Securing Cloud Infrastructure In Banking Using Encryption-Driven Strategies For Data Protection And Compliance

[1]Nagendra Kumar Musham
Celer Systems Inc,California,USA
nagendramusham9@gmail.com
[2]R. Pushpakumar
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Associate Professor
chennai,india
pushpakumarvelr@gmail.com

ABSTRACT
In modern banking, securing sensitive financial data while maintaining scalability and compliance is a critical challenge. This paper proposes a secure and scalable cloud-based banking data processing framework that ensures data integrity, regulatory compliance, and operational efficiency. The framework incorporates multi-source data collection from core banking systems, mobile and internet banking, CRM systems, ATMs, and third-party APIs. Collected data undergoes pre-processing, including data cleaning, standardization, and anonymization, ensuring consistency and privacy compliance. Triple DES (3DES) encryption is applied before storage, securing data against unauthorized access. Performance evaluations indicate linear encryption complexity, with encryption time reaching 18 seconds for 1000 files, while response time exhibits exponential growth, peaking at 8000 ms for 9 files, signalling potential performance bottlenecks. Future enhancements include AES-256 encryption for faster processing, AI-based fraud detection, and multi-cloud deployment for improved redundancy and cost efficiency. This framework provides a robust, scalable, and secure solution for modern banking institutions, ensuring optimal data protection and cloud resource utilization.

Keywords: *Cloud Security, Banking Data Processing, 3DES Encryption, Regulatory Compliance, Scalable Cloud Infrastructure.*

1. INTRODUCTION

With the rapid digitalization of the banking sector, securing sensitive financial data while ensuring scalability and compliance has become a significant challenge [1]. Cloud-based banking solutions offer improved efficiency, flexibility, and cost-effectiveness but introduce concerns related to data security, unauthorized access, and regulatory compliance [2]. Traditional on-premises banking systems often struggle with scalability and security vulnerabilities, necessitating a secure, scalable, and compliant cloud-based framework [3]. The proposed framework aims to integrate multi-source data collection, encryption, access control, and cloud storage to safeguard banking data against cyber threats. By incorporating advanced encryption mechanisms and strict access policies, it ensures the protection of sensitive data while enabling efficient processing [4]. The framework also addresses regulatory requirements such as GDPR, PCI-DSS, and ISO 27001, making it suitable for modern

financial institutions [5]. Additionally, optimized performance metrics improve storage efficiency, encryption processing speed, and data retrieval time, ensuring seamless banking operations [6].

Several existing methods have been proposed to secure banking data, including Role-Based Access Control (RBAC), Attribute-Based Encryption (ABE), Homomorphic Encryption (HE), and Blockchain-based Security Models [7]. While RBAC improves access control, it lacks scalability in dynamic cloud environments. ABE provides encryption flexibility but has high computational overhead, impacting system performance [8]. Enables secure computations on encrypted data but suffers from high latency, making it impractical for banking operations [9]. Security enhances transparency but introduces storage and processing overhead, limiting its feasibility for large-scale banking applications [10]. These methods, although effective in specific scenarios, fail to provide an integrated, scalable, and optimized security framework for modern cloud banking infrastructure.

The proposed cloud-based banking data processing framework overcomes these drawbacks by integrating 3DES encryption, RBAC with least privilege enforcement, and efficient cloud storage strategies. Unlike ABE and HE, 3DES ensures a balance between security and computational efficiency, making it suitable for high-volume banking transactions. RBAC is enhanced with audit logging and access monitoring, mitigating unauthorized access risks. Additionally, cloud storage solutions such as object storage, databases, and data lakes improve scalability, ensuring seamless handling of structured and unstructured financial data. The novelty of this study lies in its comprehensive approach to security, combining encryption, access control, and cloud resource optimization to enhance data protection, operational efficiency, and compliance with financial regulations.

2. LITERATURE REVIEW

Bose, R., et al (2013) [11] examines the importance of security and trust in cloud computing, drawing parallels with the banking sector, where both are crucial for user confidence. Organizations remain sceptical about cloud adoption due to privacy and security concerns, necessitating trust-building efforts from cloud providers similar to banks. Trust in cloud services develops gradually based on providers' security and performance reputation. For broader adoption, customers must feel as secure storing their data in the cloud as they do with banks. The study offers recommendations across technological, regulatory, and behavioural aspects to enhance security and trust in cloud environments.

