Multi-Layer Cloud Data Security Using Cryptography, Steganography and Time-Based Access Control

Mr. Anil M (Asst. Prof.)[1], Meenakshi M[2], Sidharth Sethu[3], Swathi K Santhosh[4]
[1]*Department of Electronics and Communication Engineering, Vidya Academy of Science and Technology, Thrissur (under KTU University) Thrissur, Kerala, India*
[2,3,4]*Department of Computer Science Engineering, MVidya Academy of Science and Technology , Thrissur (under KTU University) Thrissur, Kerala, India*

***Abstract*—The rise of cloud computing has brought about a new era in storing and managing large amounts of data. Nonetheless, increasing dependence on cloud computing has led to rising concerns about security features such as hacking and key management problems in clouds. Traditional methods of cryptography cannot provide sufficient security features if the keys used in cryptography are compromised regarding secret information. This work proposes the use of a multi-layered cloud security mechanism that combines cryptography, steganography, and time-based access control to effectively secure data. Data is encrypted with more secure symmetric-key encryption tech-niques like AES, DES, and RC6. This information is adequately masked with Least Significant Bit Steganography to conceal critical information like encryption key and techniques to prevent eavesdropping and tracing of the key. Furthermore, time-based access control prevents data access beyond a stipulated time, automatically denying data access afterwards. This work is an improved means of ensuring cloud data confidentiality, integrity, and controlled accessibility by institutions and governments for secure cloud storage solutions.**

I. INTRODUCTION

Cloud computing allows users to access resources such as storage, processing power, and applications over the Internet instead of being tied to their physical infrastructure. At the same time, cloud environments are susceptible to various se-curity vulnerabilities: data leakage, man-in-the-middle attacks, unauthorized accesses, or malicious insiders. Since data is housed on third-party servers, users often lose direct control of their data because this alone increases security risks. The encryption technique is one of the main techniques used to protect cloud data. Though encryption guarantees confidentiality, improper management of keys has proved to be a significant weakness that results in failure. Stolen or intercepted encryption keys allow unauthorized attackees to decrypt protected sensitive information easily. In this regard, to overcome such a limitation, more layers of security features need to be integrated. The given project proposes a hybrid security framework by integrating cryptography for protection of data, steganography for safe key hiding, and time-based access control for prevention against unauthorized access or very long time-based access.

II. METHODS AND MATERIAL

The proposed system incorporates a multilayer cloud data security framework by integrating cryptography, steganography, and time-based access. The methodology allows for the safe storage and access, with protection of the encryption keys for the data stored on the cloud. The system is designed to ensure confidentiality and integrity and regulate access through a structured and modular approach.

A. Data Encryption Using Cryptographic Algorithms

The system uses efficient symmetric encryption algorithms such as Advanced Encryption Standard (AES), Data En-cryption Standard (DES), and RC6 in order to encrypt user information. When a user is uploading any file, it uses a random 128-bit encryption key in order to encrypt information in the file. Encryption ensures that files are not accessed by any other user since encrypted files are in raw form and not readable or interpretable in any way.

B. Key Concealment Using Steganography
For overcoming the shortcomings of encryption keys, the encryption key and the algorithms are embedded into the digital image by the use of Least Significant Bit (LSB) Steganography. LSB Steganography is the process of embed-ding binary keys into the least significant bits of the image pixels. This helps in protecting the keys from being intercepted by the attacker or detected as it is embedded into the image.

C. Cloud Storage and Data Management
The cipher text and stego image with the secret key are then sent to the cloud storage. Some information like time of uploading, life time, and user identity is stored in the storage of cloud server. Ensuring secure storage in clouds ensures centralized accessibility and maintains integrity and privacy of information. Storage of metadata facilitates efficient management of access control mechanisms.

D. Time-Based Access Control Mechanism
The system also employs time-based access control to limit data availability during a specified period of time. When sharing files, the user is required to set an access time window by uploading the file. Before decrypting and accessing, it checks whether it is within the stored data expiry time or not. If it is beyond the data access time, it automatically prevents decryption, thus not allowing extended data use.

