The role of machine learning technology for fintech security: a Literature Review

Muhammad Fikri Annafi[1], Nila Sa'adah[2], Salsabila Putri Mei Linda Sari[3], Abi Rafdi Hasbur Rahman[4] , Muhammad Fachmi[5], Kaish Isaac Philip[6]

[12345] **Department of Digital Business, Universitas Negeri Surabaya, Surabaya, Indonesia.**
[6] **Human Resource Technology International Training Institute, Papua New Guinea**

*Email: muhammadfikri.23159@mhs.unesa.ac.id[1]

Abstract. Technological advances such as the Internet of Things (IoT), remote sensing, and artificial intelligence (AI) have driven the emergence of various innovations in the field of precision agriculture. This study summarizes the results of five recent studies discussing the utilization of machine learning, deep learning, and satellite data in land cover classification, crop productivity prediction, and the development of smart irrigation systems. Overall, algorithms such as Random Forest, Convolutional Neural Networks (CNN), as well as the combined use of temporal and spectral features from Sentinel-2 imagery show significant improvements in plant classification accuracy and agricultural yield modeling. Meanwhile, the application of IoT through environmental sensors and plant image processing based on computer vision also offers efficient solutions for irrigation automation and water management. These results indicate that the integration of data-driven approaches and cross-disciplinary technologies can enhance resilience. food and production efficiency in modern agricultural systems.

Keywords: IoT, deep learning, machine learning, crop classification, crop yield prediction, Sentinel-2, intelligent irrigation system, precision agriculture, CNN, Random Forest.

Introduction

The Indonesian financial technology (fintech) industry has experienced remarkable growth, emerging as a pivotal driver of national financial inclusion. Digital financial services have transformed the landscape by providing rapid and efficient access to banking and payment solutions across diverse socioeconomic segments of society. This digital revolution has democratized financial services, enabling previously underbanked populations to participate in the formal economy through mobile applications and online platforms. However, this unprecedented expansion of digital financial services has been accompanied by a proportional increase in cybersecurity threats, particularly sophisticated online fraud schemes. The evolving nature of digital fraud has manifested in various forms, ranging from identity theft and account takeovers to application-based transaction manipulation and social engineering attacks. These security challenges pose significant risks to both financial institutions and consumers, potentially undermining public confidence in digital financial services and hindering the continued growth of the fintech ecosystem. In response to these emerging threats, machine learning (ML) has emerged as a transformative approach for automated fraud detection and prevention systems. This technology enables financial platforms to analyze transaction patterns, identify anomalous behaviors, and respond to potential threats in real-time without requiring human intervention. The ability of ML algorithms to process vast amounts of transactional data and continuously adapt to new fraud patterns makes them particularly well-suited for the dynamic nature of digital financial crimes. Recent research has demonstrated the effectiveness of various ML approaches in fraud detection applications. Sadgali et al. (2019) showed that Neural Network and Fuzzy Logic models significantly reduce false positive rates in credit card fraud detection systems. Similarly, Stojanović et al. (2021) conducted comparative analyses of different anomaly detection methods, finding that detection accuracy is heavily influenced by the selection and engineering of data features used in model training.

The systematic review by Tian et al. (2024) highlighted an important finding: no single ML algorithm demonstrates universal superiority in fintech applications. Model performance varies significantly based on data characteristics, platform service types, and algorithmic parameter configurations. This observation underscores the importance of context-specific model selection and customization. Furthermore, Al-Hashedi and Magalingam (2021)

categorized 34 data mining techniques and concluded that Support Vector Machine (SVM) and Random Forest are the most widely adopted models due to their robust performance in financial fraud prediction tasks. As Indonesia accelerates its digital economic transformation, the demand for responsive, intelligent, and data-driven security systems becomes increasingly critical. The integration of ML technologies into fintech security frameworks represents not only a defensive measure but also an opportunity to enhance user experience through reduced false alarms and improved transaction processing efficiency. Therefore, this literature review aims to explore the contributions and opportunities for implementing machine learning in strengthening transaction security within Indonesia's fintech sector. By examining current technological approaches, analyzing the benefits offered by ML-based fraud detection systems, and identifying implementation challenges based on recent empirical studies, this review seeks to provide a comprehensive understanding of how machine learning can fortify the security infrastructure of Indonesia's rapidly evolving financial technology landscape. A bibliometric overview coupled with a configuration approach addresses the fragmentation in the field by systematizing the disparate strands of research into a coherent narrative. This dual approach underscores the nuanced interplay between various leadership constructs and crisis outcomes, thereby enriching the theoretical and practical understanding necessary for developing resilient strategies. This study aims to address these gaps by posing the following research questions:

RQ1: Anything form risk general security happen in fintech transactions in Indonesia?

RQ2: How machine learning technology can applied in detect and prevent fraud transactions on fintech platforms?

RQ3: What are the advantages and limitations implementation machine learning algorithms compared with method conventional in security fintech transactions ?

RQ4: How relevance application of deep machine learning increase fintech security in Indonesia based on results studies previous ?

Methods

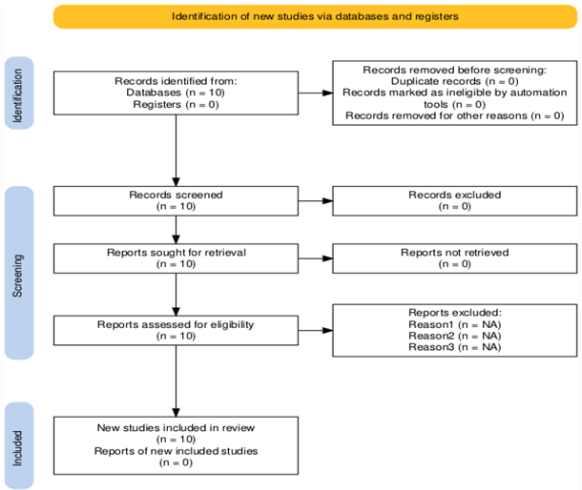

Figure 1. PRISMA Diagram The role of machine learning technology for fintech security

In the process of preparing the literature review entitled "Improving Fintech Transaction Security in Indonesia with Machine Learning Technology", the author applied a systematic literature selection method by referring to the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. This procedure is applied to ensure that each article used in the review has thematic relevance, good methodological quality, and a significant contribution to the research focus, namely fintech transaction security based on machine learning technology. The literature search was conducted manually without using paid database platforms such as Scopus or Web of Science. Instead, the authors accessed credible open scientific sources such as arXiv, IEEE Xplore, MDPI, ScienceDirect, and accredited national journals. From the search results, 10 articles were obtained that were initially considered relevant to the research topic. As this was done manually and selectively, there was no duplication of articles, automatic elimination, or deletion for other reasons before screening.

