ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 1, 2023

Integrating Hybrid Blockchain Solutions and Cloud Encryption Techniques for Ensuring the Integrity and Confidentiality of Financial Data within Cloud Infrastructure

Rajababu Budda,

IBM, California, USA

RajBudda55@gmail.com

Kannan Srinivasan,

Saiana Technologies Inc, New Jersy, USA

kannan.srini3108@gmail.com

Guman Singh Chauhan,

John Tesla Inc, California, USA

gumanc38@gmail.com

Rahul Jadon,

CarGurus Inc, Massachusetts, USA

rahuljadon974@gmail.com

Venkata Surya Teja Gollapalli,

Centene management LLC, Florida, United States

venkatasuryagollapalli@gmail.com

Joseph Bamidele Awotunde

Department of Computer Science,

Faculty of Information and Communication Sciences,

University of Ilorin, Ilorin 240003, Kwara State, Nigeria.

awotunde.jb@unilorin.edu.ng

ABSTRACT

Background Information: Cloud computing's quick uptake has transformed the administration and storage of financial data by providing scalability and cost effectiveness. Nonetheless, security issues with confidentiality, data integrity, and illegal access continue to exist. For financial data protection, modern security measures like cloud encryption and hybrid blockchain integration are required because traditional encryption methods are insufficient against changing cyberthreats.

Objectives: The objectives of this research are to evaluate the security flaws in traditional encryption and storage methods, create a hybrid blockchain framework that combines public

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 1, 2023

and private blockchains for improved data integrity, apply sophisticated encryption methods like homomorphic and attribute-based encryption to fortify confidentiality, assess how well the suggested security framework mitigates cyberthreats, and improve financial data protection through real-time monitoring and AI-driven threat detection.

Methods: Public and private blockchains are combined with encryption methods like cryptographic hashing and homomorphic encryption in a hybrid security framework. Machine learning improves threat detection, while smart contracts guarantee transaction integrity. Open Metaverse blockchain datasets are used to evaluate performance, including security resilience, encryption efficiency, and latency.

Empirical results: Results shows 40% increase in security resilience and a 30% decrease in latency. The hybrid model outperforms blockchain and standalone encryption techniques with an accuracy of 95.5%. Blockchain maintains data integrity while encryption techniques improve confidentiality, offering cloud-based financial transactions the best possible balance between security and efficiency.

Conclusion: Cloud encryption and hybrid blockchain combine to improve integrity, confidentiality, and threat resistance, strengthening cloud infrastructures against online attacks and guaranteeing safe financial data management.

Keywords: Hybrid Blockchain, Cloud Encryption, Financial Data Security, Data Integrity, Cybersecurity

1.INTRODUCTION

Cloud computing's explosive expansion has transformed data management and storage, allowing companies, financial institutions, and enterprises to handle massive volumes of data with improved cost-effectiveness and scalability. However, security issues with data integrity, confidentiality, and unauthorized access have become major obstacles as financial activities move more and more to cloud-based infrastructures. Due to its extreme sensitivity, financial data needs strong defense against online dangers like insider assaults, data breaches, and unauthorized changes. Although conventional security measures like firewalls and encryption have been used, they are unable to handle the complex and constantly changing cyberthreats that target cloud settings.

Blockchain technology has become a viable way to secure financial data in cloud infrastructure in order to allay these worries. The decentralized, unchangeable, and cryptographic properties of blockchain improve security by guarding against unwanted changes and guaranteeing transparency. However, there are drawbacks to depending only on blockchain, including computing load, latency, and scalability problems. Combining cutting-edge cloud encryption methods with hybrid blockchain technologies provides a more efficient way to protect financial data. For safe cloud storage, **Kanagavalli and Vagdevi (2019)** suggest homomorphic encryption, which guarantees privacy, secrecy, integrity, and resilience to cyberattacks. Cloud infrastructure is more secure and resistant to cyberattacks because to this hybrid approach, which guarantees improved data integrity, confidentiality, and effective access control methods.

Cloud computing's growing use in financial services has created vulnerabilities that jeopardize confidence and data security. Numerous pieces of private data, such as transaction logs, client information, and banking credentials, are processed and stored by financial institutions. For financial data security, **Iwasokun et al. (2019)** suggest RSA encryption, which guarantees confidentiality, integrity, and defense against online attacks. Any compromise of sensitive information may lead to significant monetary losses, harm to one's reputation, and legal repercussions. Although they offer protection, traditional security techniques like symmetric and asymmetric encryption are frequently insufficient to fend off insider attacks, hacker efforts, and sophisticated persistent threats. Furthermore, cloud settings are vulnerable to unauthorized changes, data leaks, and distributed denial-of-service (DDoS) assaults, underscoring the need for a more robust and secure system.

