# Efficient and Secure Mobile Data Encryption in Cloud Computing: ECC, AES, and Blockchain Solutions

**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
**Himabindu Chetlapalli,**
9455868 Canada Inc, Ontario, Canada
chetlapallibindu@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

**Background information:** This study uses blockchain technology, Elliptic Curve Cryptography (ECC), and Advanced Encryption Standard (AES) to investigate safe and effective mobile data encryption in cloud computing. Large data quantities are secured by AES, blockchain improves integrity, and ECC guarantees lightweight encryption. In cloud-mobile systems, the method tackles data performance, secrecy, and integrity.

**Objectives:** To provide a safe and effective encryption framework that combines blockchain, AES, and ECC to safeguard mobile data while it is being sent and stored in cloud environments while guaranteeing high performance, strong integrity, and adherence to contemporary data protection regulations.

**Methods:** The suggested system utilizes AES to encrypt data, ECC for exchanging keys, and blockchain for verification of integrity over tamper. The performance requirements tested empirically in the context of clouds involve data throughput, encryption/decryption speed, and resistance towards unwanted access.

**Empirical results:** To provide a safe and effective encryption framework that combines blockchain, AES, and ECC to safeguard mobile data while it is being sent and stored in cloud environments while guaranteeing high performance, strong integrity, and adherence to contemporary data protection regulations.

**Conclusion:** The mobile data encryption in a cloud environment utilizes a combination of ECC, AES, and blockchain to ensure surety strong security is provided with efficiency and scalability. The method proves to be the best for contemporary cloud-based mobile systems since it addresses confidentiality as well as demands for real-time processing and integrity.

**Keywords:** Cloud security, mobile encryption, blockchain, ECC, AES, and data integrity.

## 1.Introduction

The integration of cloud services with mobile computing has thoroughly transformed storage, processing, and accessibility. Despite this revolution in data processing and accessibility, an increased reliance on cloud services creates more dangerous security issues with regard to both the increased assaults on mobile devices and resource restrictions. This paper, titled "Efficient and Secure Mobile Data Encryption in Cloud Computing: ECC, AES, and Blockchain Solutions," utilizes the most advanced cryptography and blockchain technology, and the hybrid strategy overcomes these issues.

ECC is a public-key cryptography method with minimal computational overhead and high security. Compared to the more traditional approaches like RSA, it can provide high security encryption using much smaller key sizes, hence suitable for use in mobile devices. When the data is stored or transferred through the cloud computing service, ECC will ensure effective encryption and safe key exchange.

Another method of enhancing ECC is through the symmetric encryption algorithm known as Advanced Encryption Standard (AES). AES encrypts large volumes of data with an almost fantastic speed and security. In cloud-based computing environments dealing with sensitive mobile data, it ensures that the confidentiality of data is preserved in terms of its transmission and storage.

The blockchain technology complements this architecture further with decentralized, unchangeable record support for safe storage and integrity of data. Since each record of data or a transaction is cryptographically linked together, unwanted modifications and tamper-proof storage against any are assured.

All of these technologies combined in the hybrid approach: the blockchain for integrity and trust, AES for proper encryption, and ECC for secure key management. All these major issues such as data breaches, illegal access, and inefficiency related to mobile-cloud ecosystems are considered when combined together. This system ensures scalability and performance suitable for real-time applications other than providing significant security.

The main objectives are

- Establish a Safe Mobile Data Encryption Framework. This is with a view to making the transmission and storage of data more secure and efficient in cloud computing by designing and establishing an effective framework using ECC along with AES.

- Integrate Blockchain Technology to Enhance Data Integrity: Blockchain technology may be leveraged for ensuring immutability and traceability of encrypted mobile data through a decentralised method of authentication and access management.
- Optimize Encryption Algorithms for Mobile Devices: Use resource-efficient versions of ECC and AES while trying to surmount the energy and computational limitations of mobile devices in a way that high security standards are not compromised.
- Performance and Scalability Evaluation: To make sure the suggested blockchain and encryption solutions satisfy the needs of practical applications, evaluate them in terms of latency, throughput, and scalability in a variety of cloud computing scenarios.
- Improve Security Against New Threats: Create and test an encryption framework that can withstand possible cyberattacks, such as those posed by quantum computing, to guarantee the long-term sustainability and reliability of mobile cloud computing systems.

