restrict unauthorized access to cloud resources. This involved employing authentication mechanisms and authorization policies to define user access levels.
2. Firewalls: Firewalls were one of the earliest security measures, used to monitor and control incoming and outgoing network traffic to and from cloud environments. They were crucial in preventing unauthorized access and potential attacks.
3. Data Encryption: Encryption was utilized to protect sensitive data both at rest and in transit. Encrypting data ensured that even if unauthorized access occurred, the data would be unreadable without the appropriate decryption keys.
4. Virtual Private Network (VPN): VPNs were employed to create a secure, encrypted connection over the public internet, enabling users to access cloud resources securely, especially when using untrusted networks.
5. Secure Socket Layer (SSL)/Transport Layer Security (TLS): SSL and later TLS were utilized to secure data in transit by encrypting the communication between clients and cloud servers, ensuring confidentiality and integrity during data transmission.
6. Data Masking: Data masking techniques were used to obscure sensitive information, making it difficult for unauthorized users to interpret the actual data.
7. Regular Audits and Logging: Logging and auditing mechanisms were implemented to track and monitor user activities and system events, aiding in identifying potential security breaches and ensuring compliance with security policies.
8. Security Policies and Protocols: Establishing security policies and protocols specific to cloud environments was an early approach. These policies defined guidelines for secure practices, user behavior, and data handling.

9. Secure Data Centers: Physical security measures were applied to protect data centers hosting cloud resources. This included restricted access, surveillance, and other physical security mechanisms to safeguard the infrastructure.
10. Basic Intrusion Detection Systems (IDS): Basic IDS tools were used to monitor network traffic and detect potential intrusions or security threats, providing an initial level of security awareness.

These early methods laid the foundation for the evolving and more sophisticated data security measures we see today in cloud computing. Over time, advancements in technology and a deeper understanding of security risks have led to the development of more robust and comprehensive security strategies.

2.3 Some other early methods of Data Security Management using Cryptography

In the early stages of cloud computing, cryptography played a foundational role in data security management. Here are some early methods of data security management in cloud computing using cryptography:

1. Data Encryption at Rest: Basic encryption techniques were employed to encrypt data stored in cloud servers, ensuring that sensitive information remains secure even if unauthorized parties gain access to the storage.
2. Data Encryption in Transit: Cryptographic protocols like SSL (Secure Sockets Layer) and early versions of TLS (Transport Layer Security) were used to encrypt data as it traveled between the user's device and the cloud server, protecting it from eavesdropping and interception.
3. Hash Functions for Data Integrity: Cryptographic hash functions were utilized to generate fixed-size hash values unique to each piece of data. These hashes were used to verify data integrity and detect any alterations to the data.
4. Secure Channels for Key Exchange: Protocols like Diffie-Hellman key exchange were employed to securely exchange encryption keys between the client and the cloud server, ensuring that keys were not exposed during the exchange process.

5. Digital Signatures for Authentication: Digital signature algorithms were used to verify the authenticity and integrity of messages and data, providing a way to authenticate the sender and detect any tampering.
6. Secure Multi-Party Computation (SMPC): Although in its early stages, the concept of SMPC was explored to allow multiple parties to jointly compute a function over their inputs while keeping those inputs private. This had implications for secure data processing in the cloud.
7. Homomorphic Encryption: Even though in early phases of research, homomorphic encryption was recognized for its potential to allow computation on encrypted data, enhancing privacy and security in cloud-based processing.

These early cryptographic methods formed the basis for securing data in the cloud, providing a level of protection for sensitive information and establishing trust in cloud computing environments. Over time, cryptographic techniques have evolved, becoming more sophisticated and robust to address the evolving landscape of security threats.

CHAPTER-03

TRADITIONAL METHODS

3.1 Data Security Management

Data security management in cloud computing involves implementing measures to protect sensitive information stored, processed, and transmitted within a cloud environment. Key aspects include encryption, access control, data masking, monitoring, and compliance with regulations like GDPR and HIPAA. It's essential to choose secure cloud providers, employ strong authentication mechanisms, and regularly audit and update security protocols to mitigate risks and ensure data privacy and integrity.

Data security management in cloud computing focuses on safeguarding data throughout its lifecycle within a cloud environment. This involves various measures such as:

- Encryption: Encrypting data at rest and in transit to ensure it remains confidential and secure from unauthorized access.
- Access Control: Implementing robust access control mechanisms to restrict access to data based on roles, permissions, and authentication levels.
- Identity and Access Management (IAM): Utilizing IAM systems to manage and control user identities, permissions, and privileges for accessing resources and data.
- Data Masking and Anonymization: Applying techniques to anonymize or mask sensitive data to protect privacy while maintaining usability for authorized users.
- Monitoring and Logging: Continuously monitoring activities and logging events to detect suspicious or unauthorized access and track usage for auditing and compliance purposes.
- Regular Audits and Compliance: Conducting regular security audits to assess compliance with security policies, industry standards, and regulatory requirements.
- Secure Cloud Provider Selection: Choosing reputable and secure cloud service providers that adhere to stringent security standards and certifications.

