Indian Engineering Journal
ISSN: 2984-9047
Vol 4 Issue 2 (2026)

A Secure IoT-Enabled Banking Authentication Framework Integrating Aadhaar, Biometrics, Artificial Intelligence and Blockchain

Brijesh Nayyar[1], Dr. Vishal Kumar Goar[2]

[1]PhD Scholar, Maharaja Ganga Singh University, Bikaner (brijeshnayyar75@gmail.com)

[2]Assistant Professor, Engineering College Bikaner (dr.vishalgoar@gmail.com)

Abstract

The rapid evolution of digital banking has transformed financial services by enabling customers to perform secure and convenient transactions through online banking platforms, mobile applications, Automated Teller Machines (ATMs), and Internet of Things (IoT)-enabled banking devices. However, the increasing dependence on digital financial services has also exposed banking institutions to sophisticated cyber threats, including identity theft, phishing attacks, credential compromise, insider attacks, biometric spoofing, malware, and financial fraud. Conventional authentication techniques based on passwords, Personal Identification Numbers (PINs), and One-Time Passwords (OTPs) are no longer sufficient to defend against these evolving security challenges.

This paper proposes a secure multi-layered banking authentication framework that integrates Aadhaar-based identity verification, biometric authentication, Artificial Intelligence (AI)-based fraud detection, blockchain-enabled transaction validation, and IoT-assisted security monitoring. The proposed framework employs fingerprint and facial biometrics as primary authentication factors, while Aadhaar-based verification establishes trusted user identity. Artificial Intelligence continuously analyses user behaviour, transaction history, device characteristics, and geolocation information to identify suspicious activities in real time. Blockchain technology provides immutable authentication logs and transaction records, preventing unauthorized modifications and ensuring data integrity. IoT-enabled banking devices further strengthen security by continuously monitoring device status, environmental conditions, and transaction endpoints.

The proposed framework offers a comprehensive authentication architecture capable of improving transaction security, reducing identity fraud, enhancing customer trust, and supporting secure digital banking services. Furthermore, the framework addresses several limitations of existing authentication models by combining multiple complementary security mechanisms into a unified architecture. The proposed model can assist banking institutions in implementing next-generation authentication systems capable of adapting to evolving cyber threats while maintaining user convenience and regulatory compliance.

Keywords: Internet of Things (IoT), Banking Security, Aadhaar Authentication, Biometric Authentication, Artificial Intelligence, Blockchain, Fraud Detection, Multi-Factor Authentication, Cyber Security, Digital Banking.

1. Introduction

The banking sector has experienced remarkable digital transformation during the past decade. Traditional branch-based banking has gradually shifted towards digital platforms that provide customers with convenient access to financial services through internet banking, mobile banking applications, smart Automated Teller Machines (ATMs), Unified Payments Interface (UPI), digital wallets, and cloud-based financial systems. This technological transformation has significantly improved banking efficiency, customer experience, and financial inclusion. Nevertheless, the growing digital ecosystem has simultaneously expanded the attack surface available to cybercriminals.

Modern banking systems process millions of financial transactions every day. The confidentiality, integrity, and availability of customer information have therefore become critical security requirements. Cyber attacks targeting banking infrastructure have become increasingly sophisticated, involving phishing campaigns, ransomware, identity theft, credential stuffing, SIM swapping, insider threats, distributed denial-of-service attacks, malware injection, and biometric spoofing. Financial institutions continue investing substantial

resources to strengthen cybersecurity infrastructures; however, conventional authentication mechanisms remain vulnerable to advanced attack techniques.

Password-based authentication continues to dominate many banking applications despite well-known security limitations. Weak passwords, password reuse, brute-force attacks, and credential leakage significantly reduce the effectiveness of password-based security. Additional authentication mechanisms such as One-Time Passwords (OTPs) and security questions provide incremental improvements but remain susceptible to phishing attacks, social engineering, malware, and SIM swap frauds. Consequently, banks increasingly require stronger authentication mechanisms capable of accurately verifying customer identity while maintaining a convenient user experience.

Biometric authentication has emerged as one of the most promising authentication technologies in modern financial systems. Biometric identifiers such as fingerprints, facial recognition, iris recognition, and voice authentication provide unique physiological characteristics that are difficult to duplicate or steal. Unlike passwords, biometric characteristics remain inherently associated with individual users, making identity impersonation considerably more difficult. Many financial institutions have therefore integrated biometric authentication into mobile banking applications, smart ATMs, and digital payment platforms to strengthen customer authentication.

In India, Aadhaar has further revolutionized digital identity verification by providing every citizen with a unique biometric-based identity linked to demographic and biometric information. Aadhaar-based authentication enables secure electronic Know Your Customer (e-KYC) verification, digital onboarding, Direct Benefit Transfer (DBT), and Aadhaar Enabled Payment System (AEPS) services. The integration of Aadhaar authentication into banking systems has simplified customer verification while reducing document forgery and identity fraud. Nevertheless, Aadhaar-based authentication also introduces challenges concerning biometric privacy, centralized identity management, network dependency, and secure storage of sensitive information.

The rapid advancement of Artificial Intelligence (AI) has opened new opportunities for proactive banking security. Unlike traditional rule-based fraud detection systems, AI can continuously analyse transaction behaviour, customer profiles, geographical location, device fingerprints, transaction velocity, historical spending patterns, and behavioural characteristics to detect anomalous activities in real time. Machine learning algorithms improve continuously as new transaction data become available, enabling financial institutions to identify emerging fraud patterns more accurately than conventional systems.

Blockchain technology provides another important advancement for banking security. The decentralized and immutable characteristics of blockchain make it suitable for maintaining tamper-resistant authentication logs and secure transaction records. Since each transaction is cryptographically linked with previous records, unauthorized modification becomes extremely difficult. Blockchain therefore improves accountability, transparency, and integrity throughout the banking authentication process.

The emergence of Internet of Things (IoT) technologies has further transformed banking infrastructure. Smart ATMs, biometric authentication terminals, RFID-enabled payment devices, intelligent surveillance systems, environmental sensors, and connected banking equipment generate continuous operational data that can be utilised to improve security monitoring. Proper integration of IoT devices with authentication systems enables banks to monitor device health, detect unauthorized access, identify abnormal operating conditions, and respond rapidly to security incidents.

