IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, September 2026
Impact Factor: 8.2

Homomorphic Encryption and Secure Multiparty Computation in Banking

Nirooj Fidin
Senior Manager (IT)
Union Learning Academy – Digital Transformation, Union Bank of India, Mumbai, India

Abstract: *The rise in cyber frauds and data breaches has exposed the limitations of traditional password-based authentication. As organizations move toward a more secure and user-friendly identity management system, passwordless authentication emerges as a promising alternative. This report presents a comprehensive analysis of passwordless authentication systems, their underlying technologies, deployment challenges, and possible innovations. It evaluates various methods such as biometrics, public key infrastructure, and device-based authentication, offering a step-by-step implementation guide while addressing usability, cost, and security trade-offs.*

Keywords: Artificial Intelligence (AI), Rural Banking, Financial Inclusion, Alternative Credit Scoring, Conversational Banking, Digital Literacy, Vernacular Interfaces, AI in Agriculture, Voice-Based Financial Services, Multilingual NLP, Financial Advisory Systems, Fraud Detection, Inclusive Finance, AI in Fintech, Explainable AI

I. INTRODUCTION

The financial services landscape in India is currently navigating a pivotal transformation, characterized by the dual pressures of aggressive digital expansion and the tightening of data sovereignty regulations. For a bank that seeks to establish itself as a "Digital Bank within a Bank," the historical trade-off between utilizing data for innovation and maintaining absolute privacy has reached a critical inflection point. The emergence of Privacy-Enhancing Technologies (PETs), specifically Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMPC), offers a paradigm shift. These cryptographic frameworks permit the processing and analysis of sensitive information while it remains in an encrypted state, thereby ensuring that data is protected not only at rest and in transit but also during its most vulnerable phase: in use.

II. RESEARCH OBJECTIVES

1. To explore the applications of homomorphic encryption and secure multiparty computation in a bank
2. To explore implementation strategies for a bank

III. METHODOLOGY

The research methodology would involve a thorough analysis of publicly available documentation on HE (Homomorphic Encryption) and SMPC (Secure Multi Party Computation) standards. Based on findings, develop deployment recommendations, strategies, and directions for future implementation

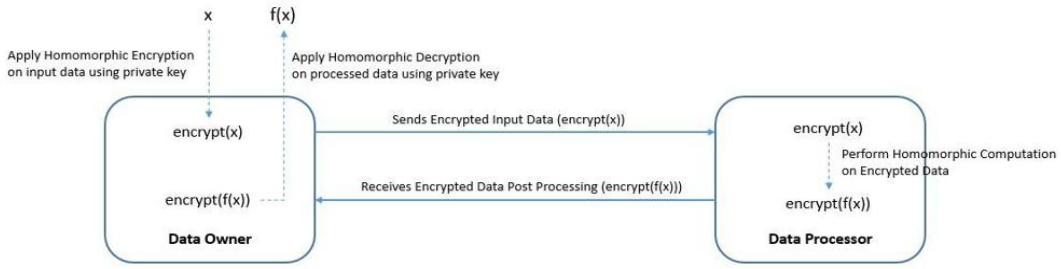
IV. DATA ANALYSIS

4.1 CURRENT CYBERSECURITY SCENARIO IN INDIAN BANKS

The foundation of secure digital banking has traditionally relied on symmetric and asymmetric encryption standards such as Advanced Encryption Standard (AES)-256 and Rivest-Shamir-Adleman (RSA). Typically, AES-256 is a symmetric algorithm, meaning it uses the same secret key for both encryption and decryption while RSA is an asymmetric algorithm, using a mathematically linked pair: a public key for encryption and a private key for decryption. In modern systems like HTTPS/TLS or secure messaging, these two are often used together in a hybrid

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, September 2026
Impact Factor: 8.2

encryption model. RSA is used to securely "handshake" and exchange a temporary, random AES session key. Then AES-256 is used to encrypt the actual data stream or file, providing the speed necessary for a smooth user experience. While these are sufficient for securing data storage and transmission, they necessitate decryption before any computational operation can be performed. This requirement creates a "decryption window" where raw data is exposed in a system's memory, making it susceptible to side-channel attacks, memory scrapers, and insider threats.



The Reserve Bank of India (RBI) has implemented comprehensive cybersecurity mandates, including the Master Directions on Cyber Resilience and Digital Payment Security Controls (July 2024), requiring extensive security measures for banks and other financial institutions. The key RBI requirements are**:**

a. **Zero Trust Architecture (ZTA)** - Moving from perimeter-based defense to assume-breach mentality
b. **24/7 Security Operations Centers (SOCs)** - Real-time threat monitoring and response
c. **Board-level accountability** - Senior executives directly responsible for cybersecurity
d. **Data localization** - Sensitive customer data must remain within India
e. **Continuous surveillance** - Real-time monitoring and threat intelligence sharing
f. **Cyber resilience drills and audits** - Regular simulation of large-scale attacks alongwith security assessments and penetration testing
g. **Data Classification**: Mandatory categorization of sensitive information
h. **Minimum Encryption Standard:** 128-bit SSL/TLS for internet banking

The major vulnerabilities identified by RBI are:

- Lack of IT governance framework
- Absence of real-time end-user monitoring
- Inadequate authentication mechanisms
- Insufficient privileged credentials management
- Absence of fine-grained access controls
- Third-party vendor security gaps

4.1.1 CURRENT ENCRYPTION STANDARDS IN INDIAN BANKS

Indian financial institutions are required to implement Advanced Encryption Standard (AES) or RSA encryption for data at rest and in transit, with direct control of encryption keys in line with RBI and DPDPA standards. When it comes to data stored inside bank systems, also known as data at rest, the most widely used standard is AES with 256 bit strength, often referred to as AES 256. A 256 bit strength implies that there are 2^{256} possible combinations, roughly a number of 78 digits long. Banks apply this protection at multiple levels. Entire hard drives may be encrypted, meaning everything stored on them is automatically secured. Individual files can also be encrypted, as well as specific databases where customer records and transaction details are kept. In addition, endpoint security measures protect devices such as employee computers and servers, ensuring that even the machines accessing the data are safeguarded.