- Incident Response Planning: Developing and implementing strategies and procedures to respond effectively to security incidents, ensuring minimal impact and rapid resolution.

By combining these measures and staying updated with evolving security threats and technologies, organizations can enhance data security in the cloud and build a robust defense against potential cyber threats.

3.2 Cloud Computing Structure

Types of Cloud Systems

There are main three systems categories: Software as a Service, Platform as a Service and Infrastructure as a Service. Let's look at them in more details as follows:

Software as a Services (SaaS): Traditionally, users prescribe software and it is license in order to install it on their hard disk and then use it, however, in the cloud users do not required to purchase the software rather the payment will be based on pay-per use model. It support multi-tenant which means that the physical backend infrastructure is shared among several users which are unique for each user.

Platform as a Service (PaaS): In PaaS the development environment provided as service. The developers will use vendor's block of code to create their own applications. The platform will be hosted in the cloud and will be accessed using the browser.

Infrastructure as a Service (IaaS): In IaaS, vendors provide the infrastructure as a service where it is delivered in form of technology, datacenters and IT services to the customer which is equivalent to the traditional "outsourcing" in the business world but with much less expenses and effort. The main purpose is to tailor a solution to the customer based on required applications. Table 2 shows cloud computing services that are currently utilized by several providers.

Security Management (SM) includes functions that control and protect access to organization's resources, information, data, and IT services in order to ensure confidentiality, integrity, and availability. Security management functions are methods for authentication, authorization, encryption, etc. Unfortunately, the expanded definitions and standards around security management do not define a common set of security management areas.

Table 1: Cloud Computing Services

	Services	Providers
SaaS	• Support running multiple instances of it. • Develop software that is capable to run in the cloud	• Google Docs • Mobile Me • Zoho
PaaS	• Platform which allows developer to create programs that can be run in the cloud. • Includes several applications services which allow easy deployment.	• Microsoft Azure • Force.com • Google App Engine.
IaaS	•Highly scaled and shared computing infrastructure accessible using internet browser. • Consists of Database, servers and storage.	• AmazonS3 • Sun's Cloud Service

Within the context of Cloud Computing, one of the most important security challenges is to manage and assure a secure usage over multi-provider Inter-Cloud environments with dedicated communication infrastructures, security mechanisms, processes and policies. The aim of Security controls in Cloud computing is, for the most part, no different than security controls in any IT environment from a functional security management perspective. The adaption and reuse of existing traditional security management areas that have to be enhanced for specific Cloud computing requirements (e.g., dynamic reconfiguration, distributed services, etc.) has been proposed.

3.3 Deployment Models of Cloud Computing

According to NIST, the cloud model is composed of four deployment models:

- Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises

- Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

3.4 CLOUD SECURITY AND PRIVACY

In cloud computing, end users' data stored in the service provider's data centers rather than storing it on user's computer. This will make users concerned about their privacy. Moreover, moving to centralized cloud services will result in user's privacy and security breaches. Security threats may occur during the deployment; also new threats are likely to come into view. Cloud environment should preserve data integrity and user privacy along with enhancing the interoperability across multiple cloud service providers. Thus, we would like to discuss data integrity, confidentiality and availability in the cloud. The security related to data distributed on three levels:

- Network Level: The Cloud Service Provider (CSP) will monitor, maintain and collect information about the firewalls, Intrusion detection or/and prevention systems and data flow within the network.
- Host Level: Itis very important to collect information about system log files. In order to know where and when applications have been logged.

- Application Level: Auditing application logs, which then can be required for incident response or digital forensics. At each level, it is required to satisfy security requirements to preserve data security in the cloud such as confidentiality, integrity and availability as follows:

Confidentiality: Ensuring that user data which resides in the cloud cannot be accessed by unauthorized party. This can be achieved through proper encryption techniques taking into consideration the type of encryption: symmetric or asymmetric encryption algorithms, also key length and key management in case of the symmetric cipher. Actually, it is all based on the CSP. For instance, Mozy Enterprise uses encryption techniques to protect customer data whereas Amazon S3 does not. It also depends on the customer awareness where they can encrypt their information prior to uploading it. Also, The CSP should ensure proper deployment of encryption standards using NIST standards in.

