FMDB *Transactions on Sustainable Computer Letters*

Revolutionizing Cloud Security: Innovative Approaches for Safeguarding Data Integrity

E. Jeslin Renjith[1, *]

[1]Department of CDOE-MCA, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India.
[1]jeslin.renjith@gmail.com

Abstract: Cloud computing uses third-party servers or private clouds to provide online services and on-demand enterprise resource access. Microsoft Azure, Amazon, IBM, and Google Apps allow customers to design and run cloud-based apps from anywhere. These cloud services store and retrieve data from faraway servers, highlighting the importance of security due to internet data transfer. Before using cloud computing, firms must handle security issues. Pay-per-use, self-service, and scalability make the model popular in banking, healthcare, retail, education, manufacturing, and business. Pay-per-use models let users use servers, networks, storage, services, and applications without buying them. Limited data control can result in account service issues, traffic hijacking, insecure APIs, malicious insiders, technology sharing issues, and multi-tenancy data failures. Continuous research and development improve security and user confidence. This paper provides a framework for understanding cloud computing, identifies security dangers and research issues, and emphasizes its relevance in major industries. It also recommends cloud security innovations and assesses worldwide data protection policies to improve data security and reduce risks. Cloud-stored data is vulnerable to programs with security weaknesses, notwithstanding its benefits. If the guest OS's security is unreliable, virtualization on a hypervisor may expose data to attacks. Additionally, data security vulnerabilities in transit and at rest will be addressed.

Keywords: Data Security; Cloud Computing; Data Protection and Privacy; Risks and Threats; Public Cloud Storage; Cloud Computing Data Security; Stream Cipher.

Received on: 05/01/2024, **Revised on:** 10/03/2024, **Accepted on:** 01/05/2024, **Published on:** 09/06/2024

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCL

DOI: https://doi.org/10.69888/FTSCL.2024.000185

Cite as: E. J. Renjith, "Revolutionizing Cloud Security: Innovative Approaches for Safeguarding Data Integrity," *FMDB Transactions on Sustainable Computer Letters*., vol. 2, no. 2, pp. 111–119, 2024.

1. Introduction

Cloud computing is a modern concept that has gained widespread acceptance recently, essentially defined as "a network solution offering affordable, reliable, and easy access to IT resources." This model is service-oriented rather than application-focused, providing users with flexibility and improved performance while reducing ownership and infrastructure costs [3]. Data protection, privacy, and integrity are crucial for cloud data management [4]. Cloud services adopt various protocols based on the type, quantity, and nature of the data to ensure security and privacy. Since cloud computing permits external access to data, the risk of data loss is a significant concern [5].

[*]Corresponding author.

Every modern computer system now integrates cloud computing, an innovative means of electronically processing and transmitting data, reliant on network infrastructure prone to attacks [6]. Distributed Denial of Service (DDoS) is among the most common attacks but can be mitigated through measures like syn cookies and cloud technology to regulate server connections [10]. Another vulnerability is the man-in-the-middle (MIT) attack, typically countered using Secure Socket Layer (SSL). However, improper SSL configuration may expose cloud users to MIT attacks, hence the need for effective data security measures in cloud computing [11].

Common attack methods such as phishing, IP spoofing, message alteration, and traffic analysis pose further threats alongside those previously mentioned [12]. Cloud computing firms employ a spectrum of data security measures ensuring authentication, confidentiality, access control, and authorization—key to addressing and resolving security challenges [13].

A significant benefit of cloud computing is data sharing across businesses, although this advantage introduces data risks. Protecting data repositories containing sensitive information, such as future product plans or national security data, is vital to prevent exposure to public clouds [14]. Storing such data in internal organizational clouds is advised to enhance security, aided by implementing on-premises data usage policies [15]. Nonetheless, achieving complete data privacy and security is challenging, as many organizations may lack the expertise to safeguard sensitive data. This paper explores global methodologies for securing data within cloud computing environments [16]. To examine the impact of Consumer-Brand Identification on Brand Loyalty.