For data that is moving between systems, such as when someone logs in to their online banking account, a different layer of protection is used. This is known as data in transit. Banks rely on Transport Layer Security, or TLS, typically version

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

1.2 or 1.3, which creates a secure channel between the browser and the bank's server. Earlier forms of Secure Sockets Layer, or SSL, are used for server authentication to verify that communication is with the bank and not an impostor. Communication between browsers and servers must use at least 128 bit encryption. RSA encryption with 2048 bit keys or higher is commonly used to help securely exchange encryption keys. In many cases, client side certificates are also required, which act like digital identity cards to confirm that both parties in a transaction are genuine.

Another crucial aspect of encryption is key management. Encryption works only if the keys that unlock the data are kept safe. Indian banks typically use Hardware Security Modules, or HSMs, which are specialized physical devices designed to securely generate, store, and manage encryption keys. These devices often comply with international standards such as FIPS 140 2 Level 3, which sets strict security requirements. Banks also follow key rotation policies, meaning encryption keys are changed periodically to reduce the risk of compromise. Centralized key management systems help monitor and control all keys in one place, and importantly, encryption keys are stored separately from the encrypted data. This separation ensures that even if someone gains access to the data, they cannot easily obtain the keys needed to unlock it.

4.2 HOMOMORPHIC ENCRYPTION

Homomorphic Encryption represents a category of algorithms that allow operations on ciphertexts to produce an encrypted result that, when decrypted, matches the result of operations performed on the plaintexts. This property is mathematically represented as a map between two algebraic systems that preserves their structure. Homomorphic encryption is categorized based on the complexity and volume of operations it supports. This taxonomy is critical when selecting schemes for specific banking workloads.

4.2.1 Partially Homomorphic Encryption (PHE): These schemes support only one type of operation—either addition or multiplication—infinitely. Because of its simplicity, this method is very fast and efficient. However, it cannot handle complex tasks.

A. **Example (Additive PHE):**Let's say we want to calculate the **total salary** of two employees without seeing their actual salaries.

- We encrypt:
- Alice's salary: E(50,000)
- Bob's salary: E(60,000)

B. We compute:
E(50,000) ⊕ E(60,000) = E(110,000)

C. When we decrypt, we get 110,000**, without ever seeing individual amounts.**

4.2.2 Somewhat Homomorphic Encryption (SHE): These schemes support both addition and multiplication but are limited to a fixed number of operations. Every operation introduces "noise" into the ciphertext. If the noise grows too large, the decryption process fails, rendering the data gibberish.

Example**:** Let's say we want to calculate tax payable i.e. (Income – Deductions) × Tax Rate.

Encrypted values:

- Income: E(20,00,000)
- Deductions: E(5,00,000)
- Tax Rate: E(30%)

Steps:

a. Subtract: E(20,00,000) – E(5,00,000) = E(15,00,000)
b. Multiply: E(15,00,000) × E(0.30) = E(4,50,000)

We decrypt and get 4,50,000.

The catch: We can do this only a few times. The encryption "gets tired" due to noise buildup.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

4.2.3 Fully Homomorphic Encryption (FHE): Introduced as a practical concept in 2009 by Craig Gentry, FHE enables arbitrary computations on encrypted data by introducing a process called "bootstrapping." Bootstrapping effectively "refreshes" the ciphertext by running the decryption circuit homomorphically, thereby resetting the noise levels and allowing for infinite computational depth. However, because of the repeated reset process, it is much slower than the other schemes.

Example: Predicting a Loan Default

We have an encrypted machine learning model and encrypted customer data:

- Income: E(45,000)
- Credit Score: E(700)
- Loan Amount: E(1,50,000)

The model computes a function like:

E(Model(Income, CreditScore, LoanAmount)) → E(Default Risk = 0.12)

The model calculates everything without decrypting any input or the model itself. Only the decrypted final output is visible to the user.

Type	What It Supports	Example Use	Limitation
PHE	Only *one* operation (add or multiply)	Add encrypted salaries	Can't do both add & multiply
SHE	Limited additions + multiplications	Simple formulas like (a + b) × c	Breaks down after a few steps
FHE	Unlimited complex computations	ML model on encrypted data	Computationally expensive

4.3 SECURE MULTI-PARTY COMPUTATION

While HE focuses on securing outsourced computation to a single party (e.g., a cloud provider), Secure Multi-Party Computation (SMPC) facilitates a decentralized trust model. SMPC enables multiple entities to jointly compute a function over their collective private inputs without any entity gaining access to the inputs of others.

4.3.1 Core Protocols and Security Models

SMPC protocols are primarily built upon the following frameworks:

D. Secret Sharing: A value is divided into multiple "shares" and distributed across participants. No single participant holds a meaningful piece of data, but they can perform mathematical operations on their shares. The final result is only revealed when a defined threshold of participants combines their processed shares.

E. Example**:** Three departments in a bank want to compute the total exposure to a borrower, without revealing their individual values.

- Department A: ₹10 lakh
- Department B: ₹8 lakh
- Department C: ₹12 lakh

Each department splits its number into **3 shares** (randomly) and sends one to each computation node.

- Dept A: (3, 4, 3) → 3+4+3 = 10
- Dept B: (2, 3, 3) → 2+3+3 = 8
- Dept C: (4, 5, 3) → 4+5+3 = 12

Each node receives one share from each department:

- Node 1 gets: 3 + 2 + 4 = 9
- Node 2 gets: 4 + 3 + 5 = 12
- Node 3 gets: 3 + 3 + 3 = 9

Sum of all: 9 + 12 + 9 = 30 → Total exposure = ₹30 lakh

Thus, No department reveals its original data**,** but the combined result is correct**.**

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

F. Garbled Circuits: A function is represented as a Boolean circuit where the truth tables are encrypted. One party "garbles" the circuit and another evaluates it using oblivious transfer, ensuring that neither party learns the other's input.

