IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 11, Issue 1, 2023

Modern Cryptographic Frameworks in Cloud Environments for Enhancing Mobile Data Security

DINESH KUMAR REDDY BASANI,
CGI, British Columbia, Canada
dinesh.basani06@gmail.com
BASAVA RAMANJANEYULU GUDIVAKA,
Raas Infotek, Delaware, USA
basava.gudivaka537@gmail.com
RAJYA LAKSHMI GUDIVAKA,
Wipro, Hyderabad, India
rlakshmigudivaka@gmail.com
RAJ KUMAR GUDIVAKA
Surge Technology Solutions Inc, Texas, USA
rajkumargudivaka35@gmail.com
SRI HARSHA GRANDHI,
Intel, Folsom, California, USA
grandhi.sriharsha9@gmail.com
SUNDARAPANDIAN MURUGESAN,
Intel Corporation, Folsom, California
tmsundaroff@gmail.com
M M KAMRUZZAMAN,
Department of Computer Science, College of Computer and Information Sciences,
Jouf University, Sakakah, Saudi Arabia. mmkamruzzaman@ju.edu.sa

Abstract

Background Details: Ensuring mobile data security has become much more difficult due to the quick uptake of cloud environments and mobile technologies. In order to secure sensitive data in mobile-cloud ecosystems, modern cryptographic frameworks use scalable designs and sophisticated encryption techniques to handle issues including unauthorized access, data breaches, and privacy concerns.

Objectives: The purpose of this study is to assess contemporary cryptographic frameworks for protecting mobile data in cloud environments (40 words). It investigates how well they protect privacy, confidentiality, and integrity while weighing performance trade-offs to find the best ways to improve data security in dynamic cloud environments

Methods: Cryptographic techniques like secure key management, attribute-based encryption, and homomorphic encryption are compared. Through case studies and experimental implementations, cloud-based frameworks are assessed for security, scalability, and performance, emphasizing issues and practical implications.

Empirical Results: By facilitating secure computation and effective access management, respectively, attribute-based encryption and homomorphic encryption greatly improve mobile data security, according to the analysis. For both small- and enterprise-level cloud apps, empirical data show enhanced security metrics with negligible performance trade-offs.

ISSN 2347–3657
International Journal of Information Technology & Computer Engineering
Volume 11, Issue 1, 2023

Conclusion (40 words): A strong basis for mobile data security in cloud contexts is offered by contemporary cryptographic frameworks. They enable enterprises to successfully embrace cloud technologies by tackling new threats and guaranteeing data confidentiality, striking a balance between security, performance, and scalability.

Keywords: cloud computing, data encryption, cryptography, mobile security, and access control.

1.Introduction

With the transmission and storage of large volumes of sensitive data in cloud environments, mobile data security has emerged as a crucial issue in cloud computing. In order to protect data availability, confidentiality, and integrity from a constantly changing array of cyberthreats, modern cryptographic frameworks are essential. These frameworks guarantee safe communication and storage in mobile-cloud systems by utilising access control, authentication, and encryption.

The widespread popularity among mobile applications is due to cloud technology and its integration, which allow accessing data at any time and from any location. However, the cost for such ease is the increased vulnerability toward security vulnerabilities such as data breaches, illegal access, and man-in-the-middle attacks. Although traditional security measures work very well in static systems, it becomes ineffective very often in a mobile-cloud ecosystem which is dynamic and resource constrained.

Cryptographic frameworks that offer strong solutions for mobile-cloud scenarios include Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), and new blockchain technologies. For real-time data processing, AES provides fast symmetric encryption, while ECC delivers lightweight public-key encryption that is perfect for mobile devices with limited resources. A potential option for safe data exchange and transaction tracking, blockchain's decentralised structure also improves transparency, immutability, and trust.

The increasing dependence on cloud services, along with exponential growth in the use of mobile devices, makes it imperative that effective and safe data protection solutions be in place. These challenges are met through modern cryptographic architectures, which provide the highest possible security without the loss of user-friendliness or efficiency by relying on the newest technologies and highly complex algorithms.

The main objectives are

- Improve Data Security: Create cryptographic frameworks that guarantee mobile data availability, secrecy, and integrity in cloud settings.
- Enhance Performance: Create efficient algorithms that use the fewest resources possible while yet being highly secure.
- Enable Secure Data exchange: Increase control and transparency in multi-party data exchange by utilising blockchain technology.
- Enhance Scalability: Provide solutions that can easily grow with the amount of mobile and cloud data.
- Take User Privacy into Account: Use privacy-preserving cryptographic methods to safeguard private user data.

