WCRG
WORLD COMET RESEARCH GROUP

International Journal of Modern Research in Science & Engineering
Vol. 1, No. 2, 2018
Doi: 10.67228/30716357/IJMRSE-2018PII8P3T
PP. 01-11

Original Article

Data Transmission Security in Cloud Computing: Protocols and Mechanisms

Dr. Rohit Malhotra[1], Dr. Sneha Banerjee[2]

[1]*Professor, University of Mumbai, India.*

[2]*Assistant Professor, Jadavpur University, India.*

Received: 06-02-2018 Revised: 06-19-2018 Accepted: 06-28-2018 Published: 07-02-2018

ABSTRACT

Cloud computing has revolutionized the IT industry by offering scalable and cost-effective solutions for data storage and processing. However, the security of data transmission in cloud environments remains a critical concern. This paper explores various protocols and mechanisms employed to secure data transmission in cloud computing. It examines encryption techniques, authentication protocols, secure transmission standards, and emerging security frameworks. We discuss challenges such as man-in-the-middle attacks, data breaches, and insider threats while analyzing existing security measures and their effectiveness. The study also explores advancements in cryptographic approaches, AI-driven security models, and quantum cryptography to enhance secure data transmission. Through a comprehensive literature review and methodological analysis, this paper presents insights into best practices and future directions in cloud security. The findings emphasize the importance of an integrated security approach that combines traditional security mechanisms with cutting-edge innovations. The conclusions highlight the necessity of continuous advancements in security protocols to combat evolving cyber threats and ensure the confidentiality, integrity, and availability of cloud-based data transmission.

KEYWORDS

Cloud Computing, Data Security, Encryption Protocols, Authentication, Cyber Threats, Secure Transmission, Cryptography, Quantum Security, AI-Driven Security, Cloud-Based Networks.

ISSN: 3071-6357
PP: 01-11.

1. INTRODUCTION

Cloud computing has become the backbone of modern IT infrastructures, enabling organizations to access computing resources on demand. Despite its numerous advantages, the security of data transmission remains a major concern due to various cyber threats. This section discusses the fundamental concepts of cloud computing, the need for data transmission security, and the threats associated with unsecured data transfer.

1.1. Cloud Computing Overview

Cloud computing is defined as the delivery of computing services over the internet, including servers, storage, databases, networking, software, and intelligence. It has transformed the way organizations store, manage, and process data, offering flexibility, scalability, and cost-efficiency. Cloud service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) provide tailored solutions to meet different business needs. However, cloud environments heavily depend on network-based data transmission, making them susceptible to various security risks. Data traversing between cloud providers and users is vulnerable to interception, unauthorized access, and cyberattacks. A single security breach can result in severe consequences, including data theft, regulatory penalties, and reputational damage. Ensuring secure data transmission is imperative for maintaining user trust and compliance with data protection laws such as GDPR and HIPAA. The adoption of robust encryption methods, secure communication protocols, and continuous monitoring mechanisms is crucial to mitigate these risks and enhance cloud security.

1.2. Importance of Secure Data Transmission

The security of data transmission in cloud computing plays a vital role in safeguarding sensitive information from potential cyber threats. Secure data transmission ensures that data remains confidential, unaltered, and accessible only to authorized entities. The foundation of secure communication is based on the CIA triad, which encompasses confidentiality, integrity, and availability. Confidentiality protects data from unauthorized access through encryption techniques such as Advanced Encryption Standard (AES) and RSA. Integrity ensures that transmitted data remains unmodified and authentic through cryptographic hash functions and digital signatures. Availability guarantees that data remains accessible to legitimate users even in the presence of cyber threats such as Denial of Service (DoS) attacks. Cloud environments must implement secure transmission protocols, including Transport Layer Security (TLS) and Internet Protocol Security (IPSec), to establish encrypted communication channels. Moreover, emerging technologies such as blockchain and quantum cryptography are being explored to further enhance data transmission security. Without adequate security measures, data can be intercepted, altered, or destroyed, leading to financial losses and reputational damage. Therefore, organizations must prioritize secure data transmission by integrating encryption mechanisms, authentication frameworks, and real-time monitoring systems into their cloud infrastructures.