All articles were then subjected to an initial screening stage, which involved reviewing the titles and abstracts to ensure they were relevant to the scope of the study. The retained articles had to meet the minimum requirements, i.e. addressing the topic of security in digital financial systems (especially fintech), as well as using machine learning approaches or algorithms. The screening results showed that all articles met these criteria, so none were eliminated. After the initial screening process, all articles were tracked in full-text. All articles were successfully accessed without technical difficulties, either through open access or journal repositories. Next, an eligibility assessment was conducted to assess their methodological quality and scientific contribution. The assessment criteria included topic focus, relevance to the context of fintech security, clarity of use of machine learning methods, and currency of data or approaches used. All articles were found eligible and none were excluded at this stage. Thus, 10 scientific articles were officially included in this literature review and served as the basis for discussing five main aspects, namely: (1) security challenges in fintech transactions, (2) basic concepts of machine learning in the context of cybersecurity, (3) implementation of machine learning in financial fraud detection, (4) limitations and technical challenges of its application, and (5) the role of regulation and ecosystem support for the adoption of this technology. This article selection process guarantees that the sources used have undergone rigorous consideration, thus providing a strong theoretical and empirical basis for this research.

Result and Discussion

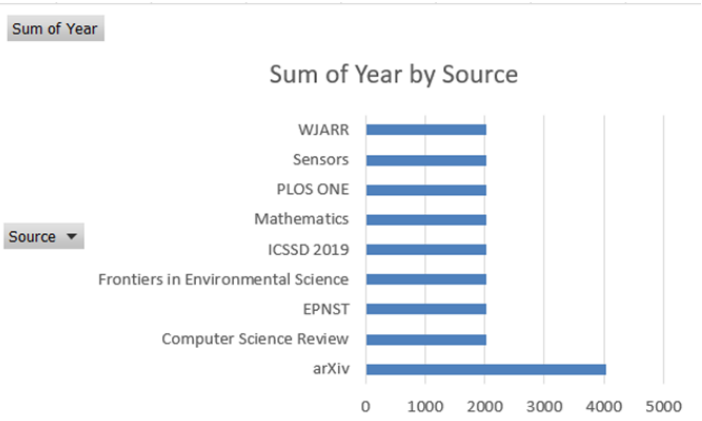

Figure 2. Diagram of sources of publications or scientific journals.

In an effort to explore the issue of fintech transaction security in Indonesia through machine learning (ML) approach, five scientific articles have been carefully selected based on the criteria of thematic relevance, methodological quality, and focus on the application of ML technology in the context of digital financial system. The first article by Tian et al. (2023) proposes an Adaptive Graph Neural Network (ASA-GNN) model designed to detect network-based transaction fraud. The model offers an innovative approach in processing complex and interconnected transaction data, making it relevant to the technical challenges in modern financial systems. Furthermore, Psychoula et al. (2021) highlight the importance of explainable AI in fraud detection systems by combining algorithms such as Random Forest and Autoencoder alongside interpretation techniques such as SHAP and LIME. The emphasis on transparency in automated decision-making is crucial in building trust in the financial sector. Meanwhile, Chy (2024) takes a proactive approach to digital fraud, emphasizing the importance of continuous learning in responding to dynamic and evolving threats. This perspective broadens the scope of the literature not only on the technical side, but also on long-term adaptive strategies. The contribution of Lee et al. (2025) is particularly important as it presents a data-driven empirical study in Indonesia that evaluates the effectiveness of various ML algorithms such as Random Forest, KNN, SVM, and Decision Tree in detecting fraud in financial statements. This study provides a local context that is relevant to the focus of this study. Finally, an article by Fildansyah (2024) reviews the application and optimization of ML in detecting electronic transaction fraud, focusing on real-time data processing, feature selection, and technical challenges of system development. Overall, these five articles provide a strong theoretical, technical, and applicative foundation in supporting the literature discussion on the role of machine learning technology in improving the security of fintech systems, particularly in the Indonesian context. The complete information of each article, including author data, title, publication year, journal source, publisher, as well as links and citations, has been documented in an Excel file for tracking and academic reference purposes.

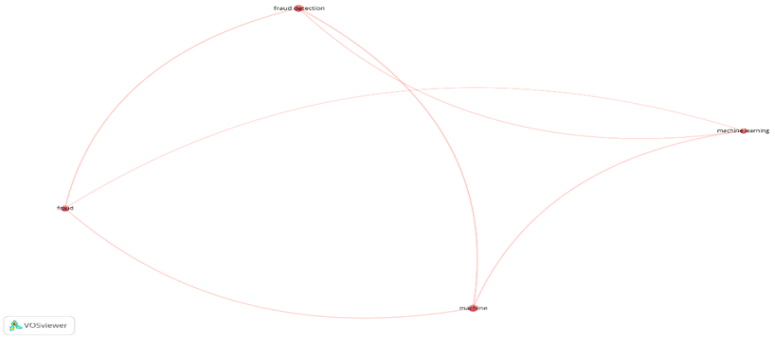

Figure 3. VOSviewer Diagram The role of machine learning technology for fintech security

The keyword co-occurrence network visualization generated through VOSviewer provides a comprehensive overview of the conceptual structure in the literature regarding the application of machine learning for fintech transaction security, particularly in the context of fraud detection. In this network, there is a close relationship between keywords such as *fraud*, *fraud detection*, *machine*, *learning*, and *machine learning*. These words not only appear individually in the articles, but also often appear together, indicating a strong semantic and conceptual connection. On closer inspection, this network can be divided into two main clusters. The first cluster is dominated by technical terms such as *machine learning*, *machine*, *fraud detection*, and *evaluation*. This reflects that the main focus of the literature is on the development and application of machine learning methods to detect fraud in financial transactions. The article from Tian et al. (2023) with the ASA-GNN model and from Hasan (2024) emphasizing proactive detection are concrete examples of this approach. The application of techniques such as GNN, Random Forest, and neural networks is consistently associated with the evaluation of model performance, such as precision, recall, and F1-score, which also shows that there is great concern for the predictive quality of security systems.