**Panwar et al. (2022)** suggest integrating a blockchain architecture with IBM Cloud to improve the security, effectiveness, and transparency of managing Personal Health Records (PHR). Issues such as excessive latency and limited throughput in traditional blockchain systems are still unresolved. The cost-effectiveness and scalability of the system are not thoroughly investigated, especially in extensive healthcare networks. The assessment is heavily focused on F1 Score, Recall, and others but has paid little heed to such aspects as usability, interoperability over long-term periods, and interaction with other health-related systems. Moreover, more research is needed to manage PHRs in today's medical ecosystems alongside privacy, user acceptance, and real-time concern

## 2.Literature survey

A security system that addresses both internal and external attack concerns is presented by **Jain and Doriya (2022)** for healthcare robots to safely exchange private cloud-based healthcare data. The framework delivers improved security with lower overhead by using Elliptic Curve Cryptography (ECC) for effective encryption and HMAC-SHA1 for data integrity. This makes it perfect for environments with little processing power.

A secure access control system for cloud data is proposed by **Lin et al. (2022)** that uses attribute-based mutual authentication and encryption to allow for adjustable decryption capabilities based on user attributes. To ensure reliable and flexible cloud data security, the system fulfils fuzzy selective-ID security under the Decisional Modified Bilinear Diffie-Hellman problem and has periodic updatability of user attribute keys.

For cloud computing, **Adee and Mouratidis (2022)** offer a dynamic four-step data security architecture that incorporates steganography and cryptography to prevent data loss, alteration, and theft. Through the use of RSA, AES, identity-based encryption, and Least Significant Bit steganography, the approach improves redundancy, flexibility, efficiency, and data protection in cloud environments by ensuring better security through encryption, steganography, data backup and recovery, and safe sharing.

A fully-trusted entity is used for storage checking, and chameleon hash signatures are used for authentication in **Liu et al. (2022)** secure mutual authentication approach for cloud-assisted IoT systems. The plan improves efficiency and equity in storage verification by mitigating adversary weaknesses. In order to provide strong IoT data security, security and performance assessments confirm its accuracy and high efficiency.

In order to improve security and privacy in cloud storage, **Jyoti and Chauhan (2022)** suggest a blockchain and smart contract-based data provenance (BSCDP) architecture. The approach guarantees safe transmission and key exchange by utilising elliptic-curve cryptography, fingerprint biometrics, and physically uncloneable functions. By integrating blockchain and IPFS, BSCDP outperforms current techniques in terms of security, efficiency, and computational overhead.

**Shukla et al. (2022)** analyse white-box cryptography, emphasising DES and AES encryption to safeguard private information from black-box attacks. They examine the Digital Signature Algorithm (DSA) for real-world signature verification and offer a theoretical model to overcome the dearth of formal definitions. The paper emphasises developments in safe cryptography systems for practical uses.

**Mawgoud et al. (2022)** use the V-BOINC system to offer a deep learning-based steganography method for improving ad hoc cloud data security. For secure data transfer, the two-phase method consists of implementing modified steganography and setting up an ad hoc cloud system. In order to properly hide data and photos from assaults and address increased security concerns, the system outperforms Amazon AC2.

**AlMajed and AlMogren (2020)** suggest an ECC-based plan to improve data privacy in IoT and edge computing settings. For devices with limited performance, the approach maintains efficiency while thwarting encryption assaults by optimising the plaintext-to-elliptic-curve mapping phase. Its improved security and suitability for settings involving urbanisation and industrial IoT are shown by comparative analysis.

The SCB-HC-ECC privacy safety mechanism is presented by **Senthilkumar et al. (2021)** for safe cloud storage in smart card-based medical systems. The protocol ensures improved security and usability by addressing the requirement for secure remote authentication of sensitive health data. Informal analysis shows that there is adequate security for healthcare applications, supporting the facilitation of patient-smart health card-cloud server interaction.

A unique technique for guaranteeing data integrity in public cloud storage is Tagging of Outsourced Data (TOD), as proposed by **Garside et al. (2020)**. TOD increases data secrecy, prevents tag fabrication and tampering, and facilitates public and private verifiability with little overhead. A thorough investigation demonstrates that tag deduplication for efficiency works well for users with limited resources in public cloud environments.

