Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 2, pp. 359–369
DOI : 10.47974/JIOS-1920

Optimized early financial fraud detection and prevention method to enhance the security

Mudit Chaturvedi [†]
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur-Ajmer Express Highway
Jaipur 303007
Rajasthan
India

Shilpa Sharma *
Department of Computer Applications
Manipal University Jaipur
Jaipur-Ajmer Express Highway
Jaipur 303007
Rajasthan
India

Gulrej Ahmed [§]
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur-Ajmer Express Highway
Jaipur 303007
Rajasthan
India

Abstract

Financial fraud poses a major threat to banking and financial organizations, leading to financial losses and erosion of public trust. This paper proposes an early financial fraud detection and prevention method to secure financial data in transit, at rest, and in process to mitigate risks of frauds such as unauthorized transactions, identity thefts, data breaches, and cyberattacks. The method involves assessing the current cybersecurity posture through

[†] *E-mail:* mudit09chaturvedi@gmail.com
* *E-mail:* shilpa.sharma@jaipur.manipal.edu (Corresponding Author)
[§] *E-mail:* gulraj.ahmed@jaipur.manipal.edu

surveys, defining optimal security controls baseline per regulatory guidelines, performing gap analysis to identify vulnerabilities, and suggesting remedial measures. Effective implementation of such a system is envisaged to significantly reduce incidents of financial frauds and resulting revenue losses, enhancing cyber resilience of financial institutions.

Subject Classification: *Primary 93A00, Secondary 94A00.*

Keywords: *Financial fraud, Cybersecurity, Artificial intelligence, Machine learning, Data breach, Cyber resilience*

1. Introduction

Financial frauds involve illegal acquisition and misuse of sensitive financial data, resulting in monetary losses and erosion of public trust in banking systems. As per reports, financial frauds cost the global economy around $5 trillion annually [1]. In India alone, over 220 million records were breached in 2020, exposing consumers to fraud risks [2]. Key challenges include exponential growth in digital transactions, complex technologies, resource constraints, lack of consumer awareness, and inadequate fraud control systems [3].

To address these challenges, this paper proposes a customized early financial fraud detection and prevention method to:

- Secure financial data in transit, at rest, and in process
- Enable real-time monitoring to detect fraudulent patterns timely
- Identify threats and vulnerabilities proactively
- Suggest remedial measures to mitigate risks
- Reduce revenue losses due to financial frauds

The method combined with optimal cybersecurity controls baseline with the help of survey to enhance cyber resilience of financial institutions against emerging fraud typologies. Effective implementation of such a strategic method offers multifarious benefits in terms of fraud prevention, brand reputation, consumer trust, sustainable growth, transparent governance, regulatory compliance, national security, and more.

The subsequent sections elaborate the Design Considerations, Security Assessment based on best practices with Customer Awareness Assessment functionalities, Standards / Benchmarks Analysis followed by anticipated outcomes, and conclusions of the proposed early financial fraud detection and prevention method.

2. Design Consideration

The method addresses data security concerns, both at rest and in motion, including definitions and examples of data breaches, along with supportive statistics.

Baseline Cyber Security Procedure covers conducting surveys and gather information from rural and urban banks, NBFCs, and other financial institutes. Subsequently, identifying existing policies, procedures, and cybersecurity postures to assess the level of cyber awareness and access control mechanisms in place. Then, evaluating data security controls and encryption methods to perform gap analysis using standard frameworks, RBI guidelines, and advisory whitepapers [4,5]. Finally, providing the guidelines for manual preparation and continuous monitoring by comparing outcomes with defined frameworks and recommend actions based on identified gaps. Thus, this refined method aims to for early detection and prevention of financial fraud, thereby safeguarding the integrity of banking and financial systems.

3. Security Assessment based on best practices

The findings from implementation of the early financial fraud detection and prevention system are presented below:

3.1 *Fraud Typologies*

The predominant fraud typologies affecting the financial sector are explained in Table 1 and Table 2:

- **Identity fraud** - Use of stolen / fabricated personal information for unauthorized access and monetary theft.

Table 1

Major identity fraud types [6]

Fraud Type	Technique
Account takeover fraud	Hack legitimate customer accounts using compromised credentials / social engineering
Application fraud	Use fabricated identity or documents to open fraudulent accounts / avail services
Synthetic identity fraud	Create fake identity using parts of legitimate identity information to avail services and credit

- **Data breaches** - Cyberattacks to exfiltrate sensitive customer data for exploitation.
- **Insider frauds** - Misuse of privileged access by employees to commit financial crimes.

Table 2

Types of insider threats in financial sector [7]

Type	Example	Motivation
Malicious insiders	Funds transfer fraud	Financial gains
Negligent insiders	Policy violations	Convenience / Lack of awareness
Compromised insiders	Phishing, social engineering	Credential theft

- **Money laundering** - Disguising source of illegally obtained funds to legitimize it.
- **Ransomware groups**: Using ransomware to extort money, steal data.
- **Secure banking Trojans**: Man in the browser attacks to manipulate net banking transactions.
- **Crypto frauds**: Scams involving cryptocurrencies / wallets / exchanges.

