STM JOURNALS

Journal of
Network Security

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 14, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoNS

https://journals.stmjournals.com/jons

Research JoNS

A Trust-Enhanced Security Architecture for Authenticating Customer Records in Banking Institutions

Mahimn B. Pandya[1,*], Gaurang M. Bhatt[2]

Abstract

The growing digital disruption of banking and financial services has completely altered the face of customer onboarding, money transactions, and financial service deliveries. Even as digital technologies provide unparalleled levels of efficiency and accessibility for consumers of financial services, they have also presented new challenges that are equally daunting. Among the growing number of financial threats that digital technology has spawned is the risk of synthetic identity fraud. Unlike identity theft, which has long been associated with financial risk in the digital era, the use of artificial identities that combine real identity data with fake demographic data is even more difficult for financial institutions to detect. Recent research has increasingly advocated blockchain-based identity management solutions due to their immutability and decentralized trust properties. However, despite their theoretical strengths, blockchain systems present critical practical limitations in real-world banking environments, including scalability constraints, high operational overhead, data privacy conflicts, governance challenges, regulatory incompatibility, and difficulties in integration with legacy core banking systems. These limitations raise a fundamental question: Is blockchain truly necessary for ensuring customer identity integrity and fraud prevention? This research answers the question posed above by proposing a complete non-blockchain solution for the prevention of synthetic identity fraud on genuine bank customers. The proposed solution combines the concept of data integrity using cryptographic techniques, multi-factor identity verification procedures, machine learning techniques for anomaly identification, and continuous monitoring under a fully secure central architecture. A system-level architecture description for a hierarchical system that includes identity verification procedures like onboarding, attribute validation checks, document and biometric verification checks, cryptographic sealing of identities, and adaptive fraud risk evaluation is proposed. A mathematical identity confidence model is developed, by which many verification scores are combined into one trust metric that supports rigorous decision-making. The experimental evaluation has been done using simulated and semi-synthetic data sets, indicating that the proposed approach significantly enhances detection accuracy and reduces false alarms with respect to traditional rule-based systems. The proposed framework provides a scalable, explainable, and deployment-ready solution suitable for modern banking ecosystems.

***Author for Correspondence**
Mahimn B. Pandya
E-mail: mahimn009@gmail.com

[1]Assistant Professor, Department of Computer science, Smt. K.B. Parekh College of Computer Science, Mahuva, Bhavnagar M.K. Bhavnagar University, Bhavnagar, Gujarat, India.
[2]Assistant Professor, Department of Computer Science, Shree Swaminarayan College of Computer Science, Sardarnagar, Bhavnagar M.K. Bhavnagar University, Bhavnagar, Gujarat, India.

Received Date: December 18, 2025
Accepted Date: December 28, 2025
Published Date: February 20, 2026

Citation: Mahimn B. Pandya, Gaurang M. Bhatt. A Trust-Enhanced Security Architecture for Authenticating Customer Records in Banking Institutions. Journal of Network Security. 2026; 14(1): 16–22p.

Keywords: Digital identity verification, financial cybersecurity, non-blockchain data integrity, secure customer records, synthetic identity fraud

INTRODUCTION

The global banking industry has witnessed swift and progressive digital transformation stimulated by advancements in information technology, mobile computing, cloud infrastructure, and artificial intelligence [1]. The bouquet of new services includes fully digital account opening, online

processing of loans, facilities for instant payment, and remote customer verification. These have significantly minimized onboarding friction and operational costs for financial institutions to reach a wider population [2]. However, this comfort has also created new avenues in the cyber dimension of identity-based fraud.

Identity fraud is also one of the most enduring risks to financial service organizations. Conventional identity fraud consists of masquerading as a genuine individual using their information or credentials that had been stolen from them [3]. Synthetic identity fraud is a more sophisticated form of fraudulent activity. This form of fraud uses genuine information, including government-issued identification numbers, along with fake surnames, addresses, phone numbers, and behavioral characteristics [4]. Because the created identity is not tied to a living person, potentially long-term financial system abuse is achieved because the individual, the target for a financial transaction, is not actually a human being.