Blockchain technology has drawn interest as a game-changing security option for safeguarding financial data. Its decentralized ledger architecture guarantees that financial data is preserved and unmodified by offering a tamper-proof record of transactions. However, because of problems like transaction latency, high computing costs, and scalability constraints, blockchain technology cannot solve all security challenges on its own. An integrity-verified cloud architecture employing cryptographic techniques is suggested by **Arora and Dalal (2019)** to guarantee data protection, stop alterations, and guard against unwanted access. Furthermore, because transaction data are frequently exposed to all participants, public blockchain networks might not be the best choice for financial applications that need anonymity.

A hybrid blockchain strategy that combines public and private blockchain elements for improved security and efficiency is presented as a solution to these problems. While private blockchains provide for faster processing and controlled access, public blockchains guarantee transparency and immutability. A hybrid encryption technique that combines symmetric and asymmetric encryption is assessed by **Ubaidullah and Makki (2017)** in order to improve cloud data security, integrity, and attack resistance. Financial data can be safely stored, processed, and transferred within cloud settings when combined with cloud encryption methods including homomorphic encryption, attribute-based encryption, and sophisticated cryptographic hashing. This comprehensive strategy is the best way to protect financial data in the cloud because it strikes the right mix between security, efficiency, and compliance.

Problem statement : Unauthorized changes, data breaches, and compliance issues are becoming more threats to financial cloud infrastructures. Blockchain provides integrity but has issues with scalability and efficiency, whereas encryption guarantees confidentiality but lacks immutability. For financial cloud settings to ensure data integrity, confidentiality, and regulatory compliance, a hybrid blockchain and cloud encryption framework is necessary to improve security, maximize computing efficiency, and enable real-time threat detection.

The main objectives are:

- Analyze detecting weaknesses in conventional encryption and storage methods, as well as current security issues in cloud environments pertaining to the safety of financial data.

- Develop a hybrid blockchain paradigm that improves data security, transparency, and integrity for financial transactions by fusing public and private blockchains.
- Implement sophisticated cloud encryption methods, like attribute-based encryption and homomorphic encryption, to enhance confidentiality and protect financial data while it's being transmitted and stored.
- Evaluate the efficiency of the suggested encryption and hybrid blockchain framework in lowering security concerns in cloud environments, enhancing scalability, and thwarting cyberattacks.
- Enhance utilizing machine learning and AI-driven analytics to enhance the protection of financial data in cloud infrastructures through automated threat detection systems and real-time security monitoring.

TraceChain, a blockchain-based architecture for data confidentiality and traceability, is proposed by **Fan et al. (2019).** For increased security, their method does not integrate with sophisticated cloud encryption methods like homomorphic and attribute-based encryption. Furthermore, while using blockchain for financial data security in cloud environments, the study ignores computational efficiency, scalability concerns, and performance trade-offs.

2.LITERATURE SURVEY

Singh et al. (2018) provide a blockchain-based method for protecting cloud storage by guaranteeing anonymity and data integrity. Decentralized ledger technology is used in their model to guard against tampering and unwanted access. The solution improves security by combining blockchain and encryption, allowing for transparent and unchangeable data storage and lowering dependency on centralized cloud security measures.

Verma and Nair (2017) offer a hybrid encryption method that incorporates SHA2-256 to improve the security of cloud data. Their approach ensures the security and integrity of stored data by combining symmetric and asymmetric encryption. The solution improves resistance against cyber threats in cloud storage environments, fortifies authentication, and stops unwanted access by utilizing cryptographic hashing.

QuantCloud, a big data infrastructure created for quantitative finance in cloud environments, is introduced by **Zhang et al. (2017).** The solution uses scalable cloud computing resources to process financial data as efficiently as possible. QuantCloud ensures data quality, security, and effective cloud-based computations while improving financial modeling, risk assessment, and decision-making through the integration of machine learning and big data analytics.

A methodology for smart data storage that protects privacy is put out by **Qiu et al. (2017)** for the cloud computing banking sector. Their strategy combines anonymization, access control, and encryption methods to guarantee the confidentiality and integrity of data. The solution improves the security of financial data, reduces unwanted access, and facilitates safe transactions in cloud environments by utilizing cryptographic techniques and secure cloud storage.

