AI Security in Contactless Payments and Education: A Review

[1]Ahmed Hamed, [2]Yojna Bansal, [3]Mostafa Mohamad, [4]Angel Jimenez-Aranda, [5]Tarek Gaber
[1]Department of Computer Science, Faculty of Computers and Information, Damanhour University, 22511, Damanhour, Egypt
[1,2]Plekhanov Russian University for Economics in Dubai, Dubai, United Arab Emirates
[3]Zayed University, College of Interdisciplinary Studies, Abu Dhabi, United Arab Emirates
[4]Centre for Sustainable Innovation Salford Business School, The University of Salford, Manchester, United Kingdom
[5]School of Science Engineering and Environment, The University of Salford, Manchester, United Kingdom
[1]ahmed_hamed@cis.dmu.edu.eg, [2]Bansal.Y@reu.tech , [3]Mostafa.Mohamad@zu.ac.ae,
[4]a.jimenez-aranda@salford.ac.uk , [5]t.m.a.gaber@salford.ac.uk

***Abstract*— In today's digital economy, contactless credit cards have become central to financial transactions, offering speed and convenience through technologies such as Near Field Communication (NFC), embedded Wi-Fi, and mobile wallets. However, this shift has also expanded the cybersecurity attack surface. While artificial intelligence (AI)-driven fraud detection has advanced, emerging threats—particularly adversarial machine learning and ransomware targeting card infrastructure—remain underexplored in academic and industrial research. This survey examines the evolving security landscape of contactless credit cards, focusing on AI threats and corresponding defenses. It identifies vulnerabilities in NFC protocols and shows how adversarial examples can bypass traditional fraud detection. The study also explores the potential for ransomware and real-time attacks that exploit digital card systems. In parallel, it evaluates AI-based defensive frameworks, outlining their strengths, limitations, and feasibility in resource-constrained environments. Beyond technical insights, this work highlights the value of integrating such real-world challenges into computer engineering education. By linking AI security with embedded systems, protocols, and threat modeling, it proposes a curriculum framework to prepare students for modern cybersecurity demands. Finally, the paper identifies key research gaps and suggests future directions, including AI solutions to secure contactless payment ecosystems.**

***Keywords*— Credit Cards, Adversarial ML, NFC Security, Fraud Detection, Cybersecurity Education, Edge AI Defenses**

***JEET Category*— Research**

I. INTRODUCTION

The digital transformation of financial services has fundamentally reshaped how consumers interact with money. A major shift in recent years is the widespread adoption of contactless credit card payments, driven by mobile computing, wireless technologies, and the demand for fast, frictionless transactions. Mobile wallets, NFC-enabled cards, and smartphone-integrated virtual cards allow users to pay with a tap or scan—trends further accelerated by the COVID-19 pandemic, which emphasized hygiene and touch-free systems (Zhong & Moon, 2022). This evolving landscape not only demands secure systems but also presents an ideal real-world context for educating computer engineering students.

These systems rely on protocols like Europay MasterCard Visa (EMV) (Yang, Hsu, & Hsu, 2025), NFC standards (Kulkarni, 2021), and ISO/IEC frameworks (Malatji, 2023) to facilitate communication between devices and point-of- sale (POS) terminals. However, operating over short-range radio frequencies, they introduce new cyberattack surfaces. Researchers have demonstrated that attackers can exploit protocol and hardware weaknesses to perform relay attacks, skimming, cloning, and eavesdropping—even remotely (Yang, Luo, Vijayalakshmi, & Shalinie, 2022; Njebiu, Kimwele, & Rimiru, 2021; Ahamad, 2021).

To mitigate such threats, researchers have proposed various cryptographic solutions. Ambient authentication (Gangwal, Paliwal, & Conti, 2024), for example, uses environmental context (light, sound) to verify proximity and reduce relay risks (Yang et al., 2022). Challenge-response protocols based on proximity tokens and cryptographic key exchanges further enhance authentication (Njebiu et al., 2021). More advanced defense-in-depth architectures span hardware, application, and communication layers—using tools like BAN logic, AES, and ECDSA to secure transactions under adversarial conditions (Ahamad, 2021; Tafti, Mohammadi, & Babagoli, 2021).

