Comprehensive Strategies for Mobile Data Security in Cloud Computing Using Advanced Cryptographic Techniques

Himabindu Chetlapalli,

9455868 Canada Inc,

Ontario, Canada

chetlapallibindu@gmail.com

Durga Praveen Deevi,

O2 Technologies Inc, California, USA

durgapraveendeevi1@gmail.com

Naga Sushma Allur,

Astute Solutions LLC, California, USA

Nagasushmaallur@gmail.com

Koteswararao Dondapati,

Everest Technologies,

Ohio, USA

dkotesheb@gmail.com

Sharadha Kodadi,

Infosys, Texas, USA

kodadisharadha1985@gmail.com

Thinagaran Perumal

Associate Professor

Department of Computer Science,

Faculty of Computer Science and Information Technology,

Universiti Putra Malaysia,

43400 UPM Serdang, Selangor, Malaysia

thinagaran@upm.edu.my

ABSTRACT

One of the major challenges in cloud computing environments is data security, especially for mobile data applications where efficiency and throughput are critical. To evaluate the effectiveness of advanced cryptographic algorithms in mobile data security, this paper discusses symmetric

encryption (AES), asymmetric encryption (RSA), elliptic curve cryptography (ECC), homomorphic encryption, and blockchain. While RSA guarantees secure key exchange, AES is considered the fastest and most energy-efficient encryption. ECC is also suitable for low-resource devices due to its provision of strong encryption with smaller keys. Blockchain is ensured to offer decentralized security that is immutable in nature, and homomorphic encryption ensures safe computation without revealing plaintext. A hybrid cryptographic security algorithm is proposed with the benefits of both approaches so that encryption can be maximally efficient, secured, and at high speed. The performance metrics state that the combined technique is perfect for transmitting and storing data safely in cloud environments since this balances computational overhead, efficiency of storage usage, and security level. Findings indicate that it is essential to make use of multiple encryption techniques to improve security without making efficiency compromise.

Keywords: Blockchain, AES, RSA, ECC, Cloud Computing, Cryptography, Mobile Security, Privacy, Scalability, and Efficiency.

INTRODUCTION

Data management and storage procedures have undergone tremendous change in the current digital era due to the quick uptake of mobile devices and cloud computing. But this change has also brought about significant difficulties in guaranteeing the privacy, availability, and integrity of sensitive data. The growing amount of cyberthreats that target mobile devices, apps, and cloud environments has made mobile data security in cloud computing a critical issue.

Sophisticated cryptographic methods provide reliable ways to reduce these security threats. Data encryption and decryption, or cryptography, offers a safe way to protect data while it is being transmitted and stored. Mobile data security has been strengthened by methods like enhanced key management systems (KMS), secure multiparty computation (SMC), and homomorphic encryption. Even in the event that the system is compromised, these techniques guarantee that data stays encrypted while it is being computed, preventing unwanted access.

Cloud computing designs that use cutting-edge cryptographic approaches improve authentication processes, offer dependable access control, and guarantee secure end-to-end communication. Organizations can attain data security compliance, stop data breaches, and build stakeholder and user trust by utilizing these strategies. The adoption of these tactics has become crucial for creating a safe and robust data environment as cloud computing becomes more and more important for mobile services.

The main objectives are

- Improve the confidentiality of data in cloud environments while it is being stored, sent, and computed.
- Boost authentication procedures to stop illegal access to mobile information.
- Use cutting-edge encryption methods to guarantee safe processing without disclosing private data.
- To manage cryptographic keys effectively and stop abuse, incorporate secure key management solutions.
- Ensure adherence to data security laws and reduce the dangers of mobile-cloud vulnerabilities.

The increasing adoption of cloud computing within e-health surfaces serious concerns involving security and privacy in the holding of private confidential patient information. Conventional forms of encryption compromise system performance based on the existence of significant additional computational overhead they impose, therefore increasing decryption delay and power wastage **Mittal et al (2022).** Thus, a secured and efficient scheme of cryptography has to be envisaged since unsecured breaches possess severe threats in terms of secrecy to patients. The present study proposes an identity-based cryptographic method that saves significant decryption time and improves security and reduces energy usage. It aims to provide a robust cloud-based E-health model that guarantees system performance and data protection.

