African Journal of Academic Publishing in Science and Technology (AJAPST)

المجلة الأفريقية للنشر الأكاديمي في العلوم والتكنولوجيا
Volume 1, Issue 4, 2025
Page No: 51-57
Website: https://easrjournals.com/index.php/AJAPST/index

Enhancing Payment Card Security: A Review of Technologies, Behavioral Factors, Threads and Protection Methods

Yahya Fakroun [1 *], Kadry Hamed [2]
[1] Department of Computer Sciences, College of Technical Sienese-Sabha, Libya
[2] Department of Computer Sciences, Faculty of Computers and Information, Minia University, Egypt

تعزيز أمن بطاقات الدفع: مراجعة للتقنيات، والعوامل السلوكية، والتهديدات وسبل الحماية

يحيى فكرون [1*]، قدري حميد [2]
[1] قسم علوم الحاسوب، كلية العلوم التقنية - سبها، ليبيا
[2] قسم علوم الحاسوب، كلية الحاسبات والمعلومات، جامعة المنيا، مصر

[*]Corresponding author: Yahya_fakroun@ctss.edu.ly

Received: October 14, 2025	Accepted: December 04, 2025	Published: December 26, 2025

Abstract:
In recent years, and with the rapid advancement of communication technologies, e-commerce, credit cards, and electronic payment methods have become among the most widely used tools in commercial transactions. This widespread adoption has led to the emergence of various risks and threats that have negatively affected cardholders, prompting researchers to develop advanced protection mechanisms and enhance awareness among users of these payment methods. Thus, this paper presents a review of electronic payment technologies and behavioral factors that shape cybersecurity outcomes in payment card systems. It presents a comprehensive analysis based on two key dimensions related to securing and protecting electronic payment cards. The first dimension examines the latest protection techniques and modern technologies integrated into electronic payment systems, while the second focuses on users' knowledge levels and behavioral patterns and their impact on payment card security. Human behavior remains a decisive factor, encompassing users' daily practices. By combining these two dimensions, this paper provides a critical analysis of the current landscape, highlighting the risks and threats arising from the imbalance between technological advancement and behavioral awareness. In addition, credit fraud and protection methods are presented.

Keywords: Cybersecurity, Payment Card, Credit Card, Credit Fraud, Artificial Intelligence.

الملخص
في السنوات الأخيرة، ومع التقدم المتسارع في تقنيات الاتصال والتجارة الإلكترونية، أصبحت بطاقات الائتمان وطرق الدفع الإلكتروني من أكثر الأدوات استخداماً في المعاملات التجارية. وقد أدى هذا الاعتماد الواسع إلى ظهور مخاطر وتهديدات متنوعة أثرت سلباً على حاملي البطاقات، مما دفع الباحثين إلى تطوير آليات حماية متقدمة وتعزيز الوعي لدى مستخدمي وسائل الدفع هذه. بناءً على ذلك، تقدم هذه الورقة مراجعة لتقنيات الدفع الإلكتروني والعوامل السلوكية التي تشكل مخرجات الأمن السيبراني في أنظمة بطاقات الدفع. كما تقدم تحليلاً شاملاً يستند إلى بُعدين رئيسيين يتعلقان بتأمين وحماية بطاقات الدفع الإلكتروني؛ حيث يتناول البُعد الأول أحدث تقنيات الحماية والتكنولوجيا الحديثة المدمجة في أنظمة الدفع، بينما يركز الثاني على مستويات معرفة المستخدمين وأنماطهم السلوكية وتأثيرها على أمن البطاقات. ويظل السلوك البشري عاملاً حاسماً يشمل الممارسات اليومية للمستخدمين. ومن خلال الجمع بين هذين البُعدين، توفر الورقة تحليلاً نقدياً للمشهد الحالي، مع تسليط الضوء على المخاطر والتهديدات الناشئة عن الفجوة بين التقدم التكنولوجي والوعي السلوكي. بالإضافة إلى ذلك، يتم عرض طرق الاحتيال الائتماني وسبل الحماية منها.

الكلمات المفتاحية: الأمن السيبراني، بطاقة الدفع، بطاقة الائتمان، الاحتيال الائتماني، الذكاء الاصطناعي.