Ryoo, J., et al (2013) [12] highlights the unique challenges of cloud security auditing compared to traditional IT auditing, emphasizing the need for tailored approaches to meet legal and organizational standards. While IT auditors focus on compliance and data protection, cloud auditing requires customization due to its distinct security risks. The study examines sector-specific challenges in banking, healthcare, and government while presenting emerging cloud-specific security auditing methods. It underscores the importance of adapting auditing techniques to ensure effective security assessment in cloud environments.

Asadi, S., et al (2017) [13] explores the factors influencing cloud computing adoption in the banking sector from the customers' perspective, addressing a gap in prior research that focused mainly on organizations. Using a model based on the Technology Acceptance Model (TAM) and diffusion theory, it identifies trust, cost, and security and privacy as key factors shaping user behaviour. Data analysis using partial least squares (PLS) confirms that these factors significantly affect perceived ease of use, usefulness, and adoption intention. The findings emphasize the need to enhance trust and security to encourage cloud adoption in banking.

Hamidi, N. A., et al (2013) [14] presents a model for implementing personalized security in e-banking using Flask architecture within a cloud environment, emphasizing the necessity of mandatory access controls. It highlights the effectiveness of role-based access control (RBAC) in securing e-payment systems through user-defined policies for different entities. The research demonstrates how cloud infrastructure enhances security implementation, particularly for large organizations like banks. By enforcing strict access controls, the proposed model ensures a clear separation between security policies and enforcement, improving overall security in e-banking.

Nosrati, L., et al (2016) [15] reviews mobile banking security by identifying and classifying key security challenges associated with mobile banking payments. It discusses various security risks, encryption methods, and the financial losses caused by bank account hacking, emphasizing the need for robust security measures. The research introduces a two-layer security approach that enhances network layer security through encryption techniques and message format authorization using checksums. By implementing these methods, the study aims to strengthen mobile banking security and protect customer data from cyber threats.

Mbelli, T. M., & Dwolatzky, B. (2016) [16] examines the growing cyber security threats facing cyber banking in South Africa, emphasizing the increasing prevalence of financial system attacks. It highlights the importance of risk management and continuous investment in security measures to mitigate financial and data losses. The study discusses various cyber threats and their economic impact on financial institutions while proposing a comprehensive security framework. This framework incorporates boundary and application security strategies to enhance protection against vulnerabilities and strengthen cyber banking defences.

2.1. PROBLEM STATEMENT

Existing challenges in securing cloud-based banking data include data privacy concerns, as sensitive financial information is vulnerable to breaches without robust encryption. Compliance with regulatory standards such as PCI-DSS and GDPR remains complex due to evolving legal requirements [17]. Latency in encryption and decryption processes affects system performance, leading to delays in transaction processing [18]. Lack of standardized security auditing frameworks creates inconsistencies in monitoring and risk assessment across different cloud providers [19]. Additionally, trust issues in third-party cloud services hinder adoption, as banks fear unauthorized access, data leaks, and vendor lock-in risks [20].

3. PROPOSED METHODOLOGY

Secure, scalable cloud-based banking data processing workflow that ensures data integrity, compliance, and efficiency is illustrated in figure 1. It begins with data collection from multiple banking sources, including core banking systems, mobile & internet banking, and CRM data. The collected data undergoes pre-processing, where data cleaning eliminates inconsistencies, and anonymization ensures regulatory compliance (GDPR, PCI-DSS). To enhance security, Triple DES (3DES) encryption is applied before data is transferred to cloud storage, ensuring protection against unauthorized access. The cloud infrastructure (AWS, Azure, or Google Cloud) incorporates role-based access control (RBAC), audit logging, and encryption at rest, securing sensitive financial information. Additionally, performance metrics continuously evaluate storage efficiency, encryption performance, and data retrieval speed, ensuring optimized cloud resource utilization. By integrating robust security measures and scalable cloud solutions, this workflow enhances data protection, operational efficiency, and regulatory compliance, making it an ideal model for modern cloud banking infrastructures.