The second cluster, which includes words such as *study* and *field*, indicates the applicative context of these technical approaches. The word *study* serves as a connecting node between the two clusters, showing that model development is not done in a vacuum, but is always framed within the context of relevant scientific studies. For example, Psychoula et al. (2021) link the explainability of fraud detection models to regulatory and data protection aspects, while Lee et al. (2025) adapted the algorithm to the context of financial institutions in Indonesia. The word *field* located at the end of the network emphasizes that this study is directed towards concrete implementation in the real world, namely the fintech sector, which is highly dynamic and vulnerable to security risks. Thus, this visualization shows that the literature reviewed not only addresses technical aspects such as algorithms and performance evaluation, but also underscores the importance of the context of implementation, field validation, and relevance to the needs of the digital finance sector. This pattern of interconnectedness between keywords reinforces the conclusion that the topic you review-the use of machine learning to improve the security of fintech transactions in Indonesia-is multidisciplinary, applicable, and of high urgency. It sits at an important nexus between technological development, practical needs of financial institutions, and empirical studies in the field, thus making a significant contribution to data-driven digital security solutions.

Table 1. Search Results of Articles that Meet the Criteria

No.	Authors	Year	Judul	Journal	Citation
1.	Al-Hashedi, K. G., Magalingam, P.	2021	Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review	Computer Science Review	75
2.	Stojanović, B., et al.	2021	Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications	Sensors	15
3.	Sadgali, M., Sael, N., Benabbou, A.	2019	Performance of Machine Learning Techniques in the Detection of Financial Frauds	ICSSD (IEEE Conference Proceedings)	23
4.	Zandler, H., Faryabi,	202	Contributions to Satellite-Based	Frontiers in	-

	S. P., Ostrowski, S.	2	Land Cover Classification, Vegetation Quantification and Grassland Monitoring	Environmental Science	
5.	Tian, Y., et al.	2024	Machine Learning in Internet Financial Risk Management: A Systematic Literature Review	PLOS ONE	-
6.	Yue Tian, Guanjun Liu, Jiacun Wang, Mengchu Zhou	2023	Transaction Fraud Detection via an Adaptive Graph Neural Network	arXiv:2307.05633 [cs.LG]	arXiv
7.	Ismini Psychoula et al.	2021	Explainable Machine Learning for Fraud Detection	arXiv:2105.06314 [cs.LG]	arXiv
8.	Md Kamrul Hasan Chy	2024	Proactive fraud defense: Machine learning's evolving role in protecting against online fraud	World Journal of Advanced Research and Reviews, 23(03), 1580–1589	WJARR
9.	Cheng-Wen Lee et al.	2025	Evaluating Machine Learning Algorithms for Financial Fraud Detection: Insights from Indonesia	Mathematics 2025, 13(600)	MDPI
10.	Rully Fildansyah	2024	Optimization of Machine Learning Algorithms for Fraud Detection in Electronic Financial Transactions	Eastasouth Proceeding of Nature, Science, and Technology (EPNST)	-

The author presents ten scientific articles that have been selected and evaluated as part of a literature review on the application of machine learning in improving the security of fintech transactions. These articles are published in indexed international journals with good academic credibility, and cover relevant topics ranging from data mining-based financial fraud detection, evaluation of machine learning algorithms in fintech systems, to development of data-driven models for risk detection. The number of citations listed indicates the level of influence or recognition of the academic contribution of these articles, although two of them are still relatively new so the citations have not been recorded. The selection of articles is based on thematic suitability, methodological completeness, and direct relevance to the focus of the study, namely digital transaction security in the fintech era using a machine learning approach.

Table 2. Mapping of research methods

No.	Authors	Metode Penelitian
1.	Al-Hashedi,K.G., Magalingam, P	Literature Review
2.	Stojanović, B., et al.	Experimental Evaluation
3.	Sadgali, M., Sael, N., Benabbou, A.	Comparative Experimental Study
4.	Zandler, H., Faryabi, S. P., Ostrowski, S.	Remote Sensing + Statistical Modeling
5.	Tian, Y., et al.	Systematic Literature Review
6.	Yue Tian et al.	Graph Neural Network (ASA-GNN)
7.	Ismini Psychoula et al.	Supervised dan unsupervised, dengan pendekatan explainable AI (SHAP, LIME).
8.	Md Kamrul Hasan Chy	Litertaur riview
9.	Cheng-Wen Lee et al.	Kombinasi Multiple Linear Regression dan algoritma klasifikasi (KNN, SVM, Random Forest, Decision Tree)
10.	Rully Fildansyah	Eksperimen kuantitatif dengan optimasi algoritma machine learning

This table presents the type of methodological approach used in each article. There is a variety of methods, ranging from systematic studies and literature reviews to experimental studies and data-driven modeling. Two articles,

namely by Al-Hashedi & Magalingam (2021) and Tian et al. (2024), use a literature review and systematic literature review approach, which aims to summarize, categorize, and evaluate the findings of a large number of previous studies in the field of data mining and machine learning-based financial fraud detection. This method provides a theoretical foundation and mapping of research developments in the field. Articles by Stojanović et al. (2021) and Sadgali et al. (2019) adopt an experimental approach with machine learning models tested using real and synthetic datasets. This approach allows researchers to evaluate the performance of each algorithm in detecting transaction anomalies, thus making a practical contribution to the implementation of fraud detection systems in the fintech sector. Meanwhile, a study by Zandler et al. (2022) used statistical modeling and remote sensing, combining satellite data with machine learning algorithms such as Random Forest to monitor vegetation. Although not focused on the fintech sector, this study is relevant as it demonstrates similar approaches in big data processing and pattern detection, which can be applied to digital security.