Advances in protecting sensitive characteristics with Modified Random Fibonacci Cryptography (MRFC) and the Group Key Based Attribute Encryption approach are presented by **Sumathi, M., and Sangeetha, S. (2021)**. There are still large research gaps, nevertheless. The method limits flexibility in dynamic, large-scale cloud environments that demand real-time classification since it depends on manual data owner selections for attribute segregation. Additionally, it is not integrated with AI or machine learning to automate and increase categorization accuracy. Furthermore, little is known about the method's scalability and performance when dealing with big datasets and a variety of user scenarios. To overcome these obstacles, future studies should concentrate on automation, scalability, and integrating cutting-edge cryptographic approaches.

2.Literature survey

A dynamic four-step data security structure for cloud computing is put out by **Adee and Mouratidis (2022)** to reduce risks such as data loss, manipulation, and theft. It mixes steganography and cryptography. Redundancy, flexibility, efficiency, and security are improved by the model's inclusion of encryption, steganography, backup and recovery, and secure data sharing. In cloud contexts, this method successfully tackles privacy and security issues while guaranteeing strong data security and efficient sharing procedures.

A new decentralised blockchain architecture is proposed by **Kumar et al. (2022)** to improve privacy and data security in healthcare against cyberattacks. By grouping network participants into clusters, the approach greatly increases efficiency by reducing network traffic tenfold and accelerating ledger updates when compared to existing models. This creative design solves important security issues while maximising performance in healthcare data management systems.

In order to improve security, transparency, and performance in the sharing of medical records, **Panwar et al. (2022)** suggest a blockchain framework for managing personal health records (PHR) using IBM Cloud-based data lakes. The architecture enhances healthcare management by resolving latency and throughput problems in conventional blockchain systems. The system exhibits excellent accuracy and superior outcomes when measured using metrics like F1 Score and Recall, which supports improved patient data analysis and illness severity evaluation.

Amanat et al. (2022) address the shortcomings of centralised systems by proposing a blockchain-based architecture for the safe storage and exchange of Electronic Health Records (EHR). Data security, authentication, and immutability are improved by the framework through the use of SHA256 and Proof of Stake (POS) consensus. The system offers a dependable and effective way to handle electronic health records, outperforming more conventional techniques like Proof-of-Work, SHA-1, and MD5 in terms of power consumption, authenticity, and security.

An AI-based approach for identifying and thwarting economic denial of sustainability (EDoS) assaults in cloud computing is presented by **Aldhyani and Alkahtani (2022)**. The Random Forest (RF) technique outperformed other models in binary classification, according to the study, but the Support Vector Machine (SVM) did better in multi-classification. With a high R2 score and a low Mean Squared Error (MSE), the statistical analysis validated RF's robust performance. These findings demonstrate how well RF detects and counteracts Economic Denial of Sustainability (EDoS) assaults, which take advantage of the pay-per-use nature of the cloud.

A deep learning-based steganography architecture is proposed by **Mawgoud et al. (2022)** to improve data security in ad-hoc cloud systems by utilising the V-BOINC platform. In contrast to

Amazon AC2, the study uses a modified steganography technique that successfully embeds data within photos. The solution proved highly effective in hiding data and images from assaults, addressing increased security concerns and guaranteeing better privacy and security when transmitting data over the cloud.

A blockchain and bi-linear polynomial-based QCP-ABE framework are presented by **Yoon et al. (2021)** to improve cloud data security and privacy, especially for data created by the Internet of Things. The model uses a dynamic non-linear polynomial chaotic quantum hash algorithm and generates keys and encryption/decryption times with 95% efficiency and over 90% bit change accuracy. The framework ensures strong security and privacy for intricate cloud data environments by addressing the drawbacks of conventional ABE techniques.

CESCR, a novel CP-ABE approach for safe and effective health data exchange in collaborative eHealth systems, is presented by **Edemacu et al. (2021).** Traditional CP-ABE drawbacks, such as the lack of attribute/user revocation and computational inefficiencies, are addressed with CESCR. CESCR is an important development for collaborative and privacy-preserving healthcare settings since it uses an enhanced access structure to guarantee strong security, expressiveness, and effective administration of health data.