Introduction

In recent years, technologies such as the Internet of Things (IoT), Blockchain, and Artificial Intelligence (AI) have penetrated numerous fields such as healthcare, industry, agriculture, etc. to present smart services [1]. Smart cities, smart transportation, and smart homes are the key applications of the IoT [2]. Blockchain technology is

integrated with IoT applications and other technologies to enable secure transactions. AI take benefits of result data and information to improve accuracy and to predict and classify actions and patterns and decisions [1]. This rapid advancement of communication technologies has significantly expanded the use of e-commerce platforms, credit cards, electronic payment methods, and in general smart payment systems (SPS), making them central to modern commercial transactions. However, smart payment approaches create new security threats to financial and urban integrity, privacy, and trust [3].

The main implication of cybersecurity, especially in financial sector, is that AI algorithms shape reality for unaware daily users [4]. With expanded use of credit cards, several fraud methods have emerged, aiming to steal card data or exploit it through illicit means. The most prominent of these methods can be classified into several categories, which differ in their attack mechanisms and the required protection measures. This research reviews the most common forms of fraud, alongside recommendations, protection solutions, and the technologies used to mitigate their impact.

However, this growing reliance on digital payment systems has introduced a range of security risks and threats that directly impact cardholders [5]. These challenges have motivated researchers to explore innovative technological solutions and promote greater user awareness to strengthen the security of payment card ecosystems. Emerging evidence suggests that both advanced security technologies and user behavioral factors will play a crucial role in shaping the future of secure payment transactions [6]. Notably, human behavior continues to be a critical determinant of security outcomes, reflected in users' daily practices and decision-making patterns. Recent studies [6] [7] further highlight the persistent gap between rapid technological progress and limited behavioral awareness, emphasizing the need for a balanced approach to achieving robust payment card security. The success of cyberattacks stems from exploiting human patterns, not merely technical weaknesses

Motivation

Fig. 1 shows recent impact of publications since 2010 on the query "payment card" using Scopus database [8].

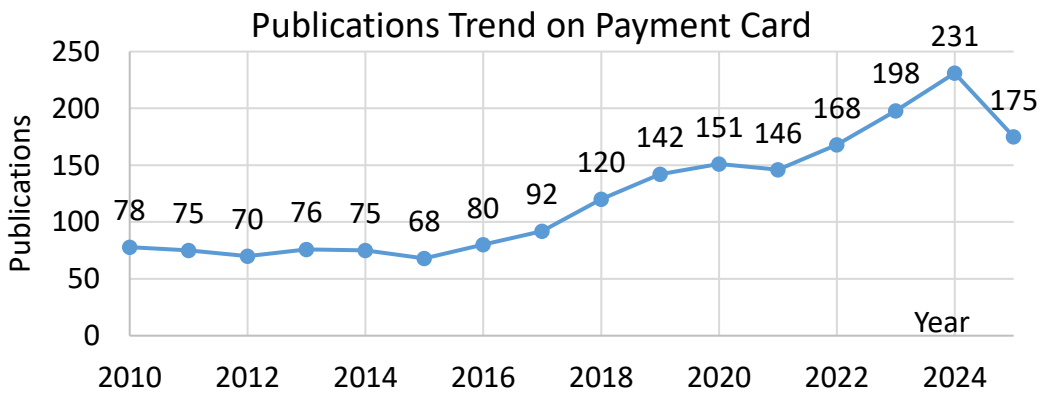

Figure 1: Scopus Report - Indexed Publications on Payment Card

Main **Contribution**

Main contribution of this paper is summarized into the following points:

1. Clarifying the main concepts and technologies related to electronic payment.
2. Surveying current technologies and behavioral factors related to payment card security.
3. Highlighting recent recommendations on securing payment card systems.

The remaining of this paper is organized as follows: Section 2 presents literature revie on electronic payment security approaches. Section 3 presents a brief overview of electronic payment methods and behavioral factors. Section 4 summarizes types of credit fraud and corresponding protection techniques.

Section 5 discusses limitations of the study and recommends AI integration to reveal threads and attacks. Finally, conclusion of this manuscript is presented in Section 6.