Yet new risks emerge from within: financial institutions increasingly depend on AI and machine

Ahmed Hamed
Department of Computer Science, Faculty of Computers and Information, Damanhour University, 22511, Damanhour, Egypt
ahmed_hamed@cis.dmu.edu.eg

learning (ML) models for real-time fraud detection. Deep learning techniques such as Convolutional Neural Networks (CNNs) (Zhao et al., 2024), Long Short-Term Memory (LSTM) networks (Huang et al., 2022), and ensemble methods have achieved high perfor- mance in identifying fraudulent activity (Mienye & Jere, 2024; NISHMA, VENANKA, BANTU, MAMIDI, & MAMINDLA,
2024; Esenogho, Mienye, Swart, Aruleba, & Obaido, 2022). These AI techniques represent practical applications of com- puter engineering concepts, offering students opportunities to explore anomaly detection, neural networks, and adversarial robustness within critical financial infrastructures.

However, these models are not immune to attack. Adver- saries can craft inputs—adversarial examples—that appear le- gitimate but are designed to bypass detection systems (Kumar, Vimal, Kayathwal, & Dhama, 2021; Tsai, Cho, Yu, Chang, & Chao, 2024). In financial settings, this can be catastrophic, enabling fraudulent transactions to pass undetected.

Such vulnerabilities are especially concerning in black- box settings, where attackers can probe detection models through trial-and-error. Evolutionary black-box attacks like ESPA have proven highly effective with minimal queries, outperforming classic methods like Zeroth Order Optimization (ZOO), Boundary Attack, and HopSkipJump (Kumar et al., 2021; Balasubramanian & Ghadimi, 2022). Neuron activation monitoring has been proposed to detect such inputs, but remains in early stages and requires refinement for real-time deployment (Tsai et al., 2024).

Adding to the complexity is the growing threat of ran- somware, which increasingly targets mobile platforms, POS systems, and financial infrastructure. Cryptocurrencies such as Bitcoin enable anonymous ransom collection and fund transfer, complicating legal and technical responses (Katagiri, 2024). The expansion of cloud-connected and app-based payment systems has only broadened the attack surface. Understanding such threats is crucial for future engineers, as it bridges theoretical knowledge in systems security with real-world implications in fintech and digital infrastructure resilience.

Credit card fraud has evolved beyond stolen credentials to include full-system exploitation—from NFC protocols to AI models and cloud interfaces. Cardless technologies like bio- metric ATMs and QR-based payments, while innovative, intro- duce new and poorly understood attack vectors (Parameswaran et al., 2024).

This survey bridges fragmented research threads in fraud detection, contactless protocol security, adversarial machine learning, and ransomware. Existing surveys often isolate cryptographic and AI topics without analyzing their inter- play—particularly under adversarial pressure.

In this survey, we present a comprehensive and multidimen- sional review of threats and defenses in modern credit card payment systems. Our main contributions include:

- Categorization of attacks on contactless and NFC-based systems (e.g., relay, replay, cloning).
- Review of deep learning applications in fraud detection and vulnerabilities to adversarial examples.
- Analysis of ransomware's impact on cardless and mobile financial systems.
- Summary of key defenses, from ambient authentication to hybrid ML models, highlighting strengths and limitations.
- A research roadmap emphasizing adversarial robustness, dataset availability, and lightweight AI for mobile secu- rity.

By unifying these perspectives, we aim to support the design of resilient, AI-aware, and secure payment infrastructures. Additionally, this paper contributes to computer engineering education by contextualizing advanced security threats, crypto- graphic methods, and AI-based detection models within a real- world financial technology framework. The multidisciplinary nature of this topic provides a practical foundation for project- based learning and curriculum development in areas such as embedded systems, secure communication protocols, and adversarial machine learning.

LITERATURE REVIEW

A. Protocol-Level and Contactless Security

The rise of NFC-enabled devices and EMV-based contact- less cards has expanded the attack surface of payment systems, particularly due to the absence of strong mutual authentication and the wireless nature of communication. To counter these threats, researchers have proposed various protocol-level en- hancements.

A notable direction is ambient authentication, which uses environmental factors like noise and light to verify whether a user device and terminal share the same context—helping to prevent relay attacks without requiring extra hardware (Yang et al., 2022). Similarly, (Njebiu et al., 2021) proposes a challenge-response mechanism using proximity tokens and cryptographic key exchange to enforce physical presence, showing strong performance in practical implementations.