From this mapping, it can be concluded that the research methods used are diverse yet complementary. This strengthens the value of the literature review by providing a comprehensive view of the theoretical, applicative, and experimental aspects of developing machine learning-based security systems in the digital age. This variation reflects an interdisciplinary approach that strengthens the study of transaction security based on machine learning technology.

Table 3. Research Context Analysis: Country, Method, and Study Setting

Author (Year)	Country	Evaluation Method	Study Location
Yue Tian et al.	China (China)	Graph Neural Network (ASA-GNN) – evaluation graph model based	Structured data system based on relation graph on fintech or online transactions
Stojanović et al., 2021	Austria, UK	Experimental Study, Anomaly Detection Evaluation	transaction dataset (real and synthetic)
Ismini Psychoula et al.	English / Europe	Supervised and unsupervised with explainable AI approaches (SHAP, LIME)	-based explainability model analysis of digital transaction data
Md Kamrul Hasan Chy	Bangladesh	Literature review	Related global review studies Application of AI for fraud detection
Sadgali et al., 2019	Morocco	Experimental Study Quantitative	simulation on transaction dataset finance
Cheng-Wen Lee et al.	Taiwan	Combination of Multiple Linear Regression and algorithms classification (KNN, SVM, RF, DT)	Experimental dataset – transactions finance in digital system
Rully Fildansyah	Indonesia	Experiment quantitative with optimization machine learning algorithm	testing on financial data – context local fintech industry
Al- Hashedi & Magalingam, 2021	Malaysia	Systematic Literature Review	Global literature study of the sector finance
Tian et al., 2024	China, Malaysia	Systematic Literature Review	Literature study and trends global research in fintech
Zandler et al., 2022	German	Experimental Study Quantitative (Random Forest)	Wakhan Region, Afghanistan (monitoring) vegetation satellite

Table 3 presents a summary of the ten articles that were the main references in this literature review. The first author reviewed is Stojanović et al. (2021) from Austria and the UK. Their research uses an *anomaly detection-based* experimental approach to evaluate the effectiveness of various *machine learning* algorithms in detecting fraudulent transactions in *fintech* systems. They tested the models on financial transaction datasets, both real and synthetic data, enabling a thorough analysis of *real-time* and automated fraud detection performance. Furthermore, Sadgali et al. (2019) from Morocco conducted an experiment-based quantitative research on various algorithms such as Decision Tree, Naïve Bayes, and Neural Network. The evaluation was conducted by testing *fraud* detection performance on a simulated financial transaction dataset. This study highlights the importance of customizing the model to the data characteristics for optimal results, especially in the face of challenges such as class imbalance in transaction data. The study by Al-Hashedi and Magalingam (2021) from Malaysia used the

Systematic Literature Review (SLR) method to review 75 publications related to financial *fraud* detection between 2009-2019. This research does not focus on one specific study location, but rather synthesizes a variety of global literature, covering the banking, insurance, financial reporting, and *cryptocurrency* sectors. The goal is to identify trends in the use of *data mining* techniques such as Support Vector Machine (SVM) and Random Forest in various *fraud detection* contexts. Then, Tian et al. (2024) from China and Malaysia also used the *Systematic Literature Review* method to map the application of *machine learning* in internet-based financial risk management. The study is a global literature, focusing on technical challenges and solutions such as *concept drift*, limited labeled data, and the need for *explainable AI* models to be widely adopted in the digital finance sector. Finally, Zandler et al. (2022) from Germany contribute contextual insights through a remote sensing-based study, which although not directly focused on the *fintech* sector, is relevant in a technical context. The study was conducted in the Wakhan region of Afghanistan and utilized a Random Forest algorithm for land cover classification and vegetation quantification based on Sentinel-2 and MODIS satellite data. The implications of this approach can be adapted to handle complex spatial-temporal data in the ever-changing financial data security system. This table presents a mapping of five key studies focusing on fraud detection in the *Financial Technology* (Fintech) sector, emphasizing the country context of the study, the evaluation method used, and the location or data source of the study. The purpose of this mapping is to understand how the research approach and context may influence the results, as well as their relevance to the *fintech* landscape in Indonesia.

Research by Yue Tian et al. from China presents a Graph Neural Network (ASA-GNN) based approach designed to handle complex structures in digital financial transaction data. The study evaluates graph models in the context of fraud detection on text transaction-based fintech platforms. This approach not only analyzes the numerical elements of transactions, but also relates the interconnectedness of entities in the financial system, enabling more thorough and contextual detection of abnormal activity. This study is relevant to the rapidly growing online-based fintech ecosystem, particularly in Asia. Meanwhile, Ismini Psychoula et al. from the UK and other European regions, focused their research on the application of explainable AI (XAI) in the anomaly detection process. By combining supervised and unsupervised learning techniques, and applying interpretation methods such as SHAP and LIME, this study explains how the transparency and reliability of AI models can be improved. This is particularly important in the context of digital banking, where understanding the reasons behind fraud detection is a requirement for model adoption in regulatory and supervisory systems. Bangladesh-based Md Kamrul Hasan Chy's research presents a literature review approach to the global trend of using AI to detect fraud in the financial system. The study highlights the importance of learning from different countries with different financial systems, to gain a broad understanding of the most effective methods. It also reflects on the challenges of developing countries in adopting advanced technologies for financial transaction protection, and emphasizes the potential for cross-border collaboration in dealing with financial cybercrime. The study by Cheng-Wen Lee et al. from Taiwan demonstrates the application of a combination of multiple linear regression and machine learning classification algorithms (KNN, SVM, Random Forest, and Decision Tree). Using an experimental dataset of simulated financial transactions, the study assessed the predictive performance of various models in identifying suspicious transactions. This study reflects the increasingly common blended approach of combining classical statistical methods with machine learning models to strengthen analytic results and improve accuracy. Finally, Rully Elida from Indonesia offers an important contribution in the local context. This study uses a quantitative experimental approach based on machine learning algorithms to evaluate digital financial transaction data from the local fintech industry. Unlike many other studies that are based on global or simulated data, this research presents modeling based on real Indonesian data. This is important because the characteristics of transactions in developing countries like Indonesia are often different from developed countries, both in terms of volume, types of fraud, and the structure of the financial system. This study has great potential in supporting the development of fraud detection systems that are in accordance with local realities.