E. Decryption and Secure Data Retrieval
The authorized users seeking access within a valid time window can download the encrypted file as well as the stego image from the cloud storage system. The secret encryption key is derived from the stego image by reverse LSB stegano-graphic techniques. The secret key is employed to decrypt the encrypted file by using the relevant cryptographic algorithm for secure retrieval of data.

F. Security Layers Involved
The proposed system employs multiple security layers to ensure robust protection:

- User Authentication: Ensures only authorized users can upload or access data.
- Data Encryption: Protects file content using strong cryptographic algorithms.
- Steganographic Key Protection: Conceals encryption keys within digital images.
- Secure Cloud Storage: Maintains data integrity and confidentiality.
- Time-Based Access Control: Restricts data access dura-tion.

G. Workflow and System Integration
The overall process starts with file uploading and encrypt-ing, then key hiding using the technique of steganography. The encrypted file and stego image are uploaded on the cloud, which then is provided with access based on time. On receipt of an authorized request, the extraction of the key and decryption will bring out the original file. With all these put together, the idea will ensure better security to the cloud, accessibility, and reliability of data protection.

Related Work
Cloud computing security has been researched a lot during the last couple of years, covering data confidentiality, encryp-tion techniques, secure key management, and mechanisms that implement access control. It reviews the existing approaches of cryptography-based cloud security, steganography techniques, access control models, their limitations, and how the proposed system addresses such challenges.

1. Cryptography-Based Cloud Security Systems
A number of researches have additionally targeted the security of cloud data using encryption algorithms such as AES, RSA, and DES. The approach is quite successful in safeguarding data privacy during data storage as well as during data transmission. Nevertheless, most current systems on data security depend entirely on the secure distribution of encryption keys. Because if encryption keys are intercepted or revealed, confidentiality is easily breached by attackers. The proposed approach eliminates this problem by using a combination of encryption and steganography.

2. Steganography for Secure Key Management
Steganography has been extensively researched as a means of hiding confidential information inside digital media like image, audio, or video files. From existing research studies, it is evident that Least Significant Bit (LSB) Steganography is an effective and image imperceptible means of embedding secret information. However, several of these solutions use

Steganography by itself without encrypting the information, such that if it is intercepted, the information is compromised. This proposed solution thus encrypts information and subse-quently conceals the encryption keys with LSB Steganography.

3. Hybrid Security Models for Cloud Data Protection
Recent studies have emerged with the concept of hybrid security models involving the combination of various secu-rity approaches including, but not limited to, cryptography, steganography, and authentication processes. Though these provide added security measures, they do not always incor-porate an efficient means of controlling data access to the point where data cannot be accessed unconstrained once the authorization to do so is gained. This new system includes the aspect of time-bound data access.

4. Access Control Mechanisms in Cloud Computing
The traditional model of access control in clouds uses a role-based model/attribute-based model for access control. Although very efficient, such a system does not take into consideration temporal constraints when accessing shared data in a situation where sensitive and/or temporary sharing of data is involved. To overcome such limitations, a model of access control using temporal constraints has been put forward; however, such a model is implemented separately by using encryption/secret key protection systems. The proposed system incorporates all of these elements.

Although existing research has gone a long way in enhanc-ing cloud security through encryption, steganography, and ac-cess control techniques, key management and controlled data accessibility still have limitations. The proposed framework of strong encryption algorithms, steganographic key conceal-ment, and time-based access control offers enhanced data confidentiality, secure key protection, and controlled access, thus making the solution quite robust for modern cloud storage environments.

III. RESULTS AND DISCUSSION

The proposed multi-layer cloud security system was eval-uated based on encryption effectiveness, access control ac-curacy, system performance, and resource utilization. Experi-mental analysis has shown that, within the defined parameters, the system works reliably and provides enhanced data confidentiality, secure key management, and controlled access to cloud-stored files.

A. Encryption and Security Performance
The encryption routine was able to effectively protect dif-ferent kinds of files by using AES, DES, and RC6 algorithms. The encrypted files could be read only by using the right key for decrypting them, which verifies robust confidential-ity protections in place. The employment of steganographic techniques to hide encryption keys added even more to their overall strength by ensuring unencrypted keys could not be intercepted in storage and transmission processes.

