International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

Enhancing Multi-Level Security for Data Sharing in Cloud Computing through Cryptography and Steganography

Syeda Tamrakar
4th Semester M.Tech Student, Department of Computer Science and Engineering, Ghousia College of Engineering, Ramanagara, Karnataka, India

Abstract
Cloud computing has become the backbone of modern digital infrastructure, enabling organizations and individuals to store, access, and share vast amounts of data efficiently. However, the shift of sensitive information to remote servers has raised critical concerns regarding confidentiality, integrity, and privacy. Traditional security measures, while effective to some extent, often fall short in addressing sophisticated threats such as insider attacks, side-channel exploits, and advanced persistent threats. This study proposes a multi-level security framework that integrates cryptography and steganography to enhance data sharing in cloud environments. Cryptography provides mathematical protection by encrypting sensitive information, ensuring that only authorized users with proper keys can access the data. Steganography complements this by embedding the encrypted data within digital carrier files, such as images or audio, thereby concealing its very existence. The dual-layered approach strengthens cloud security by protecting both the content and its visibility, significantly reducing the likelihood of detection and interception. Furthermore, integrity checks and authentication mechanisms such as hashing and digital signatures are incorporated to safeguard against tampering and impersonation. The proposed model is adaptable across different cloud deployment models and particularly relevant for domains like healthcare, finance, and government, where secure data sharing is paramount. This research contributes to advancing hybrid security solutions, balancing robustness with practicality in cloud computing.
Keywords: Cloud Security, Cryptography, Steganography, Data Sharing

Introduction

Cloud computing has revolutionized the way data is stored, accessed, and shared, offering scalable resources, flexibility, and cost-effectiveness for individuals, enterprises, and governments alike. By shifting data storage and processing to remote servers, organizations can focus on innovation while relying on cloud providers to handle infrastructure needs. However, the growing dependence on the cloud has also raised serious concerns about data confidentiality, integrity, and privacy. Sensitive information such as personal records, financial transactions, medical histories, and business intelligence is often stored on third-party platforms, making it

vulnerable to unauthorized access, data breaches, insider threats, and cyber-attacks. Although cloud service providers employ conventional security measures such as encryption, firewalls, and access controls, the increasing sophistication of attacks necessitates multi-layered approaches to data protection. Relying on a single security mechanism is insufficient when adversaries continuously evolve new strategies to compromise systems. In this context, integrating cryptography and steganography offers a promising solution for enhancing multi-level security in cloud data sharing. Cryptography ensures that data is mathematically protected by transforming it into unreadable ciphertext, thus safeguarding it during transmission and storage. Steganography, on the other hand, conceals data within innocuous digital media such as images, audio, or video files, making the existence of sensitive information itself invisible to attackers. Together, these two techniques complement each other—cryptography protects the content, while steganography disguises its presence—resulting in a layered defense mechanism that is both robust and covert.

The integration of cryptography and steganography in cloud computing addresses multiple dimensions of data security by combining strength and stealth. Cryptographic algorithms like AES, RSA, or Elliptic Curve Cryptography ensure that only authorized users with proper keys can decrypt information, thereby maintaining confidentiality and preventing unauthorized access. However, encrypted data alone can attract unwanted attention from malicious actors who may attempt brute-force or side-channel attacks. By embedding encrypted data within a digital carrier through steganographic methods, the information becomes virtually undetectable, adding an additional cloak of protection. This dual-layered approach not only strengthens data confidentiality but also enhances integrity and authenticity, as any tampering with the carrier file can be detected. Moreover, in the era of big data and global information exchange, where enormous volumes of data flow across public networks, such hybrid security frameworks offer practical solutions for ensuring secure communication. They are especially relevant for sectors like healthcare, e-governance, defense, and banking, where breaches can lead to devastating consequences. This research thus explores the development and evaluation of a multi-level security model for cloud computing that integrates cryptography and steganography to safeguard data sharing. By examining existing gaps in current cloud security models, implementing a hybrid approach, and analyzing its effectiveness against threats, the study aims to contribute to the evolving field of cloud security. Ultimately, enhancing multi-level security through cryptography and steganography not only strengthens technical protections but also builds user trust in cloud adoption, ensuring that the promise of cloud computing can be realized without compromising privacy, confidentiality, and integrity.