G. Example**:** Bank A has a credit card eligibility formula: "Approve if (income > ₹50,000 AND credit score > 700)"
Bank B has a customer whose income is ₹60,000 and credit score is 720.
How It Works:

1. Bank A converts its logic into a garbled circuit (encrypts it).
2. Bank B inputs encrypted values into the circuit.
3. Output is evaluated privately: Loan Approved

Even though Bank A never sees the input, and Bank B never sees the logic.This protects model IP and customer privacy simultaneously.

H. Oblivious Transfer: Oblivious Transfer is a protocol where a sender has multiple pieces of data and the receiver wants to access just one of those entries. The receiver accesses only that one piece without the sender knowing one was accessed.

I. Example: Bank B wants to check if a customer (account number: AC123) appears in Bank A's sanctions list without revealing the account number to Bank A.
Bank A's sanctions list: AC101: flagged, AC123: flagged, AC555: clean
Steps Using OT:

1. Bank A encrypts the list: E(AC101), E(AC123), E(AC555)
2. Bank B uses OT to privately select the 2nd entry (which corresponds to AC123)
3. Bank B receives flagged status.

Outcome: Bank B learns that AC123 is sanctioned without Bank A not knowing which account was queried.

J. Private Set Interaction: Private Set Intersection is a protocol where two (or more) parties compare their datasets to find common elements, but each party only learns the intersection (matching entries) but everything else remains hidden.
Example: Two banks want to collaborate to catch fraudsters, but can't share entire customer lists due to privacy laws.

- Bank A's suspicious list: AC001, FRAUD123, AC003
- Bank B's suspicious list: FRAUD123, AC777, AC003

Using PSI, they discover the intersection of their list (FRAUD123, AC003). Thus, Banks can take action on shared bad actors and individual customer privacy is protected

SMPC Type	Formal Definition	Banking Use Case	Simplified Calculation or Logic
Secret Sharing	Data is split into shares and distributed	Total borrower exposure	Split ₹10L into 3 shares like (3,4,3) and sum shares securely
Garbled Circuits	Encrypted function logic + encrypted inputs	Loan approval logic	Evaluate encrypted circuit: Is ₹60K > ₹50K & 720 > 700?
Oblivious Transfer	Receiver picks 1 of N values without sender knowing which	IBAN sanction check	Learn if AC123 is flagged without revealing query
Private Set Intersection	Reveal only overlapping data between sets	Shared fraud detection	Intersection: FRAUD1 from two encrypted account lists

4.4 HOMOMORPHIC ENCRYPTION VS SECURE MULTI PARTY COMPUTATION

Dimension	HE	SMPC
Decryption	Required by data owner	Not required; result known to parties
Communication	Minimal (non-interactive)	Higher (multi-round protocols)
Overhead	Extreme (100,000x+)	Moderate (10-100x)
Infrastructure	Centralized (cloud/aggregator)	Distributed (peer-to-peer networks)
Use Case	Privacy-preserving analytics	Collaborative computation without trusted intermediary

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

4.5 REGULATORY IMPACT

The adoption of HE and SMPC is not merely a technical choice but a mandatory evolution necessitated by the Digital Personal Data Protection (DPDP) Act of 2023 and the proactive stance of the Reserve Bank of India (RBI).

Implications of the DPDP Act 2023

The DPDP Act establishes privacy as a fundamental right and imposes significant responsibilities on "Data Fiduciaries".

- **Consent and Purpose Limitation:** Data can only be processed for specific purposes for which consent is obtained. PETs (Privacy Enhancing Technologies) allows banks to process data for these purposes (like credit scoring) without exposing the data to ancillary risks, thereby fulfilling the "Data Minimization" principle.
- **Reasonable Security Safeguards:** The Act mandates that fiduciaries implement technical measures to prevent breaches. HE and SMPC provide a "privacy by design" framework that effectively renders data useless to an attacker even if a breach occurs, as the data remains encrypted during processing.
- **Cross-Border Data Flows:** Section 16 of the Act allows for data transfer unless a country is blacklisted. However, local regulations often favor data stay. HE provides a mathematical solution where the data physically resides in India, but the *computation* is outsourced to global cloud centers, preserving sovereignty.

4.6 IMPLEMENTATION CASES

4.6.1. Intesa Sanpaolo & IBM – Cryptocurrency Transaction Validation

Implementation Case: Italy's largest bank worked with IBM to test Fully Homomorphic Encryption, or FHE. FHE is a special type of encryption that allows computers to perform calculations on data while it is still encrypted, meaning the data never has to be unlocked or revealed. The project focused on validating cryptocurrency transactions without exposing confidential transaction details.

Use: The system was used to verify cryptocurrency wallet addresses and balances securely without revealing the actual wallet details. A cryptocurrency wallet address is similar to a bank account number, and the wallet balance represents the amount of digital currency stored. Using Fully Homomorphic Encryption, the bank could confirm whether a wallet had sufficient funds or whether it appeared on a fraud blacklist, without ever viewing the real address or balance. This allowed secure validation of third-party cryptocurrency transactions while maintaining full privacy. It ensured compliance checks, fraud prevention, and transaction verification could be performed without exposing sensitive financial data, which is especially important when interacting with external cryptocurrency platforms.

Approach:

- Used IBM's HElayers Software Development Kit, which is a toolkit for building applications with homomorphic encryption, along with multiparty FHE, meaning multiple parties could collaborate on encrypted data without revealing their private inputs.
- Performed encrypted checks against blacklists, which are lists of suspicious or blocked wallet addresses, and verified wallets while the data remained encrypted.
- Integrated with a Web3 wallet interface, referring to blockchain-based digital wallets, and used Graphics Processing Units (GPUs), which are high-performance computer chips typically used for graphics or artificial intelligence, to speed up processing.

Outcomes:

- Processed a blacklist containing 32,000 records in under 22 seconds.
- Memory usage increased in a predictable, linear way as data size grew, and performance was 10 times faster when GPUs were used.
- Demonstrated that FHE is practical for real banking transaction environments.