Current Know Your Customer (KYC)/due diligence procedures are mainly based on document verification, database checks, and rule-based logic. Although these procedures can safeguard people against simple attempts at fraud, they prove inadequate against sophisticated synthetic identities carefully crafted to meet verification rules [5]. Furthermore, the rise of deep fake technology, fake documents, and compromised personally identifiable information makes the current identity verification procedures less trustworthy.

Blockchain technology [6] has also been suggested as a possible solution based on an immutable ledger and decentralized trust mechanisms. The use of blockchain technology for identity management has been proposed to ensure increased transparency and integrity. Financial institutions function [7] in a highly regulated marketplace that requires data privacy and centralized accountability and, at times, faces issues related to scalability and latency because of the architecture of the technology.

In this study, we argue against the premise that blockchain is necessary for secure identity management. We propose a non-blockchain alternative that uses cryptography, machine learning, and system-level mechanisms to achieve the same or better security results [8].

RESEARCH OBJECTIVES

The driving forces behind the proposed work are grounded in three observations. First, most banks have invested in infrastructural capabilities to enforce strict access control, cryptography, and real-time monitoring capabilities by design. Second, most current regulations make it impossible to design a completely distributed system by dictating that institutions must retain control of customer data. Third, current machine learning and behavior analytics capabilities make it possible to detect behaviors that would otherwise have gone unnoticed by a static system [9].

The primary objectives of this research are:

1. The design of a non-blockchain identity protection framework ensures the integrity and authenticity of customer records.
2. To develop a quantitative identity confidence model suitable for automated decision-making.
3. To evaluate the effectiveness of the framework against synthetic identity fraud.
4. To demonstrate practical deployability within existing banking ecosystems.

RELATED WORK

Identity fraud prevention systems researched in the past [10] can generally be classified into document verification systems, biometric authentication systems, machine learning algorithms for fraud prevention, and the use of blockchain for identity management systems. Document verification systems use optical character recognition techniques but are susceptible to forged documents. Biometric authentication systems are better, but have issues with spoofing attacks, privacy, and scalability.

Some of the most common machine learning methods used in financial fraud detection include decision trees, random forests, support vector machines, and various forms of deep learning. Although these methods show high accuracy in fraud detection, most of these approaches lack explicit mechanisms that ensure data integrity and traceability. Blockchain-based identity solutions ensure immutability and decentralization. However, studies have also reported several limitations related to transaction throughput, storage overhead, governance models, and compliance with data-protection regulations [11].

Unlike existing approaches, this study integrates cryptographic integrity controls with intelligent fraud detection in a centralized yet tamper-resistant architecture, eliminating blockchain-related limitations while preserving security and compliance.

PROBLEM DEFINITION AND THREAT MODEL

Let C = {c1, c2, cn} denote the set of customer identity records. Each record contained demographics, government-issued identity numbers, biometric characteristics, and session behavior data. The aim is to mark each record as authentic or suspicious without compromising integrity [12].

The threat model envisions adversary capabilities in terms of simulating biographies or IDs, document forgery, biometric spoofing, and unauthorized attempts to change the data. Insider threats can be prevented through audit trails and access controls [13].

- $C=\{c1, c2, ..., cn\}$ be the set of customer records
- $G \subset C$ be genuine customers

Genuine identities remain unaltered and confidential.

- $S \subset C$ be synthetic identities

Synthetic identities were detected onboard or during usage. The insider and external manipulation attempts were also identified.

The objective is to maximize the detection of S while ensuring the integrity and confidentiality of G.

Threats Considered

Threat actors may exploit compromised identifiers, fabricated documents, or behavioral mimicry to create fraudulent identities. Therefore, the system must continuously evaluate identity authenticity rather than relying on one-time verification [14].

1. Identity attribute manipulation
2. Insider data tampering
3. Unauthorized database access
4. Synthetic profile creation during onboarding

PROPOSED IDENTITY PROTECTION FRAMEWORK

The proposed framework adopts a layered architecture designed to protect customer identity data onboard through continuous operations. Each layer contributes to identity assurance and fraud resistance.