ISSN: 3071-6357
PP: 01-11.

1.3. Threats to Data Transmission in Cloud Computing

1.3.1. Man-in-the-Middle (MITM) Attacks

A MITM attack occurs when an attacker intercepts communication between two parties without their knowledge. In cloud computing, this type of attack can compromise sensitive data during transmission between users and cloud service providers. Attackers can manipulate the intercepted data, inject malicious payloads, or steal confidential information such as login credentials and financial data. To mitigate MITM attacks, organizations should implement end-to-end encryption, use TLS/SSL certificates, and deploy multi-factor authentication (MFA) mechanisms to ensure secure communications.

1.3.2. Eavesdropping

Eavesdropping involves unauthorized access to data being transmitted over a network. Cybercriminals exploit vulnerabilities in unsecured communication channels, such as public Wi-Fi networks, to capture sensitive information. Attackers can use packet sniffers to analyze network traffic and extract confidential data, leading to identity theft or business espionage. Preventative measures against eavesdropping include the use of VPNs, encrypted communication protocols, and intrusion detection systems (IDS) to monitor network traffic and detect anomalies.

1.3.3. Data Tampering

In cloud environments, data tampering occurs when attackers modify the contents of transmitted data before it reaches its destination. This can lead to misinformation, unauthorized transactions, and corruption of critical business data. Attackers often exploit weaknesses in data transmission protocols or manipulate database queries to alter records. To prevent data tampering, organizations should implement cryptographic hash functions, digital signatures, and blockchain technology to maintain data integrity and ensure non-repudiation.

1.3.4. Session Hijacking

Session hijacking attacks occur when an attacker takes control of an active user session by stealing session tokens or exploiting security flaws in authentication mechanisms. In cloud-based applications, session hijacking can allow attackers to impersonate legitimate users and gain unauthorized access to sensitive data. Attackers use techniques such as cookie theft, cross-site scripting (XSS), and session fixation to hijack user sessions. To mitigate session hijacking, organizations should enforce secure session management policies, implement HTTP Secure (HTTPS), and utilize token-based authentication methods such as OAuth.

1.3.5. Denial of Service (DoS) Attacks

A DoS attack aims to overwhelm cloud networks and servers by flooding them with excessive requests, rendering them inaccessible to legitimate users. Attackers use botnets and distributed denial-of-service (DDoS) techniques to disrupt cloud services, causing downtime and financial losses. Cloud providers must deploy DDoS mitigation solutions, such as rate limiting, anomaly detection, and traffic filtering mechanisms, to protect against such attacks. Additionally, the use of AI-powered threat detection systems can help identify and prevent large-scale DoS attacks in real time.

ISSN: 3071-6357
PP: 01-11.

By understanding and mitigating these threats, organizations can enhance the security of data transmission in cloud computing environments and ensure reliable and secure communication channels.

2. *LITERATURE SURVEY*

A comprehensive review of existing research provides insight into various protocols and mechanisms implemented for secure data transmission in cloud computing.

2.1. Encryption Mechanisms in Cloud Security

2.1.1. Symmetric Encryption

Symmetric encryption is a cryptographic approach where the same key is used for both encryption and decryption. Algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish play a crucial role in securing cloud data transmission. AES is widely preferred due to its high security and efficiency, offering key sizes of 128, 192, and 256 bits. DES, once a standard, has become outdated due to its vulnerability to brute-force attacks. Blowfish, known for its speed and flexibility, is used in network security applications. Symmetric encryption ensures fast data encryption, making it ideal for large-scale cloud storage and data transfer. However, the challenge lies in secure key management, as compromised keys can expose encrypted data to cyber threats. Various techniques, such as key distribution mechanisms and hardware security modules (HSMs), are employed to mitigate risks associated with symmetric encryption in cloud environments.