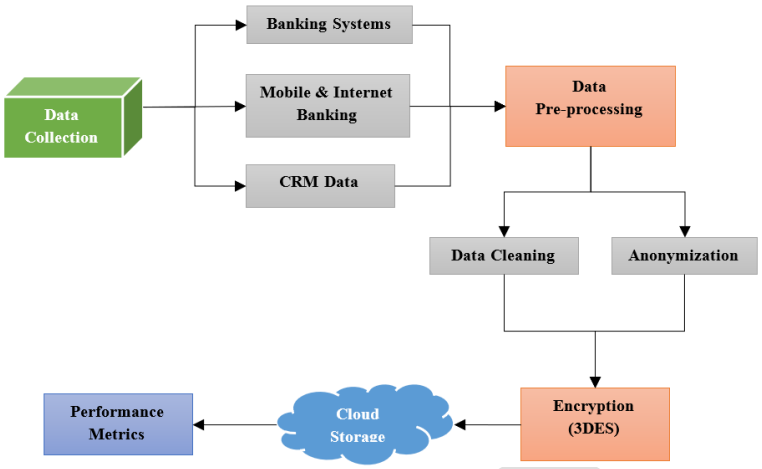

Figure 1: Secure and Scalable Cloud-Based Banking Data Processing

3.1 Data Collection

The data collection phase in the proposed framework gathers information from multiple banking sources to ensure a comprehensive and secure financial data processing system. It includes data from core banking systems, which manage transactions, accounts, and loan records, ensuring financial tracking. Additionally, mobile and internet banking applications contribute customer interactions, transaction logs, and authentication details. Customer Relationship Management (CRM) systems provide valuable insights into customer preferences, complaints, and personalized banking services. ATMs and POS (Point of Sale) systems generate real-time transaction data essential for fraud detection and financial monitoring. Third-party APIs, such as credit bureaus, payment gateways, and regulatory bodies, supply external data for risk analysis, KYC (Know Your Customer) verification, and compliance tracking. The collected data is retrieved using batch processing for scheduled reports, real-time streaming for instant transaction updates, and ETL (Extract, Transform, Load) methods for structured analytics. This diverse and multi-source data collection approach ensures the banking system remains scalable, secure, and regulatory-compliant while leveraging cloud infrastructure for efficient processing.

3.2 Data Pre-processing

Data pre-processing is essential to clean, standardize, and secure collected data before encryption and cloud storage. The steps involved are:

1. **Data Cleaning**

Removes duplicate, inconsistent, and missing values to improve data quality. Formula for missing value imputation (Mean Method) is given in equation (1).

$$X_{\text{new}} = \frac{\sum_{i=1}^{n} X_i}{n} \tag{1}$$

where X_{new} is the new value, X_i represents known values, and n is the total number of valid value.

2. **Data Standardization**

Converts data into a uniform format for consistency across different sources. Z-score Normalization Formula is given in equation (2).

$$Z = \frac{X-\mu}{\sigma} \tag{2}$$

where X is the original value, μ is the mean, and σ is the standard deviation.

3. **Anonymization**

Protects personally identifiable information (PII) by replacing sensitive data with pseudonyms. Formula for Data Masking (Hashing using SHA-256) is given in equation (3).

$$H(X) = \text{SHA} - 256(X) \tag{3}$$

where X is the original sensitive data, and $H(X)$ is the hashed value.

3.3 Encryption Using 3DES

Triple Data Encryption Standard (3DES) is a symmetric encryption algorithm used for securing sensitive banking data. It encrypts plaintext three times using the Data Encryption Standard (DES) algorithm, providing enhanced security compared to single DES. The process uses three 56-bit keys (K1, K2, K3), making the total key length 168 bits. The encryption process follows three steps:

1. First Encryption: The plaintext P is encrypted using key $K1$ is given in equation (4).
$$C1 = E_{K1}(P) \tag{4}$$
2. Decryption with Second Key: The output $C1$ is decrypted using key $K2$ is given in equation (5).
$$C2 = D_{K2}(C1) \tag{5}$$
3. Final Encryption: The intermediate output $C2$ is encrypted again using key $K3$ is given in equation (6).
$$C = E_{K3}(C2) \tag{6}$$

Here, E_K represents DES encryption, and D_K represents DES decryption. The final ciphertext C is securely stored or transmitted.

For decryption, the reverse process is applied:

1. Decrypt using $K3$: $P2 = D_{K3}(C)$
2. Encrypt using $K2$: $P1 = E_{K2}(P2)$
3. Decrypt using $K1$: $P = D_{K1}(P1)$

3.4. Cloud Storage

The proposed framework ensures secure and scalable cloud storage by systematically managing banking data from collection to encryption and storage. Data from various banking sources undergoes pre-processing, including cleaning, anonymization, and encryption using 3DES, before being transmitted to the cloud. The encrypted data is stored in cloud-based storage solutions such as object storage, databases, and data lakes to support structured and unstructured data. The system implements role-based access control (RBAC) to ensure that only authorized users can access specific datasets, enforcing least privilege access policies.