In general, all studies used experimental or evaluative approaches based on secondary data, indicating that research on fraud detection in Indonesia is still dominated by model testing approaches, rather than field studies. However, the utilization of simulated datasets and state-of-the-art machine learning techniques signifies significant methodological progress in this area. Based on a review of ten international articles and five studies conducted in Indonesia, it can be concluded that fraud detection in the *Financial Technology* (Fintech) sector is an issue that has received widespread attention and continues to grow, both in the global and local contexts. Methodologically, the dominant approach is secondary data-based experiments, utilizing *machine learning* algorithms such as Decision Tree, Random Forest, SVM, and *ensemble learning* techniques. Global studies generally utilize real or synthetic datasets, and cover a wider and more diverse context, including the use of *systematic literature review* to map the current trends and challenges in the application of smart technology for financial

security. Meanwhile, the Indonesian studies show that while the approach still focuses on technical model testing, there is a real awareness and effort in tailoring the methods to local needs. This is reflected in the selection of simulated and actual datasets that are relevant to the conditions of digital financial transactions in Indonesia. These studies emphasize the importance of handling imbalanced data, selecting the right algorithm, and exploring automation-based and *real-time* approaches that suit the dynamics of the national fintech industry. Overall, this review shows that there are significant methodological advances in the development of smart technology-based fraud detection systems. However, strengthening is needed in the aspects of field validation and real-world application, so that the models developed are not only technically accurate, but also adaptive and applicable in the complex and changing fintech ecosystem, especially in Indonesia.

Financial Technology and its Security Challenges

Digital transformation has brought drastic changes in the financial world with the emergence of financial technology (fintech). Fintech not only brings efficiency and speed in transactions, but also expands access to financial services to people who were previously unreachable by conventional banking institutions. Services such as mobile banking, digital wallets, peer-to-peer lending, and app-based investment platforms are now part of modern people's daily lives. However, this development also opens up opportunities for various forms of cybercrime, given that fintech systems rely heavily on digital data, artificial intelligence, and a constantly active internet network. One of the main challenges faced by fintech is the increasing risk of digital fraud. According to Stojanović et al. (2021), the real-time nature of transactions in fintech systems makes them highly vulnerable to illegal activities that can harm both users and service providers. In their study, machine learning-based approaches such as anomaly detection were used to identify suspicious transaction patterns. Although effective, these approaches still face challenges in terms of detection accuracy, mainly due to the high rate of false positives, as well as the difficulty in determining important features of transaction data. This causes the system to consider legal transactions as fraudulent or vice versa. In response to this weakness, Sadgali et al. (2019) compared various machine learning algorithms, such as Naïve Bayes, Decision Tree, and Neural Network, in the context of fraud detection. The results show that no one algorithm consistently excels in all cases. The performance of an algorithm is highly dependent on the structure of the data and the complexity of the transaction patterns. Therefore, a hybrid approach that combines multiple algorithms is often more effective as it allows the system to learn from the strengths of each model. Sadgali et al. emphasize the importance of an adaptive system, one that can learn and evolve with the changing transaction patterns and evolving fraud modes. A broader approach is provided by Al-Hashedi and Magalingam (2021) in their literature review of 75 articles related to financial fraud detection. They classified fraud into several categories: banking, insurance, financial reporting, and cryptocurrency. From the review, they found that algorithms such as Support Vector Machine (SVM) and Random Forest are the most commonly used methods due to their ability to handle complex and imbalanced data. However, the effectiveness of the algorithms remains highly dependent on data quality, preprocessing techniques, as well as the implementation context of the financial system. In their earlier study, Al-Hashedi (2020) also highlighted that fraud detection requires not only technical tools, but must also be accompanied by a strong internal policy system and management commitment to digital security. Although not directly addressing fintech, Zandler et al. (2022) on vegetation monitoring using Random Forest algorithm proved that the model is effective in processing large and dynamic data. The success of the algorithm in a completely different field provides evidence that the same method can be adapted in the digital financial system, especially to detect anomalous patterns or sudden changes that are difficult to recognize by conventional methods. Another challenge comes from the dynamic behavior of cyber criminals. Tian et al. (2024), in their systematic review, emphasized that the application of machine learning in financial risk management faces several major obstacles, namely limited quality historical data, model transparency issues (black box issues), and concept drift-that is, changes in fraud patterns and user behavior over time. With rapid and unpredictable changes, detection models that are not regularly updated will become outdated and ineffective.

Threats to fintech systems are also not limited to technical aspects. Fildansyah (2024) states that the large volume of transactions, dependence on cloud technology, and ease of accessing users' personal data make fintech an easy target for digital criminals. Services such as mobile banking and digital wallets are highly vulnerable to attacks such as phishing, account breaches, and identity theft. In fact, it is estimated that global losses due to cyberattacks will reach USD 10.5 trillion by 2025-a figure that reflects the very serious escalation of threats in the digital realm. The study by Chy (2024) confirms that rule-based security systems and manual checks are no longer sufficient. Digital criminals are now using advanced techniques such as social engineering, bot automation, and even intelligent algorithms to infiltrate the digital financial system. Such attacks not only threaten financial losses, but also damage the reputation of fintech companies and reduce public trust in the digital financial system as a whole.