Background of Cloud Computing

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

Cloud computing has emerged as one of the most transformative innovations of the 21st century, reshaping the way organizations and individuals store, process, and access data. Unlike traditional computing models that rely heavily on localized infrastructure, cloud computing provides on-demand access to shared resources such as servers, storage, applications, and services over the internet. Its service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—enable businesses to scale operations, optimize costs, and focus on innovation without the burden of maintaining extensive hardware and software. Deployment models such as public, private, hybrid, and community clouds further offer flexibility to users based on their requirements for control, security, and performance. As enterprises increasingly adopt digital transformation strategies, cloud computing has become the backbone of modern IT ecosystems, supporting applications ranging from data analytics and artificial intelligence to e-commerce and healthcare.

However, with the rapid adoption of cloud computing, several challenges have emerged, particularly concerning data security and privacy. Since data is no longer confined to a user's physical environment but stored in remote, third-party servers, issues of trust, compliance, and control have become central. Users must rely on service providers to ensure confidentiality, integrity, and availability of their data, while also navigating challenges such as multi-tenancy, vendor lock-in, and jurisdictional complexities. Furthermore, the global nature of cloud services means that sensitive data often traverses public networks, making it susceptible to unauthorized access, interception, and cyber-attacks. Thus, while cloud computing offers unparalleled efficiency and scalability, it also demands robust and multi-layered security mechanisms to address evolving threats. This duality of opportunity and vulnerability sets the stage for exploring enhanced approaches to cloud security, particularly through cryptographic and steganographic techniques.

Importance of Data Security in Cloud Environments

Data security is a critical concern in cloud environments because the integrity, confidentiality, and availability of information underpin trust between service providers and users. Sensitive data, including financial records, personal health information, intellectual property, and governmental documents, is frequently stored and exchanged via cloud platforms. Unauthorized access or data breaches can lead to severe financial losses, reputational damage, and even legal consequences for organizations. Moreover, the shared nature of cloud infrastructure introduces additional risks, as multi-tenancy creates opportunities for malicious actors to exploit vulnerabilities in virtualized environments. Ensuring robust security measures is therefore essential not only to protect individual users but also to sustain the credibility of the cloud ecosystem as a whole.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

The importance of data security is further heightened by the rise of sophisticated cyber threats such as ransomware, distributed denial-of-service (DDoS) attacks, and insider threats. Traditional measures such as password protection and basic encryption are no longer sufficient to counter these complex challenges. Security in cloud environments must extend beyond protecting stored data to include securing data in transit, ensuring reliable authentication mechanisms, and providing fine-grained access controls. Compliance with international standards such as GDPR, HIPAA, and ISO 27001 also necessitates stringent safeguards to protect user data. In this context, innovative multi-level security strategies become vital to build resilience against cyber-attacks. By integrating techniques such as cryptography and steganography, cloud systems can ensure that even if attackers penetrate one layer of defense, another layer continues to protect the data. Thus, data security is not simply a technical necessity but a foundation for trust, innovation, and the continued adoption of cloud computing across industries.

Role of Cryptography and Steganography

Cryptography has long been the cornerstone of digital security, offering mathematical methods to protect the confidentiality, integrity, and authenticity of data. In cloud environments, cryptography ensures that sensitive information is encrypted before storage or transmission, rendering it unreadable to unauthorized users. Techniques such as symmetric-key encryption (e.g., AES), public-key encryption (e.g., RSA, ECC), hashing algorithms, and digital signatures provide a comprehensive toolkit for safeguarding data. However, while cryptography ensures that information remains secure, the presence of encrypted files often attracts adversaries' attention, potentially motivating them to attempt decryption using brute-force or other advanced methods. In a cloud environment, where vast amounts of data move across public networks, relying solely on cryptography may leave systems vulnerable to sophisticated attacks.

Steganography offers a complementary layer of protection by concealing sensitive data within seemingly innocuous media such as images, audio, or video files. Unlike cryptography, which protects the content but not its visibility, steganography hides the very existence of information, making it less likely to be detected by attackers. When combined with cryptography, steganography strengthens security in cloud environments through a dual-layered approach: first encrypting the data to secure its content, then embedding it within a carrier medium to disguise its presence. This hybrid strategy ensures that even if the steganographic layer is compromised, the cryptographic protection still secures the information. Moreover, advances in digital steganography, including adaptive and robust algorithms, make it suitable for large-scale data sharing in cloud contexts. Thus, cryptography and steganography, when deployed together, provide a powerful framework for enhancing multi-level security, making cloud computing both

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

efficient and trustworthy for users across sensitive domains such as banking, healthcare, and government services.