Although several studies have independently investigated biometric authentication, Aadhaar verification, blockchain security, Artificial Intelligence, and IoT-based banking systems, relatively few studies have attempted to integrate these technologies into a unified multi-layered authentication framework. Most existing solutions continue to focus on individual authentication mechanisms without providing coordinated decision-making across multiple security layers. Consequently, financial institutions continue facing challenges related to authentication reliability, fraud detection accuracy, user privacy, scalability, and regulatory compliance.

To address these challenges, this paper proposes a Secure IoT-Enabled Banking Authentication Framework integrating Aadhaar-based identity verification, biometric authentication, Artificial Intelligence-driven fraud detection, blockchain-based transaction validation, and IoT-assisted security monitoring. The proposed framework combines multiple complementary security technologies into a unified architecture capable of enhancing authentication accuracy, reducing financial fraud, improving transaction transparency, and strengthening overall banking cybersecurity.

The major contributions of this research include:

- Development of an integrated multi-layer banking authentication framework combining Aadhaar, biometrics, Artificial Intelligence, blockchain, and IoT technologies.
- Introduction of an AI-assisted risk evaluation module capable of analysing transaction behaviour for intelligent fraud detection.
- Integration of blockchain technology for immutable authentication records and secure transaction validation.
- Adoption of IoT-enabled monitoring devices to improve real-time banking infrastructure security.
- Comprehensive security architecture designed to improve authentication reliability while maintaining customer convenience and supporting regulatory compliance.

The proposed framework provides a practical foundation for developing secure next-generation digital banking systems capable of addressing continuously evolving cyber threats.

2. Literature Review

Digital banking security has become one of the most actively researched areas in financial technology due to the increasing frequency of cyberattacks targeting banking infrastructure. Researchers have proposed numerous authentication mechanisms based on cryptography, biometrics, artificial intelligence, blockchain, and Internet of Things technologies. Although these approaches significantly improve security, each possesses inherent limitations when implemented independently.

Traditional banking authentication systems primarily rely on passwords, Personal Identification Numbers (PINs), and One-Time Passwords (OTPs). Numerous studies have demonstrated that password-based authentication remains vulnerable to phishing attacks, password reuse, brute-force attacks, credential stuffing, keylogging malware, and social engineering. Multi-Factor Authentication (MFA) partially mitigates these risks by combining multiple authentication factors; however, OTP interception, SIM swapping, and malware attacks continue to compromise authentication security.

Biometric authentication has emerged as an effective alternative to password-based authentication. Fingerprint recognition, iris recognition, facial recognition, and voice authentication provide unique biological characteristics that are considerably more difficult to duplicate than conventional passwords. Several researchers have reported improved authentication accuracy using biometric systems in banking applications. Nevertheless, biometric authentication remains vulnerable to spoofing attacks involving artificial fingerprints, facial masks, replay attacks, and synthetic biometric generation. Consequently, modern biometric systems increasingly incorporate liveness detection algorithms and multi-modal biometric verification.

The introduction of Aadhaar-based authentication has significantly strengthened digital identity verification within the Indian banking ecosystem. Aadhaar-enabled authentication facilitates electronic Know Your Customer (e-KYC), Direct Benefit Transfer (DBT), and Aadhaar Enabled Payment System (AEPS) services while reducing document forgery and fraudulent identity creation. Despite these advantages, researchers have identified several challenges including biometric privacy, centralized identity management, dependence on continuous network connectivity, and protection of sensitive biometric information.

Artificial Intelligence has become an essential component of modern fraud detection systems. Machine learning algorithms can analyse large transaction datasets to identify abnormal customer behaviour, unusual spending patterns, geographic anomalies, transaction velocity, and device inconsistencies. Compared with conventional rule-based fraud detection techniques, AI-based systems provide greater adaptability and improved detection accuracy. However, AI models require continuous training, high-quality datasets, and periodic model updates to remain effective against evolving cyber threats.

Blockchain technology has attracted significant attention for secure financial transaction management due to its decentralized architecture, cryptographic integrity, and immutable ledger structure. Researchers have demonstrated that blockchain can improve transparency, prevent unauthorized transaction modification, and strengthen auditability within financial systems. Nevertheless, blockchain implementations often face challenges related to scalability, computational overhead, latency, and integration with existing banking infrastructure.

Internet of Things technologies have expanded banking services through smart ATMs, biometric terminals, intelligent surveillance systems, RFID-enabled payment devices, and connected banking equipment. IoT devices continuously generate operational data that can improve security monitoring and infrastructure management. However, IoT devices frequently suffer from limited computational resources, insecure firmware, weak authentication protocols, and insufficient encryption, making them attractive targets for cyberattacks.

A comprehensive review of existing literature indicates that most published research investigates these technologies individually rather than integrating them into a unified banking authentication framework. Existing approaches generally emphasize either biometric authentication, AI-based fraud detection, blockchain security, or IoT monitoring independently. The absence of coordinated interaction among these security mechanisms limits their overall effectiveness against sophisticated cyber threats.

The present research addresses this gap by proposing a unified banking authentication framework that combines Aadhaar-based identity verification, biometric authentication, Artificial Intelligence-based fraud detection, blockchain-enabled transaction validation, and IoT-assisted infrastructure monitoring within a single security architecture. The integration of these complementary technologies is expected to improve authentication reliability, strengthen fraud prevention, enhance transaction transparency, and provide greater resilience against emerging cyber security threats.

Khan et al. proposed a blockchain-based decentralized authentication framework for Information-Centric 5G Networks to improve authentication security and eliminate single-point failures. The framework enhances trust, data integrity, and secure identity verification using blockchain technology. However, it does not address banking-specific authentication or biometric integration. **[1]**

Ghafourian et al. presented a survey on the integration of blockchain and biometric authentication systems. The study highlights secure storage of biometric templates using blockchain while discussing privacy and legal challenges. However, it does not propose a unified framework for secure digital banking applications. **[2]**

Fernandez-Carames and Fraga-Lamas reviewed blockchain applications in Internet of Things (IoT) environments. They demonstrated that blockchain improves decentralization, trust, and data integrity among IoT devices. The study mainly focuses on IoT security and does not consider banking authentication systems. **[3]**

Liu et al. reviewed Machine Learning techniques for financial fraud detection. Their study showed that AI algorithms effectively detect fraudulent transactions by analysing customer behaviour and transaction history. However, the research focuses on fraud detection rather than complete authentication systems. **[4]**

Stallings explained the fundamental concepts of cryptography, authentication protocols, encryption techniques, and network security. The book provides the theoretical foundation for designing secure authentication systems. However, it does not discuss blockchain or AI-based banking authentication. **[5]**