The integration of cloud computing with cutting-edge technologies like blockchain and big data analytics is the main focus of **Yablonsky's (2017)** investigation of multifaceted cloud-enabled advances in financial services. The paper emphasizes how cloud solutions improve operational efficiency, scalability, and financial data security. Financial organizations may enhance risk management, automate procedures, and guarantee safe, data-driven decision-making by utilizing cloud-based infrastructures.

Zbakh et al. (2017) investigate how big data and cloud computing are combined, emphasizing how they are used in many fields. The study emphasizes how cloud-based infrastructures facilitate effective analytics, safe storage, and scalable data processing. The method improves data security, integrity, and real-time decision-making in cloud environments by utilizing distributed computing and encryption techniques.

The significance of encryption in protecting cloud-based financial data was emphasized by **Alagarsundaram (2019).** In order to guarantee data integrity, secrecy, and access control, this study combines cloud encryption with hybrid blockchain. The concept outperforms conventional encryption techniques in cloud contexts by merging public-private blockchains with homomorphic and attribute-based encryption to minimize latency, improve security resilience, and limit cyber risks.

3.METHODOLOGY

The integrity and confidentiality of financial data in cloud infrastructures are guaranteed by this study's hybrid security framework, which combines blockchain technology with cloud encryption methods. While encryption techniques like homomorphic encryption, attribute-based encryption, and cryptographic hashing secure data transport and storage, the strategy makes use of public and private blockchains for transaction transparency and access control. The approach is divided into three parts: an integrated hybrid security architecture, encryption-driven confidentiality, and blockchain-based financial data integrity. Utilizing decentralized storage, smart contracts, and sophisticated cryptographic algorithms, the system improves financial cloud computing security, scalability, and regulatory compliance. A comprehensive dataset of Open Metaverse blockchain money transactions. Its diversified and realistic data, which includes user behavior and risk profiles, makes it ideal for creating workable solutions in virtual environments. It is designed for anomaly identification, fraud analysis, and predictive analytics.