4.6.2. Mastercard – Cross-Border Fraud Detection (Singapore, 2024)

Implementation Case: Mastercard tested an FHE-based fraud detection system across four countries. The goal was to allow banks to share intelligence about suspicious activity without physically transferring sensitive customer data across borders, which could violate privacy laws.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

Use: The system was designed to detect fraudulent International Bank Account Numbers (IBANs), which are unique identifiers for bank accounts used in international transactions, without exposing the actual account numbers. Fraudsters often move money across countries to avoid detection, and traditional methods require sharing sensitive account data, which can violate privacy laws. Using homomorphic encryption, banks could check whether an IBAN was associated with fraud while keeping the account number encrypted. This allowed financial institutions in different countries to collaborate and identify suspicious accounts without revealing customer information, improving fraud detection while maintaining compliance with data protection regulations.

Approach:

- Used lattice-based, quantum-safe FHE encryption. Lattice-based cryptography is a mathematical approach believed to resist attacks from future quantum computers.
- Performed encrypted IBAN risk checks, meaning the account number remained hidden during analysis, and only the originating country could decrypt results.
- Ensured compliance with each country's data protection regulations.

Outcomes:

- Successfully detected cross-border fraud patterns.
- No IBAN numbers or related background data were exposed.
- Complied with data protection laws such as the Personal Data Protection Act in Singapore, the California Consumer Privacy Act in the United States, and the United Kingdom General Data Protection Regulation.
- System was considered ready for full production use within 6 to 12 months.

4.6.3. Bank for International Settlements Project Aurora – Cross-Border Anti-Money Laundering Detection

Implementation Case: Project Aurora was a global central banking initiative that tested Privacy Enhancing Technologies, or PETs. These are tools designed to protect sensitive data during analysis. The project used homomorphic encryption and secure multiparty computation, which allows multiple institutions to compute results together without sharing their raw data, to identify complex money laundering patterns using artificial intelligence.

Use: The system enabled banks and financial institutions to detect money laundering patterns by analyzing encrypted transaction data across multiple organizations. Money laundering often involves moving illegal funds through several banks and countries, making it difficult to detect when institutions work independently. Using homomorphic encryption and secure multiparty computation, institutions could analyze combined encrypted data without sharing the original transaction details. This allowed detection of suspicious transaction chains and coordinated financial crime while ensuring customer privacy and regulatory compliance.

Approach:

- Used synthetic datasets, which are artificial data designed to mimic real anti-money laundering behavior without using real customer information.
- Compared three models: isolated institutional data (siloed), national-level pooled data, and cross-border combined analysis.
- Applied homomorphic encryption, secure multiparty computation, differential privacy (a technique that adds statistical "noise" to protect individual identities), federated learning (where models are trained locally and only updates are shared), and graph machine learning, which studies relationships between entities such as accounts and transactions.

Outcomes:

- Detected 40 percent more money laundering patterns in cross-border models compared to isolated systems.
- Artificial intelligence models performed better than traditional rule-based systems that rely on fixed conditions.
- Privacy-enhancing technologies enabled secure and scalable analysis. Considered viable for implementation within 18 to 24 months.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

4.6.4. Zama TFHE + Concrete ML – Privacy-Preserving Graph Machine Learning for Anti-Money Laundering

Implementation Case: Researchers from academia and industry developed a graph-based anti-money laundering detection system using TFHE, which stands for "Fast Fully Homomorphic Encryption over the Torus," a specific method of FHE optimized for speed, along with open-source machine learning tools.

Use: The system analyzed encrypted transaction networks to detect illegal financial behavior. Transaction networks form patterns showing how money moves between accounts, and these patterns can reveal fraud or money laundering activity. Using homomorphic encryption, the machine learning model could detect suspicious patterns such as unusual fund transfers or coordinated account activity without decrypting the data. This enabled accurate fraud detection while ensuring that sensitive financial information remained confidential.

Approach:

- Used the AMLworld dataset, which is a synthetic financial transaction generator and dataset designed for developing and benchmarking (AML) detection models. It was introduced in a 2023 paper to address the critical shortage of publicly available, high-quality labeled financial data for security research and contains between 15,000 and 50,000 transactions.
- Converted and simplified the XGBoost model through a process called quantization, which reduces numerical precision to make encrypted computation feasible, and then compiled it into FHE circuits, meaning it was transformed into a form that could operate on encrypted data.
- Analyzed network features such as scatter-gather patterns (how funds move between accounts) and fan-in or fan-out behavior (how many accounts send to or receive from a single account).

Outcomes:

- Achieved 99.7 percent accuracy and strong F1-scores, which is a metric used to evaluate a model's accuracy by balancing two competing factors: Precision and Recall. It is especially critical when working with imbalanced datasets—like the AMLworld dataset where one class (e.g., legitimate transactions) vastly outnumbers another (e.g., money laundering).
- Improved fraud detection by 26 percent for rare fraud cases in imbalanced datasets, where legitimate transactions far outnumber fraudulent ones.
- Processing was 100,000 times slower than normal computation, making it suitable for batch analysis rather than instant decisions.
- Demonstrated that open-source homomorphic encryption tools are technically feasible.

4.6.5. JPMorgan Chase & Industry – Federated Learning for Fraud Detection

Implementation Case: JPMorgan and a consortium of banks implemented federated learning, a technique where multiple organizations collaboratively train a machine learning model without sharing their raw data.

Use: The system allowed multiple banks to jointly improve fraud detection models without sharing customer data. Normally, larger datasets improve fraud detection accuracy, but privacy laws prevent banks from sharing transaction data directly. Using federated learning, each bank trained the model locally and shared only learned patterns, not the actual data. This allowed banks to benefit from shared intelligence while keeping all customer information private and secure.

Approach:

- Each bank trained the model using its own local data.
- Model updates were combined using Federated Averaging, or FedAvg, which averages model parameters rather than pooling raw data.
- Anonymised updates by adding statistical noise, ensuring that individual customer data could not be reconstructed.
- No customer data left the originating institution.