Das et al. surveyed secure authentication protocols developed for Internet of Things applications. The study discusses lightweight authentication, privacy preservation, and cryptographic approaches for IoT security. However, Aadhaar-based authentication and AI-assisted banking security are not addressed. **[6]**

Jain, Ross, and Nandakumar presented comprehensive concepts of biometric authentication, including fingerprint, face, iris, and multimodal biometrics. The book explains biometric feature extraction, matching techniques, and performance evaluation. However, blockchain-enabled authentication for banking applications is beyond its scope. **[7]**

Ebrahim et al. reviewed blockchain as a security and privacy solution for smart environments and IoT systems. Their work demonstrated that blockchain enhances confidentiality, integrity, and decentralized trust in connected environments. However, the study does not specifically focus on banking security. **[8]**

Modi and Devaraj investigated recent advancements in Artificial Intelligence-based biometric authentication. The study highlighted the application of deep learning techniques to improve biometric recognition accuracy and authentication performance. However, blockchain and IoT integration were not considered. **[9]**

The Reserve Bank of India issued the Master Directions on Digital Payment Security Controls to strengthen cybersecurity in digital banking. The guidelines recommend multi-factor authentication, encryption, fraud monitoring, and secure payment infrastructure. However, they provide regulatory recommendations rather than an integrated technical authentication framework. **[10]**

The Unique Identification Authority of India (UIDAI) developed the Aadhaar Authentication API to provide secure electronic identity verification using demographic and biometric information. The API supports fingerprint, iris, face authentication, and OTP-based verification while ensuring encrypted communication. It provides a reliable identity verification mechanism but does not incorporate AI-based fraud detection or blockchain-enabled transaction validation. **[11]**

The National Payments Corporation of India (NPCI) introduced the Unified Payments Interface (UPI) to facilitate secure, interoperable, and real-time digital payment services. The guidelines emphasize secure authentication, encrypted communication, and seamless banking transactions. However, they rely primarily on conventional security mechanisms and do not integrate Artificial Intelligence, blockchain, or IoT technologies. **[12]**

The PCI Security Standards Council developed the PCI-DSS v4.0 standard to protect payment card information through strong security controls. The framework includes encryption, authentication, access control, vulnerability management, and continuous security monitoring. However, it mainly provides compliance guidelines rather than an intelligent authentication framework for digital banking. **[13]**

The General Data Protection Regulation (GDPR) establishes comprehensive rules for protecting personal and sensitive user information. It emphasizes privacy, user consent, data minimization, and secure processing of biometric data across digital systems. Although GDPR strengthens data protection, it does not propose technical authentication mechanisms for banking applications. **[14]**

Usama et al. proposed a blockchain-enabled identity management framework for Internet of Things environments integrated with Artificial Intelligence. Their approach improves decentralized authentication, trust management, and resilience against adversarial attacks. However, the framework is designed for IoT applications and does not specifically address banking authentication systems. **[15]**

Iswarya and Vennila developed a blockchain-assisted authentication framework for decentralized IoT data management. Their framework enhances authentication security, scalability, and data integrity through distributed ledger technology. Nevertheless, the proposed model does not integrate biometric authentication or AI-based behavioural analysis for banking security. **[16]**

Ibrahim et al. proposed a Blockchain-IoT framework for secure digital banking and evaluated various blockchain consensus mechanisms. Their study demonstrated improvements in transaction security, transparency, and customer trust using distributed ledger technology. However, biometric authentication and intelligent fraud detection were not incorporated into the proposed framework. **[17]**

Latif et al. introduced a blockchain-based authentication system employing multi-factor authentication, access control, and post-quantum cryptographic techniques. The proposed framework significantly enhances

authentication security and resistance against cyber threats. However, the research primarily focuses on healthcare applications rather than banking environments. **[18]**

Natampalli et al. proposed a multi-security framework integrating GANs, steganography, blockchain, and IoT technologies for self-service banking systems. Their architecture improves transaction confidentiality, authentication strength, and cyberattack resistance. However, Aadhaar-based identity verification and AI-driven behavioural analysis are not included in the proposed model. **[19]**

Ali and Al-Dabbagh presented a systematic literature review on biometric authentication techniques used in mobile banking applications. The study analysed fingerprint, facial recognition, iris authentication, and behavioural biometrics while discussing usability and security challenges. The authors suggested integrating biometrics with Artificial Intelligence and blockchain to enhance future banking authentication systems. **[20]**

Rjab and Sliman presented a comprehensive survey on biometric authentication for decentralized identity management. The study reviewed fingerprint, facial recognition, iris recognition, and behavioural biometrics while discussing emerging trends, security challenges, and future research directions. The authors concluded that integrating biometrics with decentralized identity frameworks enhances authentication reliability and user privacy, although banking-specific implementations were not extensively explored. **[21]**

The study on securing and classifying Active Directory domain banking data proposed the integration of Blockchain and Artificial Intelligence to strengthen banking security. The framework utilizes blockchain for ensuring data integrity and AI for intelligent threat detection and data classification. The results demonstrated improved protection against unauthorized access and cyberattacks; however, the proposed approach does not incorporate Aadhaar-based identity verification or multi-modal biometric authentication. **[22]**

3. Research Gap

The widespread adoption of digital banking has significantly improved the accessibility and efficiency of financial services. However, it has also increased the complexity of securing banking transactions against sophisticated cyber threats. Existing banking authentication systems employ various security mechanisms such as password-based authentication, One-Time Passwords (OTPs), biometric authentication, Artificial Intelligence (AI)-based fraud detection, blockchain technology, and Internet of Things (IoT)-enabled monitoring. Although these technologies have individually contributed to enhancing banking security, a comprehensive analysis of the existing literature reveals several critical research gaps.

Most conventional banking systems continue to rely on password-based authentication and OTP verification. These approaches are vulnerable to phishing attacks, credential theft, SIM-swapping, replay attacks, brute-force attacks, malware, and social engineering. Multi-Factor Authentication (MFA) improves security by introducing additional verification factors; however, it still depends heavily on user interaction and communication networks, making it susceptible to network-related attacks.

Biometric authentication has emerged as a reliable alternative due to the uniqueness of physiological characteristics such as fingerprints, facial features, iris patterns, and voiceprints. Despite its advantages, standalone biometric authentication systems remain vulnerable to biometric spoofing, fake fingerprints, deepfake facial images, replay attacks, and biometric template theft. Furthermore, many existing systems lack intelligent mechanisms for detecting abnormal user behaviour after successful biometric verification.