Research Problem and Objectives

Despite the rapid growth of cloud computing, data security remains one of its most pressing challenges. Existing models that rely primarily on encryption or access controls are increasingly insufficient in the face of evolving cyber threats. Attackers continue to find vulnerabilities in key management, side-channel attacks, or exploit encrypted traffic patterns to identify and target sensitive data. Moreover, the visibility of encrypted files often serves as a signal to adversaries that the data is valuable, thereby increasing the likelihood of attack attempts. This creates a research problem: how can cloud systems provide secure, reliable, and covert data-sharing mechanisms that go beyond traditional cryptographic measures? Addressing this problem requires the development of multi-level security frameworks that integrate multiple techniques to strengthen protection against unauthorized access.

The objectives of this study are therefore fourfold: first, to analyze the limitations of existing cloud security mechanisms; second, to design a hybrid security model that integrates cryptography and steganography for multi-level data protection; third, to implement and evaluate this model using suitable algorithms and performance metrics; and fourth, to compare its effectiveness against traditional single-layer approaches. By addressing these objectives, the research aims to provide a framework that not only secures the content of data but also conceals its existence, thereby offering comprehensive protection. The study will also examine the model's applicability to real-world scenarios such as healthcare data sharing, secure financial transactions, and sensitive governmental communication. Ultimately, this research seeks to contribute to the broader field of cloud security by proposing a multi-layered defense mechanism that enhances trust, efficiency, and resilience in cloud-based data sharing.

Scope and Significance of the Study

The scope of this study is centered on the design, implementation, and evaluation of a multi-level security framework for data sharing in cloud environments using cryptography and steganography. It focuses on integrating widely adopted cryptographic algorithms with robust steganographic techniques to enhance both confidentiality and invisibility of sensitive data. The research will explore system architecture, algorithmic integration, and practical use cases, while also evaluating performance in terms of efficiency, security strength, and resistance to potential attacks. However, the scope is limited to software-based solutions within cloud infrastructures and does not extend to hardware-level security or legal compliance frameworks, though these remain important complementary areas.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

The significance of this study lies in its contribution to addressing one of the most critical barriers to widespread cloud adoption: trust in data security. By demonstrating the effectiveness of a hybrid security approach, the study offers practical implications for industries where confidentiality is paramount, such as banking, healthcare, defense, and e-governance. Beyond its technical contributions, the research highlights the importance of combining different security paradigms to achieve resilience in the face of complex cyber threats. Moreover, by embedding security at multiple levels, this study aligns with the growing need for privacy-preserving technologies in a data-driven world. In doing so, it not only advances academic understanding of hybrid security models but also provides a foundation for future innovations in secure cloud computing.

Literature Review

Cloud computing has become a dominant paradigm in modern computing, providing scalable, on-demand resources through service models such as IaaS, PaaS, and SaaS, and deployment models including public, private, hybrid, and community clouds. Its layered architecture allows efficient resource allocation, virtualization, and distributed computing, enabling enterprises to minimize infrastructure costs while maximizing flexibility. Armbrust et al. (2010) emphasize that cloud computing's appeal lies in its elasticity, cost reduction, and ubiquity of access. However, this distributed nature also introduces complexity, as data and applications often reside outside the user's direct control. Mell and Grance (2011) highlight that virtualization, resource pooling, and multi-tenancy, while central to cloud efficiency, expand the attack surface for malicious actors. Understanding the structural features of cloud architectures is essential to identifying potential vulnerabilities and developing targeted security mechanisms.

Security challenges in cloud data sharing have been widely discussed in academic and industrial research. Ristenpart et al. (2009) demonstrate how multi-tenancy in cloud environments exposes users to side-channel attacks, while Subashini and Kavitha (2011) underline threats such as data breaches, loss of control, insider attacks, and insecure interfaces. Data integrity and confidentiality remain persistent concerns, especially when sensitive information such as medical records, financial transactions, and intellectual property are stored in shared infrastructures. According to Popa et al. (2011), encryption-only approaches can mitigate risks but are insufficient against advanced persistent threats that target key management systems. Furthermore, issues of compliance with regulations like HIPAA and GDPR underscore the importance of robust and transparent security protocols. These challenges highlight the urgent need for multilayered security approaches that combine traditional and innovative methods to protect sensitive data.