Integrity: Cloud users should not only worry about the confidentiality of data stored in the cloud but also the data integrity. Data could be encrypted to provide confidentiality where it will not guarantee that the data has not been altered while it is reside in the cloud. Mainly, there are two approaches which provide integrity, using Message Authentication Code (MAC) and Digital Signature (DS). In MAC, it is based on symmetric key to provide a check sum that will be append to the data. On the other hand, in the DS algorithm it depends on the public key structure (Having public and private pair of keys). As symmetric algorithms are much faster than asymmetric algorithms, in this case, we believe that Message Authentication Code (MAC) will be the best solution to provide the integrity checking mechanism. Studies show that, PaaS and SaaS doesn't provide any integrity protection, in this case assuring the integrity of data is essential.

Availability: Another issue is availability of the data when it is requested via authorized users. The most powerful technique is prevention through avoiding threats affecting the availability of the service or data. It is very difficult to detect threats targeting the availability. Threats targeting availability can be either Network based attacks such as Distributed Denial of Service (DDoS) attacks or CSP availability. For example, Amazon S3 suffered from two and a half hours outage in February 2008 and eight hours outage in July2008.

3.4 Key Data Management Techniques

Data management encompasses various techniques to handle data effectively. Here are some key data management techniques:

- Data Collection: Gathering data from various sources, including databases, sensors, forms, or external APIs.
- Data Storage: Storing data in structured databases, data warehouses, or unstructured formats like NoSQL databases or data lakes.
- Data Cleaning: Identifying and rectifying errors or inconsistencies in data to maintain data quality.
- Data Integration: Combining data from different sources to provide a unified view for analysis.
- Data Security: Implementing measures to protect data from unauthorized access, including encryption, access controls, and regular security audits.
- Data Backup and Recovery: Regularly backing up data to prevent data loss and having mechanisms in place to recover data in case of failures.
- Data Transformation: Converting data into a suitable format for analysis, reporting, or visualization.
- Data Governance: Establishing policies and procedures to ensure data is used responsibly and complies with regulations.
- Master Data Management (MDM): Managing core data entities (e.g., customers, products) consistently across the organization.
- Data Quality Management: Monitoring and improving data quality to ensure accuracy and reliability.
- Data Cataloging and Metadata Management: Creating catalogues and metadata repositories to describe and locate data assets.
- Data Lifecycle Management: Managing data from creation to archiving or deletion, including data retention policies.
- Data Analytics and Reporting: Using tools and techniques to analyze and report insights from data.

- Data Privacy and Compliance: Ensuring that data handling complies with data privacy regulations (e.g., GDPR, HIPAA).
- Data Auditing and Monitoring: Tracking data usage, changes, and access for compliance and security purposes.
- Data Visualization: Presenting data in a visual format to facilitate understanding and decision-making.
- Data Access Control: Restricting access to data based on user roles and permissions.
- Data Migration: Transferring data from one system or storage location to another.
- Data Archiving: Moving less frequently accessed data to long-term storage for cost savings.
- Data Ethics: Consideration of ethical implications when collecting, using, and sharing data.

The specific techniques employed can vary depending on the organization's size, industry, and data needs. Effective data management is critical for deriving value from data and ensuring its reliability and security.

CHAPTER-04

TECHNOLOGICAL ADVANCEMENTS

4.1 Technological Advancements in Data Security

In recent years, data security management in cloud computing has seen remarkable technological advancements, addressing the evolving landscape of cyber threats. Homomorphic encryption has emerged as a pivotal tool, allowing computations on encrypted data without decryption, preserving privacy while performing essential operations. Multi-factor authentication (MFA) has become more sophisticated by integrating multiple authentication factors such as biometrics and tokens, fortifying user authentication and access control. Zero Trust Architecture (ZTA) has gained traction, emphasizing continuous verification and treating every access request as potentially untrusted, significantly bolstering overall security. Another notable advancement is the Software-Defined Perimeter (SDP), which dynamically creates secure network perimeters, offering granular access control and reducing the attack surface.

Machine learning, artificial intelligence, and behavior analytics have revolutionized threat detection, enabling real-time anomaly detection and quicker response. Blockchain technology has found its place in securing transactions and maintaining an immutable record of activities, enhancing data integrity. Secure containers and microservices architecture have improved security by isolating applications and minimizing attack vectors.

Advanced Data Loss Prevention (DLP) solutions are in use to monitor and prevent unauthorized data sharing or exposure. Edge computing security has also gained prominence, addressing security concerns related to data processed at the network edge. API security, automation of incident response with SOAR (Security Orchestration and Response), and compliance automation tools further augment the robustness of data security management in cloud computing. These technological strides collectively contribute to a comprehensive approach in safeguarding data, mitigating risks, and upholding the confidentiality, integrity, and availability of information within cloud environments.

