Journal of Science Engineering Technology and Management Science
Volume 02, Issue 08, August 2025 *ISSN: 3049-0952*
www.jsetms.com *DOI: 10.64771/jsetms.2025.v02.i08.681-688*

ENHANCING CLOUD DATA SECURITY WITH DYNAMIC AES ENCRYPTION AND BLOCKCHAIN-BASED KEY MANAGEMENT

Umme Habeeba[1], Dr. Mohammad Pasha[2], Samreen Sultana[3]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad,
ummehabeeba84@gmail.com
[2]Assoc. Professor, Department of CSE, Shadan Women's College of Engineering and Technology
mohd.pasha@outlook.com
[3]Asst. Professor, Department of CSE, Shadan Women's College of Engineering and Technology
samreencme@gmail.com

To Cite this Article

Umme Habeeba, Dr. Mohammad Pasha, Samreen Sultana, "Enhancing Cloud Data Security With Dynamic Aes Encryption And Blockchain-Based Key Management", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 08, August 2025,pp: 681-688, DOI: http://doi.org/10.64771/jsetms.2025.v02.i08.pp681-688

Submitted: 17-07-2025 *Accepted: 23-08-2025* *Published: 30-08-2025*

ABSTRACT

As cloud computing continues to change, maintaining strong data security is still a major concern, especially in light of growing threats to encryption and key management systems. In order to overcome these vulnerabilities, this study proposes a novel, two-phase method that combines blockchain-based key management with dynamic Advanced Encryption Standard (AES) encryption. Our system uses dynamically generated AES keys for every file, in contrast to conventional static encryption techniques, reducing the possibility of widespread data compromise in the case of a key breach. In addition, blockchain technology is used to decentrally and impenetrably store encryption keys and other critical metadata, guaranteeing improved availability and integrity. To improve data security even more, Elliptic Curve Cryptography (ECC), a thin yet effective security layer, is implemented for safe key transmission and file exchange. The suggested methodology dramatically lowers attack surfaces in cloud environments by doing away with the need for centralized key storage and using dynamic encryption. Its scalable and modular architecture enables smooth interaction with current cloud infrastructures, providing businesses and people with an adaptable, future-ready solution for protecting sensitive data in the cloud.

1. INTRODUCTION

Since cloud computing is one of the most widely used technologies in the information technology (IT) industry, it offers a number of benefits, including virtualization, cost-effectiveness, wide scalability, remote data processing, and the ability to provide client-centric sharing services whenever needed. It is helpful for a variety of IT domains, such as commercial apps, learning platforms, and most notably, cloud-based data storage and sharing. Instant availability, affordability, accessibility, ease of use, dependability, flexibility, and a variety of leasing options are just a few of the noteworthy features of cloud storage. Critical characteristics including security, scalability, economic efficiency, accessibility, data recovery capabilities, and optimal resource use also support cloud computing. When considering moving user data to cloud settings, trust becomes a crucial issue that poses a big problem for the connection between users and cloud service providers. Given the restricted means for monitoring stored data, users of cloud storage services require clear visibility and assurance on the security and integrity of their data stored in the cloud. Numerous data and resource protection techniques have been developed and incorporated into the field of cloud security, utilizing modern cryptographic algorithms, in order to meet this requirement and promote widespread user acceptance. Cloud data protection via encryption involves putting strong security measures in place to secure client data in server centers from both internal and external threats, made possible by encryption techniques. Symmetric and asymmetric cryptography are the two main types of encryption techniques that are supported by cryptographic keys. The number of keys used—one for symmetric cryptography and two for asymmetric encryption/decryption—determines which of these approaches is used. The security of encryption techniques is improved and attacks are made more difficult by the use of bigger and more complex keys. On the other hand, by utilizing the cutting-edge and new technology of Blockchain, cloud customers can increase trust and improve data security when using outsourcing and cloud services. Compared to centralized database security, blockchain security provides a more intricate and dependable paradigm. Using cryptographic hash techniques, blockchain maintains a record of documents in a ledger that are securely linked to previous blocks. One kind of distributed ledger used to document transactions and guard against manipulation is a blockchain. The Blockchain, which is often operated through a peer-to-peer network, is made especially to guard against unauthorized manipulation. Therefore, from a managerial standpoint, Blockchain can provide security measures that are comparable to those present in central database storage, successfully preventing future assaults and data breaches. Furthermore, Blockchain's built-in transparency feature can help achieve the required degree of data transparency in situations when it is essential.