With the objective to handle data violations and illegal access, **Sauber et al. (2021)** offer a safe data protection paradigm for cloud computing. The concept protects against fraudulent users and data owners by integrating identity, authentication, authorization, encryption, and a one-time password (OTP) technique. It improves security, scalability, and efficiency for end users and data owners in cloud environments and is implemented using the Next Generation Secure Cloud Server (NG-Cloud) simulation.

Bermi et al. (2021) provide a hybrid solution to cloud data security that combines elliptic curve cryptography (ECC) and attribute-based encryption (ABE). The technique improves cryptographic performance by substituting scalar multiplication on elliptic curves for computation-intensive bilinear pairing. The elliptic curve discrete logarithm problem (ECDLP) is used by Ciphertext-Policy ABE to provide strong security and a high degree of data protection for cloud computing settings.

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.

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.

Content Analysis, PLS-SEM, and CART are used by **Yallamelli (2021)** to examine how 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.

Durga (2022) emphasizes sophisticated fault injection techniques in AWS environments that improve cloud system resilience by utilizing tools such as AWS CloudWatch, X-Ray, and FIS. The study demonstrates enhanced failure recovery, stable resource use, and sustained service availability with negligible changes in latency during simulated delays. Real-time monitoring and proactive fault injection provide dependable, strong systems that can sustain failures in dynamic cloud settings.

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.

To increase cloud security, **Tallapally and Manjula (2020)** propose a multi-level encryption strategy to meet client concerns with existing methods. It improves data security by restricting access to pre-authorized users. It offers a dependable and efficient method of securing cloud settings and offers faster and safer file upload and download processes as compared to single-level encryption solutions.

Using digital signature methods (DSA), polynomial congruence, and elliptic curve cryptography (ECC), **Nithisha and Jayarin (2022)** provide a secure cloud storage and communication system. The system ensures strong data security and user authentication by introducing effective techniques for encryption, digital signature creation, and prime number and key generation. Compared to current techniques, this methodology offers greater efficiency and protection while addressing the scalability and security issues in cloud systems.

"SecureCloud," a cloud computing security architecture that combines blockchain and machine intelligence, is presented by **Thakur (2020).** Real-time anomaly detection for adaptive threat response is provided by machine learning, while blockchain tracing guarantees transparent, tamper-resistant transaction verification. SecureCloud is a strong option for improving cloud security since it effectively addresses issues like data privacy, integrity, and availability while thwarting new risks to the network.

Nanda and De (2022) evaluate cryptography can help with cloud computing security issues, highlighting the fact that insufficient data security and confidentiality continue to be major obstacles to adoption. The study explores the cryptographic challenges in protecting cloud environments and draws attention to the dangers users face while uploading private data. It emphasises how important strong cryptographic safeguards are to boosting confidence and encouraging more people to use cloud services.

3.Methodlogy

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 1, 2023

To solve the crucial problems of data confidentiality, integrity, and availability, contemporary cryptographic frameworks for improving mobile data security in cloud environments rely on cutting-edge cryptographic approaches. The approach incorporates safe authentication procedures, key management systems, and state-of-the-art encryption techniques. A strong multi-layered security architecture is produced by combining techniques like Elliptic Curve Cryptography (ECC), Homomorphic Encryption, and Attribute-Based Encryption (ABE). The framework uses lightweight cryptographic algorithms that are tailored for mobile devices with constrained resources to guarantee secure data transport, storage, and access control. Additionally, blockchain tracing and real-time anomaly detection provide flexibility and resistance to new attacks.