At a broader system level, (Ahamad, 2021) introduces a layered architecture—spanning hardware, mobile apps, and communication protocols—validated using tools like BAN logic and Scyther. This architecture defends against diverse threats including RAM scraping, Heartbleed, and phlashing. Another approach by (Tafti et al., 2021) replaces GSM's symmetric authentication with asymmetric cryptography, re- ducing key management overhead while improving resistance to eavesdropping and desynchronization.

Across these contributions, mutual authentication and prox- imity verification emerge as recurring themes. Despite promis- ing designs, real-world adoption remains

limited due to com- patibility challenges and the need for infrastructure upgrades. Furthermore, many solutions are evaluated in controlled set- tings, with little emphasis on interoperability or real-time deployment.

As contactless systems evolve toward mobile and cardless platforms, protocol security must adapt to support biometric authentication, edge computing, and integration with AI-driven fraud detection.

For computer engineering students, these protocols provide a valuable foundation in secure communication and embedded systems. Simulating or prototyping such architectures enables hands-on learning in hardware-software integration, crypto- graphic authentication, and edge-level security—key compe- tencies for future fintech and IoT applications.

B. AI-Based Credit Card Fraud Detection

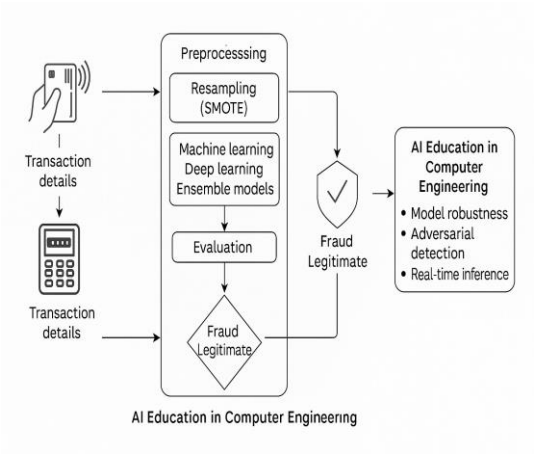

Fig. 1. System-Level AI-Based Credit Card Fraud Detection Workflow.

Machine learning has become a core component of modern credit card fraud detection, enabling institutions to process and evaluate vast volumes of transaction data in real time. As shown in Figure 1, these systems now span from transaction initiation through to model-driven classification. The field has evolved from rule-based systems to deep learning architectures capable of identifying complex, nonlinear fraud patterns.

In (Mienye & Jere, 2024), the authors review key deep learning models for fraud detection, including CNNs, RNNs, LSTMs, and GRUs, highlighting their ability to capture tem- poral dependencies in transaction streams. They also stress the importance of using metrics like AUC, F1-score, and precision-recall, especially given the class imbalance common in fraud datasets.

(NISHMA et al., 2024) compares traditional ML methods (SVM, Decision Tree, Logistic Regression) with deep learning approaches, showing that the latter offers significantly higher detection accuracy, albeit with greater computational costs and training complexity. They also note overfitting risks when using static datasets against evolving fraud behavior.

To improve model performance, (Esenogho et al., 2022) proposes an ensemble framework combining LSTM networks, AdaBoost, and hybrid resampling methods (SMOTE, ENN). Their approach addresses class imbalance while maintaining minority class integrity, yielding improved sensitivity and specificity over standalone models.

Despite these advances, challenges remain. Deep models often lack interpretability—an issue in financial systems where transparency is critical. Publicly available datasets remain lim- ited, restricting reproducibility. Additionally, most academic models are not optimized for real-time mobile deployment, where inference speed and model size are key constraints.

While AI has significantly advanced fraud detection capa-bilities, practical deployment still faces hurdles, particularly in mobile or resource-limited environments. Moreover, as discussed later, these models are vulnerable to adversarial threats that exploit their decision boundaries.

This domain offers rich opportunities for AI education in computer engineering programs. By working with fraud datasets and building deep learning pipelines, students gain hands-on experience in preprocessing, imbalance handling, and real-world model evaluation. These activities also foster discussions on explainable AI, ethical concerns, and adversar- ial robustness—core skills in intelligent system development.