Data Acquisition and Pre-Processing

Customer data is collected from multiple channels, including online forms, document uploads, biometric sensors, and external verification services. Data normalization ensures consistency across formats and encoding schemes.

Attribute Consistency Verification

Cross-field validation rules detect logical contradictions, such as mismatches between age, employment history, and financial behavior.

Document and Biometric Verification

Advanced document analysis techniques are used to verify holograms, fonts, and layout structures. Biometric verification incorporates liveness detection to mitigate spoofing attacks (Figure 1).

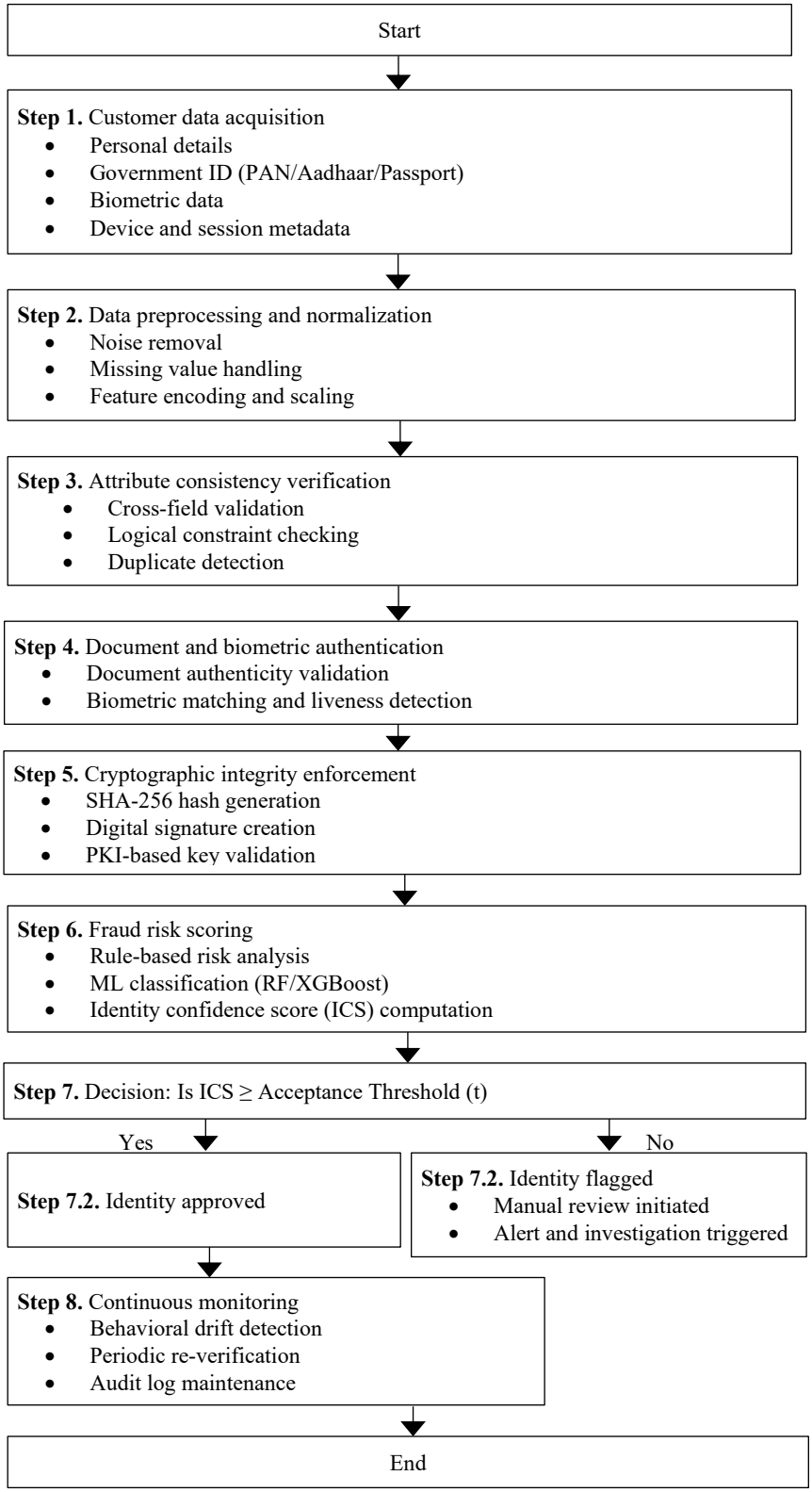

Figure 1. Layered system architecture illustrating onboarding, verification, integrity enforcement, and monitoring components.