To maintain data security and regulatory compliance, the cloud storage mechanism integrates 3DES encryption at both rest and transit, ensuring protection against unauthorized access. Encryption is applied during transmission to secure communication channels. Additionally, key management services (KMS), such as AWS KMS or Azure Key Vault, are employed for secure cryptographic key storage and management. These security measures ensure compliance with PCI-DSS, GDPR, and ISO 27001 standards, providing a robust security framework for financial data.

4. RESULT

The results section evaluates the efficiency and security of the proposed cloud-based banking framework. It analyzes encryption time, response time, and storage performance, demonstrating that encryption follows a linear complexity while response time shows exponential growth, indicating potential bottlenecks. The findings

highlight the system's scalability, security, and compliance, ensuring optimized cloud resource utilization for secure banking operations.

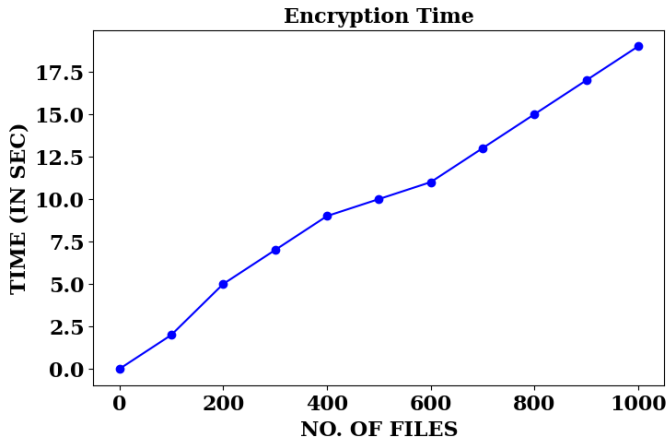

Figure 2: Performance Analysis of Encryption Time for Banking Data

Figure 2 represents the relationship between the number of files and the time taken for encryption (in seconds). The x-axis denotes the number of files (ranging from 0 to 1000), while the y-axis indicates the encryption time (in seconds), increasing up to approximately 18 seconds. The plotted line, with blue data points, shows a clear upward trend, suggesting that as the number of files increases, the encryption time also increases. This indicates that the encryption process follows a linear or near-linear time complexity, where processing more files requires proportionally more time. The smooth curve further suggests consistent encryption efficiency without sudden spikes, indicating an optimized encryption mechanism.

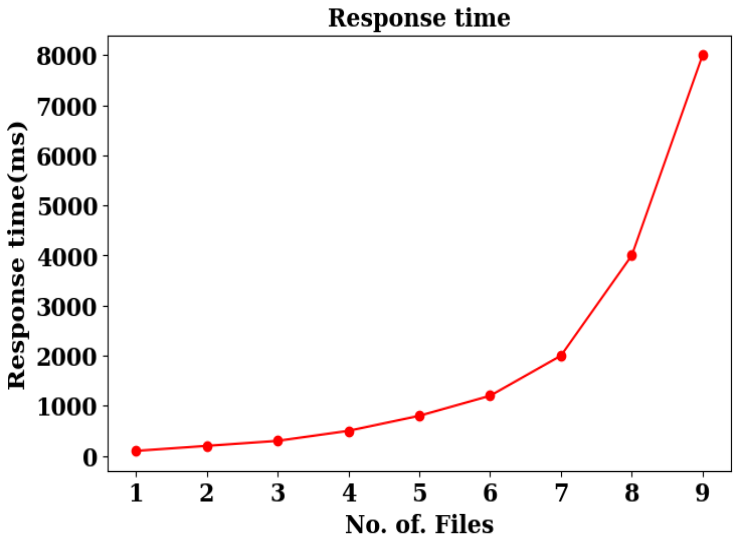

Figure 3: Performance Evaluation of Response Time in Cloud-Based Banking Security

Figure 3 illustrates the relationship between the number of files and the response time (in milliseconds). The x-axis represents the number of files (ranging from 1 to 9), while the y-axis shows the response time in milliseconds, which increases steeply, reaching nearly 8000 ms at 9 files. The plotted red line indicates a non-linear (exponential) growth, suggesting that as the number of files increases, the response time rises significantly. This trend highlights potential performance bottlenecks, implying that the system's response time becomes slower as the workload increases, possibly due to resource constraints or inefficiencies in processing.