C. Adversarial Machine Learning in Payment Systems

As shown in Figure 2, adversarial examples can compromise fraud detection pipelines by manipulating input data to deceive classifiers. These attacks exploit vulnerabilities in machine learning (ML) models used by financial institutions, allowing fraudulent transactions to be misclassified as legitimate.

Traditional fraud detection models learn from patterns in past transactions, but adversarial inputs are specifically crafted to exploit their decision boundaries. These subtle perturbations appear benign yet effectively bypass even highly accurate clas- sifiers—challenging the assumption that model performance guarantees security.

(Kumar et al., 2021) examines black-box attacks on state-of-the-art fraud models using two public datasets. Techniques

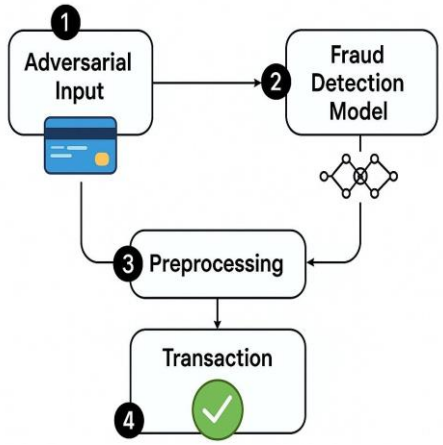

Fig. 2. Adversarial Attack Impact on Credit Card Fraud Detection Systems.

like Zeroth Order Optimization (ZOO), Boundary Attack, and HopSkipJump (HSJ) are evaluated, alongside their proposed Evolution-based Specialized Perturbation Attack (ESPA), which achieves high success with fewer queries—especially critical in limited-access real-world systems.

To defend against such threats, (Tsai et al., 2024) proposes monitoring internal neuron activations to detect adversarial inputs. Their method, tested with multiple generation tech- niques, shows promise for distinguishing adversarial from natural transactions. However, it still faces challenges related to adaptive attacks and real-time deployment.

These studies highlight that adversarial threats are not theoretical—they can undermine even robust ML systems. Current mitigation strategies, including adversarial training and internal detection, require further development to ensure generalizability and integration into live infrastructures.

As credit card systems increasingly rely on AI, adversarial robustness must be prioritized. Effective defenses will likely combine anomaly detection, introspective model analysis, and cryptographic safeguards to maintain trustworthy financial systems.

For computer engineering students, adversarial ML provides a practical lens to explore secure AI design. Labs and projects involving adversarial inputs can strengthen understanding of model vulnerabilities, robustness techniques, and real-world resilience—skills essential for AI-driven cybersecurity appli- cations in fintech.

D. Ransomware and Financial Infrastructure Threats

Beyond fraud and adversarial ML, financial systems increas- ingly face the growing threat of ransomware. Traditionally linked to enterprise data extortion, ransomware has evolved to target mobile payment platforms, banking apps, and digital wallets.

This threat has been amplified by the integration of contact- less payments with cloud services, mobile OSs, and decen- tralized financial systems. As discussed in (Katagiri, 2024), ransomware groups have adopted cryptocurrencies (e.g., Bit- coin, Monero, Ethereum) not only for anonymous payments but also as infrastructure for automating attacks, exploiting weak regulation, and leveraging poorly secured mobile apps. This intersection of technology, law, and finance has created fertile ground for such attacks.

Emerging environments—like cardless ATMs and QR-based payments—introduce additional risks, as highlighted in (Parameswaran et al., 2024). These systems rely heavily on APIs, cloud authentication, and token-based exchanges, often lacking the physical isolation of legacy card hardware. This makes them especially vulnerable to malware, privilege escalation, and ransomware campaigns.

Ransomware is now frequently coupled with credential theft, data exfiltration, and DDoS attacks. Compromised mo- bile wallets or financial apps can lead to encrypted assets, ma- nipulated transactions, and extortion via cryptocurrency—all with minimal traceability.

Despite the threat's evolution, defenses tailored specifically for the fintech-ransomware intersection remain limited. Mobile and cloud-based systems lack the robustness of enterprise setups like full-system rollbacks or endpoint isolation. More- over, existing studies often overlook ransomware's integration with broader financial manipulation schemes (e.g., disabling gateways, draining tokenized balances).