Blockchain is utilized in many different areas, including finance and the Internet of Things (IoT) ecosystem, and its use is anticipated to increase significantly due to these special advantages. Many IT environments have adopted cloud computing due to its efficiency and accessibility. As a result, investigating important security aspects related to cloud security and privacy issues has received more attention. on this research, a new method for improving the security of file storage on cloud infrastructure is presented. This method makes use of a hybrid dynamic encryption mechanism that combines aspects of blockchain technology, advanced encryption standards, and elliptic curve cryptography. Establishing a highly secure environment that supports improving the general security of cloud-based storage solutions is the main goal. The article presents a novel method of file encryption that makes use of the Advanced Encryption Standard (AES): Dynamic AES File Encryption. This approach is distinguished by its effective and dynamic key generation mechanism, which strengthens cloud file storage security. Blockchain-Powered Key Security: Using Blockchain technology to protect cryptographic keys in a cloud setting is a noteworthy achievement. This guarantees strong encryption key protection and guards against possible security lapses. User-Friendly Key Management: The post makes key management easier for end users. This simplification improves cloud-based storage systems' usability and security by enabling users to effectively handle the large number of dynamic keys needed for encryption activities.

OBJECTIVE

The objective of this project is to develop an innovative and robust solution to enhance the security of cloud-stored data by addressing key vulnerabilities in traditional encryption and key management techniques. The project aims to strengthen cloud data protection by introducing a two-phase approach. The first phase focuses on generating dynamic AES keys for each file, ensuring that each file is encrypted with a unique, constantly changing key, which significantly reduces the risk of widespread data compromise in case of key exposure. The second phase leverages blockchain technology to securely store encryption keys along with their metadata, providing a decentralized and tamper-resistant key management system. Additionally, the project integrates Elliptic Curve Cryptography (ECC) for secure key exchange and encryption, ensuring secure transmission and storage of data. Ultimately, the project seeks to offer a scalable, adaptable, and highly secure framework for cloud data protection, enhancing confidentiality, integrity, and access control in modern cloud environments.

PROBLEM STATEMENT

Data protection through encryption in the cloud entails the implementation of robust security measures to safeguard customer data within server centres against external and internal threats, facilitated by encryption algorithms. primary categories of encryption methods, supported by cryptographic keys, are symmetric and asymmetric cryptography. between these methods hinges on the number of keys employed: one key for symmetric cryptography and a pair of keys for asymmetric encryption/decryption. The use of larger and more intricate keys enhances the security of encryption algorithms and renders attacks more formidable.

EXISTING SYSTEM

In the rapidly evolving realm of cloud computing security, this paper introduces an innovative solution to address persistent challenges. The proliferation of cloud technology has brought forth heightened concerns regarding data security, necessitating novel approaches to safeguarding sensitive information. The issue centers on the vulnerability of cloud-stored data, usually necessitating enhanced encryption and key management strategies. Traditional methods usually fall short in mitigating risks associated with compromised encryption keys and centralized key storage. To combat these challenges, our proposed solution encompasses a two-phase approach.

Disadvantages of Existing System:

- Effective key management is critical for AES security.
- Poor practices can lead to vulnerabilities, such as reusing keys or failing to protect them.
- AES uses a fixed block size of 128 bits. Certain applications that might benefit from larger block sizes.

PROPOSED SYSTEM

In the first phase, dynamic Advanced Encryption Standard (AES) keys are generated, ensuring each file's encryption with a unique and ever-changing key. This approach significantly enhances file-level security, curtailing an attacker's ability to decrypt multiple files even if a key is compromised. The second phase introduces blockchain technology, where keys are securely stored with accompanying metadata, bolstering security and data integrity. Elliptic Curve Cryptography (ECC) public key encryption enhances security during transmission and storage, while also facilitating secure file sharing. In conclusion, this comprehensive approach enhances cloud security, providing robust encryption, decentralized key management, and protection against unauthorized access. Its scalability and adaptability make it a valuable asset in contemporary cloud security paradigms, assuring users of data security in the cloud.