B. Operational Metrics
The system exhibited efficient operational performance across all modules:

- File encryption and decryption were completed within acceptable time limits
- Steganographic embedding introduced negligible image distortion
- Time-based access verification executed with minimal delay
- Cloud storage and retrieval operations were efficient These results demonstrate that the layered security approach does not significantly degrade system performance.

C. System Performance and Resource Utilization
The performance of the proposed architecture was consis-tent and had moderate resource utilization. The usage of CPU and memory was in acceptable regions during the processes of encryption, key embedding, and decryption. The lightweight approach of LSB steganographic technique and symmetric encryption made it computationally efficient.

D. Operational Results
The system was successful in meeting the key objective of securing cloud data, protecting encryption keys, and managing controlled access. Both unauthorized attempts and requests that have expired have been denied, thus validating the func-tioning of the time-based controlled access method.

E. Application Potential
The security framework is applicable for scenarios

involving high confidentiality requirements for data, such as sharing of academic issues, corporate cloud storage systems, healthcare data systems, and government record systems. The controlled access feature makes it perfect for scenarios involving data sharing on a temporal basis.

F. Development Pathways

In future enhancements, the work may be integrated with advanced encryption standards, AI-based access behavior analysis, blockchain-supported access control, and enhanced steganography techniques for more robust security with scal-ability.

G. User Interface and Usability

The system provides a simple and intuitive user interface that allows users to upload files, set access durations, and retrieve authorized data without troubles. For the system to be accessible to users with different backgrounds, little technical knowledge has been required from the end users.

H. Automated Access Control and Security Enforcement

The TIM-based access control system can verify the validity of access automatically without the need for human interac-tion. Access is denied, even to the administrator, after the predefined period of access expires. This helps ensure minimal dependency on the human refereeing process, thereby ensuring reduced data misuse.

I. Low Setup and Maintenance

The system is designed to be easily deployed with low main-tenance. The system can be deployed on normal computing environments without the need for special hardware. This is made possible by utilizing minimal databases and optimized algorithms, which make the system inexpensive.

IV. CONCLUSION

This paper provides a multi-level cloud data security system which amalgamates the concepts of cryptography, steganography, and time-controlled access. This helps ensure the secure storage of critical data in the cloud. Data confidentiality is provided through the use of robust encryption methods. Steganography methods ensure the secure embedding of the cryptographic keys. Additionally, time-controlled access pro-vides an added layer of security where critical data is made available for a predetermined time period. Results indicate that the system is completely secure with low overheads. Due to its modular structure, it is suitable for the secure storage of critical data in clouds.

REFERENCES

[1] S. Achar, “Cloud computing security for multi-cloud service providers: Controls and techniques in modern threat landscapes,” *IEEE Access*, 2022.

[2] V. Agarwal, A. K. Kaushal, and L. Chouhan, “A survey on cloud computing security issues and cryptographic techniques,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 1–22, 2020.

[3] Alanwar, Y. Shoukry, S. Chakraborty, P. Martin, and P. Tabuada, “PrOLoc: Resilient localization with private observers using partial homomorphic encryption,” *IEEE Transactions on Control Systems Technology*, 2022.

[4] Y. Alghofaili *et al*., “Secure cloud infrastructure: A survey on issues, current solutions, and open challenges,” *IEEE Access*, vol. 9, pp. 128–145, 2021.

[5] B. Ali, M. A. Gregory, and S. Li, “Multi-access edge computing architecture, data security and privacy: A review,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 1–35, 2021.

[6] P. Awasthi, S. Mittal, S. Mukherjee, and T. Limbasiya, “A protected cloud computation algorithm using homomorphic encryption for preserving data integrity,” *Journal of Cloud Computing*, vol. 8, no. 1, 2019.

[7] T. Denemark, P. Bas, and J. Fridrich, “Natural steganography in JPEG compressed images,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 297–309, 2018.

[8] S. Goldwasser and M. Micali, “Probabilistic encryption,” *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[9] Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, “Permissioned blockchain and edge computing empowered privacy-preserving smart grid

networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992–8004, 2019.

[10] Qazanfari, H. Hassanpour, and K. Qazanfari, "Short-term learning framework for content-based image retrieval," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 1–18, 2017.