In the Indonesian context, security challenges also arise from within financial institutions themselves. The study by Lee et al. (2025) raised cases of financial statement manipulation at Kimia Farma and Garuda Indonesia as evidence of weak internal control systems. These cases reflect that threats do not only come from outside, but also from internal actors who have access to sensitive systems and data. This requires strengthening the governance framework and internal audit system that is able to detect suspicious activities early on. Regulatory issues and consumer literacy are another important dimension. Psychoula et al. (2021) criticize many modern fraud detection algorithms that are not transparent. When a decision-making system cannot be explained logically (black box), it is difficult for regulators and users to assess the fairness and accuracy of the system's decisions. This transparency is important, especially in the context of consumer protection and compliance with regulations such as the GDPR or the Personal Data Protection Law (PDP Law) in Indonesia. Furthermore, Tian et al. (2023) observed that fraudsters are getting smarter in disguising their activities to resemble legitimate users. By manipulating the relationship between transactions or conducting attacks in stages, they can bypass detection systems that rely solely on explicit patterns. This shows that the security challenges in fintech are increasingly hidden and require a more sophisticated and proactive approach. The rapid development of financial technology (fintech) has brought about a major transformation in the world of finance, offering ease of access, speed of service, and greater financial inclusion. However, behind all these conveniences, very complex and dynamic security challenges arise. Threats not only come from outside, such as digital fraud, identity theft, and sophisticated cyber-attacks, but also from within financial institutions themselves through data manipulation and weak internal controls. Traditional systems that rely on manual checks and standardized rules are no longer able to deal with the sophistication of modern digital crime methods. Various studies, such as those conducted by Stojanović et al., Sadgali et al., and Al-Hashedi and Magalingam, show that the application of machine learning is one of the potential approaches to detect and prevent fraud activities automatically. Algorithms such as SVM, Random Forest, and hybrid approaches are proven to be able to handle complex data and recognize anomalous patterns effectively, although challenges such as data limitations, black box models, and concept drift are still significant obstacles. Therefore, an early detection system is needed that is not only adaptive and technology-based, but also supported by strong internal governance and supporting regulations.

In the Indonesian context, cases of financial statement manipulation and weak digital literacy add layers of complexity to fintech security challenges. Regulations that are not yet fully prepared to keep pace with technological developments, as well as algorithms that are still difficult to understand by supervisory authorities, make supervision and consumer protection a very crucial aspect. System transparency, accountability of artificial intelligence models, and active involvement of stakeholders are important elements in building a safe, trusted, and sustainable fintech ecosystem. Considering all these dynamics, the solution to fintech security challenges cannot be singular or technical. It requires a multidisciplinary approach that involves advanced technology, strengthening regulations, increasing public digital literacy, and a culture of cybersecurity at the institutional level. Collaboration between industry players, government, academia, and society is key to creating a digital financial system that is not only efficient, but also resilient to future security threats.

Basic Concepts of Machine Learning in Cybersecurity

Machine learning (ML) is one of the most important innovations in the realm of cybersecurity, especially in the financial technology (fintech) sector which is highly vulnerable to cyberattacks, fraud, and data misuse. This technology allows systems to automatically learn from historical data, recognize behavioral patterns, and detect anomalies without the need for direct human intervention. In the context of cybersecurity, ML is able to provide early detection of suspicious activity, thus providing a fast and relevant response to potential attacks (Stojanović et al., 2021). This is particularly important in fintechs that operate in real-time, where late detection can lead to large financial losses. Stojanović et al. (2021) specifically highlight the effectiveness of anomaly detection techniques, which is the ability of algorithms to recognize transaction patterns that deviate from historical norms. This approach is particularly useful as many fraudulent activities are subtle and not easily detected by standardized rules. In this regard, unsupervised learning algorithms such as Isolation Forest or k-means clustering are also being used, especially when data labels are not fully available. Meanwhile, Sadgali et al. (2019) tested and compared supervised learning algorithms such as Decision Tree, Neural Network, and Naïve Bayes, showing that each algorithm has strengths and weaknesses that depend on the data structure and characteristics of the fraud at hand. The imbalance class-where the number of fraud cases is much less than normal transactions-also poses a major challenge to model accuracy. In Al-Hashedi and Magalingam's (2021) study, the effectiveness of ML is largely determined by the relevance of the algorithm to the type of fraud being addressed. They reviewed various data mining approaches and found that algorithms such as Random Forest and Support Vector Machine (SVM) were most commonly used and gave good results on financial data. However, high accuracy can only be achieved if supported by good data quality, proper feature selection, and a careful training process. Equally important

is the interpretation of the model results so that financial institutions can take appropriate actions. Despite coming from the field of satellite sensing, Zandler et al. (2022) proved that the Random Forest algorithm can process complex spatial and temporal data, which is relevant for the fintech context as financial transactions also have aspects of time, location, and recurring patterns. They pointed out the importance of cross-validation to avoid overfitting and maintain model generalization, which later became a common practice in the development of ML systems for cybersecurity. Tian et al. (2024) added that in real implementation, machine learning faces a number of significant obstacles. First, the black-box issue, which is unclear how the model makes decisions, is a major obstacle, especially in highly regulated sectors such as finance. Second, concept drift, which is changes in user or fraudster behavior over time, makes non-adaptive models quickly obsolete. Therefore, regular model updates and integration with conventional systems are required to remain effective. In previous research, Tian et al. (2023) also developed the ASA-GNN (Attention-based Self-Adaptive Graph Neural Network) model that is able to capture the relationship patterns between transactions through a graph approach, providing a solution to the challenges of noise and over-smoothing in traditional GNNs. This model is relevant in fintech security as it enables detection of fraud hidden through relationships between entities. In supporting ML implementation, data pre-processing is a crucial step that includes data cleaning, normalization, outlier detection, and data balancing techniques such as SMOTE (Synthetic Minority Over-sampling Technique). According to Psychoula et al. (2021), models such as Autoencoder are also effective in conditions of data imbalance, as they are able to reconstruct the input data and measure how much deviation occurs. They also suggest evaluating models using metrics such as precision, recall, F1-score, and AUC rather than just accuracy, as it is important to minimize false negatives in fraud detection. Fildansyah (2024) emphasized the role of ML in real-time fraud detection, which is particularly important in electronic financial transactions. ML not only records old patterns but also learns from new data, thus adapting to evolving fraud modes. Compared to static, rule-based approaches, ML is much more dynamic and responsive. However, as reminded by Chy (2024), predictions must be made within seconds to prevent further losses, so lightweight and efficient models need to be prioritized in deployment.