Outcomes:

- Maintained high model accuracy.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

- Complied with regulatory requirements such as those of the Reserve Bank of India, the General Data Protection Regulation in Europe, and the California Consumer Privacy Act.
- Required relatively low computing resources and scaled effectively across institutions.
- Particularly suitable for training models, and can be combined with homomorphic encryption for secure model usage during prediction.

4.6.6. HSBC & The Alan Turing Institute – Homomorphic Encryption Research for Financial Crime

Implementation Case: HSBC collaborated with academic researchers to identify practical and regulator-approved use cases for homomorphic encryption in financial crime detection.

Use: This research explored how homomorphic encryption could be used to detect financial crimes such as money laundering while preserving data privacy. Financial crime detection often requires analyzing large amounts of transaction data across institutions and countries. Homomorphic encryption allows this analysis to be performed while the data remains encrypted, enabling regulators and banks to identify suspicious financial patterns without exposing sensitive customer information.

Approach:

- Emphasized alignment with regulators to ensure that solutions met legal and compliance standards.
- Studied strategies for deploying homomorphic encryption tools in large enterprise banking environments.

Outcomes:

- Demonstrated that homomorphic encryption is viable for anti-money laundering analytics.
- Confirmed strong industry interest in deploying scalable encrypted analytics across global banking networks.

4.6.7. UK Finance & OmniIndex – Real-Time Encrypted Fraud Dashboards

Implementation Case: UK Finance and OmniIndex demonstrated encrypted dashboards using homomorphic encryption. A dashboard in this context is a real-time visual interface showing fraud metrics and alerts.

Use: The system enabled real-time monitoring and fraud detection on encrypted transaction data. Normally, fraud detection systems must decrypt transaction data before analysis, which creates security risks. Using homomorphic encryption, transactions could be analyzed while still encrypted, allowing banks to detect suspicious activity and generate alerts without exposing sensitive financial information. This improved security while maintaining effective fraud monitoring.

Approach:

- Encrypted live transaction feeds using homomorphic encryption.
- Applied small Large Language Models, which are artificial intelligence systems trained to analyze patterns in text and structured data, to detect suspicious activity.
- Built dashboards that displayed insights derived from encrypted data without ever exposing the raw transactions.

Outcomes:

- Achieved real-time analytics while preserving full data confidentiality.
- Proved that homomorphic encryption can integrate with existing analytics platforms.
- Demonstrated readiness for fraud detection, compliance monitoring, and audit use cases in the financial industry.

V. IMPLEMENTATION FEASIBILITY

5.1 Technical Feasibility

5.1.1 Computational Resources:

- **Homomorphic Encryption (HE):**
  - Requires powerful computing systems, including high-speed CPUs or GPUs.
  - Needs significantly more memory than traditional encryption (up to 100 times more) due to the bulkier encrypted data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

- Storage requirements increase because encrypted data can be 2 to 10 times larger than unencrypted data.

- **Secure Multiparty Computation (SMPC):**
  - Requires fast, reliable network connections between multiple participating systems.
  - Uses secure channels for transmitting data shares.
  - Needs systems capable of running parallel computations with mechanisms for synchronizing and handling errors.

5.1.2 Performance Considerations:

- HE is still slower than traditional encryption but improving quickly. For example:
  - A basic addition that takes less than 1 microsecond traditionally may take 50–100 microseconds today with HE and could reduce to 10–20 microseconds with future improvements.
  - Complex tasks like running machine learning on encrypted data could drop from minutes to seconds with optimization.
- SMPC performance depends on how many parties are involved. More parties lead to increased delay and more data traffic.

5.1.3 Integration Challenges:

- HE and SMPC are not natively supported by existing banking systems like Finacle or Flexcube.
- Real-time systems like ATM networks or UPI require responses in milliseconds, which is challenging for current HE/SMPC.
- Data must be reformatted to work with encryption systems, which requires changes in how data is stored and processed.

5.1.4 Feasible System Architecture:

- Sensitive actions go through encryption-aware systems.
- Non-sensitive data is processed using existing secure methods.
- Results are stored in an encrypted database with proper key management.

5.2 Economic Feasibility

***Initial Investment Range:* ₹16–35 Crores for a mid-sized bank.**

- Covers hardware, software, consulting, integration, and staff training.

***Annual Maintenance:* ₹5–11 Crores**

- Includes support, cloud resources, staff salaries, and compliance updates.

Potential Savings:

- Avoiding a data breach (costing up to ₹20 Crores)
- Lower regulatory fines
- Cutting manual compliance work by up to 40%

Return on Investment (ROI):

- Breakeven typically occurs in 3–5 years.
- Sooner if a major security incident is avoided.

Scalability Plan:

- **Phase 1:** Small pilot with minimal investment.
- **Phase 2:** Broader deployment for more use cases.
- **Phase 3:** Full-scale rollout across sensitive systems.

5.3 Regulatory and Compliance Feasibility

Positives:

- Meets and exceeds RBI's basic encryption and data protection requirements.
- Supports end-to-end security: even when data is being processed.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

Aligns with future laws like India's Digital Personal Data Protection Act (DPDPA).

Challenges:

- RBI has not yet published clear rules for HE/SMPC.
- Data localization laws may be difficult to interpret with encrypted cross-border data sharing.

Recommendations:

- Start engaging with RBI and industry groups now.
- Document everything carefully for audit readiness.

VI. APPLICATIONS IN BANKING

As cyber and privacy threats grow more sophisticated, the need to enhance data security and privacy, enable secure data collaboration for advanced analytics, improve risk assessment, and comply with data protection regulations, rises and becomes paramount. Below are some of the most promising and beneficial applications.