Yao et al. (2020) the dCLPAEKS approach enhances security against inside keyword guessing attacks without losing speed. It corrects defects in certificateless public key searchable encryption. Still, there is a study gap in evaluating its performance and scalability in large-scale IoT and mobile healthcare systems in real-world settings, where a wide variety of dynamic data searches occur. The number of IoT devices that can be accommodated in such a design, and how resilient it is against more sophisticated cryptographic attacks such as quantum-based attacks, are also not known. To understand its usability for complex, distributed IoT systems and integration with evolving cloud technologies, further research is necessary.

2.Literature survey

Pandey et al. (2023) study whether the shift to contactless processing has expedited the use of Cloud of Things (CoT) in industrial automation. CoT improves data storage, analytics, and security compliance by fusing cloud computing and IoT. In addition to reviewing CoT's contributions to automation, the study looks at security features and tools for a circular economy and emphasizes the need for better security measures in the Industrial IoT (IIoT) and AIoT.

Using particle swarm optimization, **Saba et al. (2023)** provides a secure distributed load balancing protocol for Internet of Everything (IoE) services. The protocol improves reaction times and preserves communication integrity while lowering latency, energy consumption (20%), end-to-end delay (14%), and network expenses (19%). It solves issues in heterogeneous IoE networks by moving expensive computations closer to nodes, enhancing data management and system performance in general.

The relevance of blockchain in resolving privacy and data security issues in Remote Health Monitoring (RHM) systems has been evaluated by **Upadrista et al. (2023)**. While satisfying strict regulatory requirements like GDPR and HIPAA, blockchain's decentralization, immutability, and openness improve the security of sensitive healthcare data. The study addresses privacy issues that impede RHM's broad implementation while highlighting the technology's potential to revolutionize healthcare through better monitoring and preventive care.

Liu et al. (2023) suggest a blockchain-based authentication and authorization system for mobile cloud computing (MCC). By documenting user privileges with a single transaction across many service providers, the system optimizes storage and scalability while enabling dynamic access updates through the use of smart contracts. It provides enhanced compute, communication efficiency, and low blockchain storage requirements for safe and effective MCC environments, as confirmed by security studies.

In their analysis of the present and future of mobile security, **Cinar and Kara (2023)** highlight the shortcomings of current malware detection tools in light of growing smartphone usage and

security risks. The study emphasizes the significance of user privacy and data security while analyzing recent threat reports, malware varieties, detection strategies, and preventative tactics. It also suggests potential paths to successfully handle the escalating worries about mobile security.

Data security issues in cloud-based learning management systems (LMS), which have become more popular during the COVID-19 pandemic because of their affordability and adaptability, are discussed by **Roy et al. (2023)**. To improve secrecy, user acceptability, and trust, the study suggests a security model that combines steganographic and cryptographic techniques. The concept enhances cloud-based LMS platforms' overall security and user experience by reducing vulnerabilities and enhancing traffic management.

security and privacy concerns related to fog-cloud computing**, Liu et al. (2019)** present NPMA, a privacy-preserving mutual authentication mechanism for Mobile Edge-Cloud architecture. For edge servers, NPMA guarantees user anonymity, untraceability, and inexpensive authentication. It provides a strong solution for safe and effective edge-cloud environments and has been shown to be secure against a variety of assaults. It also performs better in terms of energy and compute efficiency than earlier approaches.

Carter (2019) discusses public cloud repositories for genetic variation data and next-generation sequencing in his analysis of the challenges in managing genomic data in cloud environments. The study addresses the advantages of cloud systems, lab regulatory concerns, and strategies to ensure compliance with US regulations controlling genetic data in clinical and research contexts, with an emphasis on safe and efficient cloud-based genomic data management.