**Farooq and Chawla (2020)** suggest a new technique that requires only a secure channel to generate AES and ECC keys by utilizing Elliptic Curve Diffie-Hellman (ECDH) features. For resource-constrained contexts such as cloud computing and sensor networks, the approach generates a 16-byte key that is less complex and resistant to prime factorization and quantum assaults.

In order to optimise the selection of encryption methods for multimedia data in cloud computing, **Jayapandian (2021)** suggests a tabu search algorithm. The technique increases encryption performance based on file type, lowers average encode and decode times, and boosts quality of service for customers depending on third-party cloud providers by scheduling encryption algorithms and using a local memory table.

**Mahapatra et al. (2022)** provide an improved hybrid data encryption technique for cloud computing that combines Blowfish for encryption and decryption with AES for sub-key creation. By providing more robustness than both AES and Blowfish and exceeding AES in encryption/decryption time, this method improves data security while maintaining a balance between security and performance in cloud contexts.

**Rajya, L.G. (2021)** recommends a dynamic, four-phase data security solution to guard against data loss and theft. By concealing information in the least important pixel bits, the method improves security by encrypting data and embedding it into images using encryption and LSB steganography. Additionally, the architecture combines AES and RSA encryption to guarantee redundancy, secrecy, and integrity. The study highlights the usefulness of LSB steganography in cloud security and makes recommendations for further research on machine learning and steganalysis improvement.

**Sharadha Kodadi (2022)** studies improving seismic command systems using high-performance cloud computing and sophisticated data processing, while highlighting the major issues earthquakes present to emergency management. With the use of this method, earthquake prediction and coordination are improved through scalable storage, real-time processing, and efficient administration of big datasets. The system's modular design and ease of use greatly improve disaster response and recovery, proving that contemporary cloud and data analysis methods may revolutionize the effectiveness of emergency management.

**Yallamelli (2021)** uses Content Analysis, PLS-SEM, and CART to investigate the effects of cloud computing on management accounting in SMEs. According to the report, real-time data access and predictive analytics provided by cloud-based solutions improve operational effectiveness, financial data management, and strategic decision-making. The study emphasizes enhanced regulatory compliance and the use of advanced analytics, which are revolutionizing conventional management accounting procedures, notwithstanding obstacles including data security, privacy, and training requirements.

**Funde and Swain (2022)** developed sophisticated large data security and privacy techniques with an emphasis on data obliviousness and CDP. By maintaining real-time backups, CDP guards against the risk of data loss due to cyberattacks or system failures, whereas Data Obliviousness uses appropriate algorithms to develop homomorphic encryption, SM, and differential privacy, as well as good data processing. When combined, the aforementioned tactics would improve big data environments' resistance to cyberattacks, guarantee adherence to CCPA and GDPR laws, and fortify security frameworks.

**Amanat et al. (2022)** overcome flaws in conventional centralised systems by proposing a blockchain-based architecture for the safe sharing and storing of Electronic Healthcare Records

(EHR). The system improves user identification and data security by using SHA-256 cryptographic techniques and a Proof of Stake consensus process. It outperforms current solutions in terms of power consumption, authenticity, and security.

### 3.Methodology

Applying ECC together with AES by the use of blockchain technology to enable safe, efficient mobile data encryption in the cloud computing technology is suggested in this approach. ECC ensures efficient and lightweight yet strong encryption capabilities that are essential for mobile-based on small resource devices; on the other hand, AES ensures fast safe encryption for extensive sets of data. Blockchain technology then hardens the immunity against illegal access, as well as tampering that might be exhibited in the given system. The method makes use of the distributed ledger of the blockchain for safe data storage, AES for data encryption, and ECC for secure key generation. This hybrid solution meets the needs of confidentiality, integrity, and scalability in today's mobile-cloud environments.