2.1.2. Asymmetric Encryption

Unlike symmetric encryption, asymmetric encryption utilizes a pair of cryptographic keys: a public key for encryption and a private key for decryption. RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC) are widely adopted in cloud security for secure key exchange and data protection. RSA, with its large key sizes, provides robust encryption but is computationally intensive. ECC, on the other hand, offers equivalent security with smaller key sizes, making it more efficient for cloud applications. Asymmetric encryption is fundamental in securing cloud-based authentication, digital signatures, and Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols. Despite its advantages, asymmetric encryption poses challenges in processing speed, requiring optimized implementations to balance security and performance in cloud computing.

2.1.3. Homomorphic Encryption

Homomorphic encryption is an advanced cryptographic technique that enables computations to be performed on encrypted data without decryption. This feature is particularly beneficial for cloud computing, where data privacy and security are critical. Fully homomorphic encryption (FHE) allows complex computations, making it a promising solution for secure cloud storage and data analytics. However, FHE is computationally expensive and requires optimization for practical implementation. Partial homomorphic encryption (PHE) and somewhat homomorphic encryption (SHE) offer a trade-off between efficiency and security by supporting specific types of operations.

ISSN: 3071-6357
PP: 01-11.

Research in homomorphic encryption focuses on improving processing efficiency and integrating it into cloud-based applications such as secure data outsourcing and privacy-preserving computations.

2.2. Authentication and Access Control Mechanisms

2.2.1. Multi-Factor Authentication (MFA)

Multi-Factor Authentication enhances security by requiring users to verify their identity using multiple authentication factors. These factors include something they know (password), something they have (one-time password or smart card), and something they are (biometric data like fingerprints or facial recognition). MFA significantly reduces the risk of unauthorized access by adding additional security layers. In cloud computing, MFA is widely adopted to protect user accounts and sensitive data from credential theft and brute-force attacks. Organizations implement MFA using tools such as Google Authenticator, Microsoft Authenticator, and biometric authentication systems. Despite its effectiveness, MFA faces challenges related to user convenience and implementation costs. Adaptive authentication techniques, which assess risk factors before requiring additional authentication, are gaining traction to enhance usability while maintaining security.

2.2.2 OAuth and OpenID Connect

OAuth (Open Authorization) and OpenID Connect are standardized authentication protocols designed to enhance security in cloud-based services. OAuth is an authorization framework that enables secure access delegation, allowing users to grant applications limited access to their data without sharing credentials. OpenID Connect extends OAuth by adding authentication capabilities, enabling secure user authentication across cloud platforms. These protocols are widely used in Single Sign-On (SSO) solutions, reducing the need for users to manage multiple credentials. Cloud service providers such as Google, Facebook, and Microsoft leverage OAuth and OpenID Connect for seamless and secure authentication. However, security risks such as token interception and phishing attacks necessitate the adoption of additional security measures, including token expiration policies and encrypted token storage.

2.2.3. Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is a security mechanism that restricts data access based on predefined user roles and permissions. In cloud environments, RBAC ensures that only authorized users can access specific data or resources, reducing the risk of insider threats and unauthorized data exposure. Organizations define roles based on job functions and assign permissions accordingly, ensuring compliance with security policies and regulatory requirements. RBAC is widely implemented in enterprise cloud applications to enforce the principle of least privilege. However, managing access control in dynamic cloud environments presents challenges, necessitating the adoption of automated policy management and continuous access monitoring. Emerging models such as Attribute-Based Access Control (ABAC) and policy-based access control enhance traditional RBAC by incorporating contextual factors into access decisions.

ISSN: 3071-6357
PP: 01-11.

2.3. Secure Transmission Protocols

2.3.1. Transport Layer Security (TLS)

Transport Layer Security (TLS) is a cryptographic protocol designed to secure data transmission over the internet. TLS ensures data confidentiality, integrity, and authenticity by encrypting communication between cloud users and service providers. It is widely used in cloud applications, email security, and secure web browsing. TLS operates using a handshake mechanism, where encryption keys are securely exchanged before data transmission begins. Modern TLS versions (TLS 1.2 and TLS 1.3) address vulnerabilities present in older protocols and improve security efficiency. Despite its robustness, TLS is susceptible to attacks such as TLS stripping and certificate spoofing. Organizations mitigate these risks by enforcing strict certificate validation, implementing Perfect Forward Secrecy (PFS), and regularly updating cryptographic algorithms.