5. CONCLUSION

The proposed secure and scalable cloud-based banking data processing framework integrates data collection, pre-processing, encryption using 3DES, and cloud storage to ensure data integrity, security, and compliance. It employs RBAC, encryption at rest and in transit, and regulatory compliance (PCI-DSS, GDPR, ISO 27001) to protect sensitive financial data. Performance evaluations indicate that encryption time follows a linear complexity, reaching 18 seconds for 1000 files, ensuring optimized security. However, response time exhibits exponential growth, reaching 8000 ms for 9 files, highlighting potential bottlenecks. Storage efficiency is optimized through object storage, databases, and data lakes, ensuring seamless scalability and high availability. For future enhancements, AES-256 encryption can be integrated for faster processing, while machine learning-based anomaly detection can enhance fraud detection. Additionally, multi-cloud deployment strategies will improve fault tolerance, redundancy, and cost optimization, ensuring robust and adaptable financial data security.

REFERENCE

[1] Bogdanov, D., Talviste, R., & Willemson, J. (2012). Deploying Secure Multi-Party Computation for Financial Data Analysis: (Short Paper). In *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers 16* (pp. 57-64). Springer Berlin Heidelberg.

[2] Opala, O. J. (2012). *An analysis of security, cost-effectiveness, and it compliance factors influencing cloud adoption by it managers* (Doctoral dissertation, Capella University).

[3] Gurkok, C. (2017). Securing cloud computing systems. In *Computer and Information Security Handbook* (pp. 897-922). Morgan Kaufmann.

[4] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and data protection by design-from policy to engineering. *arXiv preprint arXiv:1501.03726*.

[5] Van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation and Governance*, *19*(6), 429-448.

[6] Conti, F., Schilling, R., Schiavone, P. D., Pullini, A., Rossi, D., Gürkaynak, F. K., ... & Benini, L. (2017). An IoT endpoint system-on-chip for secure and energy-efficient near-sensor analytics. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *64*(9), 2481-2494.

[7] Rajeswari, S., & Kalaiselvi, R. (2017, December). Survey of data and storage security in cloud computing. In *2017 IEEE International Conference on Circuits and Systems (ICCS)* (pp. 76-81). IEEE.

[8] Servos, D. (2012). *A role and attribute based encryption approach to privacy and security in cloud based health services* (Doctoral dissertation).

[9] Bhatia, T., & Verma, A. K. (2017). Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues. *The Journal of Supercomputing*, *73*, 2558-2631.

[10] Abolfazli, S., Sanaei, Z., Ahmed, E., Gani, A., & Buyya, R. (2013). Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. *IEEE Communications Surveys & Tutorials*, *16*(1), 337-368.

[11] Bose, R., Luo, X. R., & Liu, Y. (2013). The roles of security and trust: comparing cloud computing and banking. *Procedia-Social and Behavioral Sciences*, *73*, 30-34.

[12] Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2013). Cloud security auditing: challenges and emerging approaches. *IEEE Security & Privacy*, *12*(6), 68-74.

[13] Asadi, S., Nilashi, M., Husin, A. R. C., & Yadegaridehkordi, E. (2017). Customers perspectives on adoption of cloud computing in banking sector. *Information Technology and Management*, *18*, 305-330.

[14] Hamidi, N. A., Rahimi, G. M., Nafarieh, A., Hamidi, A., & Robertson, B. (2013). Personalized security approaches in e-banking employing flask architecture over cloud environment. *Procedia Computer Science*, *21*, 18-24.

[15] Nosrati, L., & Bidgoli, A. M. (2016, May). A review of mobile banking security. In *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1-5). IEEE.

[16] Mbelli, T. M., & Dwolatzky, B. (2016, June). Cyber security, a threat to cyber banking in South Africa: an approach to network and application security. In *2016 IEEE 3rd international conference on cyber security and cloud computing (CSCloud)* (pp. 1-6). IEEE.

[17] Δέλγα, A. (2014). *Compliance of an airline company with the payment card industry data security standard (PCI DSS): case study* (Master's thesis, Πανεπιστήμιο Πειραιώς).

[18] Srinivas, N. S., & Akramuddin, M. D. (2016, March). FPGA based hardware implementation of AES Rijndael algorithm for Encryption and Decryption. In *2016 international conference on electrical, electronics, and optimization techniques (ICEEOT)* (pp. 1769-1776). IEEE.

[19] Raj, G., M. Thanjaivadivel, M. Viswanathan, and N. Bindhu. "Efficient sensing of data when aggregated with integrity and authenticity." Indian J. Sci. Technol 9, no. 3 (2016).

[20] Almanea, M. I. M. (2015). *The role of transparency and trust in the selection of cloud service providers* (Doctoral dissertation, Newcastle University).