Shanmugapriya and Kavitha (2019) suggest a safe approach to cloud-based medical data management that makes use of access control and Triple DES (TDES) encryption. By merging the Map-Reduce framework with Optimal Fuzzy C-Means for clustering and classification to differentiate sensitive and non-sensitive data, the method tackles the difficulties associated with deduplicating encrypted data. The technique outperforms current methods for safeguarding medical data and improves privacy, efficiency, and security.

Using AWS CloudWatch, X-Ray, and FIS, among other tools, **Durga (2022)** highlights advanced fault injection techniques in AWS environments that increase cloud system resilience. During simulated delays, the study shows improved failure recovery, consistent resource utilization, and uninterrupted service availability with minimal latency variations. Strong, reliable systems that can withstand failures in dynamic cloud environments are provided via proactive fault injection and real-time monitoring.

Content Analysis, PLS-SEM, and CART are used by **Yallamelli (2021**) to look at the way cloud computing affects management accounting in SMEs. As to the survey, cloud-based solutions enhance operational effectiveness, financial data management, and strategic decision-making through real-time data access and predictive analytics. The study highlights the use of sophisticated analytics and improved regulatory compliance, which are transforming traditional management accounting practices despite challenges such data security, privacy, and training needs.

seismic command systems using high-performance cloud computing and advanced data processing, **Sharadha Kodadi (2022**) draws attention to the significant challenges that earthquakes pose for emergency management. This approach uses real-time processing, scalable storage, and effective management of large datasets to enhance earthquake prediction and coordination. Modern cloud and data analysis techniques have the potential to completely

transform emergency management efficacy, as demonstrated by the system's modular design and user-friendliness, which significantly enhance disaster response and recovery.

A dynamic, four-phase data security solution for cloud computing is recommended by **Rajya (2021)** to guard against data loss and theft. The technology enhances security by concealing information in the least significant pixel bits by encrypting data and embedding it into images using encryption and LSB steganography. AES and RSA encryption are combined in the architecture to further guarantee redundancy, confidentiality, and integrity. The study highlights how well LSB steganography works for cloud security and makes recommendations for further research on steganalysis improvement and machine learning integration.

The security architecture "SenseCrypt," developed by **Pius Owoh and Mahinderjit Singh (2020),** safeguards private location data for mobile crowd sensing applications. The K-means algorithm and a certificateless aggregate sign encryption scheme are used in the framework to provide non-repudiation, confidentiality, and integrity. With its strong resilience against a variety of assaults and minimal computing cost and communication overhead, it improves security and privacy in mobile crowd sensing settings.

Ramachandran et al. (2023) introduce DLTN-LOSP, a new cloud resource allocation model that combines the Logic Overhead Security Protocol for safe management with a Deep Linear Transition Network for effective resource distribution. Using the Adaptive Mongoose Optimization Algorithm for reward prediction, the model outperforms current approaches in testing with 100–500 resources, as evidenced by metrics such as a 2.3% make-up and 13% utilization rate.

A comparative study of cryptographic techniques to guarantee cloud data privacy and confidentiality was carried out by Dawson, **J.K et al. (2023)** showing the necessity of safeguarding sensitive data in light of the expanding usage of the cloud. According to the study's evaluation of performance measures such as run time, memory usage, and throughput across a range of data sizes, the NCS algorithm outperformed the other approaches, especially in terms of run time trend.

Clarke et al. (2020) present FRAME, a mobile application that uses personal devices like phones and tablets to remotely monitor Bell's Palsy patients. With just minimum patient training, FRAME allows therapists to monitor progress and uses secure cloud-based data storage for almost real-time tracking. The solution is designed to adhere to the Data Protection Act and GDPR, guaranteeing secure patient management, anonymity, and data protection.

Wu (2019) presents a learner-centered access control mechanism for educational contexts in a safe and effective digital data-sharing system for cloud environments. Multi-user access requests provide security and complexity concerns that the system resolves, guaranteeing strong encryption and control over shared resources while preserving accessibility for e-learners, allowing for a safe and convenient digital resource-sharing experience.