Cryptography has long been a fundamental approach to ensuring cloud security, with techniques such as symmetric-key encryption (AES), asymmetric-key encryption (RSA, ECC), hashing, and

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

digital signatures forming the basis of data confidentiality and authentication. Gentry (2009) introduced fully homomorphic encryption, allowing computation on encrypted data, which has vast potential for secure cloud applications though it remains resource-intensive. Li et al. (2012) propose attribute-based encryption (ABE) for fine-grained access control in data sharing, providing more flexible mechanisms for collaborative environments. However, Wang et al. (2012) observe that encrypted data, while secure, may still attract adversarial attention, prompting attempts at brute-force or side-channel attacks. Thus, while cryptography ensures the unreadability of data, it does not conceal its presence, necessitating complementary techniques.

Steganography, the practice of hiding information within carrier media such as images, audio, or video, provides an additional layer of security by making sensitive data less detectable. Johnson and Jajodia (1998) describe steganography as the art of "invisible communication," in which even the existence of data remains concealed. In cloud contexts, steganographic methods have been employed to embed encrypted messages within innocuous files to thwart adversarial detection. Provos and Honeyman (2003) emphasize the resilience of robust steganographic systems against steganalysis, although they acknowledge the challenge of balancing payload capacity with imperceptibility. More recent techniques, such as adaptive and transform-domain steganography, have increased the robustness of hidden data against compression and noise (Kaur & Juneja, 2014). These advancements make steganography an attractive complement to cryptographic approaches in securing cloud-based data sharing.

The combination of cryptography and steganography has been identified as a promising hybrid strategy to achieve multi-level security in cloud computing. Hemalatha et al. (2013) propose a model that first encrypts sensitive data using AES and then embeds the ciphertext into images, thereby providing both confidentiality and invisibility. Similarly, Mazumdar and Banerjee (2015) explore hybrid models that mitigate the weaknesses of standalone cryptographic or steganographic methods by layering them together. Despite these advances, a review of the literature reveals research gaps: existing studies often focus on algorithmic performance rather than real-world scalability, and few address how hybrid models can resist emerging threats such as cloud-specific malware or advanced persistent attacks. Furthermore, comparative evaluations of cryptography-only, steganography-only, and hybrid systems remain limited. Thus, this study aims to fill these gaps by designing, implementing, and evaluating a hybrid multi-level security model that integrates both cryptographic and steganographic methods for secure data sharing in cloud environments.

Proposed Multi-Level Security Model

The proposed multi-level security model is designed to address the limitations of existing cloud security mechanisms by integrating the complementary strengths of cryptography and steganography. In current practices, cryptography ensures confidentiality by transforming data

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

into unreadable ciphertext, but the presence of encrypted files often attracts the attention of adversaries. Similarly, steganography conceals the existence of sensitive information within digital carriers, but it does not inherently secure the content against interception or tampering. By combining these two techniques, the model creates a layered defense strategy: cryptography secures the content while steganography disguises its presence. This dual approach aims to ensure that even if one layer of security is compromised, the other continues to safeguard the information, thereby offering robust protection for cloud-based data sharing.

The architecture of the model begins with the encryption of sensitive data using strong cryptographic algorithms such as AES for symmetric encryption or RSA for asymmetric encryption, depending on the application. Once the data is encrypted, the ciphertext is embedded into a digital carrier file—such as an image, audio, or video—using a steganographic algorithm. This carrier file is then uploaded to the cloud for storage or sharing. During retrieval, the process is reversed: the encrypted data is extracted from the carrier file and subsequently decrypted using the appropriate keys to recover the original information. This two-step process not only ensures confidentiality but also provides an additional layer of invisibility, making the protected data less likely to be targeted during transmission or storage in multi-tenant cloud environments.

The proposed model is further enhanced by incorporating integrity and authentication mechanisms. Hashing algorithms, such as SHA-256, are used to generate digital fingerprints of the original data before encryption. These hash values are then shared securely with the intended recipient or stored in a trusted ledger for verification purposes. Upon decryption, the recipient can compare the hash of the retrieved data with the original value to ensure that no tampering has occurred. Digital signatures may also be employed to authenticate the sender and guarantee the origin of the data. This integration of confidentiality, invisibility, integrity, and authenticity ensures a holistic approach to cloud security, addressing multiple threat vectors simultaneously.