Another important issue is transparency and interpretability. In a regulated environment such as fintech, system decisions need to be explainable to regulators and users. Therefore, explainable AI (XAI) approaches such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) are important to explain the logic of decisions made by the model, especially when it comes to rejecting transactions or freezing accounts. Machine learning is now a key foundation in modern cybersecurity systems, especially in the highly dynamic fintech sector that is vulnerable to digital threats. With its ability to automatically and adaptively detect anomalous patterns, ML can provide more proactive protection than conventional approaches. Various algorithms such as Decision Tree, Random Forest, Neural Network, and advanced models such as ASA-GNN have been proven to improve the accuracy of fraud detection if implemented properly. However, this success is highly dependent on several important factors, such as data quality and representativeness, effective pre-processing techniques, and careful model training and validation strategies. Challenges such as data imbalance, lack of model transparency, and concept drift are still major obstacles. Therefore, the ideal fintech security system should be hybrid, combining the power of machine learning technology with strong governance policies, model transparency, and integration with adequate supervision and regulation. An explainable AI approach is increasingly crucial so that models are not only accurate, but also accountable. By utilizing ML strategically and wisely, the fintech sector can be better prepared for the complexity of cyber threats in this digital era. In the future, this data-driven security system will not only be a complement, but a primary requirement in maintaining public trust and the stability of the digital financial system as a whole.

Application of Machine Learning in Fintech Security

Financial technology (fintech) has revolutionized the way people access and use financial services, but it also brings great challenges in terms of security, especially against the threat of digital fraud, identity theft, and transaction data manipulation. In response to these challenges, machine learning (ML) technology is emerging as a powerful solution capable of automatically detecting suspicious patterns based on historical data and operating at scale in real-time. The study by Stojanović et al. (2021) underlines the effectiveness of using anomaly detection in detecting suspicious activity in fintech transactions. This approach allows the system to automatically identify patterns that deviate from normal behavior as an indication of potential fraud, without requiring explicit rules from humans. With an unsupervised learning approach, the system is able to learn from normal data distributions and then identify significant deviations. In the context of fintech, which operates in large and fast transaction volumes, this approach adds immense value. Along the same lines, Sadgali et al. (2019) evaluated the performance of various algorithms such as Decision Tree, Neural Network, and Naïve Bayes, and found that despite their high accuracy in detecting fraud, these models still require adjustments such as balancing techniques (e.g. SMOTE or undersampling) in order to adapt to the fast-changing dynamics of fintech transaction data. Another challenge they highlighted is the need for continuous model testing, as algorithm performance may degrade due to concept drift or changes in fraudster behavior over time. Adding a broader perspective, Al-Hashedi and Magalingam (2021) analyzed more than 30 data mining techniques in fraud detection in

the banking and fintech sectors, and identified models such as Support Vector Machine (SVM), Random Forest, and Logistic Regression as commonly used models due to their robustness in managing large and complex data. They emphasized the importance of feature selection and data preprocessing as key determinants of model success, as the quality of the input will greatly affect the final performance of the algorithm. In practice, a combination of techniques (ensemble) is often used to maximize classification results by combining the advantages of several approaches. Although the main focus of Zandler et al. (2022) is vegetation monitoring based on spatial-temporal data, the study demonstrates the effectiveness of models such as Random Forest in handling non-linear and dynamic data structures, which is relevant for fintech systems that also process data in both time and location dimensions.
They also emphasized the importance of thorough model evaluation with metrics such as AUC (Area Under Curve) to measure effectiveness in the context of data imbalance. This approach is further emphasized by Tian et al. (2024) who outlined challenges such as concept drift, limited labeled data, and the need for integration with conventional security systems. They suggest the use of semi-supervised and incremental learning as solutions to ensure the system remains relevant and adaptive over time. In addition, they raised the issue of black-boxes in neural network models, which makes it difficult for financial institutions to justify decisions to regulators, emphasizing the need for the adoption of explainable AI technologies. In particular, Tian et al. (2023) introduced an innovative approach ASA-GNN (Adaptive Sampling and Aggregation-based Graph Neural Network) to detect fraud in graph-based transactions. The model is able to identify fraud patterns hidden in multi-hop (more than one connection) relationships between accounts or devices, which are often used by criminals to disguise their activities. By reducing noise and improving classification accuracy, ASA-GNN is an important representation of the advancement of relation-based algorithms in fintech. Meanwhile, Psychoula et al. (2021) compared the performance of supervised and unsupervised models such as Random Forest, Decision Tree, Autoencoder, and Isolation Forest. They emphasized the importance of interpretability of model results using SHAP and LIME methods, which is crucial for financial institutions to explain the rationale behind system decisions to auditors, regulators, or other internal parties. They also suggested continuous monitoring of evaluation metrics such as precision, recall, and F1-score to keep the system accurate and fair, especially in the context of imbalanced data. The importance of real-time detection was also emphasized by Chy (2024), who stated that ML models should be able to prevent fraud before it happens, not just detect it after the fact. Chy emphasized that response time is crucial, especially in fintech services such as digital payments, microloans, and e-wallets. In this context, approaches such as online learning and streaming data processing are becoming increasingly relevant. Fildansyah's research (2024) adds that the successful implementation of ML in fintech depends on choosing the right features and parameters, and suggests using ensemble or hybrid approaches to combine the advantages of several models. He also emphasized the importance of data governance and privacy, especially when processing real-time customer data. The combination of speed, accuracy, and data security is an important benchmark for fintech companies in adopting ML.

In the local context, a study by Lee et al. (2025) showed the application of ML in detecting fraud in the financial statements of companies in Indonesia. Using algorithms such as Logistic Regression, KNN, SVM, and Random Forest, the study found that Random Forest provided the best performance in identifying fraud indicators such as accounts receivable turnover ratio and gross profit margin. These findings expand the scope of application of ML from just individual transactions to the corporate and financial reporting level. The application of machine learning in fintech security has undergone a significant evolution from rule-based systems to adaptive and data-driven predictive approaches. ML technology offers flexibility and early detection capabilities against digital fraud threats through various approaches, such as anomaly detection, graph-based modeling, ensemble learning, and explainable AI. The combination of various algorithms such as Random Forest, SVM, Neural Network, and ASA-GNN has shown significant success in detecting suspicious activities in the fintech sector. However, the success of ML implementation is largely determined by a number of key factors: data quality and completeness, appropriate feature selection, model selection that fits the operational context, and consistent model evaluation using accurate metrics. Challenges such as concept drift, interpretability, data imbalance, and the need for integration with conventional security systems must be anticipated with technical and strategic solutions. Furthermore, explainable AI approaches such as SHAP and LIME are important to bridge the need between model complexity and accountability in financial regulation. Real- time fraud detection, continuous data processing, and data security are key prerequisites for the adoption of ML by fintech companies. Therefore, ML is not only a detection tool, but also a strategic component in building a resilient, secure, and sustainable digital financial system.