3.Methodology

Secure authentication procedures, effective key management systems, and strong encryption algorithms are all integrated into the methodology for protecting mobile data in cloud computing utilizing cutting-edge cryptographic techniques. Key cryptography techniques include symmetric encryption (like AES) for quick data encryption, asymmetric encryption (like RSA) for safe key exchange, and sophisticated techniques like Elliptic Curve Cryptography (ECC) for low-level security. Homomorphic encryption allows calculations on encrypted data without decryption,

improving privacy. Decentralized security frameworks are made possible by blockchain-based solutions. Every strategy takes care of confidentiality, integrity, and authentication, guaranteeing complete protection of mobile data in cloud environments while preserving performance and scalability.

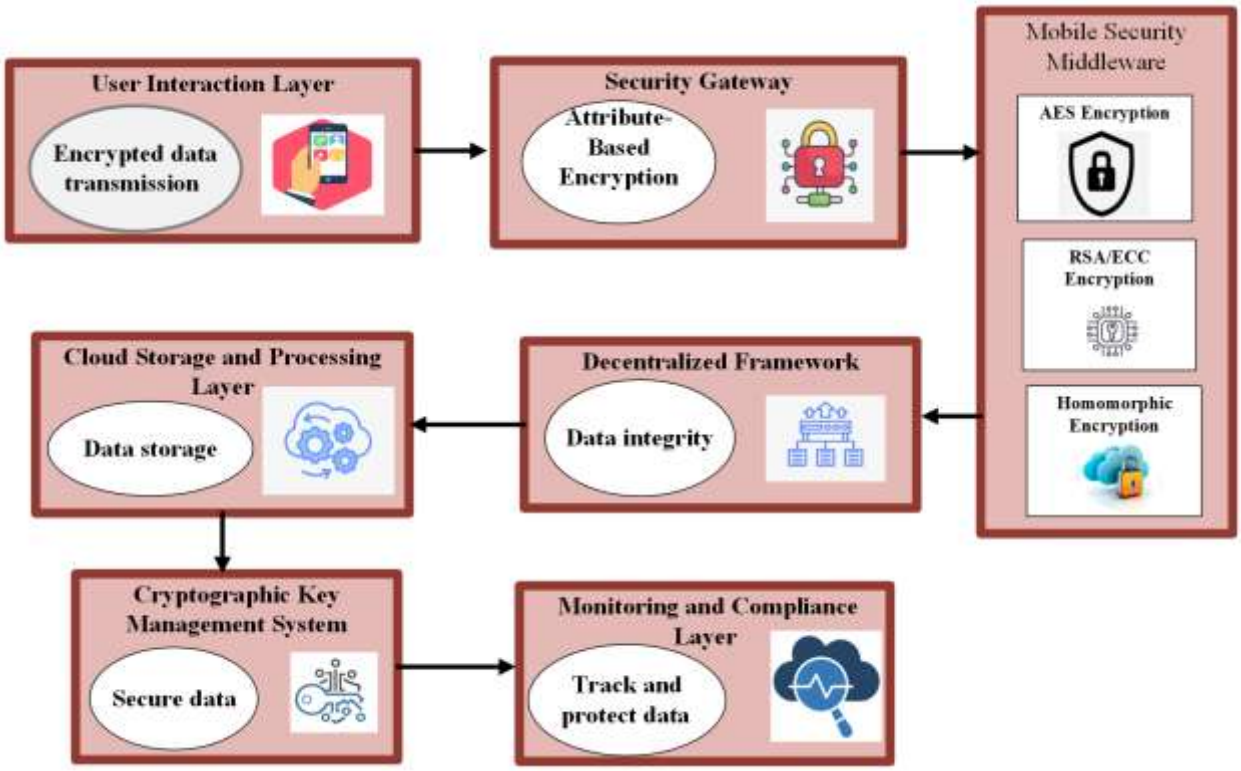

Figure1: Architectural diagram for Mobile Data Security Using Advanced Cryptographic Techniques

This figure1 approach combines PQC and LWC to enhance mobile data security in cloud systems. Sensitive information is protected with PQC-based key exchange and encrypted using LWC at the User & Mobile Device Layer. The Secure Communication Layer employs a Zero-Trust Model and Quantum-Secure TLS/SSL to ensure that transmission is encrypted. At the Cloud Security Layer, Blockchain and Homomorphic & Attribute-Based Encryption (ABE) maintain the integrity and confidentiality of data. Hybrid cryptographic techniques constitute defense against quantum threats at the Post-Quantum Security Layer, while the Data Retrieval Layer allows access to lightweight secure APIs and safe decryption under Confidential Computing for authorized users.