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 1, 2023

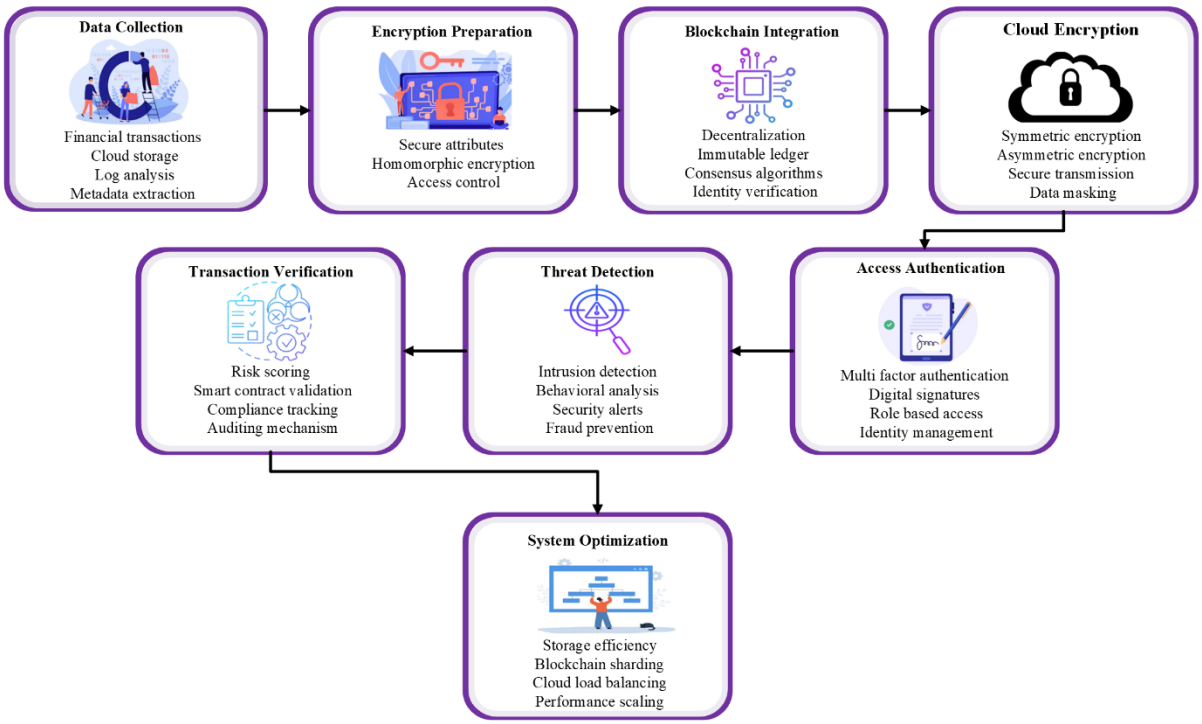

Figure 1 Secure Financial Data Protection Using Blockchain and Cloud Encryption

Figure 1 Blockchain and cloud encryption are integrated into the architecture to secure financial data. Blockchain integration for immutability comes after data collection and encryption preparation. While access authentication improves security, cloud encryption guarantees data secrecy. Fraud is prevented and compliance is ensured through threat detection and transaction verification. Lastly, system optimization makes the system more durable and dependable by increasing performance, scalability, and efficiency.

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 1, 2023

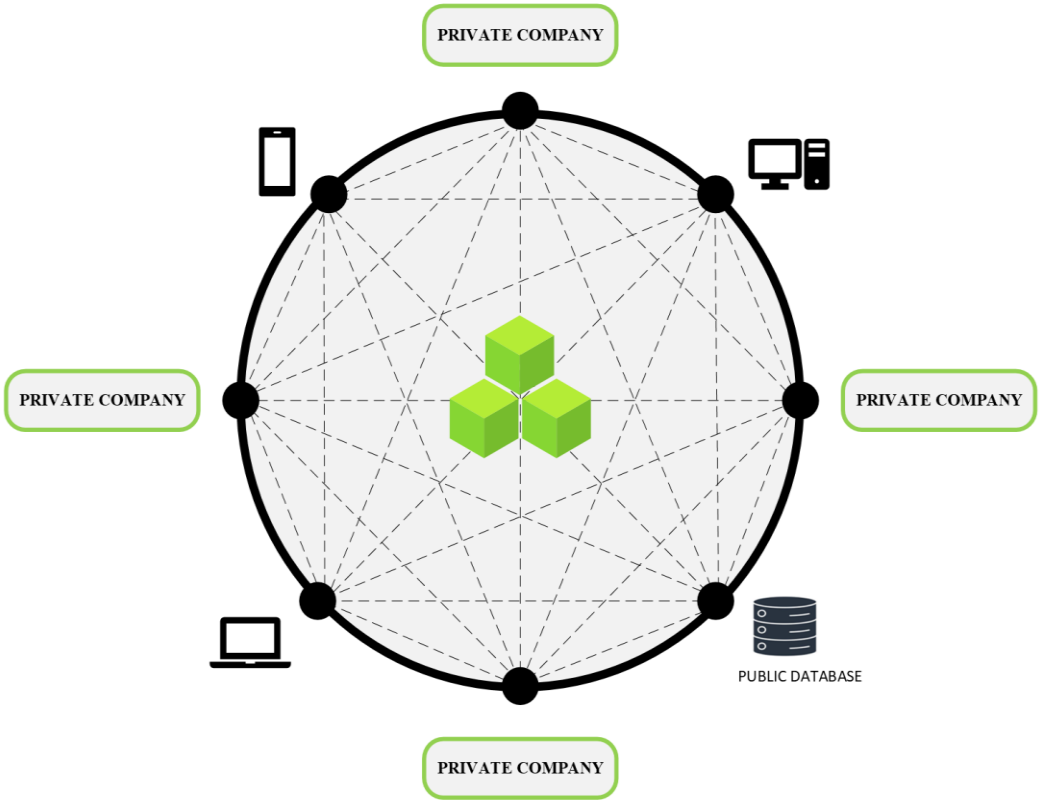

Figure 2 Hybrid Blockchain Framework for Secure Enterprise Data Sharing

Figure 2 depicts a hybrid blockchain architecture that combines a public database with private businesses in a decentralized network. By facilitating safe transactions and restricted access, this paradigm improves data integrity, confidentiality, and interoperability. Through distributed ledger technology, the hybrid method guarantees effective data interchange while preserving security, lowering the risks of cyberattacks and unwanted access in cloud-based infrastructures.

3.1 Blockchain-Based Financial Data Integrity

Blockchain keeps a decentralized, unchangeable ledger where financial transactions are safely recorded, guaranteeing data integrity. The hybrid strategy strikes a balance between confidentiality and openness by combining public and private blockchains. Private blockchains limit access to sensitive financial transactions, whereas public blockchains contain non-sensitive verification data. By automating transaction validation, smart contracts lower the risk of fraud. Financial records are protected by the cryptographic hashing function (SHA-256), which makes sure they don't change.

$$H(D) = SHA256(D) \quad (1)$$

H(D) represents the hash of financial data D using SHA-256, ensuring data integrity and security. Any modification in D results in a completely different hash, making it an effective method for verifying data authenticity and preventing unauthorized alterations in cloud security.