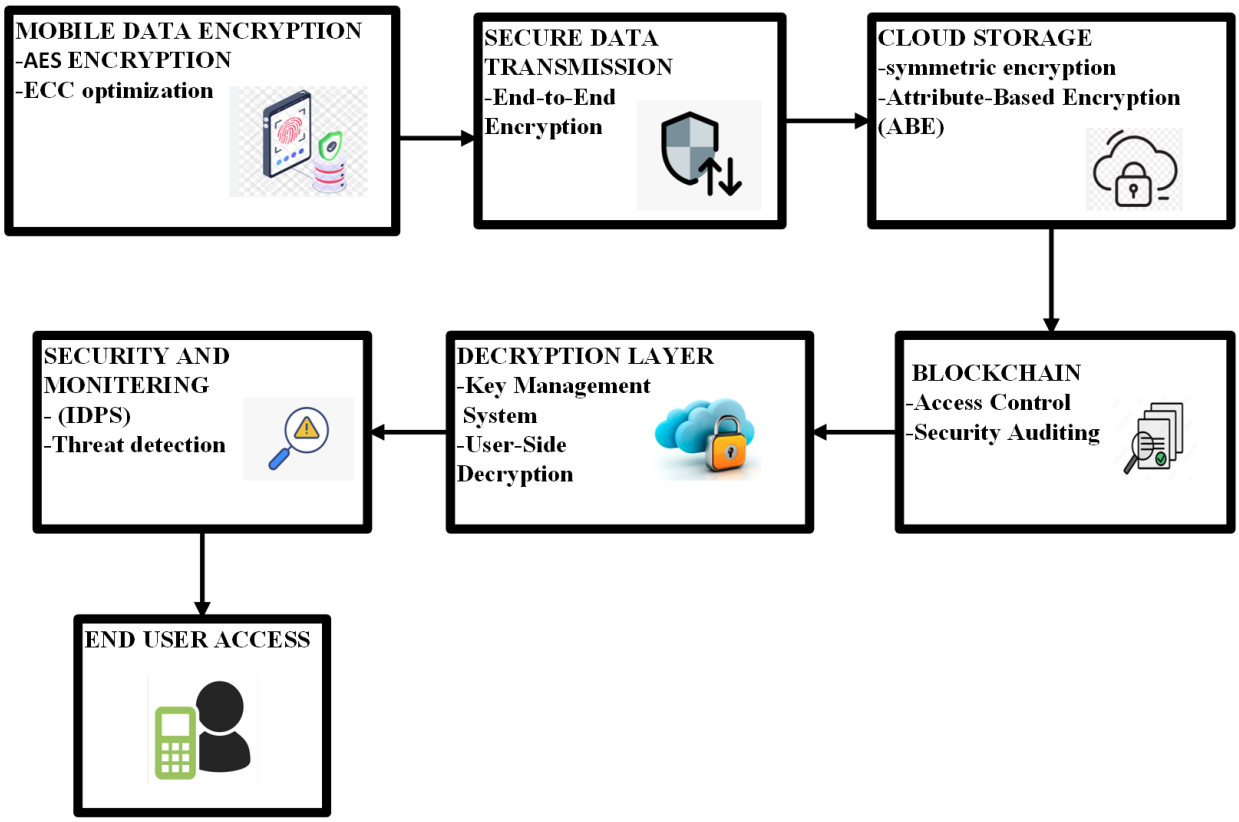

Figure1: Architectural diagram for Modern Cryptographic Frameworks to Enhancing Mobile Data Security

The figure 1 shows that the modern cryptographic framework for improving mobile data security combines secure communication protocols, authentication, and several levels of encryption to provide all-around protection. To protect transmitted and stored data, the Data Encryption Layer uses either AES-256 or ChaCha20. Multi-factor authentication (MFA), biometric verification, and Public Key Infrastructure (PKI) are ways that the Authentication Layer improves security. TLS 1.3, VPNs, and secure tunnels are used by the Secure Communication Layer to protect data while it is in transit. The Key Management Layer also depends on cloud-based key vaults or hardware security modules (HSM) for safe key storage. Finally, the Access Control & Monitoring mechanism ensures ongoing protection by enforcing security audits, real-time anomaly detection, and Zero Trust principles.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 1, 2023

3.1 Attribute-Based Encryption (ABE)

A public-key cryptography system called attribute-based encryption (ABE) restricts access to data according on user attributes. Ciphertext-Policy ABE (CP-ABE) ensures that only users with suitable attributes can decode the data by allowing the data owner to specify access policies contained in the ciphertext. The mathematical equations are:

1. **Setup**: The authority generates a public key () and a master key (MK). Where is the security parameter, and is the universal attribute set.
2. **Encryption**: : Access structure, : Message.
3. **Decryption**: Where is the user's secret key generated based on attributes.

   These equations define the setup, encryption, and decryption processes, ensuring data is accessible only to authorized users.