Literature Review

This section surveys recent reviews published on "payment card security" since 2020. Results are filtered and selected by running the following query on Scopus database [8]. All reviews are analyzed and summarized as presented in Table1

((TITLE-ABS-KEY (payment AND card) AND TITLE-ABS-KEY (credit AND card)) AND PUBYEAR > 2019 AND PUBYEAR < 2027) AND (security) AND (LIMIT-TO (DOCTYPE , "re")) AND (LIMIT-TO (LANGUAGE , "English"))

As indicated, almost studies discuss how AI techniques (ML and DL) could aid in fraud detection, while few studies ([9] and [10]) consider behavioral factors.
To sum up, the two factors for studying fraud in credit card payment are essential, Oladipo et al. [6] discuss human factors implications on cybersecurity (e.g., cardholders' awareness of potential risks and threads) and recommend developing robust cybersecurity frameworks that account for human elements. Kaur et al. [11] discussed ethical issues concerning ATM highlighting privacy concerns and rise in skimming-related fraud. This manuscript will tackle all aforementioned factors

Payment Terminologies and Techniques

This section covers main terminologies and techniques relating to electronic payment. First subsection presents concepts of smart payment (SP) and summarizes current types of implemented technologies in SP. Second subsection classifies them according to implemented technology and according to primary function

Types Of Technologies And Tools

Mobile wallets, mobile banking, mobile cash, online payment, credit cards, online payment platforms are known as SP or electronic payment (EP) methods. SP is used in this context. SP methods provide enhanced authentication, integrity and security compared to traditional methods (barcodes or magnetic stripes) [12].

Table 1: A Summary of Recent Reviews Indexed by Scopus on "Payment Card Security" Since Jan. 2020 till Nov. 2025

Ref.	Year	Main Topic	Contributions	Behavioral Factors	Recommendations
[13]	2025	Phishing website detection using AI	review phishing techniques, and detection methods using AI	×	improving ML-based detection systems to overcome limitations of traditional anti-phishing approaches
[14]	2024	Digital payment fraud and financial crime trends	Bibliometric analysis identifying key research themes and collaboration networks	×	invest in fraud prevention technologies and training;
[15]	2024	Blockchain adoption across sectors	Highlights decentralization benefits and impact on healthcare, aviation, and e-commerce	×	Further exploration of blockchain's potential to enhance policy and process efficiency in various industries
[16]	2024	Credit card fraud detection challenges	Reviews class imbalance, concept drift, and latency issues; compares ML and DL solutions	×	Suggests developing more robust fraud detection systems using advanced learning models
[5]	2023	Credit card fraud detection using disruptive tech	Systematic review of ML/DL methods from 2015–2021; identifies limited use of deep learning	×	Encourages adoption of big data, cloud computing, and large-scale ML for improved fraud detection
[17]	2022	Machine learning (ML) for credit card fraud detection	Compares ML techniques and proposes a hybrid ANN model in a federated learning framework	×	Recommend hybrid models to enhance accuracy while preserving data privacy
[18]	2022	Impact of cryptocurrencies on global economics	Examines post-pandemic digital payment trends and crypto market growth	×	Calls for regulatory frameworks to manage crypto integration into traditional economies
[9]	2021	Behavioral effects of nudging in credit card payments	Field experiment showing reminders reduce late fees but may increase overdraft fees	✓	Suggests tailored nudging strategies to avoid unintended financial consequences

[10]	2021	Household consumption smoothing	Analyzes account data to show mental accounting influences spending despite liquidity	✓	Supports mental accounting models over pure liquidity constraint theories in policy design
[19]	2020	Legal aspects of carding as cyber fraud	Examines carding through criminal, commercial, and transnational law lenses	×	Advocates for stronger national and international legal frameworks to combat carding

Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized security framework designed to protect cardholder data (CHD) [20] and secure payment transactions. SP techniques are summarized as follows:

- **Card-Present / Chip & PIN:** The transaction is authenticated via an embedded microchip and a customer-entered Personal Identification Number (PIN). Magnetic Stripe is a legacy technique, where card's magnetic stripe is swiped through a reader.
- **Card-Present / Contactless:** Near-Field Communication (NFC)/ Radio-Frequency Identification (RFID) technology is a contactless encrypted payment system that encrypts and transmits cardholder's payment information over short distances to make secure transactions. The payment device (card, phone, or wearable) is simply tapped or held near a compatible reader, without physical contact. It uses tokenization to generate a unique, one-time code for each transaction [21] [22].
- **Card-Not-Present (CNP) / E-commerce:** Payment details are manually entered on a website or app. 3D Secure (e.g., Visa Secure, Mastercard Identity Check) is implemented.
- **Digital Wallets / In-App:** Tokenized E-commerce technology, where payment details are stored securely in a digital wallet (e.g., Apple Pay).
- **Payment Links and Invoicing:** a unique, payable link or digital invoice is generated and sent to a customer via email, SMS, or messaging app.
- **QR Code Payments:** A Quick Response code is scanned by a smartphone camera to initiate payment.
- **Buy Now, Pay Later (BNPL):** it is a point-of-sale installment loan.