2. Literature Review

Numerous studies have been reviewed to gain insight into cloud computing and secure cloud storage basics. This section aims to provide a comprehensive overview of the literature to prepare for a discussion on various data security challenges.

Srinivas et al. [1] offer an insightful exploration of the fundamental concepts of cloud computing in their study. They critically examine key ideas and present practical examples of cloud computing applications that can be developed to harness the full potential of this transformative technology. By emphasizing the adaptability of cloud solutions, the authors illustrate how these innovations can significantly benefit emerging markets. The study highlights various sectors, including education, healthcare, and agriculture, showcasing how cloud computing can improve accessibility, efficiency, and cost-effectiveness. Through real-world applications, the authors demonstrate that cloud technology not only enhances operational capabilities but also fosters economic growth in developing regions. Their research underscores the importance of adopting cloud computing as a strategic tool for driving innovation and enabling sustainable development, ultimately contributing to a more connected and technologically advanced global landscape.

Vouk [2] tackles user concerns surrounding data migration to the cloud, particularly focusing on the significant hesitancy exhibited by large enterprises in transferring their data. This apprehension primarily stems from security concerns, which have become a critical barrier to cloud adoption. Their thorough analysis of privacy protection and data security issues associated with cloud computing stands out, offering an exemplary examination of the challenges faced by organizations. They delve into the intricacies of potential vulnerabilities and risks, providing insights into how these factors affect users' trust in cloud solutions. Furthermore, he proposes viable solutions to mitigate these challenges, emphasizing the need for robust security measures and compliance protocols. Their work contributes to a deeper understanding of cloud security and its implications for enterprise data management.

Hu and Klein [7] propose a comprehensive standard aimed at safeguarding data during the migration to the cloud. They highlight baseline encryption as an essential method for protecting data in transit, ensuring that sensitive information remains secure while being transferred. Their research suggests that while implementing additional layers of encryption can significantly enhance security, it also increases the demand for computational resources, potentially impacting system performance. By addressing this trade-off, Hu and Klein [7] strive to achieve a balance between robust data security and manageable encryption overhead. Their findings emphasize the importance of adopting effective encryption strategies that do not compromise operational efficiency, ultimately providing a framework for organizations to securely migrate their data to the cloud without incurring excessive resource costs.

Descher et al. [8] address the critical privacy issue in cloud computing by empowering end users with greater control over their data, thereby fostering trust in digital services. Their research delves into various threats associated with distributed computing, highlighting the vulnerabilities that can compromise user privacy and data integrity. By exploring these potential risks, the authors provide a comprehensive overview of the challenges users face in managing their information in cloud environments. Furthermore, they suggest practical countermeasures to mitigate these threats, emphasizing the need for robust security protocols and user-centric solutions. Their work contributes to the ongoing dialogue on privacy in cloud computing, advocating for approaches that prioritize user agency and trust in an increasingly interconnected digital landscape.

Mohamed [9] introduces an innovative model for data security in cloud computing, significantly enhancing the traditional concepts of data protection in this environment. This model addresses the evolving security challenges associated with cloud storage and computing by integrating advanced techniques and methodologies that go beyond conventional approaches. By focusing on a comprehensive security framework, he emphasizes the importance of not only safeguarding data at rest and in transit but also ensuring continuous monitoring and proactive threat detection. The proposed model incorporates features such as encryption, access controls, and user authentication, creating a multi-layered security strategy that enhances overall data integrity and confidentiality. His work contributes to the field by providing a robust blueprint for organizations seeking to strengthen their data security posture in an increasingly complex cloud landscape.

3. Cloud Computing: Risks and Security Concerns

Cloud computing and cloud data storage entail various security risks. This study will cover multitenancy, public cloud storage, and virtualization, all intrinsically linked to cloud data security.

3.1. Virtualization

Virtualization maximizes using an operating system's resources by creating an image that runs fully within another system. A hypervisor is a technology that enables a guest OS to function as a virtual machine within a host OS [17]. While vital to realizing cloud computing's principles, virtualization poses data security risks. For instance, a compromised hypervisor can become the main target, leading to potential data breaches compromising the entire system [18]. Another risk involves resource allocation and release; if VM operational data isn't erased before memory reallocation, data may be exposed to subsequent virtual machines. Careful use and thorough vetting of data are recommended to mitigate these risks [19].