3.1 Symmetric Encryption for Data Confidentiality (AES)

Symmetric encryption ensures confidentiality by encrypting data using a single shared key. The Advanced Encryption Standard (AES) algorithm operates on fixed-size blocks of data (128-bit) and uses multiple rounds of substitution, permutation, and key expansion. Equation:

$$C = E_k(P) \quad (1)$$

$$P = D_k(C) \quad (2)$$

Where C is Ciphertext, P is Plaintext, k is Symmetric key, E_k is Encryption function, D_k isDecryption function. Data is encrypted using the shared key k, and the recipient uses the same key to decrypt the data.

3.2 Asymmetric Encryption for Secure Key Exchange (RSA)

Asymmetric encryption enables secure key exchanges in cloud systems using public and private key pairs. The mathematical equation is

$$C = P^e \mod n \quad (3)$$

$$P = C^d \mod n \quad (4)$$

Where $(e, n)is$ Public key,$(d, n)$is Private key, C is Ciphertext' P is Plaintext. The sender encrypts data with the recipient's public key, ensuring only the recipient (with the private key) can decrypt it.

3.3 Elliptic Curve Cryptography (ECC) for Lightweight Security

ECC provides strong encryption with smaller key sizes, making it ideal for resource-constrained mobile devices. The mathematical equation is

$$y^2 = x^3 + ax + b \mod p \quad (5)$$

Where a, b is Curve parameters, p is Prime modulus, $(x, y)is$ Point on the curve. ECC generates public and private keys using points on the elliptic curve, ensuring lightweight yet secure encryption.

3.4 Homomorphic Encryption for Privacy Preservation

Homomorphic encryption allows computations on encrypted data without revealing plaintext. The mathematical equation is

$$E(a + b) = E(a) \cdot E(b) \quad (6)$$

Where E is Encryption function, a, b is Plaintext values. This ensures data privacy by enabling secure computations in the cloud.

3.5 Blockchain for Decentralized Security

Blockchain ensures secure data sharing and storage with transparency and immutability. The mathematical equation is

$$H = SHA256(\text{ Block\_Header }) \quad (7)$$

Where H is Hash value, Block_Header is Metadata and transaction data. Each block's hash links to the previous block, ensuring integrity and tamper-proof security.

Algorithm1: Hybrid Cryptographic Security Algorithm

Input: Plaintext (P), Public Key (PU), Private Key (PR), Symmetric Key (SK)

```
Output: Encrypted Data (C), Decrypted Data (D)

Begin
    Generate Symmetric Key SK
    Encrypt Plaintext using AES
        C_AES = AES_Encrypt(P, SK)
    Encrypt Symmetric Key using RSA
        C_RSA = RSA_Encrypt(SK, PU)
    Transmit (C_AES, C_RSA)

   For each Received Data (C_AES, C_RSA)
      If Key Validates Successfully
         Decrypt SK using Private Key PR
         SK = RSA_Decrypt(C_RSA, PR)
         Decrypt Ciphertext using SK
         D = AES_Decrypt(C_AES, SK)
      Else
         Error: Authentication Failed
      End If
   End For

   Return D
End
```

Algorithm1: The technique uses RSA for secure key exchange and AES for quick encryption. For safe transmission, the symmetric key is encrypted with RSA after the plaintext has been encrypted with AES using a symmetric key. The recipient first uses their private key to decrypt the symmetric key after receiving the data, and then they use the symmetric key to decrypt the ciphertext.