Aadhaar-based authentication has transformed identity verification in India by enabling secure e-KYC services and simplifying customer onboarding. Nevertheless, existing Aadhaar authentication systems primarily focus on identity verification without integrating behavioural analytics, fraud prediction, or decentralized transaction validation. Consequently, security decisions are often based on a single authentication factor rather than multiple coordinated security layers.

Artificial Intelligence has demonstrated considerable potential for detecting fraudulent banking activities by analysing historical transactions, customer behaviour, and device characteristics. However, most AI-based fraud

detection models operate as independent modules that identify suspicious transactions only after authentication has been completed. They rarely participate directly in the authentication decision-making process.

Blockchain technology provides immutable transaction records, cryptographic integrity, and transparent auditing. Existing blockchain-based banking solutions primarily focus on transaction logging or cryptocurrency applications, with limited integration into customer authentication workflows. As a result, blockchain is not fully utilized for strengthening authentication reliability and preventing identity-related fraud.

Similarly, IoT technologies have enabled the deployment of smart ATMs, biometric terminals, RFID-enabled payment devices, intelligent surveillance systems, and connected banking infrastructure. However, many IoT deployments operate independently from authentication mechanisms, resulting in fragmented security architectures and limited coordination between physical devices and digital identity verification.

Based on these observations, the following research gaps are identified:

- Existing banking authentication mechanisms rely heavily on individual security techniques rather than integrated security architectures.
- Current systems perform authentication sequentially but lack intelligent coordination among identity verification, behavioural analysis, and transaction validation.
- AI-based fraud detection is generally applied after authentication instead of participating in real-time authentication decisions.
- Blockchain technology is rarely integrated with biometric authentication and Aadhaar-based identity verification.
- Existing IoT-enabled banking systems focus primarily on infrastructure monitoring rather than intelligent authentication support.
- Few authentication frameworks combine Aadhaar, biometrics, Artificial Intelligence, blockchain, and IoT within a unified multi-layer security architecture.

To bridge these gaps, this research proposes the **Secure Intelligent Banking Authentication Framework (SIBAF)**, which integrates multiple complementary security technologies into a single authentication model capable of improving authentication accuracy, fraud prevention, transaction integrity, and infrastructure security.

4.1 Proposed Secure Intelligent Banking Authentication Framework (SIBAF) Framework Overview

This research proposes a novel multi-layer banking authentication model named the **Secure Intelligent Banking Authentication Framework (SIBAF)**. The framework integrates Aadhaar-based identity verification, biometric authentication, Artificial Intelligence-driven fraud detection, blockchain-based transaction validation, and IoT-enabled infrastructure monitoring into a unified authentication architecture.

Unlike traditional authentication systems that rely on passwords or OTPs, SIBAF performs authentication through multiple independent verification layers. Each layer contributes to the overall authentication confidence, thereby reducing the probability of unauthorized access and financial fraud.

The framework is designed to achieve the following objectives:

- Strengthen user identity verification using Aadhaar and biometrics.
- Detect fraudulent transactions using AI-based behavioural analysis.
- Maintain immutable transaction records using blockchain technology.
- Monitor banking devices continuously using IoT sensors.
- Improve transaction transparency and customer trust.

- Reduce identity theft, phishing attacks, and transaction manipulation.
- Enhance regulatory compliance and banking cybersecurity.

The proposed framework provides a scalable architecture suitable for modern digital banking environments and future smart banking applications.

4.2 Components of the Proposed Framework

The proposed SIBAF consists of six interconnected security layers.

Layer 1: User Access Layer

Customers access banking services through secure digital channels, including:

- Mobile Banking Applications
- Internet Banking Portals
- Smart ATMs
- Banking Kiosks
- IoT-enabled Banking Devices
- Digital Payment Terminals

All communication between user devices and banking servers is encrypted using secure communication protocols.

Layer 2: Aadhaar Identity Verification Layer

This layer establishes the authenticity of the customer's identity using Aadhaar-based verification.

The verification process includes:

- Aadhaar Number Validation
- UIDAI Authentication
- e-KYC Verification
- Demographic Validation
- Virtual ID (VID) Authentication

Only authenticated users are permitted to proceed to the biometric authentication stage.

Layer 3: Biometric Authentication Layer

After successful identity verification, biometric authentication is performed.

The framework supports multiple biometric modalities including:

- Fingerprint Recognition
- Facial Recognition
- Iris Recognition
- Voice Recognition

Liveness detection techniques are incorporated to protect the system against biometric spoofing attacks.

Layer 4: Artificial Intelligence Risk Assessment Layer

This layer evaluates transaction risk using machine learning algorithms.

The AI engine analyses various behavioural and transactional parameters such as:

- Transaction Amount
- Login Time
- Device Fingerprint
- Geographical Location
- Transaction Frequency
- Previous Transaction History
- User Behaviour
- Failed Login Attempts
- Device Trust Score

Based on these parameters, the AI engine computes a dynamic **Risk Score**.

Transactions are classified as:

- Low Risk
- Medium Risk
- High Risk

High-risk transactions are automatically rejected or subjected to additional verification procedures.

Layer 5: Blockchain Validation Layer

Transactions approved by the AI module are recorded within a blockchain ledger.

Each block contains:

- Customer Identifier
- Transaction Identifier
- Authentication Status
- Timestamp
- Device Identifier
- Previous Block Hash
- Current Block Hash

Blockchain ensures immutability, traceability, and transparency while preventing unauthorized modification of transaction records.

Layer 6: IoT Security Monitoring Layer

The final layer continuously monitors the operational status of banking infrastructure.

IoT devices supervise:

- Smart ATMs
- Biometric Authentication Devices
- RFID Payment Systems

- CCTV Surveillance
- Environmental Sensors
- Network Health
- Device Tampering
- Communication Status

Whenever abnormal activity is detected, alerts are immediately transmitted to the banking security management system.

4.3 Advantages of the Proposed Framework

The proposed SIBAF offers several advantages over existing authentication systems:

- Multi-layer authentication improves security by eliminating dependence on a single verification mechanism.
- AI-based behavioural analysis enables proactive fraud detection before transaction completion.
- Blockchain technology provides immutable authentication logs and tamper-proof transaction records.
- IoT-enabled monitoring improves situational awareness and infrastructure security.
- Aadhaar-based identity verification strengthens customer authentication.
- Multi-modal biometric verification significantly reduces impersonation attacks.
- The framework enhances transparency, accountability, scalability, and customer confidence.
- The modular architecture allows future integration with emerging technologies and regulatory requirements.