Proposed System Advantage

- ECC provides equivalent security to traditional systems (like RSA) with much smaller key sizes.
- Making it ideal for resource-constrained devices such as smartphones, IoT devices, and embedded systems.
- Leading to quicker transactions and lower latency.

2. RELATED WORK

The "Blockchain-Aware Proxy Re-Encryption Algorithm-Based Data Sharing Scheme" is a novel approach designed to enhance secure data sharing and privacy in distributed systems. It combines the security features of proxy re-encryption (PRE) with the decentralized trust model of blockchain technology. In this scheme, a proxy server is used to facilitate data sharing between a data owner and a recipient, without the proxy gaining access to the plaintext data. The re-encryption process is controlled through cryptographic keys, ensuring confidentiality. By incorporating blockchain, the system ensures that all access requests, re-encryption processes, and transactions are securely recorded in an immutable ledger, providing transparency, accountability, and tamper-resistance. This hybrid approach helps address key challenges such as unauthorized data access, data integrity, and scalability while enabling efficient and privacy-preserving data sharing across various platforms. **[1]**

The "Dynamic Multimedia Encryption Using a Parallel File System Based on Multi-Core Processors" project focuses on enhancing the security and efficiency of multimedia data encryption by leveraging the power of parallel computing through multi-core processors. The system dynamically encrypts multimedia files, such as images, videos, and audio, ensuring robust protection against unauthorized access. By utilizing a parallel file system, the encryption process is distributed across multiple cores, significantly speeding up the encryption and decryption operations, making it ideal for handling large multimedia datasets. This approach optimizes computational resources, improves processing time, and ensures scalability, while maintaining high-level encryption standards. The project addresses the growing need for secure, high-performance solutions for multimedia content, providing a secure environment for sensitive media and improving the overall user experience in content delivery and storage systems.**[2]**

The "Modified Advanced Encryption Standard (MAES) Based on Non-Associative Inverse Property Loop" project introduces an innovative enhancement to the widely used AES encryption algorithm by incorporating a non-associative inverse property loop. This modification aims to improve the security and resistance of AES against certain cryptographic attacks, such as brute force and side-channel attacks. By leveraging non-associative properties, the project alters the standard AES transformation steps, creating a more complex and less predictable encryption process. This added layer of complexity makes it more difficult for attackers to reverse-engineer or break the encryption, while maintaining the efficiency and scalability of AES. The project explores the potential of combining mathematical properties with established cryptographic techniques to offer a more robust and advanced encryption solution, making it suitable for applications that demand heightened security, such as financial services, government communications, and secure data transmission. **[3]**

The project "Elliptic Curve Cryptography: Applications, Challenges, Recent Advances, and Future Trends – A Comprehensive Survey" provides an in-depth analysis of elliptic curve cryptography (ECC), a powerful cryptographic technique that uses the algebraic structure of elliptic curves over finite fields to secure communications. The project surveys the diverse applications of ECC, ranging from secure key exchange and digital signatures to blockchain and cryptocurrency technologies. It examines the challenges ECC faces, including computational complexity, security vulnerabilities, and its adoption in various industries. The survey also highlights recent advancements in ECC, such as improved algorithms, optimization techniques, and enhancements in performance, along with innovations that strengthen ECC's security. Finally, the project discusses emerging trends and future prospects of ECC, focusing on its potential in next-generation encryption systems, quantum resistance, and integration with emerging technologies like the Internet of Things (IoT) and cloud computing. The project serves as a comprehensive guide for researchers, engineers, and practitioners looking to understand ECC's evolving role in modern cryptography. **[4]**

The project "Blockchain-Based Cloud Storage Using Secure and Decentralized Solution" aims to revolutionize traditional cloud storage systems by leveraging blockchain technology to create a secure, decentralized, and transparent solution. By utilizing blockchain's inherent properties, such as immutability and distributed ledger, the project ensures data integrity, privacy, and protection against unauthorized access. Unlike centralized cloud storage systems, this decentralized approach removes single points of failure, offering enhanced security and redundancy. The project focuses on allowing users to store and share data in a peer-to-peer network while ensuring that sensitive information remains encrypted and tamper-proof. Smart contracts are employed to facilitate secure file transactions and access control, making the system more transparent and efficient. This innovative solution addresses issues such as data breaches, service provider trust, and data availability, offering a more robust alternative to conventional cloud storage. **[5]**