6.1 Homomorphic Encryption Applications

6.1.1. Fraud Detection and Risk Analysis

Use Case: Banks analyze encrypted transaction data for fraud patterns

Implementation:

- Customer transactions encrypted at source
- ML models run on encrypted data
- Fraud alerts generated without exposing customer details
- Privacy-preserved across multi-bank collaboration

Benefits:

- Real-time fraud detection without data exposure
- Cross-institutional pattern recognition
- Regulatory compliance

Example: IBM demonstrated ML predictions on fully encrypted banking data with accuracy matching unencrypted models

6.1.2. Credit Scoring and Risk Assessment

Use Case: Assess creditworthiness using encrypted financial data

Implementation:

- Income, transaction history encrypted
- Credit models compute scores on ciphertext
- Results delivered encrypted to authorized parties
- Privacy-preserving credit bureau operations

Benefits:

- Protects sensitive financial information
- Enables data sharing between institutions
- Supports financial inclusion for underbanked populations

6.1.3. Secure Cloud Computing

Use Case: Banks outsource computational tasks to cloud providers

Implementation:

- Sensitive data encrypted before cloud upload
- Cloud performs analytics on encrypted data
- No cloud provider access to plaintext
- Results returned encrypted

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

Benefits:

- Leverages cloud scalability without security compromise
- Reduces infrastructure costs
- Maintains data sovereignty compliance

6.1.4. Privacy-Preserving Regulatory Reporting

Use Case: Banks submit encrypted compliance reports to regulators

Implementation:

- Financial data encrypted by banks
- Regulators perform audits on encrypted data
- Aggregate insights generated
- Individual customer privacy maintained

Benefits:

- Streamlines compliance processes
- Protects customer confidentiality
- Enables regulatory oversight without data exposure

6.1.5. Anti-Money Laundering (AML) Analytics

Use Case: Detect money laundering across encrypted transaction networks

Implementation:

- Transaction patterns analyzed while encrypted
- Cross-border collaboration without data sharing
- Suspicious activity flagged without revealing identities
- Law enforcement access to relevant encrypted data

Real-World Example: Fintel Alliance (Australia) uses HE for AML investigations across member institutions

6.2 Secure Multi-Party Computation Applications

6.2.1. Cross-Institutional Fraud Detection

Use Case: Multiple banks collaborate to identify fraud without sharing customer data

Implementation:

- Each bank holds encrypted transaction data
- SMPC protocol computes fraud patterns jointly
- No bank sees others' customer information
- Collective intelligence without data centralization

Benefits:

- Enhanced fraud detection accuracy
- Reduced false positives
- Faster response to emerging threats

Example: Cyber Defence Alliance (UK) - 4 banks + Metropolitan Police using MPC for cybercrime investigations

6.2.2. Collaborative Risk Assessment

Use Case: Banks jointly evaluate portfolio risk

Implementation:

- Each bank contributes encrypted risk metrics
- SMPC calculates aggregate exposure
- Systemic risk identified without competitive data leakage

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

- Individual positions remain confidential

Benefits:

- Improved systemic risk management
- Enables stress testing across institutions
- Maintains competitive confidentiality

6.2.3. Privacy-Preserving Customer Analytics

Use Case: Banks analyze customer behavior across institutions

Implementation:

- Customer transaction patterns encrypted
- SMPC computes aggregate insights
- No single institution accesses full customer profile
- Enhanced personalization without privacy violation

Benefits:

- Better customer segmentation
- Improved product recommendations
- GDPR/DPDPA compliance

6.2.4. Secure Authentication Systems

Use Case: Multi-party biometric authentication

Implementation:

- Biometric templates split using secret sharing
- Authentication performed on distributed shares
- No single server holds complete biometric data
- Compromise of one server doesn't breach privacy

Benefits:

- Enhanced security against data breaches
- Distributed trust model
- Scalable authentication infrastructure

Example: NEC's SMPC implementation for FIDO-based authentication in FinTech

6.2.5. Syndicated Lending

Use Case: Multiple banks jointly evaluate large loan applications

Implementation:

- Each bank contributes credit assessment data
- SMPC aggregates evaluation without sharing proprietary models
- Collective lending decision without exposing individual criteria
- Fair risk distribution

VII. RECOMMENDED IMPLEMENTATION ROADMAP

7.1 Phase 1: Foundation

7.1.1 Activities

In this phase, the focus is on building a strong and secure base for protecting sensitive data. The organization deploys Partially Homomorphic Encryption (Paillier), which is a special type of encryption that allows certain calculations to be performed on encrypted data without revealing the actual information. Encryption means converting readable data into

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

coded form so unauthorized users cannot access it. This technology is used within the Accenture-managed data lake, which is a centralized storage system that collects and stores large volumes of organizational data for analysis.

The organization also selects two expert vendor partners, such as IBM or Duality, to provide specialized tools and technical support for encryption. These partners bring experience in cryptography, which is the science of protecting information through secure encoding techniques.

Additionally, the organization implements Secure Multi-Party Computation (SMPC) for managing encryption keys. Encryption keys are secret digital codes used to lock and unlock encrypted data. Instead of storing the key in one place, SMPC splits the key into multiple parts and distributes them across different systems. This approach, called threshold key management, ensures that no single person or system can access the full key alone, improving security.

7.1.2 Expected Outcome

As a result of this phase, the organization establishes a strong internal security foundation for protecting sensitive data. It also builds a trusted network of specialized vendor partners who support the encryption infrastructure. Most importantly, encryption key control becomes decentralized, meaning it is distributed across multiple secure locations instead of being concentrated in one place.

7.1.3 Challenges

One major challenge is the shortage of skilled professionals who understand advanced encryption technologies, as these are highly specialized skills. Selecting the right vendor is also difficult because many encryption solutions are still evolving, and it can be hard to evaluate their long-term reliability and scalability. Another challenge is integrating encryption into existing legacy systems, which were not originally designed to handle encrypted data processing and may require significant modification.

7.2 Phase 2: Collaborative Pilots – Cross-Institution and Customer-Facing Trials

7.2.1 Activities

In this phase, the organization begins testing encryption technologies in real-world scenarios involving other banks, customers, and regulators. It participates in the Reserve Bank of India (RBI) Theme-Neutral Sandbox, which is a controlled testing environment created by the central bank. This sandbox allows banks to safely test new technologies such as cross-bank Anti-Money Laundering (AML) systems. AML refers to processes used to detect and prevent illegal financial activities. Using SMPC, multiple banks can analyze suspicious transactions together without sharing their actual confidential customer data.