5. System Architecture

The proposed architecture ensures that each banking transaction passes through multiple independent security layers before authorization. Every layer contributes to enhancing authentication reliability and minimizing the risk of unauthorized access, identity theft, transaction fraud, and cyberattacks. The integration of Aadhaar verification, biometrics, AI, blockchain, and IoT enables a comprehensive security solution suitable for next-generation digital banking systems.

The overall architecture of the proposed Secure Intelligent Banking Authentication Framework (SIBAF) is presented conceptually in Figure 1 as below.

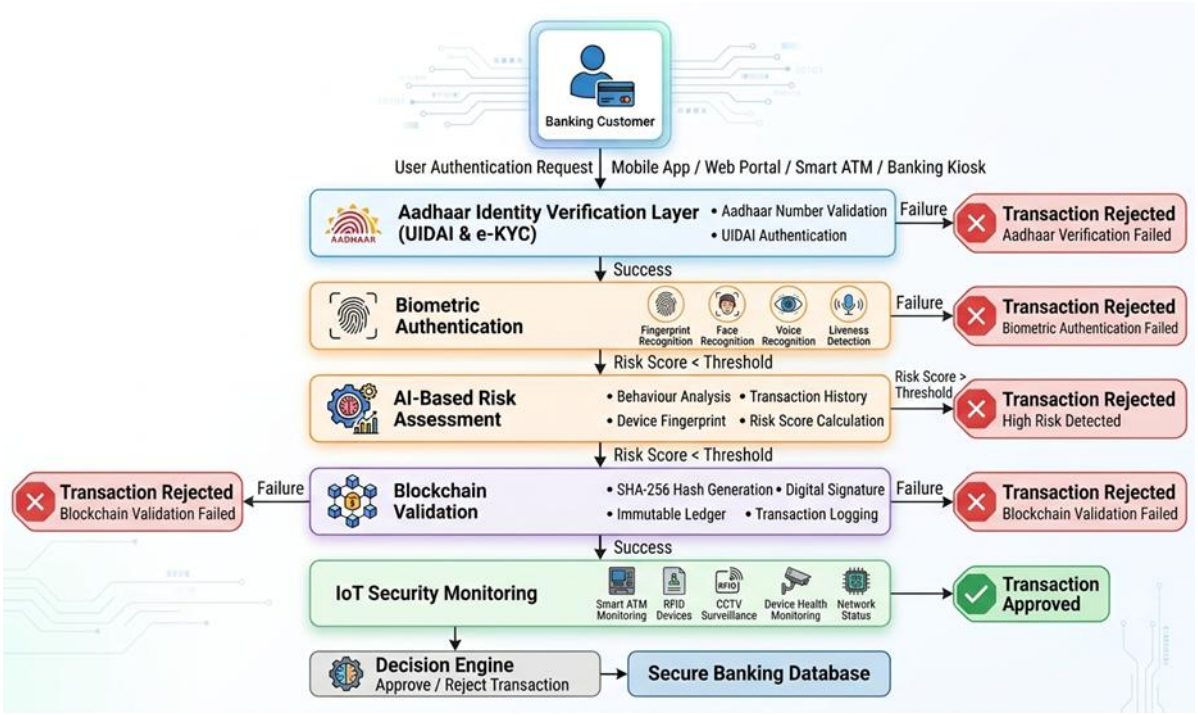


Figure 1. Overall Architecture of the Proposed Secure Intelligent Banking Authentication Framework (SIBAF).

6.1 Research Methodology

This research adopts a **design science research methodology** to develop a secure and intelligent banking authentication framework. The objective is to integrate multiple authentication technologies into a unified architecture capable of providing stronger security than conventional banking authentication systems.

The proposed Secure Intelligent Banking Authentication Framework (SIBAF) combines Aadhaar-based identity verification, biometric authentication, Artificial Intelligence (AI)-based fraud detection, blockchain-based transaction validation, and Internet of Things (IoT)-enabled security monitoring. Each authentication layer independently validates the user and transaction before granting authorization.

The research methodology consists of the following phases:

Phase 1: Requirement Analysis

The first phase involves analysing the limitations of existing banking authentication systems. Current banking platforms primarily rely on passwords, OTPs, or standalone biometric authentication, making them vulnerable to phishing attacks, credential theft, replay attacks, biometric spoofing, and identity fraud. Security requirements identified during this phase include:

- Secure identity verification
- Multi-factor authentication
- Fraud detection
- Data integrity
- Device monitoring
- Transaction transparency
- Regulatory compliance

Phase 2: Framework Design

Based on the identified requirements, a six-layer authentication framework was designed. The framework consists of:

- User Access Layer
- Aadhaar Verification Layer
- Biometric Authentication Layer
- AI Risk Assessment Layer
- Blockchain Validation Layer
- IoT Security Monitoring Layer

Each layer performs an independent security assessment before forwarding the authentication request to the next layer.

Phase 3: Authentication Process

The authentication workflow begins when a customer initiates a banking transaction. The system performs:

1. Aadhaar Identity Verification
2. Biometric Verification
3. AI-Based Risk Assessment
4. Blockchain Transaction Validation
5. IoT Infrastructure Monitoring

Only after successful completion of all authentication stages is the transaction approved.

Phase 4: Security Evaluation

The proposed framework is evaluated conceptually by comparing it with conventional banking authentication systems based on the following parameters:

- Authentication Strength
- Identity Verification
- Fraud Detection Capability
- Transaction Integrity
- Scalability
- Transparency
- Infrastructure Monitoring
- Resistance to Cyber Attacks

The evaluation demonstrates the advantages of integrating multiple complementary security mechanisms into a unified authentication framework.

6.2 Authentication Workflow

The authentication process follows a sequential multi-layer approach.

Step 1: The customer accesses banking services using:

- Mobile Banking
- Internet Banking
- Smart ATM
- Banking Kiosk

The authentication request is securely transmitted to the banking server.

Step 2: The Aadhaar authentication module verifies:

- Aadhaar Number
- UIDAI Authentication
- e-KYC Verification
- Virtual ID (VID)

If authentication fails, access is denied immediately.

Step 3: The biometric authentication module verifies:

- Fingerprint
- Face
- Iris
- Voice

Liveness detection algorithms eliminate spoofing attempts.