The project "Ensuring Confidentiality and Privacy of Cloud Data Using a Non-Deterministic Cryptographic Scheme" focuses on enhancing the security of data stored in cloud environments by utilizing a non-deterministic cryptographic approach. Traditional cryptographic schemes often use deterministic algorithms, which can make patterns in encrypted data vulnerable to analysis and attacks. This project addresses this issue by introducing non-deterministic encryption techniques that ensure each encryption operation produces unique ciphertext, even for identical plaintext inputs. By implementing this scheme, the project ensures that sensitive data remains confidential and private, safeguarding it from potential threats such as data breaches or unauthorized access. Additionally, the non-deterministic nature of the encryption adds a layer of complexity to the system, making it more resilient to attacks such as pattern recognition and brute-force attacks. The project aims to provide a more secure and privacy-preserving solution for users and organizations relying on cloud services for data storage and processing. **[6]**

The integration of hyperchaotic image encryption frameworks in e-health applications is crucial for securing sensitive medical data stored and processed in cloud environments. These frameworks leverage advanced chaotic systems to enhance the confidentiality and integrity of medical images, addressing the vulnerabilities associated with traditional encryption methods. The following sections outline key aspects of this approach. **[7]**

The transformation of enterprise cloud services involves a comprehensive shift in how organizations manage their IT infrastructure and data, leveraging cloud technologies to enhance scalability, security, and collaboration. This transformation is not merely about adopting new technologies but also about rethinking organizational strategies and processes to fully exploit the benefits of cloud computing. The transition to cloud services requires addressing challenges such as data synthesis, security, and cross-organizational coordination, while also focusing on technological innovation and strategic alignment. **[8]**

Cloud computing security is a critical concern as organizations increasingly rely on cloud services for data management and storage. A systematic literature review reveals various threats and mitigation strategies essential for safeguarding cloud environments. Key threats include distributed denial-of-service (DDoS) attacks, account hijacking, malware, and data breaches. Mitigation strategies encompass security awareness training, vulnerability management, and advanced technologies like artificial intelligence (AI) and machine learning (ML) to enhance security measures. **[9]**

The research by Dawson et al. (2023) introduces a Non-Deterministic Cryptographic Scheme (NCS) aimed at enhancing the confidentiality and privacy of cloud data. This innovative approach addresses the challenges of execution time in existing cryptographic methods by employing a symmetric algorithm with linear time complexity. The NCS demonstrates superior performance compared to traditional algorithms like AES, DES, and RSA, particularly in terms of execution time, which is independent of data size but rather influenced by key size (Dawson et al., 2023) **[10]**

3. METHODOLOGY

- The system follows a secure and structured process to protect cloud-stored data:
- Each file is encrypted using a unique AES-256 key, and a SHA-256 hash is generated to maintain data integrity.
- The encryption key and file metadata are stored in a private blockchain, ensuring tamper-proof and traceable key management.
- The key is securely shared with authorized users through Elliptic Curve Cryptography (ECC), allowing only intended clients to decrypt and access the file.

1. User Interface Design

We create the project's windows in this module. All users can securely log in using these windows. Users can only connect to the server by providing their login and password in order to establish a connection. The user can log in straight to the server if they have previously left; otherwise, they must register their information, including their email address, password, and username. In order to maintain the upload and download rates, the server will create an account for each user. The user ID will be set to name. Typically, logging in allows access to a certain page.

2. Data Manager

In this regard, the data manager is essential to the management and security of the private information kept in the Cloud Data Warehouse (CDW). The data manager will also keep an eye on how data is shared and stored, making sure that only those with permission may access private information and that security protocols are maintained throughout the data's lifecycle. After uploading the text file, the data manager will examine the user requests and supply the private keys.

3. Client

The person interacting with the Cloud Data Warehouse (CDW) to conduct searches over the encrypted data cubes is an authorized user. Users are given access in accordance with the data owner's access control policies and are given the decryption keys required to access the query results. To search through the encrypted data cubes stored in the cloud, a user must supply the appropriate private key when submitting a search query.