Bank Transfers: direct transfer of funds from the customer's bank account to the merchant's account

Electron Payment Classification

SP could be classified according to underlying technology as follows:

- **Physical Card**: **Europay, Mastercard, and Visa** (EMV) Chip, Magnetic Stripe, Contactless (NFC).
- **Virtual Card:** No Physical Form, specifically designed to reduce fraud for "card-not-present" transactions, Exists only as a 16-digit number, expiry date, and Card Verification Value (CVV).
- **Digital Wallet:** it is In-App, and Online payments. Replaces card details with a unique "token" for each transaction. Examples Apple Pay, Google Pay.

SP classification according to primary function and funding source are as follows:

- **Credit/Secure Credit/Charge Cards**, allow you to pay it back later (Bank's money).
- **Debit/Prepaid Cards,** money already in an account or loaded onto the card.

Behavioral Factors

Behavioral factors are the beginning of the thread towards cyberattacks and payment card fraud. The following positive behaviors contribute to responsible credit management and reduce fraud risk [23] [24].

- **Demonstrates Control:** Low credit utilization and on-time payments are classified as responsible credit management, which is rewarded by credit scoring models.
- **Proactive Security:** Monitoring transactions, enabling alerts, and maintaining stable spending patterns create a "normal" baseline, which enables the rapid detection and reporting of potential fraud.

The following points outline negative behaviors, which damage creditworthiness and increase the likelihood of fraud or financial distress [25].

- **Signals Financial Distress:** Maxing out limits, using cash advances, and missing payments are strong indicators of financial trouble, which severely harms creditworthiness.

Triggers Fraud Alerts: Erratic and geographically impossible spending deviates from the user's established profile, which is the primary signal that activates a bank's fraud detection system

To sum up, secure use of SP is characterized by sustained, disciplined oversight, while risky use is marked by instability, unpredictability, and irresponsibility.

Credit Card Fraud and Protection Techniques

Table 2 reviews the most prominent fraud methods used, as well as the proposed solutions to reduce them.

Table 1: A summary of the most prominent fraud and corresponding protection methods

Technique / Reference	Description	Protection
Skimming [26]	A small device installed on ATMs or Points of Sale (POS) terminals to copy contents from the magnetic tape of the payment card.	• Use EMV Cards. • Machine Learning • Fraud Detection Systems
Card Cloning / CNP Fraud (Card-Not-Present) [27]	Creating a fraudulent card using the original card details or Fraud using stolen card details for online purchases.	• Dynamic Encryption / Data Authentication (DDA) in EMV Cards. • One-Time Password (OTP)
Phishing /Smishing [28]	Fake websites/emails: SMS messages, deceptive emails or fraudulent links used to phish cardholders for their card data.	• SMS filtering • 2FA Authentication Systems. • URL Classification via ML
Vishing / Social-Engineering [29]	Phishing/scamming the victim via phone calls where the fraudster impersonates a bank representative.	• Voice Biometrics. • AI-based Call Filtering
Contactless (NFC) Fraud [30]	Stealing card data through a nearby NFC reader or by executing a Relay Attack	• RFID-Shielding Sleeves. • NFC Encryption Protocols. • Proximity Verification • Transaction limits

Cardholders, financial institutions, and digital stores face significant challenges and security threats resulting from the unauthorized use of payment and credit cards, known as "fraud or impersonation." This involves either the physical theft of the card or obtaining its data through electronic means. The most widespread fraudulent transactions occur online (card-not-present fraud), where stolen credit card information is used to complete purchases or make money transfers [31].

Protection must be presented by three parties as 3D security protocol relies on for improving authentication to prevent card-not-present (CNP) fraud. They are: (a) acquirer domain, (b) issuer domain, and (c) interoperability domain.

Future Directions

Recent studies recommend balance integration for multiple security techniques such as IoT, Blockchain, AI, and Quantum computing [2] [32] [33] [34]. Quantum cryptography and blockchain are the most promising solutions in electronic payment [3] [32]. Authors in [35] and [36] present a framework-based AI to improve credit card data security. Kaur et al. [11] recommend improving security protocols and public awareness to mitigate cloning risks.

For behavioral factors, to protect contactless payment cards, researchers are developing aluminum credit card holders, But the following behavioral factors are essential.