3.2. Public Cloud Storage

Public cloud storage introduces additional security risks. Centralized storage in cloud computing makes it appealing to hackers. Even a minor breach can involve complex systems comprising hardware and software. Storing sensitive data in a private cloud is often recommended to reduce concerns [20].

3.3. CRM on Brand Experience

Shared access, or multitenancy, poses significant threats to cloud data security. Multiple users sharing computer resources like memory, storage, and CPU increase the risk of others inadvertently accessing sensitive data [21]. A single system failure could expose data to unintended users or hackers. To mitigate multitenancy issues, thorough user verification before data access is critical, employing various authentication methods [22].

4. Cloud Computing Data Security

Beyond encryption, cloud computing encompasses other data protection aspects. Standards differ based on the service model used: SaaS, PaaS, or IaaS. Data transit—moving and storing data in the cloud—and data at rest are two vulnerable stages. The confidentiality and integrity of personal data hinge on the methods, regulations, and practices employed to safeguard it, with the primary concern being information disclosure in these states.

4.1. Data at Rest

Data at rest includes any Internet-accessible or cloud-stored information, both current and backed-up. Companies without a private cloud may face challenges securing this data due to a lack of physical control. This issue can be addressed by maintaining a private cloud with restricted access.

4.2. Data in Transit

"Data in transit" refers to information moving to and from the cloud, whether stored as a file or database and accessed from another location. This category can be more susceptible to threats than data at rest due to its movement. While sensitive data, such as usernames and passwords, often undergoes encryption, unencrypted data remains in transit (Figure 1).

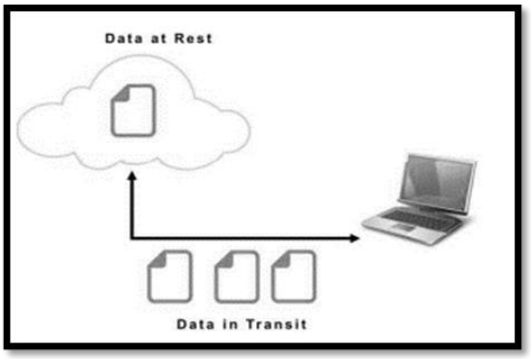

Figure 1: Data at Rest and in Transit

5. Key Security Challenges

When multiple computers or clients are connected, ensuring the protection and safety of these interconnected systems is known as the "multitenancy" issue. Cloud service providers and cloud computing face numerous obstacles, particularly concerning security. Addressing these concerns involves focusing on client security, establishing a secure cloud computing environment, and implementing safeguard models. When multiple companies share resources, there is a risk of data exploitation. Protecting both data repositories and data in transit, storage, or processing is crucial to mitigate this risk. Data security stands out as a primary issue in cloud computing. Enhancing cloud computing security entails providing access control, authorization, and authentication for cloud-stored data.

The key domains of data security involve actively checking for vulnerabilities to ensure data remains secure from intrusions. Security assessments, such as those examining access control measures and cross-site scripting, are crucial to safeguard data from malicious actors. In resource-scarce scenarios, thin clients are employed to protect client data. Users are advised not to store sensitive data like passwords to maintain data integrity. Data in cloud computing is distributed across multiple locations, posing challenges for data localization and differing data regulations. Cloud computing encounters compliance challenges concerning data protection regulations; service providers must inform customers about data storage locations. Data breaches are significant security concerns in cloud computing due to the substantial amounts of data stored and the potential for malicious intrusions.