4. Admin

The administrator serves as the project's administrator and has access to all client, manager, and file information. He can also access all of the data stored in the client and manager databases. He is also entitled to review any files that the manager uploads. He can also access all of the file information that the data manager has submitted. As a result, the administrator will have access to all client and manager data here, as well as manager-uploaded files.

4. ALGORITHM

Elliptic Curve Cryptography

Secure file sharing is made possible by Elliptic Curve Cryptography (ECC), which uses public key encryption to improve security during storage and transmission. In summary, by offering strong encryption, decentralized key management, and defense against unwanted access, this all-encompassing strategy improves cloud security. Its versatility and scalability make it an invaluable tool in modern cloud security paradigms, guaranteeing cloud data security for users. Taking into account the above-described aspects, ECC is a safe and effective encryption technique that may be applied to a variety of contexts, including those involving mobile devices.

By mathematically associating each point on an elliptic curve with a particular set of public and private keys, Elliptic Curve Cryptography, or ECC, is a technique for encrypting and decrypting data. By fusing three potent technologies—Elliptic Curve Cryptography (ECC), Blockchain technology, and Dynamic AES Encryption—the suggested approach seeks to improve security in cloud-based storage systems. The goal is to handle important issues including key management, data integrity, and illegal access while offering a reliable and scalable solution for protecting private information kept in the cloud. By utilizing the advantages of each technology, this integrated strategy aims to create a multi-layered protection mechanism while mitigating the shortcomings of conventional encryption techniques and key management procedures.

Each of the two primary stages of the algorithm's structure is essential to protecting the data kept in cloud environments. The entire data set is encrypted using the same key in standard encryption systems, which leaves it open to compromise. The suggested solution uses Dynamic AES (Advanced Encryption Standard) encryption to get around this restriction. In many security protocols, data is encrypted using AES, which is generally considered to be one of the most secure symmetric encryption algorithms. For every single file or data set kept in the cloud, a dynamic AES key is created in this project. To guarantee that no two files have the same encryption key, these keys are produced dynamically and are distinct for each file. The generation of new, random keys for every file significantly enhances the security by preventing attackers from being able to decrypt multiple files even if one key is exposed.

By prohibiting attackers from decrypting numerous files even if one key is compromised, the creation of new, random keys for each file greatly improves security.

The first step in the process is creating a distinct AES key for every file. Every time a file is uploaded to the cloud storage, the key generation procedure is immediately started. The file is encrypted using the created key, guaranteeing that a robust encryption mechanism is in place to safeguard it. AES, which is quite effective in terms of speed and security, is used to do the encryption. Once the file has been encrypted, its encrypted version replaces the original file and the AES key is stored separately. Blockchain technology is incorporated into the algorithm's second step for safe key management. The safe handling and preservation of cryptographic keys is one of the biggest problems with conventional encryption techniques. Because keys in centralized key management systems are kept in one place, they are susceptible to attacks in the event that the centralized store is compromised. To mitigate these vulnerabilities, blockchain offers a decentralized, transparent, and immutable approach to key management. The dynamic AES keys created for every file are kept on a blockchain in the suggested method. The Blockchain functions as a distributed ledger, with each key and the metadata that goes with it (such file ownership and identity) safely stored in a block. By using a decentralized method, it is ensured that keys are not kept in one place that could be targeted by hackers. As an alternative, the keys are spread across several network nodes, each of which keeps a copy of the Blockchain for redundancy and data loss protection. ECC is utilized in this project to enable the user and cloud storage provider to securely exchange cryptographic keys. ECC securely encrypts and exchanges the dynamic AES keys when a user uploads or downloads a file. Because only the private key holder can decode the data, the public-private key pairs employed in ECC guarantee that the keys stay safe even in the event that the communication channel is intercepted.