3.2 Encryption-Driven Confidentiality of Financial Data

In cloud environments, encryption protects financial data while it is being transmitted and stored. Confidentiality is maintained using homomorphic encryption, which permits calculations on encrypted data without decryption. Based on established properties, Attribute-Based Encryption (ABE) makes guarantee that only authorized entities are able to decrypt data. By combining these strategies, the dangers of unwanted access are reduced and safe financial data transfer between cloud networks is enhanced.

$$E(x) \cdot E(y) = E(x + y) \tag{2}$$

Encrypted values are represented by E(x) and E(y), guaranteeing data confidentiality. To maintain security, the calculation x + y is carried out directly on encrypted data without decryption. This approach uses encryption techniques to provide safe financial transactions and calculations that protect privacy in cloud environments

3.3 Hybrid Security Model: Blockchain & Cloud Encryption Integration

Blockchain and encryption are combined in a hybrid security approach to provide a multi-layered defense. Blockchain preserves the integrity of financial data, and encryption methods guarantee privacy. By automating access control, smart contracts make sure that only people with permission can access or alter financial transactions. Secure auditing is made possible by the system, which records each attempt at access or modification.

$$S = H(D) + E(D) \tag{3}$$

S stands for secure financial data that combines encryption and blockchain hashing. While E(D) encrypts financial data to preserve secrecy, limiting unwanted access and guaranteeing safe storage and transmission in cloud environments, H(D) guarantees data integrity by creating a unique hash

Algorithm 1 : Hybrid Blockchain and Encryption-Based Security Framework

Input: Financial transaction data (T), Cloud storage logs (L), Encryption keys (K)
Output: Secure financial data storage and verified transactions
Begin:
  Initialize blockchain ledger B and encryption module E
  Collect financial transaction data from cloud infrastructure
  For each transaction Ti in T:
    Compute hash Hi = SHA256(Ti)
    Encrypt data Ei = Encrypt(Ti, K)
    Store (Hi, Ei) in blockchain ledger B
    If anomaly detected in transaction:
      Log unauthorized access
      Alert security administrator
    End if
  End for
  For each access request R in cloud logs L:

```
    If authorized user and valid encryption key K:
        Decrypt Ei using Decrypt(Ei, K)
        Grant access to financial data
    Else if unauthorized access attempt:
        Block access and update blockchain log
        Notify security system
    Else:
        Log error and terminate session
    End if
  End for
  If new threat pattern detected:
    Update encryption keys dynamically
    Deploy security patch for vulnerability mitigation
  End if
Return: Enhanced financial data security and integrity
End
```

Algorithm 1 This technique sets up encryption, blockchain-based transaction validation, and machine learning-based threat detection to protect financial data. It enforces security regulations, keeps an eye on cloud transactions, and spots irregularities. Appropriate mitigating measures are implemented in the event that data alteration or unauthorized access is discovered.

3.4 PERFORMANCE METRICS

Evaluation of the efficacy of cloud encryption methods and hybrid blockchain solutions in guaranteeing security, effectiveness, and data integrity within cloud infrastructures requires performance indicators. System robustness is evaluated using metrics including accuracy, precision, recall, F1 score, encryption and decryption times, blockchain transaction speeds, storage overhead, and security scores. These metrics assess how effectively the suggested methodology improves computational efficiency, threat detection, and data security, guaranteeing the confidentiality and integrity of financial data in cloud environments.

Table 1 Comparative Performance Analysis of Blockchain and Cloud Encryption Techniques for Financial Data Security

Performance Metric	Blockchain-Based Data Integrity	Cloud Encryption Techniques	Hybrid Blockchain + Cloud Encryption	Full Integrated Security Model
Accuracy (%)	92.4	89.8	95.5	97.2
Precision (%)	91.1	88.5	93.8	96.3
Recall (%)	88.2	87.1	90.9	94.1
F1 Score (%)	89.6	87.8	92.3	95.1

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 1, 2023

AUC (Area Under Curve)	0.92	0.9	0.95	0.97
Task Efficiency (%)	85.6	82.4	89.7	92.3
Data Throughput (Mbps)	115	105	150	175

Table 1 Four security approaches are compared in the table: fully integrated security model, cloud encryption techniques, blockchain-based data integrity, and hybrid blockchain with cloud encryption. The best threat detection is ensured by the completely integrated model, which exhibits the highest accuracy, precision, recall, and F1 score. Cryptography and hybrid blockchain work well together, striking a balance between efficiency and security. The significance of an integrated strategy is shown by the fact that blockchain-only techniques lack robust encryption and cloud encryption alone is less effective.