Cryptographic Integrity Enforcement

Each verified identity record is cryptographically sealed using secure hash functions and digital signatures [15].

Hi =SHA-256(Di||Bi||Hi)

Machine Learning Risk Analysis

Supervised classifiers analyze identity patterns and assign anomaly scores [16].

CRYPTOGRAPHIC INTEGRITY MODEL

Each customer record Ri is hashed:

Hi=SHA256(Ri ‖ Ti)

Any modification invalidates Hi, enabling tamper detection.

IDENTITY CONFIDENCE MODEL

The identity confidence score is computed as:

$$ICS = \sum_{k=1}^{m} wkvk$$

Where, vk represents the verification factors (biometric match, document validation, and behavioral score) [17].

EXPERIMENTAL SETUP

Dataset Description

Synthetic and genuine identity datasets were generated by using realistic demographic distributions (Table 1). A synthetic dataset of 50,000 customer records was generated with 20% synthetic identity. A Random Forest classifier was trained using behavioral and identity attributes (Table 2 and Figure 2).

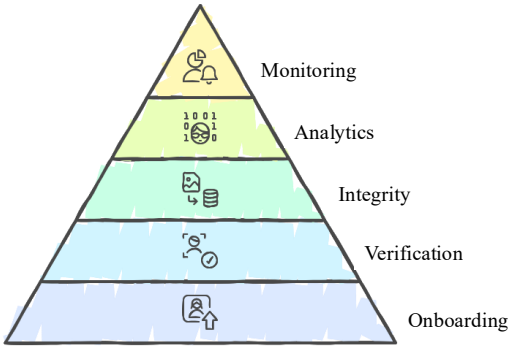

Figure 2. Algorithm flow diagram for identity protection.

Table 1. Dataset composition.

Identity type	Count
Genuine	25,000
Synthetic	15,000

Table 2. Performance comparison.

Method	Accuracy	Recall	False positive rate (FPR)
Rule-based	82%	76%	9%
Proposed	94%	91%	3%

SECURITY AND PRIVACY ANALYSIS

The framework ensures:

- Confidentiality via encryption
- Integrity via hashing
- Accountability via audit logs
- Privacy via minimal data exposure

SECURITY, PRIVACY, AND COMPLIANCE ANALYSIS

The framework ensures confidentiality through encryption, integrity through cryptographic hashing, availability through redundancy, and accountability through secure audit logs. It aligns with regulatory guidelines such as ISO/IEC 27001 and national banking cybersecurity frameworks [18].

CONCLUSION

The rapid digitalization of banking services has transformed how financial institutions acquire, manage, and authenticate customer identities. Although this transformation has enabled efficiency, scalability, and customer convenience, it has also exposed systemic vulnerabilities in identity verification processes, particularly in the form of synthetic identity fraud. Unlike conventional identity theft, synthetic identity fraud exploits the structural weaknesses of digital onboarding systems by blending legitimate personal identifiers with fabricated demographic, behavioral, and biometric attributes. This complexity renders many traditional KYC and rule-based fraud detection systems insufficient, allowing fraudulent identities to persist undetected over long periods and inflict substantial financial and reputational damage on institutions.

One of the key strengths of the present work is that it employs system-level integration of various tools for the generation of a more justified and scalable framework. Contrary to other approaches that rely on a single point of trust in a trust anchor, this study proposes a framework that disperses various levels of trust based on document authenticity analysis, biometric analysis with liveness analysis, cross-attribute analysis, and cryptographic sealing of every verified identity record. Moreover, utilizing well-proven techniques in the field of secure system design enables financial institutions to build robust identity integrity in a simplified manner. The proposed framework that relies on a non-blockchain approach offers a viable solution in this case, which corresponds to a future-ready solution for a critical necessity in banking identity-related issues.