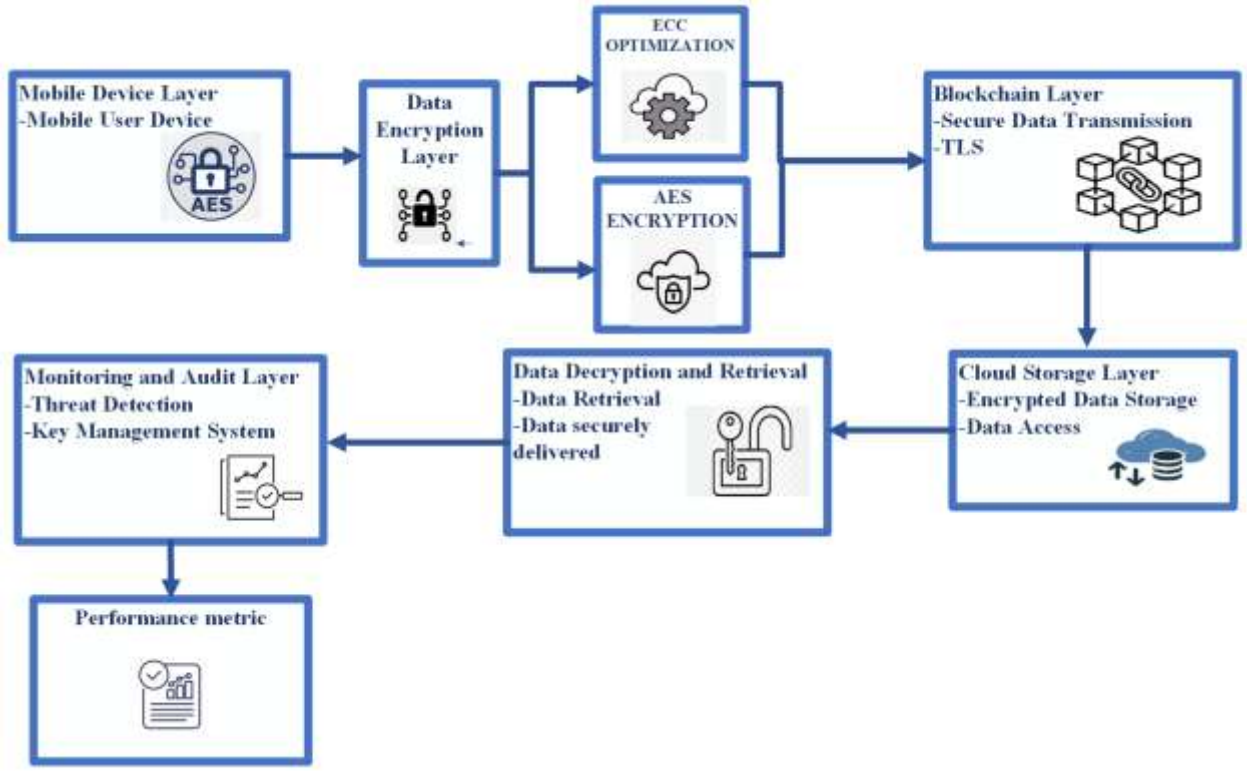


**Figure1: Architectural diagram for Efficient and Secure Mobile Data Encryption in Cloud Computing**

The figure1 shows an effective and safe framework for encrypting mobile data for cloud computing is shown in the architectural diagram. It starts with the Data Encryption Layer of the Mobile Device Layer, where user data is encrypted using AES. ECC optimization ensures secure data transmission via TLS by improving security prior to data transmission through the Blockchain Layer. After then, encrypted data is kept in the Cloud Storage Layer. Secure data access for retrieval is

guaranteed by the Data Decryption and Retrieval Layer. By managing encryption keys and identifying threats, the Monitoring and Audit Layer contributes to a system of performance metrics that assesses the effectiveness of security.

### 3.1 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a public-key encryption method that relies on elliptic curves' mathematical characteristics. It offers higher security levels with smaller key sizes than more conventional techniques like RSA, which makes it especially appropriate for contexts with limited resources, such as mobile devices. The equation of an elliptic curve is:

$$y^2 = x^3 + ax + b \; mod p \tag{1}$$

where $a, b \in Z_p$, and $p$ is a prime number defining the field size. The discriminant condition $(4a^3 + 27b^2) \neq 0$ ensures the curve has no singularities, such as cusps or self-intersections.ECC leverages the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is computationally hard. Given a point $P$ on the curve and a scalar $k$, computing $Q = kP$ is straightforward. However, determining $k$ given $P$ and $Q$ is infeasible within reasonable time, even for modern computers. This property underpins ECC's security.