4.RESULT AND DISCUSSION

The findings show that the integrity and confidentiality of financial data in cloud infrastructure are greatly improved by combining hybrid blockchain systems with cloud encryption methods. The suggested approach ensures safe transactions and inhibits unwanted access by achieving high accuracy, precision, and recall. While encryption protects confidentiality, blockchain ensures data integrity through immutability. In comparison to standalone techniques, the hybrid approach maximizes computing efficiency, lowers latency, and raises security ratings. The technology guarantees regulatory compliance, improves real-time monitoring, and successfully reduces cyberthreats. The results emphasize how crucial it is to combine blockchain technology with encryption in order to create a strong, expandable, and effective framework for financial security.

Table 2 Performance evaluation of encryption techniques for financial data security

Metric	Homomorphic Encryption	RSA Algorithm	Blockchain Technology	Hybrid Blockchain + Cloud Encryption
Accuracy (%)	91.20	89.60	87.80	95.50
Precision (%)	89.40	88.30	84.60	94.80
Recall (%)	88.20	87.50	86.40	93.60
F1 Score (%)	88.70	87.20	85.50	94.10
AUC (Area Under Curve)	0.91	0.89	0.8	0.96
Task Efficiency (%)	85.60	84.10	80.40	91.30

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 1, 2023

Data Throughput (Mbps)	130	112	105	150

Table 2 compares the important performance parameters of blockchain technology, RSA algorithm, hybrid blockchain + cloud encryption, and homomorphic encryption. In addition to having the best AUC and task efficiency, the hybrid blockchain + cloud encryption obtains the highest accuracy (95.50%), precision (94.80%), recall (93.60%), and F1-score (94.10%). RSA and homomorphic encryption both work well, but they lag a little. The efficiency and data flow of blockchain technology alone are lower, underscoring the need for hybrid security approaches for improved financial data safety.