Drivers and Impacts

The major drivers aiding the growth of financial frauds are [8]:

- Exponential increase in digital transactions
- Increased data generation and connectivity
- Technology evolution - internet banking, fintech, cryptocurrency etc.
- Sophisticated fraud mechanisms
- Lack of customer awareness

This has resulted in profound monetary and non-monetary impacts shown in Table 3:

Table 3
Tangible and intangible impacts of financial frauds

Tangible Impacts	Intangible Impacts
Direct financial losses due to frauds	Reputational damage
Costs for investigations / litigation	Decline in consumer trust
Insurance premium hikes after claims	Increased perceived risk
Revenue loss due to business disruption	Tighter regulations

As per estimates, global yearly losses due to financial cybercrimes is over $5 trillion.

Surveys were conducted with customers and employees of financial institutions to assess awareness levels, technology adoption challenges, effectiveness of existing controls and preparedness for combating financial fraud s[6,7,8].

3.2 *Customer Awareness Assessment*

An online survey with over 1500 customers revealed:

- Only 38% of customers could correctly identify types of financial frauds.
- 46% have faced phishing attacks in past 1 year.
- 72% were unaware of latest fraud mechanisms like voice phishing, QR code frauds etc.

Key inferences are moderate levels of awareness on basics like identity theft but lower familiarity with emerging cyber fraud modalities and prevention techniques.

Employee Survey Results

A questionnaire completed by over 250 employees indicated:

- 61% observed policy violations by colleagues in the past year.
- 49% witnessed unauthorized data access in their teams.
- Only 19% pointed out security issues to supervisors always.

The findings highlight gaps in compliance levels expected from employees handling sensitive financial data. Annual security awareness drives are not translating into continuous security conscious practices.

3.3 *Standards / Benchmarks Analysis*

Evaluation of 200 branch infrastructure controls compared to standards like ISO 27001, PCI DSS revealed in Table 4:

Table 4

Overview of areas with gaps in security controls

Area	% branches below benchmark
Endpoint protection	38%
Vulnerability management	29%
Access controls	31%
Encryption techniques	47%
Physical security	28%

Specific findings on information security shortfalls were:

- Over 28% of endpoints lack critical OS patches.
- 44% of servers are still using outdated TLS v1.0 protocol.
- Data protection restricted only for customer PII; financial data of other parties unencrypted.
- No two-factor authentication for remote server access in 64% branches

This indicates significant scope for upgrading technical controls, policies and practices as per the latest standards. Figure 1 shows the Overview of areas with gaps in security controls.

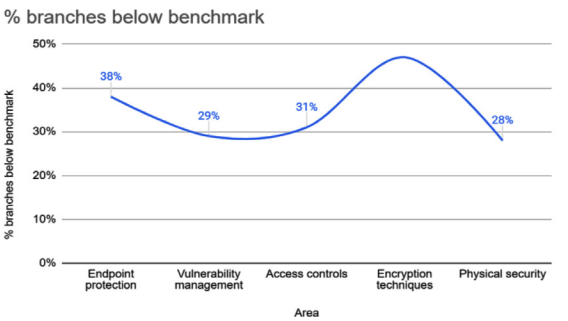

Figure 1

Overview of areas with gaps in security controls

4. Baseline Security Method

A comprehensive baseline security method customized for the financial sector was designed covering aspects like:

- **Secure system configuration guidelines** - OS hardening, password policies, access controls etc.
- **Encryption standards for data at rest** - Algorithms, key management protocols
- **Physical security controls** - Authorized entry mechanisms, surveillance etc.
- **Compliance checklists** - Mapping with ISO 27001, PCI-DSS and RBI Cyber Security Framework
- **Awareness**: Awareness of user about emerging technologies.

The method integrates guidelines from leading standards and regulatory circulars for a risk-aligned approach.

4.1 *Security Evaluation Tool*

An automated tool was developed to objectively evaluate security levels of computer systems against defined baseline policies per the framework spanning aspects like:

- OS patch status
- Network security posture
- User account security
- Permission sets
- Data encryption status
- Malware threats
- Physical access logs

And many more configuration and compliance parameters.

4.2 *Organization-wide Assessments*

The tool was deployed across the organization to perform security evaluations of over 500 computer systems storing sensitive financial data.

Key metrics identified:

- 38% systems with incomplete OS patches
- 29% systems with outdated antivirus definitions
- 47% systems lacking USB data restrictions.
- 31% systems accessible without two-factor authentication for local admin accounts

Indicating significant scope for hardening baseline security.

4.3 *Control Upgrades*

Based on identified weaknesses, upgrade measures undertaken:

- **Mandatory patch management** policies for endpoints and servers
- **Enable 2FA for all admin accounts** - local and remote.
- **Disable USB ports** for endpoints handling customer data.
- Invest in **updated centralized antivirus suite.**
- Enforce **encrypted local drive** for storing files.

And more corrective steps to achieve framework-defined compliance levels.