Cloud environments are vulnerable to attacks, including breaches resulting from intruder activities or unforeseen transmission issues. Multitenancy, a key feature of cloud computing, poses data security risks by allowing multiple users to store their data on shared cloud servers. Proper data segregation through measures like SQL injection and data validation tests is necessary to prevent data theft and breaches from shared resources. Challenges exist regarding data integrity in virtual machines, with the need to balance data storage reliability against potential security risks when storing virtual machines in physical infrastructures. Cloud service providers wield significant authority, posing risks of compromised security and data access problems if not regulated by robust Service Level Agreements. Data portability limitations and shared resource use in cloud computing challenge data's secure storage and management. Security risks like guest-hopping attacks further complicate the adoption and usage of cloud computing services. Malicious internal management attacks highlight the risks posed by deceptive cloud service providers. Removing data in cloud computing presents challenges in ensuring accurate deletion, affecting customer trust in cloud services.

Data interception risks during data transit in cloud computing arise from weaknesses like reply attacks, third-party interventions, and spoofing. Compromised administrator interfaces can lead to harmful activities in cloud computing. Security challenges encompass data transfer between applications, data leakage risks, encryption key management, and disagreements between clients and service providers regarding usage protocols. Challenges beyond security concerns in cloud computing include network-related issues like traffic fluctuations, equipment theft risks, natural disasters, and social engineering attacks.

6. Solutions To Data Security Challenges

Information security experts recommend encryption as the best choice. Encrypting data before storing it on a cloud server is advised. Some group members can easily view the data if the data owner grants access. Data access control will be applied using heterogeneous data-centric security. A model incorporating user protection, data recovery, data encryption, and data integrity must be developed to improve data security over the cloud. Data security and privacy can be ensured by using data protection as a service. Encrypted data is completely useless, and if encryption happens frequently, it may become more difficult to maintain data availability to prevent access by unauthorized individuals.

Users are advised to ensure that data is kept on backup disks and that file keywords are unaltered before uploading any files to the cloud. Before sending the file to cloud servers, compute its hash to ensure its contents haven't changed. Although maintaining this hash calculation is extremely difficult, it can be used to verify data integrity.

RSA Signature and identity-based encryption can provide RSA-based data integrity verification. In order to isolate data from different users, SaaS requires unique boundaries at both the physical and application levels. Cloud computing access management can benefit from distributed access control architecture. It is better to employ credential-based or attribute-based controls to detect illegitimate users. You may use permission as a service to notify the user about which data sections they have access to.

The owner can delegate the bulk of computation-intensive jobs to cloud servers with fine-grained access control methods without disclosing the data's contents. Creating a data-driven architecture that allows cloud users to handle and exchange data safely is feasible. Real-time threat detection is performed by utilizing network-based intrusion prevention systems. To manage remote data security and calculate large files of different sizes. One possible storage security approach is RSA-based.

7. Protecting Data Using Encryption

The encryption methods applied for data in transit and at rest may differ. For example, encryption keys may be temporarily stored for transit data but permanently stored for data at rest.

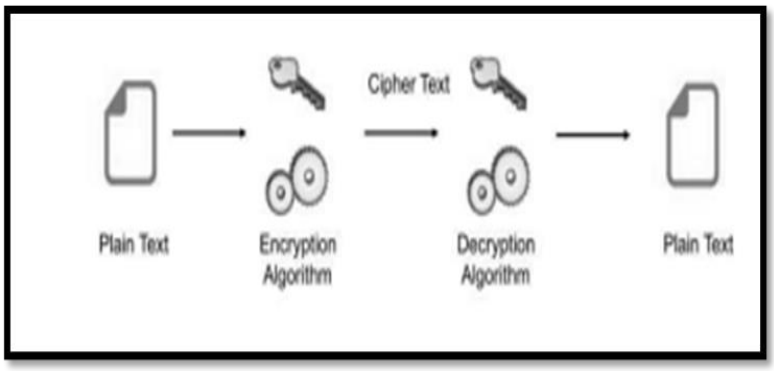

Figure 2: Basic Cryptography Process

Data is encrypted using various cryptographic protocols. Cryptography has raised the data protection level necessary to ensure content availability, validity, and integrity. The fundamental method of cryptography involves first encrypting plaintext with an encryption key and then using a decryption key to decrypt the cipher text, as shown in Figure 2. The applications of cryptography are as follows:

7.1. Cipher Blocks

A cipher block is a data encryption technique in which the key and algorithm decrypt an entire data set instead of just one piece at a time. This technique ensures that different encryption techniques are applied to identical text blocks inside a message. Typically, the next encrypted block in a series is encrypted using the cipher text from the preceding encrypted block. The plain text is divided into data blocks, each with 64 bits on average, as shown in Figure 3. To produce a ciphertext, these data blocks are encrypted using an encryption key.