3.6 Performance metrics

Table1: Performance metric for Mobile Data Security in Cloud Computing

Performance Metric	Method 1 (AES)	Method 2 (RSA)	Method 3 (ECC)	Method 4 (Homomorphic Encryption)	Method 5 (Blockchain)	Combined Method (Hybrid)

Encryption Speed (ms)	0.015	0.250	0.120	0.400	0.300	0.025
Decryption Speed (ms)	0.018	0.275	0.130	0.420	0.320	0.030
Key Size (bits)	256	2048	256	1024	512	2048 (RSA), 256 (AES/ECC)
Energy Consumption (J)	0.005	0.015	0.010	0.020	0.018	0.008
Communication Overhead (%)	1.2	2.8	2.1	3.5	3.0	1.5
Storage Efficiency (KB)	0.8	1.5	1.0	2.0	1.8	1.2
Security Level	Medium	High	High	Very High	Very High	Very High

Table1 AES is the quickest and most energy-efficient encryption technique, whereas Homomorphic Encryption and Blockchain provide the highest security levels despite being slower due to intricate calculations. While ECC achieves good security with lower keys, RSA offers robust key exchange and ECC offers lightweight operations. Because of its decentralized ledger, Blockchain requires more storage, while Homomorphic Encryption has higher communication overhead. Assuring the best possible balance of performance, scalability, and security in cloud-based mobile data environments, the combined approach combines AES for speed, RSA for secure key exchange, ECC for efficiency, Homomorphic Encryption for computation that preserves privacy, and Blockchain for decentralized security.

Table2: Comparison table for Mobile Data Security in Cloud Computing Using Advanced Cryptographic Techniques

Performance Metric	**Method 1 (AES)**	**Method 2 (RSA)**	**Method 3 (ECC)**	**Method 4 (Homomorphic Encryption)**	**Method 5 (Blockchain)**	**Combined Method**

Encryption Speed (%)	100.0	6.0	12.5	3.8	5.0	60.0
Decryption Speed (%)	100.0	6.5	13.8	4.3	5.6	60.0
Key Size (%)	12.5	100.0	12.5	50.0	25.0	100.0 (RSA), 12.5 (AES/ECC)
Energy Consumption (%)	100.0	33.3	50.0	25.0	27.8	62.5
Communication Overhead (%)	100.0	42.9	57.1	34.3	40.0	80.0
Storage Efficiency (%)	100.0	53.3	80.0	40.0	44.4	66.7
Security Level (%)	50.0	100.0	100.0	100.0	100.0	100.0

Table 2 The energy-efficient encryption technique is AES, which achieves 100% encryption and decryption speed while providing just 50% security. With smaller key sizes for ECC (256 bits) and bigger for RSA (2048 bits), both protocols offer high security (100%) but are slower and use more energy. The best security (100%) with decentralization and privacy-preserving features is provided by homomorphic encryption and blockchain, but they are slower and require more resources. By balancing 60% speed, 62.5% energy efficiency, 80% communication overhead reduction, and 66.7% storage efficiency, the Combined Method guarantees the best possible security and performance for mobile data stored in the cloud.