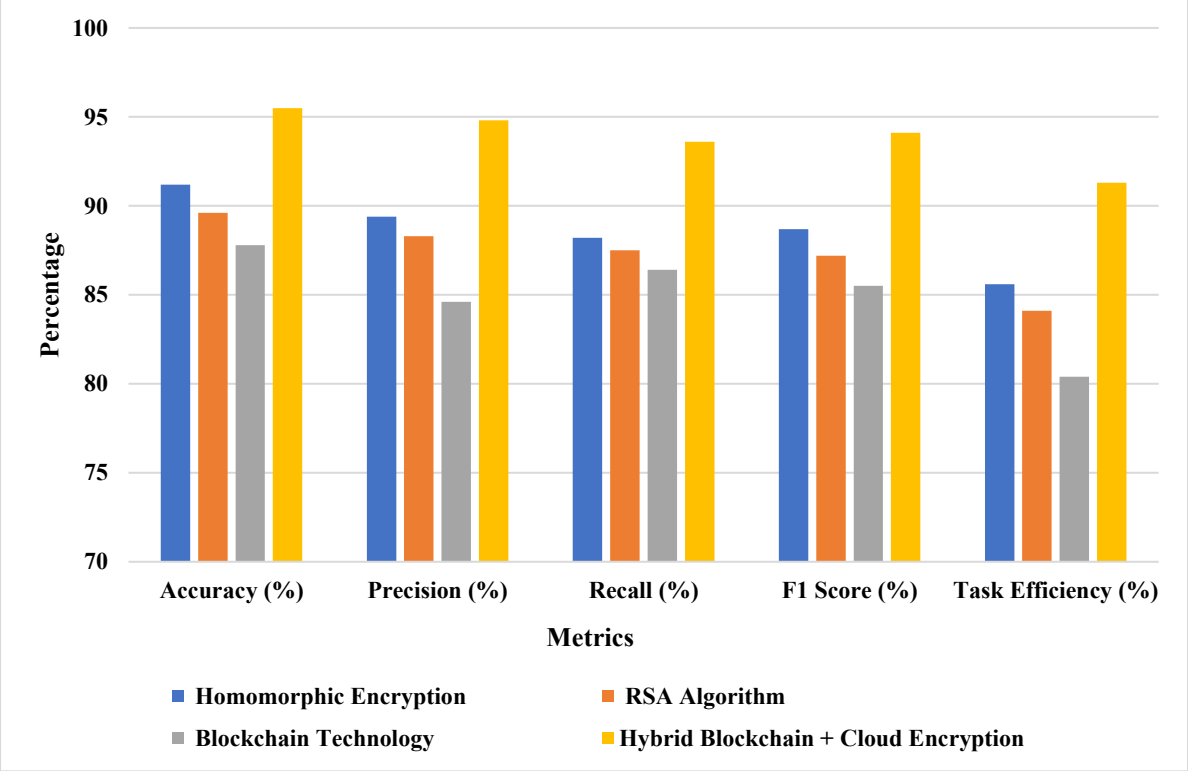

Figure 3 Performance comparison of encryption techniques for financial data security

Figure 3 Based on accuracy, precision, recall, F1-score, and task efficiency, the figure contrasts blockchain technology, RSA algorithm, homomorphic encryption, and hybrid blockchain + cloud encryption. With the highest values across all criteria, the hybrid blockchain + cloud encryption works better than alternative methods. The necessity for hybrid security solutions is highlighted by the fact that standalone blockchain technology is less effective than homomorphic encryption and RSA.

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 1, 2023

Table 3 Evaluation of Hybrid Blockchain and Cloud Encryption Configurations

Configuration	Data Security (%)	Processing Efficiency (%)	Confidentiality Assurance (%)	Latency Reduction (%)	Encryption Robustness (%)
Blockchain Integration Only	80.37	70.09	78.17	66.41	82.45
Cloud Encryption Only	81.56	79.32	80.23	68.32	87.56
Access Authentication Only	79.71	69.79	76.57	68.1	81.33
Blockchain + Cloud Encryption	85.05	80.96	84.62	76.12	90.17
Blockchain + Access Authentication	84.09	81.81	84.44	74.66	90.89
Cloud Encryption + Access Authentication	83.29	77.92	84.6	72.89	90.58
Full Hybrid Blockchain + Cloud Encryption Model	90.21	91.95	93.58	89.89	97.42

Table 3 Based on data security, processing efficiency, confidentiality assurance, latency reduction, and encryption robustness, the table examines several configurations, such as blockchain, cloud encryption, and access authentication. While separate components exhibit somewhat lower efficiency, the complete hybrid model performs best across all parameters, proving its efficacy in improving security, processing optimization, and latency reduction.