7.2. Stream cipher

Because it depends on the cipher's present state, this data encryption method is known as a state cipher. Instead of encrypting entire data blocks, this method encrypts individual bits, and every bit is tested bit by bit using an encryption key and algorithm.

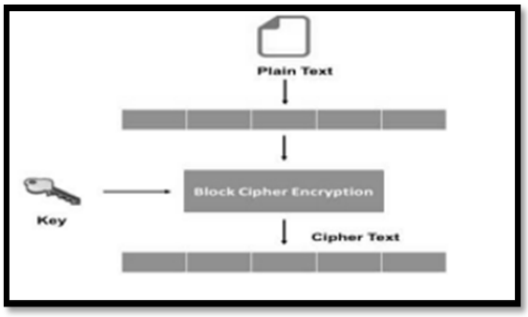

Figure 3: Block Cipher Mechanism

Stream ciphers work quicker than block ciphers because they require less complex hardware. But, if not used properly, this method could be vulnerable to serious security problems.

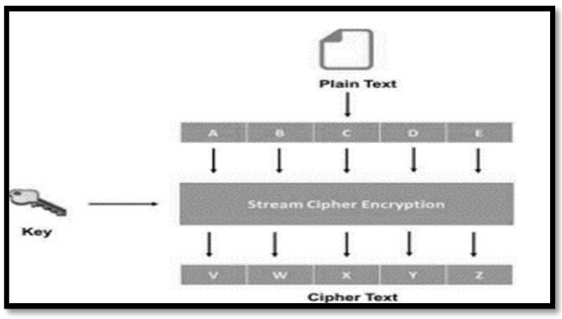

Figure 4: Stream Cipher Mechanism

The stream cipher encrypts each bit rather than a text block using an encryption key, as seen in Figure 4. The cipher text results in a stream of encrypted bits that can be restored to the original plain text using a decryption key later.

7.3. Functions of Hashing

This technique uses a hash function, which is a mathematical calculation; in this, the input text string is converted into an alphanumeric string. Usually, the resulting alphanumeric string has a predetermined length. This technique ensures that no two alphanumeric strings can have the same outcome. Even if they only differ slightly from one another, the output strings they generate can deviate significantly from the input ones. This hash function can be extremely sophisticated or as basic as the mathematical function displayed in equation (1).

$$F(x) = x \bmod 10 \qquad (1)$$

Figure 5 shows the cryptographic Hash function mechanism.

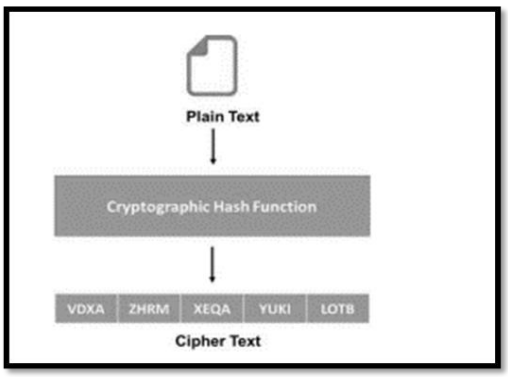

Figure 5: Cryptographic Hash Function Mechanism

The strategies and tactics are normally employed to encrypt data in the cloud to guarantee security. The way these strategies are applied differs depending on the situation. Ensuring data security in private and public clouds is highly advised, regardless of the technique employed.

8. Recommendations for Improved Data Security in Cloud Computing

One key recommendation is for cloud consumers to ensure that effective governance, risk, and compliance systems are in place. This entails ensuring that security measures in cloud computing are on par with those used in traditional IT systems. However, cloud computing may present unique risks to a company compared to traditional IT solutions. Therefore, it's crucial for companies utilizing cloud computing to comprehend their level of risk tolerance. Additionally, it's advised that cloud customers have confidence in their cloud provider's capability and policies to regulate access to their applications and data, as this is vital for monitoring and restricting access within the cloud environment.