The organization also launches a pilot project using Homomorphic Encryption (HE) for credit scoring. Credit scoring is the process banks use to assess whether a customer is likely to repay a loan. This pilot focuses on customers in retail banking, agriculture, and MSME (Micro, Small, and Medium Enterprises) sectors, which include small businesses that often need financial support.

In addition, SMPC is integrated into the e-Rupee system, which is India's digital currency issued by the central bank, also called a Central Bank Digital Currency (CBDC). This ensures user privacy while still allowing regulators to monitor and prevent illegal activities.

7.2.2 Expected Outcomes

This phase allows the organization to test encryption technologies in real-world environments with actual partners and regulators. It demonstrates improved fraud detection and more accurate credit risk assessment. It also creates a clear plan for securely integrating encryption into digital currency systems while protecting user privacy.

7.2.3 Challenges

Working with multiple banks creates coordination challenges, as each institution may use different technical systems and standards. Encryption technologies such as HE and SMPC can also slow down processing speeds, which may affect performance during testing. Additionally, regulatory guidelines for encryption are still evolving, requiring continuous alignment with RBI requirements.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

7.3 Phase 3: Scaling and Strengthening Cryptographic Security

7.3.1 Activities

In this phase, the organization expands encryption use across the entire bank. Homomorphic Encryption is applied to cloud-based data analysis, allowing the organization to generate personalized financial insights and marketing recommendations while keeping customer data encrypted and private.

To improve speed and efficiency, specialized hardware such as HPUs (Homomorphic Processing Units) and FPGAs (Field-Programmable Gate Arrays) are deployed. These are advanced computer chips designed to handle encryption operations much faster than standard processors. This helps enable faster fraud detection and secure validation of digital wallet transactions.

The organization also establishes a Post-Quantum Cryptography (PQC) Task Force. Post-quantum cryptography refers to encryption methods designed to remain secure even against future quantum computers, which are expected to be powerful enough to break current encryption methods.

7.3.2 Expected Outcomes

Encryption capabilities are successfully expanded across the entire organization, allowing secure data processing at scale. Specialized hardware improves system performance and reduces delays. The organization also prepares its systems to remain secure against future threats from quantum computing.

7.3.3 Challenges

Specialized hardware such as HPUs and FPGAs is expensive and requires complex integration with existing systems. Even with hardware acceleration, advanced encryption methods can still introduce delays in real-time applications like fraud detection or transaction approvals. Additionally, post-quantum encryption standards are still evolving, and transitioning to these new methods involves technical and operational risks.

7.4 Comparative Analysis: In-House vs Vendor Implementation for Encryption in an Indian Bank

7.4.1 Vendor Landscape in India

Several global and Indian companies already provide encryption solutions and have a strong presence in India.

A. Large Technology Providers (e.g., Microsoft, IBM etc.): These companies offer enterprise-ready solutions and operate cloud data centers within India, which helps meet RBI data localization requirements. These companies offer reliable, compliant, and scalable encryption infrastructure.

B. Specialized Encryption Vendors (e.g., Partisia, Zama etc): These companies focus specifically on privacy-enhancing encryption technologies and work with financial institutions globally and in India.

7.4.2 Cost Comparison

7.4.2.1 Option A: Full In-House Implementation

The bank builds and manages encryption systems internally.

Estimated 5-year cost: ₹46 crore to ₹94 crore.

Major expenses include:

- Purchasing high-performance servers and storage systems
- Hiring cryptography
- Software licenses and development tools
- System integration, consulting, and security audits
- Ongoing maintenance and staff salaries

Advantages:

- Full control over customer data
- Strong RBI compliance
- No dependency on external vendors

Disadvantages:

- Very high cost

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

- Difficult to hire cryptography experts in India
- Slow implementation (2 to 3 years)

7.4.2.2 Option B: Vendor-Based Implementation

- The bank uses vendors such as Microsoft, IBM, or TCS to provide encryption as a service.

Estimated 5-year cost: ₹42 crore to ₹86 crore

Major expenses include:

- Vendor setup and integration fees
- Annual platform subscription
- Transaction-based usage fees
- Vendor support and maintenance

Advantages:

- Faster implementation (6 to 12 months)
- Lower hiring and infrastructure costs
- Access to advanced and regularly updated technology

Disadvantages:

- Partial dependency on vendor
- Less direct control over systems

7.4.2.3 Option C: Hybrid Model

- The bank manages sensitive systems internally and uses vendors for specialized encryption tasks.
- **Estimated 5-year cost:** ₹27 crore to ₹54 crore.

Advantages:

- Lowest cost option
- Strong RBI compliance
- Balanced control and flexibility
- Faster deployment with long-term independence

7.4.3 Financial Benefits

- Encryption systems help reduce fraud, improve efficiency, and prevent financial losses.

Estimated annual benefits:

- Fraud loss reduction: ₹10 crore to ₹30 crore
- Reduced compliance and manual work costs: ₹2 crore to ₹8 crore
- Prevention of data breaches: ₹15 crore to ₹50 crore potential savings
- Operational efficiency improvements: ₹1 crore to ₹5 crore
- **Total estimated benefit over 5 years:** ₹65 crore to ₹465 crore

7.4.4 Cost Comparison Summary

Option	Year 1 Cost (₹ Cr)	5-Year Total (₹ Cr)	Key Points
In-House	20–40	47–94	Highest control and customization but costly and slow.
Vendor Outsourcing	13–26	43–86	Fastest implementation and up-to-date tech. Some data control trade-offs.
Hybrid Model	7–14	27–54	Best balance of cost, speed, and security. Recommended.

7.4.5 ROI Comparison:

In-House: High upside, but risk of low ROI if poorly executed.

Vendor: Moderate gains, faster.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, September 2026
Impact Factor: 8.2

Hybrid: Best cost-benefit balance.