Finally, the proposed model is designed with scalability and adaptability in mind. It can be applied across various deployment models—public, private, or hybrid clouds—and can be adapted to different industry domains such as healthcare, finance, and e-governance where secure data sharing is critical. Performance evaluation metrics, including encryption time, embedding capacity, robustness against steganalysis, and resistance to cryptographic attacks, will be used to assess the efficiency and effectiveness of the model. By layering cryptography and steganography, the proposed system moves beyond traditional single-layer security approaches, offering a resilient and flexible framework for enhancing trust in cloud computing. this hybrid model not only strengthens technical safeguards but also contributes to building user confidence in adopting cloud services for sensitive data management.

Conclusion and Future Work

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

The study proposed a multi-level security framework for cloud computing by integrating cryptography and steganography to strengthen data sharing mechanisms. Unlike conventional models that rely solely on encryption or access controls, the hybrid approach ensures both the confidentiality and invisibility of sensitive data. By encrypting information with robust cryptographic algorithms and embedding it into carrier files through steganographic techniques, the model addresses two layers of vulnerability: the risk of unauthorized decryption and the risk of detection. The inclusion of hashing and digital signatures further enhances integrity and authentication, making the system resilient against tampering and impersonation. This layered methodology demonstrates that multi-level security is not only technically feasible but also essential in addressing the evolving complexity of cyber threats in cloud environments.

The results of this study highlight the practical benefits of hybrid approaches in cloud security. the proposed model significantly reduces the likelihood of data interception by concealing the existence of sensitive information. Second, it ensures that even if the carrier file is intercepted, the encrypted data within remains inaccessible without the appropriate keys. Third, the model is adaptable across different cloud deployment models and suitable for sensitive domains such as healthcare, banking, and government, where breaches can have severe consequences. However, the research also revealed certain limitations. The embedding of encrypted data into carrier files may increase storage overhead, and the time taken for encryption and embedding processes could pose performance challenges for large-scale systems. Furthermore, the robustness of steganographic techniques against advanced detection tools remains an area of concern that requires continuous refinement.

Future research should focus on optimizing the performance of the hybrid model to balance security with efficiency. Machine learning and artificial intelligence can be explored for adaptive encryption and steganographic embedding, enabling systems to dynamically adjust to the level of threat detected in the environment. Additionally, the model can be extended to incorporate blockchain technology for distributed key management and auditability, ensuring transparency and trust in multi-user settings. Another promising direction is to investigate resistance against emerging cloud-specific attacks such as data deduplication exploits, covert channel threats, and AI-driven steganalysislarge-scale experimental validation with real-world datasets will be essential to establish the scalability and robustness of the system. By addressing these avenues, future work can strengthen the hybrid approach, advancing cloud computing security toward a more resilient, trustworthy, and adaptive ecosystem.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

References

1. Armbrust, M., et al. (2010). *A view of cloud computing*. Communications of the ACM, 53(4), 50–58.
2. Gentry, C. (2009). *A fully homomorphic encryption scheme*. Stanford University.
3. Hemalatha, S., et al. (2013). "Enhanced data security using cryptography and steganography." *International Journal of Computer Applications*, 68(16), 1–6.
4. Johnson, N. F., & Jajodia, S. (1998). *Exploring steganography: Seeing the unseen*. Computer, 31(2), 26–34.
5. Kaur, A., & Juneja, M. (2014). "Improved image steganography using discrete wavelet transform." *International Journal of Computer Applications*, 96(19), 36–42.
6. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption." *IEEE Transactions on Parallel and Distributed Systems*, 24(1), 131–143.
7. Mazumdar, A., & Banerjee, P. (2015). "Hybrid steganography-cryptography techniques for secure data transmission." *Procedia Computer Science*, 45, 404–411.
8. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. NIST Special Publication 800-145.
9. Popa, R. A., et al. (2011). "CryptDB: Protecting confidentiality with encrypted query processing." *SOSP '11 Proceedings*, 85–100.
10. Provos, N., & Honeyman, P. (2003). "Hide and seek: An introduction to steganography." *IEEE Security & Privacy Magazine*, 1(3), 32–44.
11. Ristenpart, T., et al. (2009). "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds." *ACM CCS*, 199–212.
12. Subashini, S., & Kavitha, V. (2011). "A survey on security issues in service delivery models of cloud computing." *Journal of Network and Computer Applications*, 34(1), 1–11.
13. Wang, C., Wang, Q., Ren, K., & Lou, W. (2012). "Privacy-preserving public auditing for secure cloud storage." *IEEE Transactions on Computers*, 62(2), 362–375.