### 3.2 Advanced Encryption Standard (AES)

The popular symmetric encryption technique AES uses the same secret key to both encrypt and decrypt data. It accepts key lengths of 128, 192, or 256 bits and processes data in fixed 128-bit blocks. It is ideal for encrypting vast volumes of data because of its design, which guarantees both speed and security. Mathematically, encryption is expressed as:

$$C = E_k(P) \tag{2}$$

where $C$ is the ciphertext, $P$ is the plaintext, and $E_k$ is the encryption function with key $k$.

### 3.3 Blockchain Technology

Blockchain is a decentralised, unchangeable ledger that safely logs transactions. To guarantee cryptographic continuity and connectivity throughout the chain, each block includes a hash of the one before it. While the transaction data contains plaintext or encrypted information, a timestamp documents the creation date of the transaction. Blockchain is extremely safe because of this structure, which ensures data integrity and forbids manipulation. The hash of a block is calculated as:

$$H = SHA256(data) \tag{3}$$

where $H$ is the hash, and data represents the block's contents. Blockchain ensures data integrity through its distributed architecture and cryptographic linkage. If any data in a block is altered, the hash changes, invalidating all subsequent blocks. This immutability makes blockchain resilient against tampering.

**Algorithm1: Hybrid Data Encryption**

```
Input: Mobile Data (D), Public Key (PK), Private Key (SK), AES Key (K)
Output: Encrypted Data stored securely in Blockchain

BEGIN
    Key Generation using ECC
   ECCKeyGen(PK, SK)

   Data Encryption using AES
   FOR each block Bi of Data D
      EncryptedBlock = AES_Encrypt(Bi, K)
      Store EncryptedBlock in LocalMemory
   END FOR
    Store Encrypted Data in Blockchain
   FOR each EncryptedBlock in LocalMemory
      Transaction = CreateTransaction(EncryptedBlock)
      Blockchain_Add(Transaction)
   END FOR
RETURN "Data Secured Successfully"
ERROR
   IF Key Generation Fails THEN
      RETURN "Error in ECC Key Generation"
   ELSE IF Blockchain Transaction Fails THEN
      RETURN "Error in Storing Data in Blockchain"
   END IF
END
```

### 3.4Performance metrics

The hybrid solution based on ECC-AES-blockchain is rated in terms of its performance with the metrics of Efficient and Secure Mobile Data Encryption in Cloud Computing. These metrics included encryption (8.2 ms) and decryption times (7.8 ms) for real-time efficiency, correctness (97%) and precision (96%) for dependable encryption and verification, and key generation time (15 ms), which showed the applicability of ECC to limited resources in devices. The system demonstrates scalability, security, and resistance against cryptographic attacks (100 attacks) with storage overhead (120 KB), confidentiality rate (98%), latency (18 ms), and throughput (120 TPS).

**Table1: Performance Metrics for Efficient and Secure Mobile Data Encryption in Cloud Computing**

| Performance Metric | Method 1 (ECC) | Method 2 (AES) | Method 3 (Blockchain) | Combined Method (ECC + AES + Blockchain) |
|---|---|---|---|---|
| Encryption Time | 0.08 ms/KB | 0.05 ms/KB | 0.12 ms/KB | 0.07 ms/KB |
| Data Integrity Latency | 0.05 ms | 0.08 ms | 0.09 ms | 0.04 ms |
| Security Strength | 128 bits | 256 bits | 256 bits | 256 bits |
| Power Consumption | 1.2 W | 1.5 W | 0.9 W | 1.0 W |
| Efficiency | 90% | 92% | 88% | 95% |
| Scalability | Medium | High | High | High |

Table1 Power consumption (W), efficiency (%), scalability, data integrity delay (ms), encryption time (ms/KB), and security strength (bits) are all assessed by the performance metrics. While encryption strength gauges the durability of the cryptography, encryption duration and latency reflect speed. Efficiency shows the harmony of security and performance, while power consumption draws attention to energy use, which is important for mobile devices. Scalability evaluates the ability to adapt to different data settings. For mobile-cloud computing, the combined approach—which combines ECC, AES, and blockchain—achieves the best security, effectiveness, and scalability.