- Password Strength and Management
- Awareness of Phishing and Social Engineering
- Safe Mobile and Internet Usage
- Frequency of Checking Bank Statements
- Updating Apps and Devices
- Use of Strong PIN Practices
- Cautious Online Shopping Behavior
- Reaction to Security Alerts
- Saving Card Information Online
- Overall Cybersecurity Literacy

Conclusion

Minimum baseline of security controls is to prevent (a) card data theft, (b) fraudulent transactions, (c) data breaches, and (d) unauthorized access to cardholder environment. Cybersecurity rules must be applied in the payment card industry, particularly by entities and institutions that store cardholder data, including financial

institutions, merchants, and service providers. This is to reduce payment card fraud and ensure compliance with global data security standards related to payment cards, namely PCI-DSS. In addition, behavioral factors are bases for tracking fraud and anomaly actions. AI techniques are recommended to be integrated with financial systems for card fraud and anomaly detection

References

[1] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial internet of things: A comprehensive review," *Measurement, vol. 151, p. 107198, 2020..*

[2] E.H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, "Internet of Things in Smart Cities: Comprehensive Review, Open Issues and Challenges," *IEEE INTERNET OF THINGS JOURNAL,* pp. 1-12, 2024.

[3] Pooya TEIMOORY, "Towards robust security in smart payment systems: challenges and solutions," *Smart Cities and Regional Development Journal,* vol. 9, no. 3, pp. 29-38, 2025.

[4] Rahwan, I., Cebrian, M., Obradovich, N., Bongard, J., Bonnefon, J.F., Breazeal, C., Crandall, J.W., Christakis, N.A., Couzin, I.D., Jackson, M.O. and Jennings, N.R., "Machine behaviour," *Nature,* Vols. 568(7753), pp.477-486., 2019.

[5] Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M. and Imine, A., "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University-Computer and Information Sciences,* Vols. 35(1), pp.145-174, 2023.

[6] Oladipo, J.O., Okoye, C.C., Elufioye, O.A., Falaiye, T. and Nwankwo, E.E., "Human factors in cybersecurity: Navigating the fintech landscape," *International Journal of Science and Research Archive,* Vols. 11(1), pp.1959-1967, 2024.

[7] Melumad, S. and Pham, M.T., "The smartphone as a pacifying technology. Journal of Consumer Research,," Vols. 47(2), pp.237-255., 2020.

[8] "scopus," [Online]. Available: https://www.scopus.com. [Accessed 11 Nov. 2025].

[9] Medina, P.C., "Side effects of nudging: Evidence from a randomized intervention in the credit card market," *The Review of Financial Studies,* Vols. 34(5), pp.2580-2607, 2021.

[10] Baugh, B., Ben-David, I., Park, H. and Parker, J.A., "Asymmetric consumption smoothing," *American Economic Review,* Vols. 111(1), pp.192-230., 2021.

[11] Kaur, P., Krishan, K., Sharma, S.K. and Kanchan, T., "ATM card cloning and ethical considerations," *Science and engineering ethics,* Vols. 25(5), pp.1311-1320., 2019.

[12] R. Yuvarani and R. Mahaveerakannan, "Payment Security Expert: Analyzing Smart Cards and Contactless Payments with Cryptographic Techniques," *in the 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India,* pp. 511-516, doi: 10.1109/ICSCSS60660.2024.10625350., 2025.

[13] Deshpande, K.V. and Singh, J., "A Systematic Review on Website Phishing Attack Detection for Online Users," *International Journal of Image and Graphics,* vol. p.2750013., 2025.

[14] Laxman, V., Ramesh, N., Prakash, S.K.J. and Aluvala, R., "Emerging threats in digital payment and financial crime: A bibliometric review," *Journal of Digital Economy,* Vols. 3, pp.205-222., 2024.

[15] Bugawa, A.M., "Blockchain technology trends in different sectors: A review," *Journal of Statistics Applications & Probability,* Vols. 13(2):691-706, 2024.

[16] Nadher, I. and Hameed, S.M., "Credit card fraud detection challenges and solutions: A review," *Iraqi Journal of Science,* pp. 2287-2303., 2024.

[17] Bin Sulaiman, R., Schetinin, V. and Sant, P., "Review of machine learning approach on credit card fraud detection," *Human-Centric Intelligent Systems,* Vols. 2(1), pp.55-68., 2022.

[18] Masiha, R.Y., "Effects of cryptocurrencies on global economics: A review study," *Qubahan Academic Journal,* Vols. 2(2), pp.9-15., 2022.