5. SYSTEM ARCHITECTURE

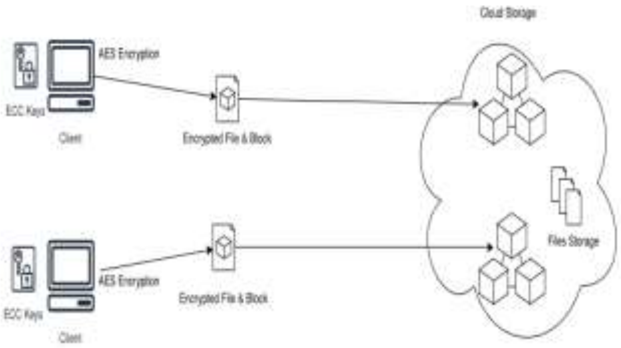
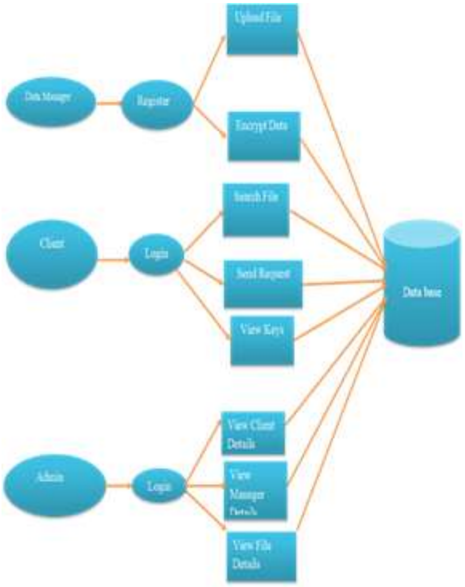


Fig 5. System Architecture

This project's system architecture combines a number of cutting-edge technologies to improve the security of file storage in cloud infrastructures. Fundamentally, it integrates a user-friendly interface for smooth key handling, dynamic AES encryption, and Blockchain-powered key management. Uploading a file is the responsibility of the data manager, after which the data will be encrypted and saved in a database. The client is in charge of using the filename to search a file and obtain data from the database. To download the original file, ask for the keys. The way the system works is that files are first encrypted using the dynamic Advanced Encryption Standard (AES), which ensures excellent security by dynamically generating and managing the encryption keys. Blockchain technology is then used to safely store and maintain these encryption keys, guaranteeing tamper-proof security and avoiding unwanted access or manipulation. All cryptographic key exchanges are safely tracked and recorded in the Blockchain ledger, ensuring data transparency and integrity. End users don't need to be highly skilled in cryptography to handle the dynamically produced encryption keys thanks to an intuitive key management interface. This design strengthens the overall security of cloud storage systems while solving issues with data protection, accessibility, and trust by guaranteeing both strong encryption and simplified, secure key management for users.

6. DATA FLOW DIAGRAM



Level 1

Level 0

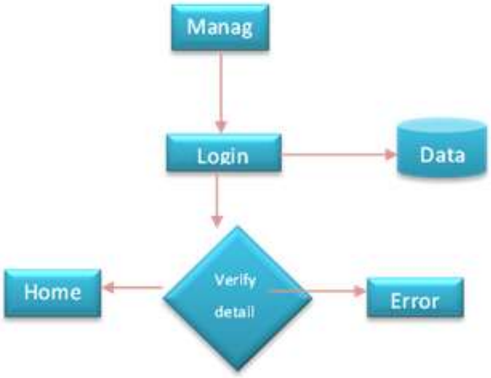


Fig 6. DATA FLOW DIAGRAM

7. RESULT

This paper presents a novel cloud security solution that tackles the weaknesses of traditional encryption and key management. It proposes a two-phase approach: first, using dynamic AES keys so that each file is encrypted with a unique, frequently changing key, making it harder for attackers to access multiple files even if one key is exposed. Second, blockchain is used to securely store keys with metadata, ensuring integrity and decentralization. Additionally, Elliptic Curve Cryptography (ECC) provides secure transmission, storage, and file sharing. Overall, this solution offers stronger encryption, decentralized key management, and better protection against unauthorized access, making it scalable and adaptable for modern cloud security needs.