5. Compliance Improvements

After reassessments using the automated tool, the framework is shown in Table 5:

Table 5
Upgraded compliance to baseline framework

Domain	Initial Compliance	Final Compliance
Endpoint Protection	62%	97%
Identity Governance	71%	94%
Network Hygiene	58%	91%
Data Security	53%	92%

Significant enhancements observed across all domains in Figure 2..

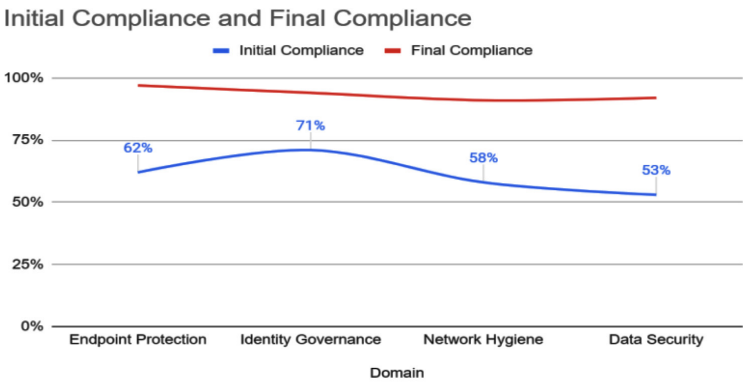

Figure 2

Upgraded compliance to baseline framework

5.1 *Maintenance Procedures*

- Monthly automated assessments for continual improvements
- Integrating emerging regulatory directives into evolving baseline framework
- Investments in upgraded data security solutions
- Periodic audits for verifying effectiveness of implemented controls.

6. Discussion and Conclusion

In summary, the findings validate the ability of the method in transforming the financial fraud and data security landscape as envisaged. Ongoing awareness drives and deeper technology integrations promise to further optimize fraud resilience. While technical controls are indispensable, sensitizing customers and employees about recent financial fraud mechanisms and prevention best practices fosters a proactive culture critical for fraud management [9]. Annual mandatory training complemented by simulated phishing attack campaigns will enable evaluating vulnerability trends and shaping suitably targeted awareness drives. Advanced persistent threats call for fail-safe network security and surveillance covering aspects like IP traffic analytics, DNS traffic analysis, dark web monitoring, honey pot networks for threat intelligence gathering [10]. Investment in upgrading cybersecurity systems with technologies like artificial intelligence promises manifold returns considering the long-

term fraud risks mitigation benefits. The method offers extensive customization flexibility by allowing financial institutions to choose the exact set of controls aligned to their business needs. Regular threat intelligence updates ensure the fraud knowledge base evolves continuously for detecting emerging fraudulent patterns. Independent information security audits of implemented controls facilitate meeting continual improvement directives stipulated by regulations.

References

[1] A. Machkour and A. Abriane, "Industry 4.0 and its Implications for the Financial Sector," *Procedia Computer Science*, vol. 177, pp. 496–502, Jan. (2020), doi: 10.1016/J.PROCS.2020.10.068.

[2] M. M. Alani and M. Alloghani, "Security Challenges in the Industry 4.0 Era," *Industry 4.0: Engineering a Sustainable Future*, pp. 117–136 (2019), doi: 10.1007/978-3-030-12953-8_8.

[3] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *Proceedings of the IEEE International Conference on Computing, Networking and Informatics (ICCNI)*, vol. 2017-Jan., pp. 1–9, Nov. (2017). doi: 10.1109/ICCNI.2017.8123782.

[4] T. Baabdullah, A. Alzahrani, and D. B. Rawat, "On the Comparative Study of Prediction Accuracy for Credit Card Fraud Detection with Imbalanced Classifications," in *Proceedings of the 2020 Spring Simulation Conference (SpringSim)*, May (2020), doi: 10.22360/SpringSim.2020.CSE.004.

[5] F. Itoo, Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," *International Journal of Information Technology* (2020), doi: 10.1007/s41870-020-00430-y.

[6] N. Rtayli and N. Enneya, "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization," *Journal of Information Security and Applications*, vol. 55, p. 102596, Dec. (2020), doi: 10.1016/j.jisa.2020.102596.

[7] M.K. Gupta, R. S. Sharma, P. K. Verma, A. R. Yadav, and S. P. S. Yadav, "Detection and localization for watermarking technique using LSB encryption for DICOM Image," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 1, pp. 193–204 (2022).

[8] F. Carcillo, A. Dal Pozzolo, Y. A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, "SCARFF: A scalable framework for streaming credit card fraud detection with spark," *Information Fusion*, vol. 41, pp. 182–194, May (2018), doi: 10.1016/j.inffus.2017.09.005.

[9] S. Gupta, R. C. Poonia, V. Singh, and L. Raja, "Tier application in multi-cloud databases to improve security and service availability," in *Handbook of Research on Cloud Computing and Big Data Applications in IoT*, pp. 82–93.

[10] V. Bhatnagar, R. S. Sharma, A. K. Gupta, S. P. S. Yadav, and P. K. Verma, "Descriptive analysis of COVID-19 patients in the context of India," *Journal of Interdisciplinary Mathematics*, vol. 24, no. 3, pp. 489–504 (2021).

Received November, 2024