Step 4: The Artificial Intelligence engine analyses customer behavior features which includes:

- Login Time
- Device Information
- Geographical Location
- Previous Transaction History
- Transaction Amount
- User Behavior
- Failed Login Attempts

The AI engine calculates a Risk Score. Transactions are classified into:

- Low Risk
- Medium Risk
- High Risk

High-risk transactions are rejected automatically.

Step 5: Approved transactions are validated through blockchain. Transaction details are converted into cryptographic hashes before storage.

Blockchain guarantees:

- Data Integrity

- Tamper Resistance
- Transparency

Step 6: IoT sensors continuously monitor banking devices.

The monitoring module supervises:

- Smart ATM
- RFID Devices
- CCTV
- Smart Payment Devices
- Environmental Sensors
- Device Status

Alerts are generated whenever abnormal activities are detected.

7. Proposed Authentication Algorithm

The proposed Secure Intelligent Banking Authentication Framework performs authentication through multiple independent verification stages.

Input:

Banking Transaction Request

Output:

Transaction Approved / Rejected

Begin

Receive Banking Request → Verify Aadhaar Identity

If Aadhaar Verification = Failed

    Reject Transaction

Else

    Capture Biometric Sample

    Match Biometric Template

    If Match = Failed

        Reject Transaction

    Else

        Execute AI Fraud Detection

        Calculate Risk Score

        If Risk = High

            Reject Transaction

        Else

Generate Blockchain Hash

Validate Transaction

Store Transaction Record

Monitor IoT Devices

If Device Status = Normal

Approve Transaction

Else

Reject Transaction

End If

End If

End If

End If

End

The proposed algorithm ensures that authentication cannot be bypassed by compromising any single security layer. The proposed algorithm's working is shown in the following diagrams (figure 2 and figure 3).