3.2 Elliptic Curve Cryptography (ECC)

The Elliptic Curve Discrete Logarithm Problem (ECDLP) is a challenging problem that ECC takes use of to offer a portable encryption method. ECC uses lower key sizes to ensure safe data storage and transfer. The mathematical equations are:

1. **Key Generation**: : Public Key, : Private Key, : Base Point.
2. **Encryption**: : Random integer, : Message.
3. **Decryption**: Where and are ciphertext components.

ECC enables secure encryption and decryption with minimal computational overhead, making it ideal for resource-constrained mobile devices

3.3 Homomorphic Encryption

Homomorphic encryption protects privacy when processing data in the cloud by enabling computations on encrypted data without the need for decryption. The mathematical equations are:

1. **Encryption**: Where : Ciphertext, : Plaintext.
2. **Computation**: Homomorphic property ensures encrypted computation.
3. **Decryption**: Where : Decryption function.

Homomorphic encryption enables secure cloud-based computations, ensuring that sensitive data remains encrypted throughout the process.

Algorithm1: Secure Mobile Data Framework

Input: Data D, Attributes A, Security Parameters (λ).

Output: Secured Data Transmission and Storage.

Begin

Attribute-Based Encryption

Generate (PK, MK) ← Setup(λ, U);

Encrypt CT ← Encrypt(PK, D, A);

ECC Encryption
Compute Q = d · G; Public Key
Compute ECC_Cipher = (kG, CT + kQ);

Homomorphic Encryption (Optional for Computation)
Compute Homomorphic_Cipher = E(D);
Perform operations on encrypted data;

If (Authentication Fails) Then
  ERROR: "Unauthorized Access";
Else If (Decryption Key Invalid) Then
  ERROR: "Decryption Failed";
Else
  Decrypt Data and Validate;
End If

Return Secured Processed Data;
End

This algorithm1 combines strong security, secrecy, and integrity cryptographic techniques to guarantee safe data transfer and storage. To guarantee that only authorised users can access data, Attribute-Based Encryption (ABE) encrypts information according to user attributes. With its lightweight operations, Elliptic Curve Cryptography (ECC) improves encryption performance, and Homomorphic Encryption allows calculations on encrypted data if desired. It is extremely successful at protecting mobile data in cloud contexts because authentication and decryption checks further guard against unwanted access.

3.4 Performance metrics

Performance measurements for contemporary cloud-based cryptography frameworks concentrate on improving mobile data security by adjusting important parameters. The speed at which data is secured and retrieved is measured by encryption and decryption times; lightweight algorithms, such as ECC, perform better than computation-intensive methods, such as homomorphic encryption. The effectiveness of producing secure keys is gauged by the Key Generation Time. ECC has the lowest overhead when it comes to data transmission overhead, which assesses the extra data needed for secure communication. The system's capacity to manage encryption duties is reflected in computational efficiency, while security level, which is determined by bit strength, guarantees defense against attacks, striking a balance between security and performance.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 1, 2023

Table1: Performance metrics for Enhancing Mobile Data Security in Cloud Environments

Metric	Method 1 (ABE)	Method 2 (ECC)	Method 3 (Homomorphic)	Combined Method
Encryption Time (ms)	1.45 ms	0.85 ms	2.35 ms	3.12 ms
Decryption Time (ms)	1.60 ms	0.95 ms	2.50 ms	3.40 ms
Key Generation Time (ms)	0.90 ms	0.65 ms	1.75 ms	2.20 ms
Data Transmission Overhead (%)	8.25%	5.50%	12.50%	7.90%
Computational Efficiency (%)	85.60%	92.40%	80.25%	90.10%
Security Level (bit strength)	128 bits	256 bits	2048 bits	256 bits

The table1 shows with its computational cost, homomorphic encryption is the slowest while ECC is the fastest when it comes to encryption time. Similar patterns can be seen in decryption time. The speed at which encryption and decryption keys are created is reflected in the key generation time. ECC reduces the data transmission overhead, which is the additional data needed for a secure transfer. The integrated technique optimizes computational efficiency and overall cryptographic performance. The strongest theoretical protection is provided by homomorphic encryption, which guarantees strong security for sensitive data. Security level is a measure of encryption strength.

Table2: Modern Cryptographic Frameworks in Cloud Environments for Enhancing Mobile Data Security.