7.4.6 Multi-Dimensional Comparison

Dimension	In-House	Vendor Outsourcing	Hybrid Model
Customization	Fully customizable for UBI needs	Limited to vendor's product offerings	Customizable core + vendor extensions
Technology Access	Slower to adopt new innovations	Rapid access to latest breakthroughs	Best of both worlds
Data Control	Full control over sensitive data	Relies on vendor policies	Sensitive data retained internally
Regulatory Compliance	Strong for RBI localization	Needs guarantees and audits	Can ensure full compliance
Speed of Deployment	Slow (12–36 months)	Fast (6–18 months)	Moderate (9–24 months)
Talent & Expertise	Requires hiring rare skillsets	Access to global experts	Build internal skills with vendor help
Cost Efficiency	Highest initial and long-term costs	Mid-range cost with scalable pricing	Most cost-effective approach

7.5 Ideal Approach

- Phase 1: Start with a vendor-led pilot while building an internal cryptography team.
- Phase 2: Gradually shift critical operations in-house.
- Phase 3: Develop in-house capabilities for long-term sustainability.

VII. CONCLUSION

Homomorphic Encryption and Secure Multi-Party Computation represent a significant advancement in banking cybersecurity and privacy protection. Unlike traditional encryption methods, these technologies enable computation on encrypted data without exposing sensitive information, thereby eliminating the critical vulnerability associated with data decryption during processing. From an economic perspective, although initial implementation requires significant investment, the long-term financial and operational benefits outweigh the costs. These benefits include reduced fraud losses, lower compliance costs, improved operational efficiency, and reduced risk of costly data breaches. The research indicates that breakeven is achievable within three to five years, depending on implementation scope and scale.

Strategically, the adoption of Homomorphic Encryption and Secure Multi-Party Computation positions banks to meet current and future cybersecurity challenges. It enhances customer trust, strengthens regulatory compliance, and establishes a robust foundation for secure digital banking innovation. In conclusion, a phased hybrid implementation strategy seems suitable. This approach will enable banks to enhance its cybersecurity posture, ensure regulatory compliance, reduce operational risks, and establish itself as a leader in privacy-preserving digital banking in India.

X. REFERENCES

[1]. Marcella Hastings, Brett Hemenway Falk and Gerry Tsoukalas, "Privacy-Preserving Network Analytics," *Management Science*, 2022.

[2]. Emmanuela Orsini, "Efficient, Actively Secure MPC with a Dishonest Majority: a Survey," *Cryptology ePrint Archive, Paper 2022/417*, 2022.

[3]. "Concretely Efficient Secure Multi-Party Computation Protocols: Survey and More," *Security and Safety*, Vol. 1, Article 2021001, 2022.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, September 2026 Impact Factor: 8.2

[4]. "Efficient Optimisation Framework for Convolutional Neural Networks with Secure Multiparty Computation," *Computers & Security*, 2022, Article 102679.

[5]. Junyoung Byun, Hyungjin Ko and Jaewook Lee, "A Privacy-Preserving Mean–Variance Optimal Portfolio," *Finance Research Letters*, Vol. 54, Article 103794, 2023.

[6]. Hyungjin Ko, Junyoung Byun and Jaewook Lee, "A Privacy-Preserving Robo-Advisory System with the Black-Litterman Portfolio Model: A New Framework and Insights into Investor Behavior," *Journal of International Financial Markets, Institutions and Money*, Vol. 89, Article 101873, 2023.

[7]. Elette Boyle, Geoffroy Couteau and Pierre Meyer, "Sublinear-Communication Secure Multiparty Computation Does Not Require FHE," *Cryptology ePrint Archive, Paper 2023/1802*, 2023.

[8]. Takeshi Nakai and Kazumasa Shinagawa, "Secure Multi-Party Computation with Legally-Enforceable Fairness," *International Journal of Information Security*, Vol. 23, pp. 3609–3623, 2024.

[9]. Haijun Bao, Minghao Yuan, Haitao Deng and Jiang Xu, "Secure Multiparty Computation Protocol Based on Homomorphic Encryption and Its Application in Blockchain," *Heliyon*, Vol. 10, No. 14, Article e34458, 2024.

[10]. Carmit Hazay, Muthuramakrishnan Venkitasubramaniam and Mor Weiss, "The Price of Active Security in Cryptographic Protocols," *Journal of Cryptology*, Vol. 37, Article 30, 2024.

[11]. Sean Shun Cao, Lin William Cong and Baozhong Yang, "Distributed Ledgers and Secure Multiparty Computation for Financial Reporting and Auditing," *Management Science*, Vol. 71, No. 5, pp. 3852–3872, 2025.

[12]. Idoia Gamiz, Cristina Regueiro, Oscar Lage, Eduardo Jacob and Jasone Astorga, "Challenges and Future Research Directions in Secure Multi-Party Computation for Resource-Constrained Devices and Large-Scale Computations," *International Journal of Information Security*, Vol. 24, Article 27, 2025.

[13]. Shancheng Zhang, Gang Qu, Zongyang Zhang, Minzhe Huang, Haochun Jin and Liqun Yang, "Efficient and Secure Multi-Party Computation Protocol Supporting Deep Learning," *Cybersecurity*, Vol. 8, Article 46, 2025.

[14]. Amitesh Kumar Pandit and Kakali Chatterjee, "Secure Multiparty Computation in Heterogeneous Environment: Survey and Challenges," *Current?* 2025.

[15]. "Quantum Secure Protocols for Multiparty Computations," *Journal of Information Security and Applications*, Vol. 90, Article 104033, 2025.

[16]. Zhe Li, Chaoping Xing, Yizhou Yao and Chen Yuan, "On the Power of Sumcheck in Secure Multiparty Computation," *Cryptology ePrint Archive, Paper 2025/177*, 2025.

[17]. "Towards Trustworthy and Privacy-Preserving Decentralized Auctions," *Journal of Banking and Financial Technology*, 2024.

[18]. Trung Nguyen-Nam, Phat T. Tran-Truong, Phien Nguyen-Ngoc, Ha X. Son and Trung H. T. Phan, "Privacy-Preserving Computation in Financial Systems: A Systematic Survey and Quantitative Analysis," 2026.