REFERENCES

1. Zhang CJ, Gill AQ, Liu B, Anwar MJ. AI-based identity fraud detection: A systematic review. [Preprint]. 2025. arXiv:2501.09239. doi:10.48550/arXiv.2501.09239
2. Wang W, Zhang J, Li Q, Zong C, Li Z. Are you for real? Detecting identity fraud via dialogue interactions. In: Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP); 2019 Nov; Hong Kong, China. Association for Computational Linguistics; 2019. p. 1762–1771. doi:10.18653/v1/D19-1185.
3. Borketey B. Real-time fraud detection using machine learning. J Data Anal Inf Process. 2024;12:189–209. doi:10.4236/jdaip.2024.122011.
4. Pakina AK, Kejriwal D, Goel A, Pujari TD. AI-generated synthetic identities in fintech: Detecting deepfake KYC fraud using behavioral biometrics. IOSR J Comput Eng. 2023;25(3):26–37.
5. Igba E, Olarinoye HS, Nwakaego VE, Sehemba DB, Oluhaiyero YS, Okika N. Synthetic data generation using generative AI to combat identity fraud and enhance global financial cybersecurity frameworks. Int J Sci Res Mod Technol. 2025;4(2):1–19. doi:10.5281/zenodo.14928919.
6. Mungai R. Synthetic identity fraud: A critical primary national security priority. SSRN Electron J. 2024. doi:10.2139/ssrn.4770398.
7. Awosika T, Shukla RM, Pranggono B. Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. IEEE Access. 2024;12:64551–64560. doi:10.1109/ACCESS.2024.3394528.

8. Iqbal A, Iqbal A, Ahmed E, Rahman A, Ontor MRH. Enhancing fraud detection and anomaly detection in retail banking using generative AI and machine learning models. Am J Eng Technol. 2024;6(11):78–91. doi:10.37547/tajet/Volume06Issue11-09.
9. Dixit S. Generative AI-powered document processing at scale with fraud detection for large financial organizations. Int J Sci Res Comput Sci Eng Inf Technol. 2024;10(5):1057–1084. doi:10.32628/CSEIT2410612455.
10. Chitraju S. Artificial intelligence in detecting synthetic identity fraud. SSRN. 2025. doi:10.2139/ssrn.5353731.
11. Anasuri S. Synthetic identity detection using graph neural networks. Int J Artif Intell Data Sci Mach Learn. 2023;4(4):87–96.
12. Liu J, Huang W, Li T, Ji S, Zhang J. Cross-domain knowledge graph chiasmal embedding for multi-domain item–item recommendation. IEEE Trans Knowl Data Eng. 2022;35(5):1–1. doi:10.1109/TKDE.2022.3151986.
13. Riccio D, Galdi C, Manzo R. Biometric/cryptographic keys binding based on function minimization. 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Naples, Italy. 2016. p. 144–150. doi:10.1109/SITIS.2016.31.
14. Crosby SA, Wallach DS. Efficient data structures for tamper-evident logging. In: Proceedings of the 18th USENIX Security Symposium (SSYM '09); 2009; Montreal, Canada. USENIX Association; 2009. p. 317–334.
15. Pandya M, Joshi H, Jani A. A novel digital watermarking algorithm using random matrix image. Int J Comput Appl. 2013;61:18–21. doi:10.5120/9900-4481.
16. Pandya M, Joshi H, Jani A. A bespoke technique for secret messaging. Int J Comput Netw Inf Secur. 2013;5:40–46. doi:10.5815/ijcnis.2013.05.05.
17. Pandya M, Jani A. A novel algorithm for information hiding. Int J Adv Res Comput Sci. 2018;9(2):7–10. doi:10.26483/ijarcs.v9i2.5489.
18. Pandya M, Jani A. A hybrid approach for secure message communication and color image watermarking. Elixir Digit Process. 2018;114:49488–49491.