[19] Arifin, R., Atikasari, H. and Waspiah, W., "The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud," *Jurnal Hukum Novelty,* Vols. 11(2), pp.235-246., 2020.

[20] Chippagiri, S. and Ramesh, A., "PCI DSS: A Critical Analysis of Implementation, Effectiveness, and Legislative Impact in Payment Card Security," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* vol. 11, no. 1, pp. 1258-1266, 2025.

[21] worldpay, "Contactless payments: Definition, types, and examples," *worldpay, [available at]*

https://platforms.worldpay.com/blog/contactless-payments-definition-types-and-examples/, 2025.

[22] Gupta, K., Bhanodia, P., Sethi, K.K., Rajput, S., Patidar, M. and Iyer, V.H., "A Review on NFC for Secure Transaction its Fundamental Challenges and Future Directions," *In 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET),* pp. 1-7, IEEE, 2024.

[23] Yuspin, W., Putri, A.O., Fauzie, A. and Pitaksantayothin, J., "Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities," *International Journal of Safety & Security Engineering, ,* vol. 14(6), pp. 1699-1706, 2024.

[24] Madhavi, A. and Sivaramireddy, T., "Real-time credit card fraud detection using spark framework," *In Machine Learning Technologies and Applications: Proceedings of ICACECS 2020, Singapore: Springer Singapore.,* pp. 287-298, 2021.

[25] Andrew, A., Candy, C. and Robin, R., "Detecting fraudulent of financial statements using fraud score model and financial distress," *International Journal of Economics, Business and Accounting Research (IJEBAR),* Vols. 6(1), pp.696-707, 2022.

[26] Tanouz, D., Subramanian, R.R., Eswar, D., Reddy, G.P., Kumar, A.R. and Praneeth, C.V., "Credit card fraud detection using machine learning," *In 2021 5th international conference on intelligent computing and control systems (ICICCS), IEEE,* pp. 967-972, 2021.

[27] Yang, M.H., Luo, J.N., Vijayalakshmi, M. and Shalinie, S.M., "Contactless credit cards payment fraud protection by ambient authentication," *Sensors,* Vols. 22(5), p.1989., 2022.

[28] Abedin, N.F., Bawm, R., Sarwar, T., Saifuddin, M., Rahman, M.A. and Hossain, S., "Phishing attack detection using machine learning classification techniques," *In 2020 3rd International conference on intelligent sustainable systems (ICISS), IEEE,* pp. 1125-1130, 2020.

[29] European Payments Council (EPC), "European Payments Council Fraud Report," https://share.google/gkGPrA9IkNcDFZM3T, 2024.

[30] Onumadu, P. and Abroshan, H., "Near-field communication (nfc) cyber threats and mitigation solutions in payment transactions: A review," *Sensors,* Vols. 24(23), p.7423, https://doi.org/10.3390/s24237423, 2024.

[31] Bodker, A., Connolly, P., Sing, O., Hutchins, B., Townsley, M. and Drew, J., "Card-not-present fraud: Using crime scripts to inform crime prevention initiatives," *Security Journal, https://doi.org/10.1057/s41284-022-00359-w,* pp. 1-19, 2022.

[32] M. Younan, M. Elhoseny, A. A. Ali, and E. H. Houssein, "Quantum chain of things (qcot): A new paradigm for integrating quantum computing, blockchain, and internet of things," *in 2021 17th International Computer Engineering Conference (ICENCO). IEEE, 2021, pp. 101–106.*

[33] Nanda, A.P., Veluri, K.K. and Beura, D., "Role of ai in enhancing digital payment security," *African Journal of Biomedical Research,* pp. 2112-2119, 2024.

[34] Martinez, D., Magdalena, L. and Savitri, A.N., "Ai and blockchain integration: Enhancing security and transparency in financial transactions," *International Transactions on Artificial Intelligence,* Vols. 3(1), pp.11-20, 2024.

[35] Kashyap, D.N., Naikade, K., Pandey, A.K., Sharma, N., Hashmi, S. and Pund, S.S., "Enhancing Credit Card Data Security Using AI-integrated Encryption and Tokenization Framework," *ournal of Internet Services and Information Security (JISIS),* Vols. 15(1):316-29, 2025.

[36] Seera, M., Lim, C.P., Kumar, A., Dhamotharan, L. and Tan, K.H., "An intelligent payment card fraud detection system," *Annals of operations research,* Vols. 334(1), pp.445-467., 2024.