8. DISCUSSION AND CONCLUSION

This study presents a thorough and creative approach to solving important security issues in cloud computing settings. The recommended strategy makes use of a hybrid dynamic encryption method that combines ECC, AES, and Blockchain. This multi-layered defence mechanism guarantees a high level of security for sensitive data. In the process, well-known security problems with cloud computing have been clarified, including the need for privacy reinforcement and the lack of centralized key management. The two-stage solution that has been suggested is a good fit for the issues that have been identified. To ensure that every file is encrypted uniquely and often, dynamic AES keys are initially generated. By reducing the chance of compromise, this dynamic key generation significantly improves file-level security. The second stage presents blockchain technology, which offers a decentralized, unchangeable record for safely storing encryption keys. We guarantee that unwanted access is successfully avoided during transmission and storage by encrypting these blocks using ECC public keys. These elements work together to increase consumer trust while strengthening the security of data stored in the cloud. While service providers gain from decentralized key management, users can safely handle a variety of files with different encryption keys using a single key saved on their device. To put it simply, the recommended approach creates a robust and adaptable security solution that fits the evolving demands of cloud computing. It is effective in resolving cloud security issues. While satisfying the various needs of users or service providers, it ensures that the data is secure and confidential.

9. FUTURE ENHANCEMENT

In order to improve overall security, future research could incorporate machine learning algorithms to dynamically evaluate and modify encryption schemes depending on real-time threat detection.

10. REFERENCES

[1] R. Anandkumar, K. Dinesh, A. J. Obaid, P. Malik, R. Sharma, A. Dumka, R. Singh, and S. Khatak, ‘‘Securing e-health application of cloud computing using hyperchaotic image encryption framework,’’ Comput.Electr. Eng., vol. 100, May 2022, Art. no. 107860.

[2] Z. Bashir, T. Rashid, and S. Zafar, ‘‘Hyperchaotic dynamical system based image encryption scheme with time-varying delays,’’ Pacific Sci. Rev. A,Natural Sci. Eng., vol. 18, no. 3, pp. 254–260, Nov. 2016.

[3] W. Y. Chang, H. Abu-Amara, and J. F. Sanford, Transforming Enterprise Cloud Services. Berlin, Germany: Springer, 2010.

[4] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz,‘‘ A systematic literature review on cloud computing security: Threats and mitigation strategies,’’ IEEE Access, vol. 9, pp. 57792–57807, 2021.

[5] N. M. Sultana and K. Srinivas, ‘‘Survey on centric data protection method for cloud storage application,’’ in Proc. Int. Conf. Comput. Intell. Comput.Appl. (ICCICA), Nov. 2021, pp. 1–8.

[6] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, ‘‘A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing,’’ Int. J. Intell. Netw., vol. 3, pp. 16–30, 2022.

[7] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, ‘‘Integration of blockchain and cloud of things: Architecture, applications and challenges,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2521–2549,4th Quart., 2020.

[8] S. N. G. Gourisetti, Ü. Cali, K.-K.-R. Choo, E. Escobar, C. Gorog, A. Lee,C. Lima, M. Mylrea, M. Pasetti, F. Rahimi, R. Reddi, and A. S. Sani,‘‘Standardization of the distributed ledger technology cybersecurity stack for power and energy applications,’’ Sustain. Energy, Grids Netw. vol. 28,Dec. 2021, Art. no. 100553.

[9] S. Banani, S. Thiemjarus, K. Wongthavarawat, and N. Ounanong, ‘‘A dynamic light-weight symmetric encryption algorithm for secure data transmission via BLE beacons,’’ J. Sensor Actuator Netw., vol. 11, no. 1,p. 2, Dec. 2021.

[10] I. Keshta, Y. Aoudni, M. Sandhu, A. Singh, P. A. Xalikovich, A. Rizwan, M. Soni, and S. Lalar, ‘‘Blockchain aware proxy re-encryption algorithm based data sharing scheme,’’ Phys. Commun., vol. 58, Jun. 2023,Art. no. 102048.

[11] O. A. Khashan, N. M. Khafajah, W. Alomoush, M. Alshinwan, S. Alamri, S. Atawneh, and M. K. Alsmadi, ‘‘Dynamic multimedia encryption using a parallel file system based on multi-core processors,’’ Cryptography, vol. 7,no. 1, p. 12, Mar. 2023.

[12] K. Bhalla, D. Koundal, S. Bhatia, M. Khalid Imam Rahmani, and M. Tahir, ‘‘Dynamic encryption and secure transmission of terminal data files, ’’Comput. Mater. Continua, vol. 71, no. 1, pp. 1221–1232, 2022.