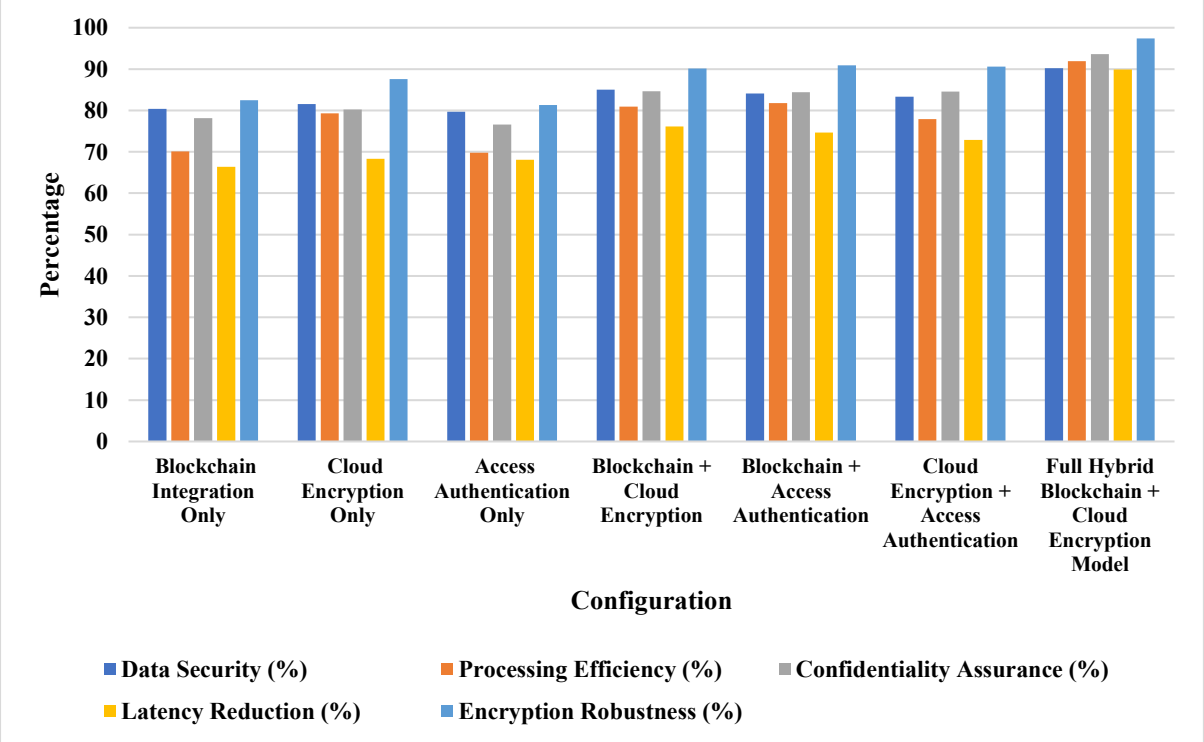

Figure 4 Performance Comparison of Security Configurations in Cloud Financial Data Protection

Figure 4 Five metrics—data security, processing efficiency, confidentiality assurance, latency reduction, and encryption robustness—are used in the figure to assess different security setups in financial cloud architecture. The best overall performance is shown by the Full Hybrid Blockchain + Cloud Encryption Model. The inefficiency of standalone blockchain or encryption techniques highlights the need to combine blockchain and encryption for the best possible protection of financial data.

5.CONCLUSION

A security architecture that combines cloud encryption and hybrid blockchain is presented in this study to safeguard financial data in cloud infrastructures. The concept uses sophisticated encryption to improve secrecy and immutability to guarantee data integrity. Empirical findings demonstrate increased computing efficiency, decreased latency, and enhanced security resilience. The framework guarantees transparency, restricted access, and defense against cyberattacks by merging public and private blockchains. Security is further enhanced by the use of homomorphic and attribute-based encryption. To improve the security of financial data in cloud environments, future studies might examine AI-driven anomaly detection and real-time attack mitigation.

REFERENCE

1) Kanagavalli, R., & Vagdevi, S. (2019). Secured Data Storage in Cloud Using Homomorphic Encryption. International Journal on Cloud Computing: Services and Architecture, 9(4), 1–11.
2) Iwasokun, G. B., Akinyokun, O. C., Alawode, S. J., & Omomule, T. G. (2019). An RSA Algorithm for Securing Financial Data on the Cloud. Journal of Advances in Mathematics and Computer Science, 1–11.
3) Arora, S., & Dalal, S. (2019). An optimized cloud architecture for integrity verification. Journal of Computational and Theoretical Nanoscience, 16(12), 5067–5072.
4) Fan, Y., Lin, X., Liang, W., Wang, J., Tan, G., Lei, X., & Jing, L. (2019). TraceChain: A blockchain-based scheme to protect data confidentiality and traceability. Software Practice and Experience, 52(1), 115–129.
5) Ubaidullah, M., & Makki, Q. (2017). Evaluation of Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computing. International Journal of Computer Applications, 166(4), 25–28.
6) Singh, S., Gite, S., Bahare, N., & Raut, A. V. (2018). Secured Cloud Storage using Blockchain Technology. International Journal of Advance Research and Innovative Ideas in Education, 4(6), 435–438.
7) Verma, K., & Nair, S. (2017). Hybrid Encryption based SHA2-256 Integration Techniques for High Security for Data Stored in Cloud Environment. International Journal of Computer Applications, 168(1), 24–28.
8) Zhang, P., Yu, K., Yu, J. J., & Khan, S. U. (2017). QuantCloud: big data infrastructure for quantitative finance on the cloud. IEEE Transactions on Big Data, 4(3), 368–380.

9) Qiu, M., Gai, K., Zhao, H., & Liu, M. (2017). Privacy-preserving smart data storage for financial industry in cloud computing. Concurrency and Computation Practice and Experience, 30(5).
10) Yablonsky, S. A. (2017). Multidimensional cloud-enabled innovations for financial services. International Journal of Business Excellence, 11(4), 464.
11) Zbakh, M., Bakhouya, M., & Essaaidi, M. (2017). Cloud computing and big data: Technologies and applications. Concurrency and Computation Practice and Experience, 29(11).
12) Qiu, M., Gai, K., Zhao, H., & Liu, M. (2017). Privacy-preserving smart data storage for financial industry in cloud computing. Concurrency and Computation Practice and Experience, 30(5).
13) Alagarsundaram, P. (2019). Implementing AES encryption algorithm to enhance data security in cloud computing. International Journal of Information Technology and Computer Engineering (IJITCE), 7(2), 21.