2.3.2. Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a predecessor to TLS that provides encryption for internet communications. Although SSL has been largely replaced by TLS due to security vulnerabilities, it remains relevant in legacy systems. SSL secures data transmission by encrypting connections between web browsers and servers, preventing eavesdropping and data tampering. However, vulnerabilities such as the POODLE (Padding Oracle on Downgraded Legacy Encryption) attack have led to the deprecation of SSL 3.0. Cloud service providers strongly recommend transitioning to TLS for improved security. Organizations using SSL must ensure proper configuration, disable outdated versions, and adopt TLS-based encryption to protect cloud data transmission effectively.

2.3.3. IPSec and VPNs

Internet Protocol Security (IPSec) and Virtual Private Networks (VPNs) are essential for securing cloud network communication. IPSec is a suite of protocols that provides encryption, authentication, and integrity for IP traffic, making it suitable for securing data transmission in cloud environments. It operates in two modes: transport mode (securing data packets) and tunnel mode (securing entire communication channels). VPNs leverage IPSec to establish secure connections between remote users and cloud networks, preventing unauthorized access. Organizations use VPNs to enable secure remote access, ensuring that sensitive data remains protected even when accessed over untrusted networks. While VPNs enhance security, they may introduce latency and require careful configuration to prevent vulnerabilities such as DNS leaks and man-in-the-middle attacks. The integration of AI-driven network security and Zero Trust Architecture (ZTA) is being explored to strengthen cloud transmission security beyond traditional VPN solutions.

This literature survey highlights the key protocols and mechanisms used to enhance data transmission security in cloud computing. Advancements in encryption, authentication, and secure communication protocols continue to shape the future of cloud security, addressing emerging threats and ensuring robust data protection.

ISSN: 3071-6357
PP: 01-11.

3. METHODOLOGY

This study employs a systematic approach to analyzing data transmission security in cloud computing. By integrating qualitative and quantitative methodologies, this research aims to evaluate the effectiveness of security protocols in real-world cloud environments. The methodology encompasses research design, data collection techniques, and security implementation frameworks, ensuring a comprehensive assessment of existing security mechanisms and emerging innovations.

3.1. Research Design

3.1.1. A Combination of Qualitative and Quantitative Research Methodologies

This study adopts both qualitative and quantitative research approaches to provide a holistic analysis of data transmission security in cloud computing. Qualitative methods involve an in-depth review of literature, case studies, and expert opinions to understand the theoretical foundations and practical challenges of security implementations. Quantitative methods, on the other hand, focus on empirical evaluations, including performance benchmarking of encryption and authentication mechanisms. By combining these methodologies, the research ensures a balanced assessment of security frameworks and their impact on cloud data protection.

3.1.2. Analysis of Security Protocols Based on Effectiveness, Computational Complexity, and Real-World Applicability

Security protocols play a crucial role in safeguarding data transmission in cloud environments. This study evaluates protocols such as TLS, IPSec, and VPNs based on their effectiveness in preventing cyber threats, computational overhead, and feasibility for large-scale cloud adoption. Metrics such as encryption strength, latency, resource utilization, and scalability are analyzed to determine the optimal security solutions for cloud computing. By considering both theoretical and practical aspects, this research identifies security protocols that offer a balance between robust protection and operational efficiency.

3.2. Data Collection Methods

3.2.1. Review of Scholarly Articles, Security Frameworks, and Case Studies

The study involves an extensive review of existing literature, including peer-reviewed journal articles, whitepapers, and security standards. Prominent security frameworks such as the National Institute of Standards and Technology (NIST) guidelines, ISO/IEC 27001, and the Cloud Security Alliance (CSA) best practices are examined to establish industry benchmarks. Additionally, case studies of real-world cloud security incidents provide insights into vulnerabilities, attack vectors, and mitigation strategies.