4.2 Key Advancements of Data Security in Cloud Computing

1. Homomorphic Encryption: Allows computation on encrypted data without decrypting it, enhancing privacy and security while still performing necessary operations.
2. Software-Defined Perimeter (SDP): Dynamically creating secure network perimeters, providing granular access control and reducing the attack surface.
3. Advanced Threat Detection: Utilizing machine learning, AI, and behavior analytics to detect anomalies and potential security threats in real-time, allowing for faster response.
4. Blockchain for Security: Implementing blockchain to secure transactions, maintain an immutable record of activities, and enhance data integrity.
5. Secure Containers and Microservices: Employing secure containerization and microservices architecture to isolate applications and enhance security through segmentation and reduced attack vectors.
6. Data Loss Prevention (DLP) Solutions: Integrating advanced DLP solutions to monitor, detect, and prevent unauthorized sharing or exposure of sensitive data.
7. Edge Computing Security: Addressing security concerns related to data processed at the edge of the network, ensuring secure transmission and storage.
8. API Security: Implementing robust API security measures to safeguard data during interactions between applications and services.
9. Automated Security Orchestration and Response (SOAR): Automating incident response processes to handle security incidents efficiently and effectively.
10. Compliance Automation: Utilizing automation tools to streamline and ensure compliance with various industry and regulatory standards.

These advancements collectively contribute to a more comprehensive and sophisticated approach to data security management in cloud computing, enabling organizations to mitigate risks, protect sensitive information, and maintain the confidentiality, integrity, and availability of their data.

4.3 Cloud computing threats to data security

While cybersecurity threats that apply to on-premises infrastructure also extend to cloud computing, the cloud brings additional data security threats. Here are some of the common ones:

- **Unsecure application programming interfaces (APIs):** Many cloud services and applications rely on APIs for functionalities such as authentication and access, but these interfaces often have security weaknesses such as misconfigurations, opening the door to compromises.
- **Account hijacking or takeover**: Many people use weak passwords or reuse compromised passwords, which gives cyber attackers easy access to cloud accounts.
- **Insider threats:** While these are not unique to the cloud, the lack of visibility into the cloud ecosystem increases the risk of insider threats, whether the insiders are gaining unauthorized access to data with malicious intent or are inadvertently sharing or storing sensitive data via the cloud.

4.4 The Shared Responsibility Model of the Cloud

One data security area that organizations struggle with in cloud computing is who bears the responsibility for security. With on-premises data centers and infrastructure, the responsibility falls to the organization. But in the cloud, they're using vendor's services, and the lines of responsibilities may feel blurry.

Cloud service providers use the so-called shared responsibility model, also known as "shared controls." The challenge is that the way the responsibility is shared varies among the different cloud models.

In all models, cloud providers are responsible for the physical security of the infrastructure and the customers are responsible for data classification and accountability. For all the other security components, the responsibility either falls on one of the parties or is shared. For example, the cloud provider is responsible for identity and access management if the enterprise uses IaaS, but they share the responsibility if they're using SaaS, PaaS, or FaaS.

4.5 Safeguards for Data Security in Cloud Computing

Data security in the cloud starts with identity governance. Organizations need a comprehensive, consolidated view of data access across its on-premises and cloud platforms and workloads. Identity governance provides:

- **Visibility**—the lack of visibility results in ineffective access control, increasing both risks and costs.
- **Federated access**—this eliminates manual maintenance of separate identities by leveraging Active Directory or another system of record.
- **Monitoring**—the enterprise needs a way to determine if the access to cloud data is authorized and appropriate.

Governance best practices include automating processes to reduce the burden on enterprise's IT team, as well as auditing security tools routinely to ensure continuous risk mitigation as the organization's environment evolves.

In addition to governance, other recommended data security safeguards for cloud computing include:

- **Deploy encryption.** Ensure that sensitive and critical data, such as PII and intellectual property, is encrypted both in transit and at rest. Not all vendors offer encryption, and the enterprise should consider implementing a third-party encryption solution for added protection.
- **Back up the data.** While vendors have their own backup procedures, it's essential to back up cloud data locally as well. Use the 3-2-1 rule for data backup: Keep at least three copies, store them on at least two different media, and keep at least one backup offsite (in the case of the cloud, the offsite backup could be the one executed by the vendor).
- **Implement identity and access management (IAM).** IAM technology and policies ensure that the right people have appropriate access to data, and this framework needs to encompass the cloud environment. Besides identity governance, IAM components include access management (such as single sign-on, or SSO) and privileged access management.

- **Manage organizational password policies.** Poor password hygiene is frequently the cause of data breaches and other security incidents. Use password management solutions to make it simple for employees and other end users to maintain secure password practices.
- **Adopt multi-factor authentication (MFA).** In addition to using secure password practices, MFA is a good way to mitigate the risk of compromised credentials. It creates an extra hurdle that threat actors must overcome as they try to gain entry to cloud accounts.