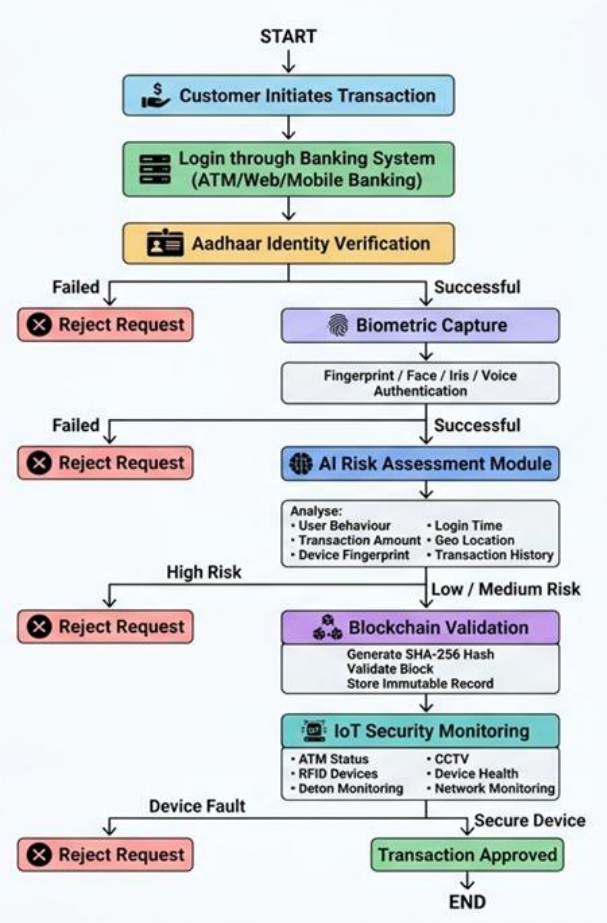


Figure 2

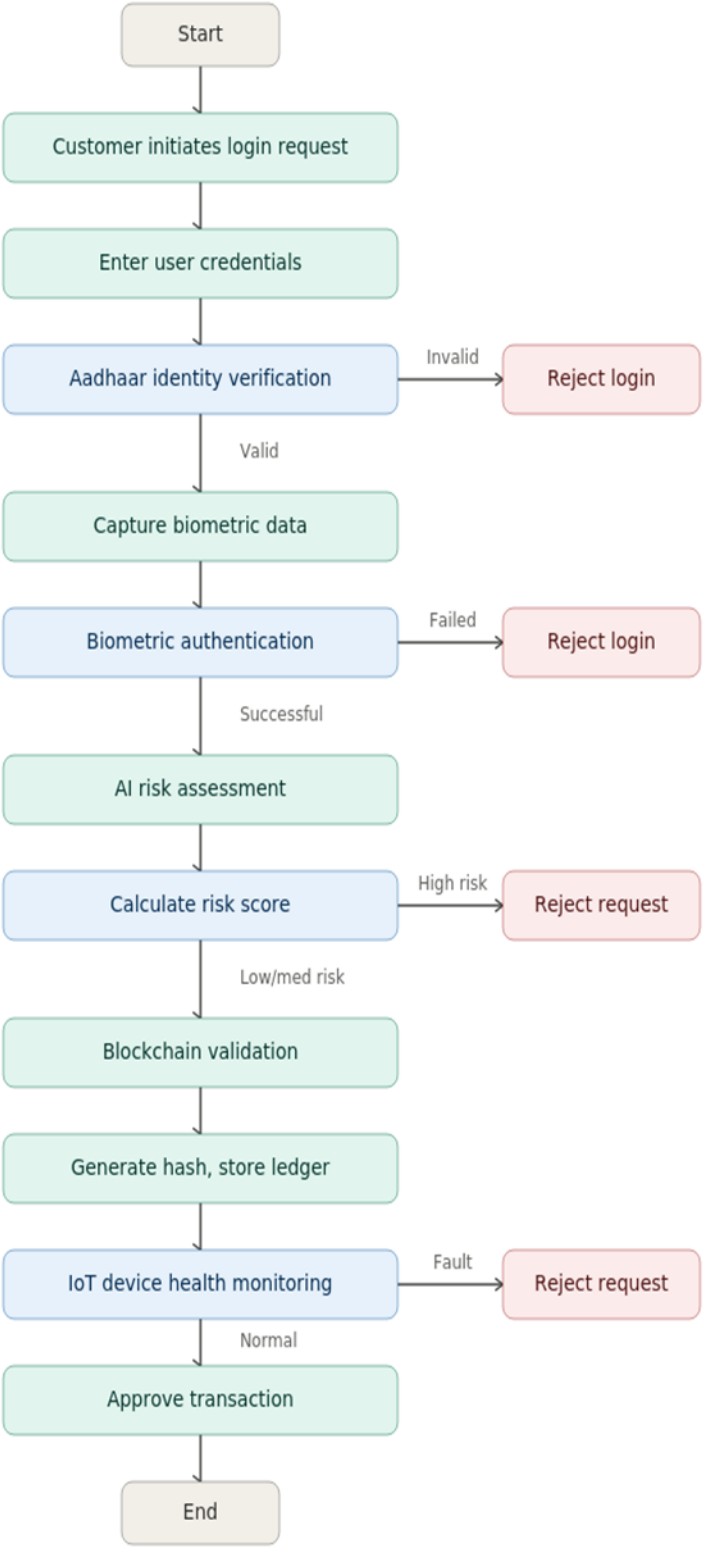

Start
Customer initiates login request
Enter user credentials
Aadhaar identity verification
Invalid
Reject login
Valid
Capture biometric data
Biometric authentication
Failed
Reject login
Successful
AI risk assessment
Calculate risk score
High risk
Reject request
Low/med risk
Blockchain validation
Generate hash, store ledger
IoT device health monitoring
Fault
Reject request
Normal
Approve transaction
End

Figure 3

8. Artificial Intelligence-Based Fraud Detection Module:

Artificial Intelligence serves as the decision-making engine of the proposed authentication framework. Unlike conventional rule-based fraud detection systems, AI continuously analyses customer behavior and transaction characteristics before financial authorization.

The AI engine evaluates multiple parameters, including:

- Transaction Amount
- Login Frequency
- Device Fingerprint
- Customer Behavior
- Geographical Distance
- IP Address
- Time of Transaction
- Previous Spending Pattern
- Failed Authentication Attempts
- Beneficiary Details

Machine Learning algorithms identify behavioural deviations by comparing current transaction characteristics with historical customer profiles. The AI module computes a dynamic **Risk Score (RS)**.

Risk Classification

Risk Score	Decision
0 – 30	Low Risk – Transaction Approved
31 – 70	Medium Risk – Additional Verification Required
71 – 100	High Risk – Transaction Blocked

The AI model continuously updates its knowledge using newly generated transaction data, thereby improving fraud detection performance over time.

9. Blockchain-Based Transaction Validation Module

Blockchain technology enhances banking security by maintaining an immutable transaction ledger. Each successful authentication generates a blockchain block containing:

- Customer ID
- Transaction ID
- Authentication Status
- Timestamp
- Previous Block Hash
- Current Block Hash
- Digital Signature
- Device Identifier

The blockchain process consists of the following steps:

1. Generate Transaction Record.
2. Compute SHA-256 Hash.
3. Link the Current Block with the Previous Block.
4. Digitally Sign the Transaction.
5. Append the Block to the Distributed Ledger.
6. Verify Ledger Integrity.

Because each block contains the cryptographic hash of the previous block, unauthorized modification of transaction records becomes computationally infeasible.

The blockchain module provides the following security benefits:

- Immutable Authentication Records
- Transaction Integrity
- Digital Audit Trail
- Non-Repudiation
- Protection Against Insider Attacks
- Tamper-Proof Financial Logs
- Enhanced Customer Trust

10. Integration of AI and Blockchain

The proposed framework combines Artificial Intelligence and Blockchain to provide intelligent and secure banking authentication.

Artificial Intelligence performs:

- Behavioural Analysis
- Fraud Detection
- Risk Prediction
- Transaction Classification

Blockchain performs:

- Transaction Validation
- Immutable Record Storage
- Cryptographic Verification
- Distributed Audit Logging

The interaction between these technologies enables intelligent decision-making while ensuring that every approved transaction is permanently recorded in a secure and tamper-resistant ledger.

The integrated architecture significantly strengthens banking authentication by combining predictive intelligence with cryptographic security, thereby reducing financial fraud, unauthorized access, and transaction manipulation.

11.1 Performance Evaluation

The proposed Secure Intelligent Banking Authentication Framework (SIBAF) was conceptually evaluated by comparing it with commonly used banking authentication mechanisms. The comparison focuses on the security capabilities of each authentication approach rather than measured implementation performance.

The following evaluation parameters were considered:

- Identity Verification
- Authentication Strength
- Fraud Detection Capability
- Resistance to Cyber Attacks
- Transaction Integrity
- Infrastructure Monitoring
- Scalability
- Transparency
- Overall Security

11.2 Comparative Analysis

Security Feature	Password	OTP	MFA	Biometrics	Proposed SIBAF
Password Security	Medium	High	High	Excellent	Excellent
Identity Verification	Low	Medium	High	High	Excellent
Biometric Authentication	✗	✗	Optional	✓	✓
Aadhaar Verification	✗	✗	✗	✗	✓
AI Fraud Detection	✗	✗	✗	✗	✓
Blockchain Security	✗	✗	✗	✗	✓
IoT Monitoring	✗	✗	✗	✗	✓
Tamper Resistance	Low	Medium	Medium	High	Excellent
Real-Time Risk Assessment	✗	✗	Limited	Limited	✓
Transaction Transparency	Low	Medium	Medium	Medium	Excellent

Table 1. Comparison of Existing Authentication Mechanisms and the Proposed SIBAF Framework

The comparison demonstrates that conventional authentication techniques generally rely on one or two security mechanisms, whereas the proposed SIBAF framework combines multiple complementary technologies into a unified security architecture.

11.3 Security Analysis

The proposed framework improves banking security through multiple independent verification layers.

Protection Against Phishing Attacks: Even if customer credentials are compromised through phishing, attackers cannot complete authentication without successful biometric verification and AI-based behavioural validation.

Protection Against Identity Theft: The integration of Aadhaar verification with biometric authentication significantly reduces the possibility of identity impersonation.

Protection Against Biometric Spoofing: The incorporation of liveness detection techniques reduces the effectiveness of fake fingerprints, facial images, and replay attacks.

Protection Against Insider Attacks: Blockchain-based immutable transaction records prevent unauthorized modification or deletion of authentication logs by internal users.

Protection Against Transaction Manipulation: Every transaction is cryptographically linked within the blockchain ledger, making unauthorized modification computationally impractical.

Intelligent Fraud Detection: Artificial Intelligence continuously analyses customer behaviour, transaction history, device characteristics, and login patterns to detect suspicious activities before transaction authorization.

Infrastructure Security: IoT-enabled monitoring provides continuous surveillance of ATMs, biometric devices, payment terminals, RFID readers, and communication networks, enabling rapid identification of operational anomalies.