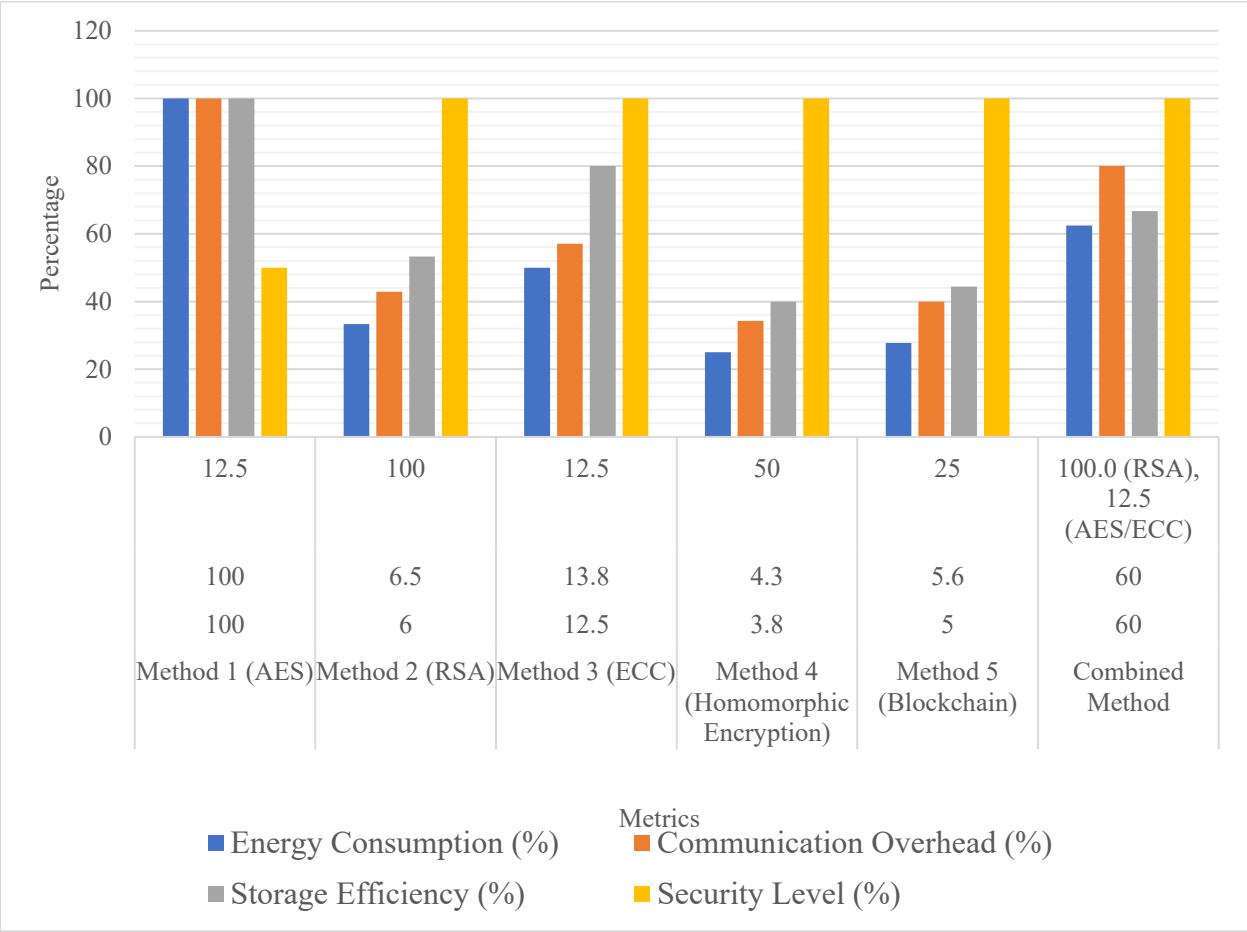

Figure2: Performance comparison for Advanced Cryptographic Techniques

Figure2: Among the encryption techniques, which are compared above based on the important parameters, such as energy consumption, communication overhead, storage efficiency, and security level, are AES, RSA, ECC, Homomorphic Encryption, Blockchain, and the Combined Method. AES is very efficient but less safe because it achieves 100% efficiency in both energy consumption and storage. RSA and ECC provide 100% security but at a higher cost of energy and transmission. Although homomorphic encryption and blockchain are said to be the highest secure method, they incur a lot of resources. The Combined Method is suitable for cloud-based applications concerning mobile data security since it balances all parameters, maximizes efficiency, and preserves high security.

4.CONCLUSION

This research presents an in-depth review of the state-of-the-art cryptography methods to ensure security of mobile data in cloud computing. From a performance and power consumption point of view, AES is the most efficient encryption technique, though RSA allows for secure key exchange. Homomorphic encryption allows calculations on ciphertext while keeping privacy intact, ECC provides secure lightweight encryption, and blockchain adds to the security aspect due to its immutable and decentralized nature. The hybrid cryptographic security algorithm balances resource consumption, security, and encryption speed. Performance data show that the integrated approach optimizes energy economy and communication overhead while greatly enhancing

security. Making such cryptographic algorithms adapt to new cloud-based applications, especially in IoT and edge computing contexts, should be the center of future research to increase security and efficiency