3.2.2. Empirical Analysis of Encryption and Authentication Protocols

This research conducts empirical testing of encryption algorithms (AES, RSA, ECC) and authentication mechanisms (MFA, OAuth, RBAC) to assess their performance in cloud-based environments. The evaluation includes encryption speed, decryption time, key generation efficiency, and resistance to attacks. By simulating cloud data transmission scenarios, the study measures the

ISSN: 3071-6357
PP: 01-11.

impact of security protocols on data integrity, confidentiality, and access control. The findings contribute to identifying best practices for securing cloud data transmission while minimizing computational overhead.

3.3. Security Implementation Frameworks

3.3.1. Zero Trust Architecture (ZTA): Ensures That No Entity Is Trusted by Default:

Zero Trust Architecture (ZTA) is a security model that enforces strict identity verification for every user and device accessing cloud resources. Unlike traditional perimeter-based security, ZTA assumes that threats exist both inside and outside the network. This research examines the implementation of ZTA in cloud computing, focusing on identity and access management (IAM), micro-segmentation, and continuous authentication. The study explores how ZTA mitigates insider threats, unauthorized access, and lateral movement attacks, enhancing overall cloud security.

3.3.2. Blockchain for Secure Transactions: Enhances Transparency and Integrity

Blockchain technology provides a decentralized and immutable ledger that enhances security in cloud transactions. This research investigates the role of blockchain in securing data transmission by ensuring transparency, integrity, and tamper resistance. Use cases such as blockchain-based identity management, secure data sharing, and decentralized cloud storage are analyzed. The study also examines the limitations of blockchain, including scalability challenges and computational overhead, proposing optimization techniques for seamless integration into cloud security frameworks.

3.3.3. AI-Driven Security Models: Detects Anomalies and Potential Threats

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for enhancing cloud security. This research explores AI-driven security models that detect anomalies, predict cyber threats, and automate security responses. Techniques such as behavioral analysis, anomaly detection, and predictive analytics are applied to identify suspicious activities in real time. The study evaluates AI-powered intrusion detection systems (IDS), fraud detection mechanisms, and adaptive security measures that enhance cloud resilience against evolving cyber threats. Additionally, challenges related to AI bias, false positives, and data privacy concerns are addressed, ensuring responsible AI deployment in cloud security.

This methodological framework ensures a thorough assessment of data transmission security in cloud computing. By integrating empirical research, security framework analysis, and emerging technologies, this study provides actionable insights for strengthening cloud security practices and mitigating cyber risks.

4. RESULTS AND DISCUSSION

The study evaluates the performance of security protocols and mechanisms in cloud computing environments. By assessing encryption techniques, authentication mechanisms, and

ISSN: 3071-6357
PP: 01-11.

secure transmission protocols, the research provides insights into the effectiveness, computational efficiency, and real-world applicability of these security measures.

4.1. Effectiveness of Encryption Algorithms

4.1.1. AES Provides High Security with Minimal Computational Overhead

Advanced Encryption Standard (AES) is widely adopted in cloud security due to its robust encryption capabilities and efficiency. AES operates on symmetric key cryptography, which allows for faster encryption and decryption processes compared to asymmetric methods. Its block cipher mechanism, available in 128-bit, 192-bit, and 256-bit key sizes, provides strong resistance against brute-force attacks. The research findings indicate that AES offers an optimal balance between security and computational performance, making it a preferred choice for securing cloud data transmission.

4.1.2. RSA Ensures Secure Key Exchanges but Is Computationally Expensive

Rivest-Shamir-Adleman (RSA) encryption is an asymmetric cryptographic method used primarily for secure key exchange in cloud environments. While RSA provides robust security through large key sizes (typically 2048-bit or higher), its computational complexity results in higher processing time and resource consumption. The study reveals that although RSA is effective for establishing secure communication channels, it may not be suitable for large-scale encryption due to its slower performance compared to symmetric encryption techniques like AES.

4.1.3. Homomorphic Encryption Is Promising but Has High Processing Costs

Homomorphic encryption (HE) allows computations to be performed on encrypted data without requiring decryption, ensuring confidentiality in cloud environments. This feature is particularly beneficial for privacy-preserving computations in sensitive applications such as healthcare and finance. However, the research highlights that HE incurs significant processing costs due to its complex mathematical operations, making it less practical for real-time data transmission. Optimized implementations of homomorphic encryption are still in development to enhance its feasibility for cloud security.