12. Results and Discussion

The proposed Secure Intelligent Banking Authentication Framework (SIBAF) integrates multiple security technologies to strengthen authentication within digital banking environments. Unlike conventional banking authentication systems that rely primarily on passwords or OTP verification, the proposed model adopts a multi-layer authentication strategy incorporating Aadhaar-based identity verification, biometric authentication, Artificial Intelligence-driven fraud detection, blockchain-enabled transaction validation, and IoT-assisted infrastructure monitoring.

The conceptual evaluation indicates that combining complementary security mechanisms improves overall authentication reliability while reducing dependence on any single verification factor. Biometric authentication enhances identity assurance, Aadhaar verification provides trusted identity validation within the Indian banking ecosystem, Artificial Intelligence contributes adaptive fraud detection capabilities, blockchain ensures immutable transaction records, and IoT devices strengthen infrastructure monitoring.

The proposed architecture also offers improved transparency and accountability because authentication events are permanently recorded within a blockchain ledger. This feature supports auditing, dispute resolution, and regulatory compliance.

Furthermore, the modular design allows additional authentication technologies to be integrated in future without significant modification of the overall framework. Consequently, the proposed architecture is suitable for deployment in evolving digital banking environments where new cyber threats continuously emerge.

Although the present work focuses on conceptual framework development, future implementation and performance evaluation using real banking datasets would provide quantitative evidence regarding authentication accuracy, fraud detection effectiveness, computational overhead, and transaction latency.

13. Conclusion

Digital banking continues to transform financial services by providing customers with fast, convenient, and accessible transaction platforms. However, this transformation has simultaneously increased exposure to sophisticated cyber threats, including identity theft, phishing, credential compromise, insider attacks, financial fraud, and transaction manipulation.

This paper proposed the **Secure Intelligent Banking Authentication Framework (SIBAF)**, a multi-layer authentication architecture integrating Aadhaar-based identity verification, biometric authentication, Artificial

Intelligence-based fraud detection, blockchain transaction validation, and Internet of Things-enabled infrastructure monitoring.

The proposed framework addresses several limitations of conventional authentication mechanisms by combining multiple complementary security technologies into a unified authentication process. Aadhaar verification establishes trusted identity, biometric authentication strengthens user verification, Artificial Intelligence provides intelligent behavioural analysis and fraud detection, blockchain guarantees immutable transaction records, and IoT devices continuously monitor banking infrastructure.

A conceptual comparison with existing authentication mechanisms indicates that the proposed framework offers broader security coverage, stronger transaction integrity, improved fraud resistance, and enhanced transparency. The modular architecture further supports future technological enhancements while maintaining compatibility with modern digital banking systems.

The proposed framework provides a practical foundation for developing secure, scalable, and intelligent banking authentication systems capable of supporting next-generation financial services.

14. Future Work

Future research may focus on implementing and experimentally validating the proposed framework using simulated or real-world banking environments. Additional work may include:

- Development of a prototype using cloud-based banking infrastructure.
- Integration of deep learning models for adaptive fraud detection.
- Performance benchmarking using real transaction datasets.
- Comparative analysis with Zero Trust Architecture-based authentication.
- Evaluation of computational overhead and transaction latency.
- Integration with Central Bank Digital Currency (CBDC) platforms.
- Privacy-preserving biometric template protection using advanced cryptographic techniques.
- Investigation of quantum-resistant cryptographic algorithms for future banking systems.

References

[1] M. Khan, D. Pesavento, and L. Benmohamed, "Blockchain-Based Decentralized Authentication for Information-Centric 5G Networks," *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, 2022.

[2] M. Ghafourian, B. Sumer, R. Vera-Rodriguez, J. Fierrez, R. Tolosana, A. Moralez, and E. Kindt, "Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis," 2023.

[3] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," 2024.

[4] Y. Liu et al., "Machine Learning Techniques for Financial Fraud Detection: A Review," *Expert Systems with Applications*.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed., Pearson.

[6] A. K. Das, M. Wazid, and N. Kumar, "Secure Authentication Protocols for IoT Applications: A Survey," *IEEE Communications Surveys & Tutorials*.

[7] R. Jain, A. Ross, and K. Nandakumar, *Introduction to Biometrics*, Springer.

[8] M. Ebrahim, A. Hafid, and E. Elie, "Blockchain as Privacy and Security Solution for Smart Environments: A Survey," 2022.

[9] K. Modi and L. Devaraj, "Advancements in Biometric Technology with Artificial Intelligence," 2022.

[10] Reserve Bank of India, *Master Directions on Digital Payment Security Controls*.

[11] Unique Identification Authority of India (UIDAI), *Aadhaar Authentication API Specification*.

[12] National Payments Corporation of India (NPCI), *Unified Payments Interface (UPI) Procedural Guidelines*.

[13] PCI Security Standards Council, *PCI DSS v4.0 Requirements and Security Assessment Procedures*.

[14] European Union, *General Data Protection Regulation (GDPR)*.

[15] M. Usama et al., "Blockchain-Enabled Identity Management for IoT: A Multi-Layered Defense Against Adversarial AI," *Scientific Reports*, vol. 16, 2026.

[16] G. Iswarya and C. Vennila, "A Secure and Scalable Blockchain-Assisted Authentication Framework for Decentralized IoT Data Management," *Scientific Reports*, vol. 16, 2026.

[17] M. Y. Ibrahim, K. I. Musa, A. Ahmad, et al., "A Blockchain IoT Framework for Secure Digital Banking with Simulation and Consensus Mechanism Evaluation," *Discover Networks*, 2026.

[18] R. Latif et al., "BBAS: A Blockchain-Based Authentication System for e-Health with Multi-Factor Authentication, Access Control, and Post-Quantum Security," *Scientific Reports*, vol. 16, 2026.

[19] M. Natampalli et al., "Multisecurity GAN-Steganography-Blockchain for IoT-Cloud Self-Service Banking," *Journal on Internet of Things*, vol. 8, no. 1, pp. 1–30, 2026.

[20] H. N. Ali and S. S. M. Al-Dabbagh, "A Systematic Literature Review on Biometric Authentication in Mobile Banking," *F1000Research*, 2026.

[21] I. Rjab and L. Sliman, "Survey on Biometric Authentication for Decentralized Identity Management: Trends, Challenges, and Future Directions," *Future Internet*, 2026.

[22] "Securing and Classification of Active Directory Domain Banking Data Using the Integration of Blockchain and Artificial Intelligence," *Engineering Applications of Artificial Intelligence*, 2026.