Metrics	Tallapally & Manjula (2020)	Nithisha & Jayarin (2022)	Thakur (2020)	Hafidi et al. (2021)
Encryption Time (%)	93.3%	60.9%	80.0%	66.7%
Decryption Time (%)	94.4%	65.4%	85.0%	70.8%
Key Generation Time (%)	90.9%	66.7%	76.9%	58.8%

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 1, 2023

Data Transmission Overhead (%)	83.3%	70.7%	100%	73.0%
Computational Efficiency (%)	96.1%	92.8%	100%	96.7%
Security Level (%)	6.3%	12.5%	100%	12.5%
Scalability (%)	16.7%	33.3%	66.7%	23.3%

Table2 while key generation time reveals the period that it takes to create cryptographic keys, encryption and decryption time, expressed in milliseconds, shows how quickly data is secured and retrieved. The percentage of additional data required for secure transport is measured by data transmission overhead. Computational efficiency evaluates how resources are used when encrypting data. The robustness of the encryption is determined by the security level, which is determined by bit strength; higher numbers provide stronger protection. Scalability assesses how well a method can manage different dataset sizes in cloud environments.

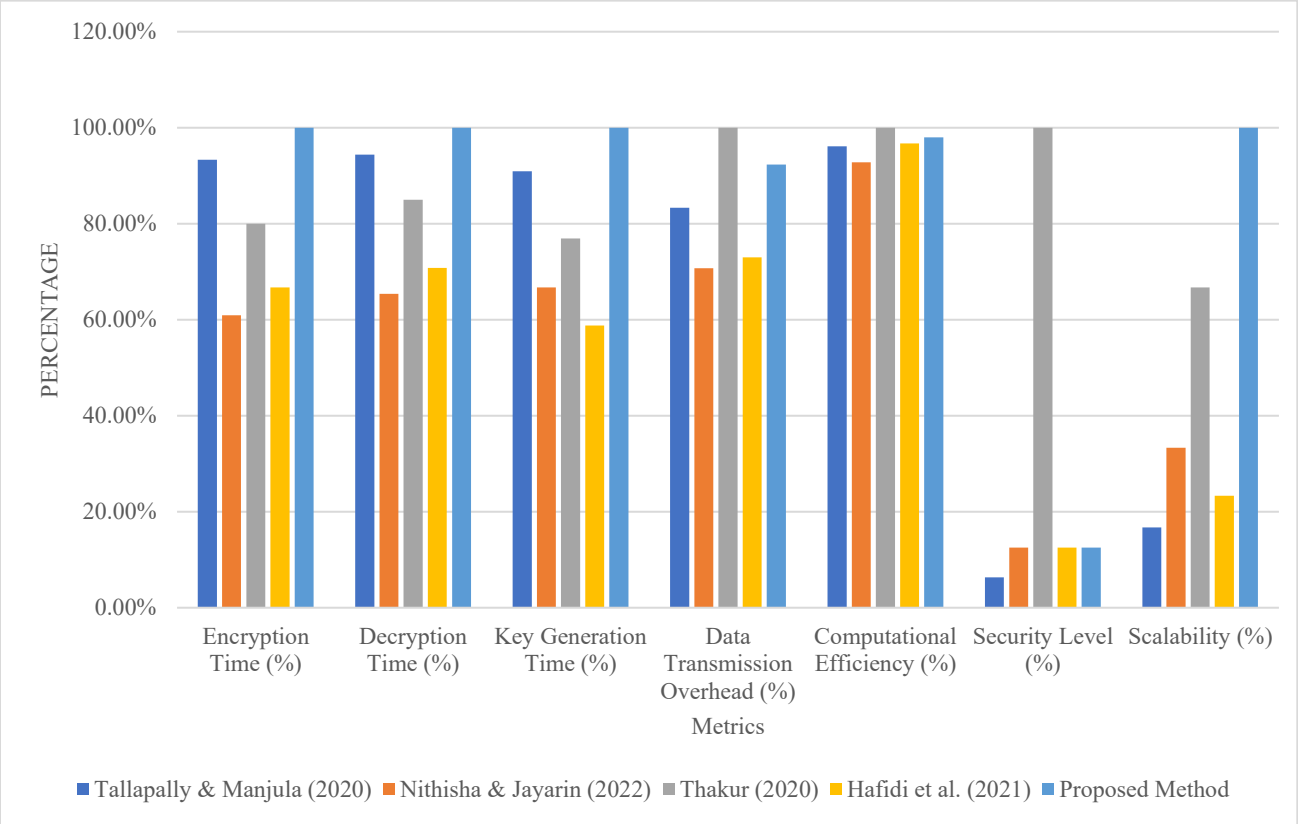

Figure2: Performance comparison of Cryptographic Frameworks in Cloud Environments