Successful management of people, roles, and identities is essential for deploying cloud services. When a consumer application transitions to the cloud, the provider should enable the consumer to assign their user identities to access groups and roles that align with their business and operational security standards. Ensuring adequate data and information security is fundamental to maintaining a secure cloud environment. Security concerns must be addressed for data stored on a storage system and transmitted through communication channels.

Data in cloud computing is susceptible to various threats, including theft, unauthorized disclosure, manipulation, loss, and unavailability. To protect data in cloud computing, it is essential to have appropriate controls, consider various data and privacy concerns, implement confidentiality, create a data asset catalog, ensure integrity and availability, and implement identity and access management. It is paramount to ensure that cloud networks and connections are secured to protect data in the cloud. Cloud users must be aware of internal network risks, such as confidentiality, integrity, and availability breaches. They should evaluate the cloud service provider's internal network controls by their needs and any security restrictions that may be in place.

An important recommendation is to evaluate the security measures for physical infrastructure and facilities in cloud computing. Typically maintained and owned by the cloud service provider, cloud users are responsible for ensuring adequate security controls. This involves data protection via encryption, data loss prevention, integrity protection, authentication, and authorization methods. It is crucial for cryptographic algorithms to be widely recognized and for enterprises to understand the security regulations governing data in multi-tenant cloud environments. Hardware Security Modules (HSMs) are advised for key storage.

Furthermore, proper usage of administrative privileges includes limiting access, using complex passwords, changing default passwords before installing new devices, employing multifactor authentication, and implementing access control lists. Additionally, organizations with wireless networks should utilize commercial wireless scanning and detection technologies and perform regular wireless data analysis. System backup mechanisms should be automated and comply with official or regulatory requirements, with a testing team assessing system backups periodically.

Boundary defense can be achieved using IDS and sniffers to detect external assaults, blocking connections from malicious IP addresses, employing network-based IPS devices, and implementing two-factor authentication for remote login access. Application proxies and application-aware firewalls are recommended for connecting DMZ systems to private network systems. NetFlow collection and analysis in the DMZ network can facilitate promptly identifying anomalous activity.

9. Conclusion

The increasing popularity of cloud computing as a data storage solution has sparked significant interest in enhancing data storage methods to meet the evolving demands of users and organizations. However, despite its many advantages, cloud-stored data remains vulnerable without robust security measures. This research thoroughly investigates the primary security challenges associated with cloud data storage, focusing on various threats and risks that can compromise data integrity and confidentiality. Particular attention is given to virtualization and the potential dangers of hypervisors, which can serve as gateways for malicious attacks if not properly secured. Additionally, the research addresses the inherent threats to multitenancy in public cloud environments, where multiple clients share the same infrastructure, increasing the risk of data breaches. The paper emphasizes the critical importance of data security in cloud computing, outlining the various risks organizations face when storing sensitive information in the cloud. To mitigate these risks, the research explores effective techniques for encrypting cloud-stored data, considering data in various states, whether in transit or at rest. An overview of cryptographic methods, including block ciphers, stream ciphers, and hash algorithms, highlights their roles in securing data against unauthorized access. By implementing these

encryption strategies, organizations can enhance the security of their cloud data, thereby protecting against potential vulnerabilities and ensuring the privacy of their information.

Acknowledgment: I am deeply grateful to the B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India.

Data Availability Statement: The data for this study can be made available upon request to the corresponding author.

Funding Statement: This manuscript and research paper were prepared without any financial support or funding

Conflicts of Interest Statement: The authors have no conflicts of interest to declare. This work represents a new contribution by the authors, and all citations and references are appropriately included based on the information utilized.

Ethics and Consent Statement: This research adheres to ethical guidelines, obtaining informed consent from all participants.