The urgency to build ransomware-aware payment platforms is clear. Future efforts should emphasize secure design, real- time threat detection, and cross-sector coordination. Cardless infrastructures, in particular, should embed anti-ransomware logic, context-aware authentication, and rollback mechanisms to prevent critical failure.

From an educational perspective, ransomware in financial systems provides an excellent multidisciplinary case study. It links AI and cybersecurity through intrusion detection, system recovery, and attack surface modeling—ideal for computer en- gineering students focused on intelligent, secure infrastructure.

DISCUSSION

This study highlights key insights at the intersection of AI and credit card security, emphasizing both the benefits and risks of modern financial technologies. While innovations like NFC, EMV, and mobile wallets enhance convenience, they also increase the attack surface.

At the protocol level, ambient authentication (Yang et al., 2022) and formal verification frameworks (Ahamad, 2021) provide effective defenses against relay and replay attacks. However, widespread adoption remains limited due to hard-ware constraints, integration challenges, and slow institutional uptake.

AI-based fraud detection has shown significant promise. Deep learning models such as CNNs and LSTMs outperform traditional ML approaches (Mienye & Jere, 2024; NISHMA et al., 2024), and ensemble methods (Esenogho et al., 2022) further improve detection, especially

when combined with techniques like SMOTE and ENN. Still, these systems are not immune to adversarial inputs (Kumar et al., 2021), and gradient-free attacks like ESPA demonstrate the feasibility of evading fraud detection in black-box settings.

Figure 1 illustrates how AI integrates into real-world payment pipelines—from transaction initiation to fraud detection—highlighting critical vulnerability points. As shown in

Figure 2, a single adversarial input can disrupt the entire pipeline if appropriate defenses are not in place.

Ransomware presents another layer of risk, particularly in cloud-connected and cardless payment environments (Katagiri, 2024). Emerging technologies like QR-based ATMs and app- based wallets (Parameswaran et al., 2024) introduce new vectors for attack, particularly when integrated with cloud authentication and mobile operating systems.

Educationally, this study offers a robust foundation for teaching AI security in computer engineering. From fraud detection pipelines to adversarial testing and protocol design, these use cases support hands-on labs and interdisciplinary learning. As summarized in Table I, students can gain expe- rience in adversarial robustness, secure embedded design, and ethical system development.

Future work should explore hybrid defenses combining cryptographic protocols with robust AI models, supported by adversarial training and optimized for mobile environments. Collaboration among academia, industry, and regulators is essential to standardize evaluation frameworks and promote secure-by-design practices in the evolving fintech ecosystem.

CONCLUSION

The rise of contactless credit cards and mobile payment systems has revolutionized financial transactions, delivering speed and convenience while introducing new security chal- lenges. These threats span multiple layers—from communi- cation protocols and AI-driven fraud detection to broader financial infrastructures increasingly targeted by ransomware. This survey provided a comprehensive review of threats and countermeasures across these layers. At the protocol level, we examined attacks like relay, replay, and cloning, alongside defenses such as ambient authentication and formal verification-based architectures. At the algorithmic level, we assessed the strengths and vulnerabilities of deep learning models used in fraud detection, particularly their exposure to adversarial manipulation. We also explored how ransomware exploits decentralized, mobile-based systems, expanding the
threat surface through cloud and app-based platforms.
Our synthesis revealed key gaps: limited adversarial robustness in AI models, a lack of standardized datasets for evaluating fraud and attack resilience, and minimal integration between security mechanisms and user experience. With financial systems increasingly moving to edge and mobile devices, there is a growing need for lightweight, explainable, and resilient AI architectures.
In addition to advancing research, this survey supports computer engineering education. Each layer of the payment ecosystem—NFC protocols, fraud analytics, adversarial AI, and ransomware defense—offers practical, real-world scenar- ios for courses in cybersecurity, machine learning, embedded systems, and digital forensics. These use cases foster both technical expertise and critical thinking around ethics and system-level design.
By aligning technical depth with pedagogical value, this work can inform curriculum development, interdisciplinary

TABLE I
EDUCATIONAL INTEGRATION OPPORTUNITIES BASED ON STUDY FINDINGS

Topic	Example Integration in Courses
AI Fraud Detection	Labs on imbalanced data (SMOTE), CNN-based classification
Adversarial ML	Projects on input perturbation, black-box model robustness
NFC / Protocol Security	Prototyping secure EMV/NFC modules in embedded systems
Ransomware Resilience	Case studies on layered defenses in mobile financial platforms

projects, and AI security labs—helping prepare future engineers for the complexities of secure, intelligent financial technologies.