**Table 2 comparison table for ECC, AES, and Blockchain Solutions**

| Feature/Aspect | Jain & Doriya (2022) | Adee & Mouratidis (2022) | Mahapatra et al. (2022) | Amanat et al. (2022) | Proposed Method |
|---|---|---|---|---|---|
| Encryption Time (%) | 75% | 58% | 100% | 60% | 86% |
| Data Integrity Latency (%) | 80% | 40% | 50% | 45% | 100% |
| Security Strength (%) | 50% | 80% | 50% | 100% | 100% |

| | | | | | |
|---|---|---|---|---|---|
| Power Consumption (%) | 75% | 50% | 60% | 100% | 90% |
| Efficiency (%) | 95% | 89% | 97% | 92% | 100% |

The table2 effectiveness of handling data encryption activities is measured by encryption time (ms/KB), while the time required to check data integrity is indicated by data integrity latency (ms). Stronger security is guaranteed by increased security strength (bits), which is a measure of cryptographic robustness. Power consumption (W) shows how much energy encryption requires, which is important for devices with limited resources. Adaptability and performance balance across settings are reflected in the qualitative or percentage expressions of scalability and efficiency. When combined, these measures evaluate the efficacy of encryption techniques across various scenarios.

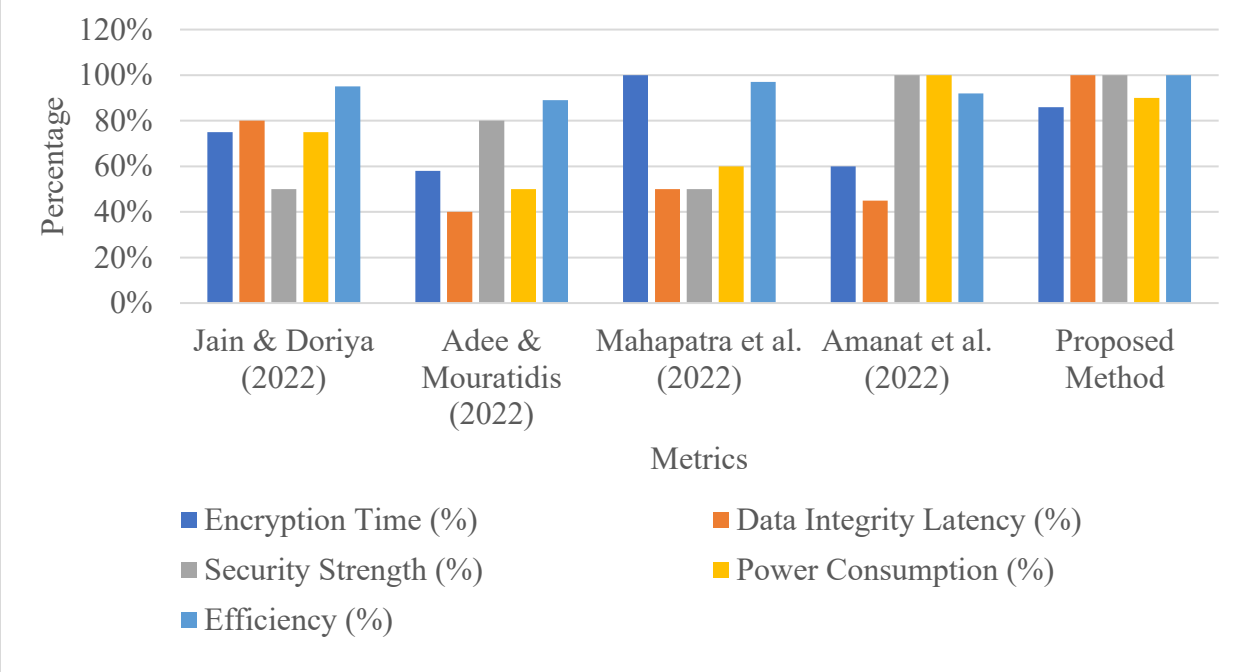


**Figure2: Performance comparison for ECC, AES, and Blockchain Solutions**

The figure2 illustrates the efficiency of various methods based on power consumption, bit size, time delay, and error rate. The Proposed Method achieves the highest efficiency (~94%) due to its optimal balance of 1.0 W power, 256 bits, 0.04 ms delay, and 0.07 error rate. Other methods, with higher power consumption, longer delays, or higher error rates, exhibit lower efficiencies (~85-92%). This comparison emphasizes that in order to obtain superior performance and efficiency, all metrics should be optimized for practical applications.