4.2. Performance of Authentication Mechanisms

4.2.1. MFA Significantly Enhances Security Compared to Single-Factor Authentication

Multi-Factor Authentication (MFA) is a critical security measure that requires users to verify their identity using multiple authentication factors such as passwords, one-time passcodes (OTPs), and biometrics. The study finds that MFA drastically reduces the risk of unauthorized access compared to single-factor authentication, as it mitigates password-based attacks such as phishing and credential stuffing. Cloud service providers increasingly implement MFA to strengthen user authentication and enhance overall data security.

4.2.2. Biometric Authentication Improves User Security but Has Privacy Concerns

Biometric authentication methods, including fingerprint scanning, facial recognition, and iris scanning, offer a high level of security by verifying unique physiological traits. The study reveals that

ISSN: 3071-6357
PP: 01-11.

biometric authentication improves access control by preventing credential-based attacks. However, privacy concerns arise regarding the storage and processing of biometric data, as unauthorized access to biometric databases could lead to identity theft. The research suggests implementing encryption and decentralization techniques to safeguard biometric data in cloud environments.

4.3. Comparison of Secure Transmission Protocols

4.3.1. TLS 1.3 Outperforms SSL in Terms of Security and Efficiency

Transport Layer Security (TLS) 1.3 is the latest encryption protocol designed to secure data transmission over the internet. Compared to its predecessor, Secure Sockets Layer (SSL), TLS 1.3 eliminates outdated cryptographic algorithms and reduces handshake latency, leading to enhanced security and performance. The study demonstrates that TLS 1.3 provides robust protection against cyber threats such as man-in-the-middle (MITM) attacks and session hijacking while maintaining efficient communication speeds in cloud environments.

4.3.2. VPNs Enhance Secure Connectivity for Remote Cloud Access

Virtual Private Networks (VPNs) are widely used to establish secure remote connections to cloud services. The study evaluates VPN implementations and finds that they effectively encrypt network traffic, preventing eavesdropping and unauthorized data interception. VPNs are particularly beneficial for enterprises with remote workforces, as they ensure secure access to cloud applications while maintaining data confidentiality. However, the research also notes that VPN performance depends on network latency and server capacity, which may affect user experience in high-demand environments.

4.3.3. IPSec Ensures End-to-End Security in Multi-Cloud Environments

Internet Protocol Security (IPSec) is a network-layer security protocol that provides end-to-end encryption and authentication for cloud-based communications. The study highlights that IPSec is highly effective in securing data transmission between multi-cloud infrastructures, making it a preferred choice for organizations utilizing hybrid cloud environments. IPSec's integration with VPNs further strengthens cloud security by encrypting traffic at the IP layer, ensuring data confidentiality and integrity across interconnected cloud networks.

The findings of this study reinforce the importance of encryption, authentication, and secure transmission protocols in safeguarding cloud data. While each security mechanism has its strengths and limitations, the combined implementation of advanced encryption, multi-factor authentication, and secure communication protocols enhances the overall security posture of cloud computing environments. Future research could explore the optimization of homomorphic encryption and the integration of AI-driven threat detection to further improve cloud data transmission security.

5.CONCLUSION

Securing data transmission in cloud computing is essential to mitigating cyber threats. This paper has analyzed various encryption, authentication, and transmission security mechanisms. The

ISSN: 3071-6357
PP: 01-11.

results indicate that a multi-layered security approach is necessary to address evolving threats. Future research should explore quantum cryptography and AI-enhanced security models to strengthen cloud data protection.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
[2] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.
[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
[4] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 6, pp. 847–859, 2011.
[6] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2009.
[7] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," Proceedings of IEEE CloudCom, 2010.
[8] R. Buyya, J. Broberg, and A. M. Goscinski, Cloud Computing: Principles and Paradigms, Wiley, 2011.
[9] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.
[10] J. Rittinghouse and J. Ransome, Cloud Computing: Implementation, Management, and Security, CRC Press, 2017.
[11] S. Takabi, J. B. D. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24–31, 2010.
[12] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A Survey of Intrusion Detection Techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013.
[13] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.