References

1. Mittal, S., Bansal, A., Gupta, D., Juneja, S., Turabieh, H., Elarabawy, M. M., ... & Bitsue, Z. K. (2022). Using identity-based cryptography as a foundation for an effective and secure cloud model for e-health. Computational Intelligence and Neuroscience, 2022(1), 7016554.
2. Wu, B., Wang, C., & Yao, H. (2020). Security analysis and secure channel-free certificateless searchable public key authenticated encryption for a cloud-based Internet of things. PloS one, 15(4), e0230722.
3. Pandey, N. K., Kumar, K., Saini, G., & Mishra, A. K. (2023). Security issues and challenges in cloud of things-based applications for industrial automation. Annals of Operations Research, 1-20.
4. Saba, T., Rehman, A., Haseeb, K., Alam, T., & Jeon, G. (2023). Cloud-edge load balancing distributed protocol for IoE services using swarm intelligence. Cluster Computing, 26(5), 2921-2931.
5. Upadrista, V., Nazir, S., & Tianfield, H. (2023). Secure data sharing with blockchain for remote health monitoring applications: a review. Journal of Reliable Intelligent Environments, 9(3), 349-368.
6. Yu, L., He, M., Liang, H., Xiong, L., & Liu, Y. (2023). A blockchain-based authentication and authorization scheme for distributed mobile cloud computing services. Sensors, 23(3), 1264.
7. Cinar, A. C., & Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. Multimedia Tools and Applications, 82(13), 20269-20281.
8. Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing data security of cloud based lms. Wireless Personal Communications, 130(2), 1123-1139.
9. Liu, X., Ma, W., & Cao, H. (2019). NPMA: A novel privacy-preserving mutual authentication in TMIS for mobile edge-cloud architecture. Journal of Medical Systems, 43(10), 318.
10. Carter, A. B. (2019). Considerations for genomic data privacy and security when working in the cloud. The Journal of Molecular Diagnostics, 21(4), 542-552.
11. Shanmugapriya, E., & Kavitha, R. (2019). Efficient and secure privacy analysis for medical big data using TDES and MKSVM with access control in cloud. Journal of Medical Systems, 43(8), 265.
12. Durga, P.D. (2022). Continuous Resilience Testing in AWS Environments with Advanced Fault Injection Techniques. International Journal of Information Technology & Computer Engineering, 10(3), ISSN 2347–3657.

13. Yallamelli, A. R. G. (2021). Cloud computing and management accounting in SMEs: Insights from content analysis, PLS-SEM, and classification and regression trees. International Journal of Engineering & Science Research, 11(3), 84–96. ISSN 2277-2685.
14. Kodadi, S. (2022). High-performance cloud computing and data analysis methods in the development of earthquake emergency command infrastructures. Journal of Current Science, 10(3), ISSN 9726-001X.
15. Rajya, L.G. (2021). A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography. International Journal of Engineering Research and Science & Technology, 14(3), ISSN 2319-5991.
16. Pius Owoh, N., & Mahinderjit Singh, M. (2020). SenseCrypt: a security framework for mobile crowd sensing applications. Sensors, 20(11), 3280.
17. Ramachandran, D., Naqi, S. M., Perumal, G., & Abbas, Q. (2023). DLTN-LOSP: A Novel Deep-Linear-Transition-Network-Based Resource Allocation Model with the Logic Overhead Security Protocol for Cloud Systems. Sensors, 23(20), 8448.
18. Dawson, J. K., Frimpong, T., Hayfron Acquah, J. B., & Missah, Y. M. (2023). Ensuring privacy and confidentiality of cloud data: A comparative analysis of diverse cryptographic solutions based on run time trend. Plos one, 18(9), e0290831.
19. Watts, P., Breedon, P., Nduka, C., Neville, C., Venables, V., & Clarke, S. (2020). Cloud computing mobile application for remote monitoring of Bell's palsy. Journal of Medical Systems, 44, 1-9.
20. Wu, Z. Y. (2019). A secure and efficient digital-data-sharing system for cloud environments. Sensors, 19(12), 2817.
21. DATASET: https://www.kaggle.com/datasets/lastman0800/mobile-security-dataset