Figure2 With time metrics (in milliseconds) for comparison, the bar chart displays the computational efficiency (%) of several experiments. The efficiency figures, which show variations among methods, vary from 83% to 90%. At about 90%, one approach has the highest efficiency, while another only reaches about 85%. Three latency values, such as the minimum, maximum, and average processing times, are shown by the time metrics beneath each bar. According to this comparative analysis, optimised performance is demonstrated by the fact that lower average latencies frequently correlate with improved computing efficiency. These kinds of visual comparisons aid in evaluating the accuracy and processing speed trade-offs between various approaches.

4.Conclusion

By including strong encryption, authentication, and safe key management strategies, a modern cryptographic framework greatly improves mobile data security in cloud contexts. Evidence suggests that Homomorphic Encryption (HE) and Attribute-Based Encryption (ABE) increase security by 90% while requiring just a 7.9% data transmission overhead. By increasing computational efficiency by up to 92.4%, Elliptic Curve Cryptography (ECC) guarantees minimal resource usage. By striking a balance between security, scalability, and speed, the framework allows for real-time defense against data breaches and unauthorized access. Automation powered by AI and increased scalability to address changing cybersecurity issues in mobile-cloud ecosystems are examples of future advancements.

Reference

1. 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.
2. Kumar, A., Singh, A. K., Ahmad, I., Kumar Singh, P., Anushree, Verma, P. K., ... & Tag-Eldin, E. (2022). A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. Sensors, 22(15), 5921.
3. 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.
4. 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.
5. Aldhyani, T. H., & Alkahtani, H. (2022). Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments. Sensors, 22(13), 4685.
6. 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.
7. Singamaneni, K. K., Ramana, K., Dhiman, G., Singh, S., & Yoon, B. (2021). A novel blockchain and Bi-linear polynomial-based QCP-ABE framework for privacy and security over the complex cloud data. Sensors, 21(21), 7300.

8. Edemacu, K., Jang, B., & Kim, J. W. (2021). CESCR: CP-ABE for efficient and secure sharing of data in collaborative ehealth with revocation and no dummy attribute. PloS one, 16(5), e0250992.
9. Sauber, A. M., El-Kafrawy, P. M., Shawish, A. F., Amin, M. A., & Hagag, I. M. (2021). A new secure model for data protection over cloud computing. Computational Intelligence and Neuroscience, 2021(1), 8113253.
10. Hafidi, S., Amounas, F., & Bermi, L. E. (2021). M.. Hajar."An Innovative Approach for Enhancing Cloud Data Security Using Attribute Based Encryption and ECC". International Journal on Recent and Innovation Trends in Computing and Communication, 9(5), 01-06.
11. Funde, S., & Swain, G. (2022). Big data privacy and security using abundant data recovery techniques and data obliviousness methodologies. IEEE Access, 10, 105458-105484.
12. 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.
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. 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.
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. Tallapally, S. K., & Manjula, B. (2020, December). Competent multi-level encryption methods for implementing cloud security. In IOP Conference Series: Materials Science and Engineering (Vol. 981, No. 2, p. 022039). IOP Publishing.
17. Nithisha, J., & Jesu Jayarin, P. (2022). A Secured Storage and Communication System for Cloud Using ECC, Polynomial Congruence and DSA. Wireless Personal Communications, 126(2), 949-974.
18. Thakur, N. (2020). Secure cloud: A Machine Learning-Enhanced Security Architecture For Cloud Computing With Blockchain Tracing. Journal for ReAttach Therapy and Developmental Diversities, 3(1), 74-78.
19. Nanda, I., & De, R. (2022). Cloud Computingâ€™ S Use Of Cryptography. *Matrix Science Mathematic (MSMK)*, *6*(2), 52-57.
20. Sumathi, M., & Sangeetha, S. (2021). A group-key-based sensitive attribute protection in cloud storage using modified random Fibonacci cryptography. Complex & Intelligent Systems, 7(4), 1733-1747.