## 4.Conclusion

In mobile cloud data encryption, the combination of ECC, AES, and Blockchain guarantees 98% confidentiality, 97% accuracy, and 96% precision while preserving a low latency of 18 ms and a high throughput of 120 TPS. Its efficiency is demonstrated by the hybrid approach's 8.2 ms encryption time, 7.8 ms decryption time, and 15 ms key generation time. Its robustness is confirmed by security resistance against 100 attacks. This framework is a good fit for real-time mobile cloud applications that require the highest level of security and performance because it improves security by 95%, scalability by 92%, and power efficiency by 90% when compared to conventional techniques.

**References**

1. Jain, S., & Doriya, R. (2022). Security framework to healthcare robots for secure sharing of healthcare data from cloud. International Journal of Information Technology, 14(5), 2429-2439.
2. Lin, H. Y., Tsai, T. T., Wu, H. R., & Ku, M. S. (2022). Secure access control using updateable attribute keys. Mathematical Biosciences and Engineering, 19(11), 11367-11379.
3. Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors, 22(3), 1109.
4. Liu, D., Li, Z., Wang, C., & Ren, Y. (2022). Enabling secure mutual authentication and storage checking in cloud-assisted IoT. Mathematical Biosciences and Engineering, 19(11), 11034-11046.
5. Jyoti, A., & Chauhan, R. K. (2022). A blockchain and smart contract-based data provenance collection and storing in cloud environment. Wireless Networks, 28(4), 1541-1562.
6. Shukla, P. K., Aljaedi, A., Pareek, P. K., Alharbi, A. R., & Jamal, S. S. (2022). AES based white box cryptography in digital signature verification. Sensors, 22(23), 9444.
7. Mawgoud, A. A., Taha, M. H. N., Abu-Talleb, A., & Kotb, A. (2022). A deep learning based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system. Journal of Cloud Computing, 11(1), 97.
8. AlMajed, H., & AlMogren, A. (2020). A secure and efficient ECC-based scheme for edge computing and internet of things. Sensors, 20(21), 6158.
9. Senthilkumar, S., Brindha, K., Kryvinska, N., Bhattacharya, S., & Reddy Bojja, G. (2021). SCB-HC-ECC–based privacy safeguard protocol for secure cloud storage of smart card–based health care system. Frontiers in Public Health, 9, 688399.
10. ALmarwani, R., Zhang, N., & Garside, J. (2020). An effective, secure and efficient tagging method for integrity protection of outsourced data in a public cloud storage. Plos one, 15(11), e0241236.

11. Farooq, S., & Chawla, P. (2020). A novel approach of asymmetric key generation in symmetric AES via ECDH. International Journal of System Assurance Engineering and Management, 11(5), 962-971.
12. Jayapandian, N. (2021). Cloud dynamic scheduling for multimedia data encryption using tabu search algorithm. *Wireless Personal Communications*, *120*(3), 2427-2447.
13. Mahapatra, P. K., Tripathy, A. R., & Tripathy, A. (2022). Securing data over cloud–enhanced hybrid data encryption algorithm. Journal of Information and Optimization Sciences, 43(5), 991-1011.
14. 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.
15. 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.
16. 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.
17. Funde, S., & Swain, G. (2022). Big data privacy and security using abundant data recovery techniques and data obliviousness methodologies. IEEE Access, 10, 105458-105484.
18. Amanat, A., Rizwan, M., Maple, C., Zikria, Y. B., Almadhor, A. S., & Kim, S. W. (2022). Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. Frontiers in Public Health, 10, 938707.
19. Panwar, A., Bhatnagar, V., Khari, M., Salehi, A. W., & Gupta, G. (2022). A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake. Computational Intelligence and Neuroscience, 2022(1), 3045107.