References

1. J. Srinivas, K. Reddy, and A. Qyser, “Cloud Computing Basics,” in Building Infrastructure Cloud Security, vol. 1, no.5, pp. 3–22, 2014.
2. M. A. Vouk, “Cloud Computing - Issues, Research, and Implementations,” in Proceedings of the International Conference on Information Technology Interfaces (ITI), Cavtat, Croatia, pp. 31–40, 2008.
3. P. S. Wooley, “Identifying Cloud Computing Security Risks,” Continuing Education, vol. 1277, no. 2, p.11, 2011.
4. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A Survey on Security Issues and Solutions at Different Layers of Cloud Computing,” Journal of Supercomputing, vol. 63, no. 2, pp. 561–592, 2013.
5. 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.
6. F. Zhang and H. Chen, “Security-Preserving Live Migration of Virtual Machines in the Cloud,” Journal of Network and Systems Management, vol.21, no.9, pp. 562–587, 2012.
7. J. Hu and A. Klein, “A Benchmark of Transparent Data Encryption for Migration of Web Applications in the Cloud,” in 8th IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC), pp. 735–740, Chengdu, China, 2009.
8. D. Descher, M. Masser, P. Feilhauer, T. Tjoa, A. Muresan, and H. Huemer, “Retaining Data Control to the Client in Infrastructure Clouds,” in International Conference on Availability, Reliability and Security, Fukuoka, Japan, pp. 9–16, 2009.
9. E. Mohamed, “Enhanced Data Security Model for Cloud Computing,” in Informatics Systems (INFOS), 2012 8th International Conference, Giza, Egypt, pp. 12–17, 2012.
10. V. J. Winkler, Securing the Cloud, Cloud Computing Security Techniques and Tactics. Elsevier, vol.49, no.9, pp. 20-20, 2011.
11. F. Sabahi, “Virtualization-Level Security in Cloud Computing,” in 2011 IEEE 3rd International Conference on Communications Software and Networks, Xi’an, China, pp. 250–254, 2011.
12. L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, "Building Safe PaaS Clouds: A Survey on Security in Multi-tenant Software Platforms," Computer Security, vol. 31, no. 1, pp. 96–108, 2012.
13. A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, “Security Risks and Their Management in Cloud Computing,” in 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, Taiwan, pp. 121–128, 2012.
14. F. Yahya, V. Chang, J. Walters, and B. Wills, “Security Challenges in Cloud Storage,” in Proceedings of 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, Singapore, pp. 1–6, 2014.
15. I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun, “Home Is Safer Than the Cloud!: Privacy Concerns for Consumer Cloud Storage,” in Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania, p. 13, 2011.
16. T. A. Lipinski, “Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements,” in International Symposium on Information Management in a Changing World, Limerick, Ireland, pp. 92–111, 2013.
17. Y. Wang, S. Chandrasekhar, M. Singhal, and J. Ma, “A Limited-Trust Capacity Model for Mitigating Threats of Internal Malicious Services in Cloud Computing,” Cluster Computing, vol. 19, no. 2, pp. 647–662, 2016.
18. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On Technical Security Issues in Cloud Computing,” in 2009 IEEE International Conference on Cloud Computing, Bangalore, India, pp. 109–116, 2009.
19. H. Qian, J. He, Y. Zhou, and Z. Li, “Cryptanalysis and Improvement of a Block Cipher Based on Multiple Chaotic Systems,” Mathematical Problems in Engineering, vol. 2010, no. 4-6, pp. 7–9, 2010.

20. P. Gope and T. Hwang, “Untraceable Sensor Movement in Distributed IoT Infrastructure,” IEEE Sensors Journal, vol. 15, no. 9, pp. 5340–5348, 2015.
21. V. Poduval, A. Koul, D. Rebello, K. Bhat, and R. M. Wahul, “Cloud-Based Secure Storage of Files Using Hybrid Cryptography and Image Steganography,” International Journal of Recent Technology and Engineering, vol. 8, no. 6, pp. 665–667, 2020.
22. R. Sivan and Z. A. Zukerman, “Security and Privacy in Cloud-Based E-Health System,” Symmetry, vol. 13, no.5, p. 742, 2021.