Looking forward, future work should focus on unified frameworks that integrate protocol-level security, AI robustness, and end-to-end threat mitigation. Cross-sector collaboration between academia, industry, and regulators is essential to develop evaluation standards and embed secure-by-design principles in the evolving fintech landscape.

REFERENCES

Ahamad, S. S. (2021). A novel nfc-based secure protocol for merchant transactions. IEEE Access, 10, 1905–1920.

Balasubramanian, K., & Ghadimi, S. (2022). Zeroth- order nonconvex stochastic optimization: Handling constraints, high dimensionality, and saddle points. Foun- dations of Computational Mathematics, 22(1), 35–76.

Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. IEEE access, 10, 16400–16407.

Gangwal, A., Paliwal, A., & Conti, M. (2024). De-authentication using ambient light sensor. IEEE Access, 12, 28225–28234.

Huang, R., Wei, C., Wang, B., Yang, J., Xu, X., Wu, S., & Huang, S. (2022). Well performance prediction based on long short-term memory (lstm) neural network.

Journal of Petroleum Science and Engineering, 208, 109686.

Katagiri, N. (2024). From prepaid cards to bitcoin: How did ransomware hackers adopt cryptocurrencies? Journal of Cyber Policy, 9(2), 239–255.

Kulkarni, R. (2021). Near field communication (nfc) technology and its application. In Techno-societal 2020: Proceedings of the 3rd international conference on ad- vanced technologies for societal applications—volume 1 (pp. 745–751).

Kumar, N., Vimal, S., Kayathwal, K., & Dhama, G. (2021). Evolutionary adversarial attacks on payment systems. In 2021 20th ieee international conference on machine learning and applications (icmla) (pp. 813–818).

Malatji, M. (2023). Management of enterprise cyber security: A review of iso/iec 27001: 2022. In 2023 international conference on cyber management and engineering (cy- maen) (pp. 117–122).

Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. IEEE Access.

NISHMA, B., VENANKA, S., BANTU, V. K., MAMIDI, S. K., & MAMINDLA, R. (2024). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. International Journal of HRM and Organizational Behavior, 12(2), 169–180.

Njebiu, V., Kimwele, M., & Rimiru, R. (2021). Secure contactless mobile payment system. In 2021 ieee latin- american conference on communications (latincom) (pp. 1–6).

Parameswaran, S., Gogia, Y., Williams, M. J., Nayak, R., Ashfaq, A., Monica, L., & et al. (2024). Cardless society: Assessing the role of cardless atms in shaping the future of financial transactions. In 2024 interna- tional conference on trends in quantum computing and emerging business technologies (pp. i–v).

Tafti, F. S. M., Mohammadi, S., & Babagoli, M. (2021). A new nfc mobile payment protocol using improved gsm based authentication. Journal of Information Security and Applications, 62, 102997.

Tsai, M.-Y., Cho, H.-H., Yu, C.-M., Chang, Y.-C., & Chao, H.-C. (2024). Effective adversarial examples identification of credit card transactions. IEEE Intelligent Systems.

Yang, M.-H., Hsu, Y.-S., & Hsu, H.-C. (2025). Enhanced emv security: Preventing credit card fraud from a distance. IEEE Access.

Yang, M.-H., Luo, J.-N., Vijayalakshmi, M., & Shalinie, S. M. (2022). Contactless credit cards payment fraud protection by ambient authentication. Sensors, 22(5), 1989.

Zhao, X., Wang, L., Zhang, Y., Han, X., Deveci, M., & Parmar, M. (2024). A review of convolutional neural networks in computer vision. Artificial Intelligence Review, 57(4), 99.

Zhong, Y., & Moon, H.-C. (2022). Investigating customer behavior of using contactless payment in china: A comparative study of facial recognition payment and mobile qr-code payment. Sustainability, 14(12), 7150.