Challenges and Limitations of Machine Learning Implementation

Although the application of machine learning (ML) in detecting and preventing fraud in the fintech sector has shown promising results, its practical application still encounters various obstacles that need to be addressed systematically and thoroughly. These challenges range from technical issues such as overfitting, data imbalance, and model interpretability, to implementation issues such as infrastructure limitations and regulatory compliance. As explained by Stojanović et al. (2021), ML-based fraud detection systems often produce a large number of false

positives. This not only decreases operational efficiency, but can also disrupt legitimate user experience due to unnecessary precautions. They also highlighted that models that are not regularly updated are prone to performance degradation due to their inability to keep up with changing user behavior patterns and evolving fraud techniques. In a further study, Sadgali et al. (2019) emphasized that the quality and quantity of data determine the effectiveness of the algorithm. When the data used is imbalanced-that is, fraud transactions are much less than normal transactions-then the model tends to be biased and has difficulty detecting real fraud cases. To overcome this, techniques such as oversampling, undersampling, and SMOTE (Synthetic Minority Oversampling Technique) need to be applied so that the model has a balanced understanding of both classes. In addition, they highlighted the importance of hyperparameter adjustment and cross-validation techniques to prevent overfitting, as well as the need for a dynamic approach to keep the model relevant in a fast-changing environment. Al-Hashedi and Magalingam (2021) highlighted the issue of interpretability which is a major concern in finance. They mentioned that although algorithms such as Random Forest and Neural Networks have high accuracy, these models often function as black boxes, making them difficult to explain to regulators and auditors. Therefore, explainable AI (XAI) approaches are becoming increasingly important. They also propose the utilization of rule-based systems combined with predictive models to improve transparency and accountability in decision-making. Another obstacle is the need to process large volumes of data in real-time, which requires technological infrastructure that is not always available, especially among small-medium institutions. Although the study by Zandler et al. (2022) focused on spatial modeling in an environmental context, they conveyed strong relevance to heterogeneous data processing in the fintech sector, particularly in the face of non-stationary data and changing temporal structures. These challenges require ML models to have high generalization capabilities as well as rigorous evaluation systems to prevent misjudgment of model performance. In addition, thorough cross-validation and ensembling techniques are considered crucial to ensure that the model can perform optimally in various data scenarios.

In a more technical approach, Tian et al. (2024) describe the concept drift phenomenon as a major challenge in digital transaction security. Concept drift refers to changes in data distribution over time, so that previously accurate models become irrelevant. They suggested using online learning or continual learning methods so that the model can gradually adapt to these changes. Tian also emphasized the importance of labeling costs, as most fraud data is unlabeled and requires semi-supervised or unsupervised learning techniques to identify anomalies without complete historical data. In their follow-up study in 2023, Tian introduced ASA-GNN, which not only effectively handles noise and camouflage in data, but can also extract relationships between financial entities, providing more in-depth detection potential than conventional methods. Psychoula et al. (2021) make an important contribution to the understanding of the need for interpretability in the regulatory context. They emphasize that hard-to-explain models, such as deep learning and GNN, need to be equipped with interpretation tools such as SHAP and LIME in order to provide transparency to end users and policy makers. Without transparency, ML models will not only be difficult to adopt but also risk violating regulations such as GDPR that demand legitimate explanations of automated decision-making processes. In the context of Indonesia, Lee et al. (2025) showed that algorithms such as KNN are prone to overfitting, while Random Forest and Logistic Regression tend to be more stable. Their study also shows that the application of ML is not only limited to individual transaction detection, but can be extended to the analysis of company financial statements, broadening the scope of benefits from this technology. On the other hand, Chy (2024) emphasized the urgency of continuous model updates, as fraud is adaptive and constantly evolving. Static models will quickly become obsolete, thus the need for systems that are able to learn from new data on an ongoing basis. Finally, Fildansyah (2024) pointed out the importance of data quality and feature selection in building a reliable fraud detection system. He emphasized that ensemble learning or hybrid approaches can be a solution to combine the strengths of various models, so that the system becomes more robust to complex data dynamics. In addition, operational challenges such as computational limitations and integration into existing fintech systems should not be ignored. ML models that require high computational processing may be inefficient for real-time implementation without adequate infrastructure support.

Regulation and Ecosystem Support

Besides emphasizing the importance of adaptive regulations, Stojanović et al. (2021) also highlighted the need for standardization in financial data processing so that ML-based systems can operate across institutions securely. They note that inconsistencies in data protocols and lack of harmonization between institutions can slow down early detection of suspicious activity. In this regard, they suggested the establishment of a regulatory sandbox that would allow fintechs to test new ML technologies in a controlled environment with the assistance of regulators. This will minimize the risk to consumers while accelerating the technology adoption process. Sadgali et al. (2019) extended their argument by emphasizing the importance of good data governance. They state that the application of ML in the financial sector needs

to be accompanied by policies that guarantee data access rights for innovators without violating user privacy. They also highlighted the need for increased digital literacy and continuous training for regulators to be able to evaluate and approve the use of increasingly complex ML models. Without adequate institutional capacity, regulation can become a bottleneck rather than a catalyst. In terms of ethics and transparency, Al-Hashedi and Magalingam (2021) emphasize that ML systems used to detect fraud should not only be technically effective, but also publicly auditable. Therefore, they recommend the development of policies that require documentation of model training processes, activity logs, and performance measurements as a condition of technology implementation. This aims to bridge the industry's need to prioritize efficiency with the need for regulators to keep digital financial systems accountable. Although not directly addressing the financial sector, Zandler et al. (2022) still make a valuable contribution in terms of data system integrity. They highlight that cross-validation and transparency of analytic methods are key to avoiding systematic biases that not only impact model results, but also the legitimacy of the system in the eyes of regulators and the public. This principle is relevant for fintech ecosystems that must ensure the reliability and accuracy of ML predictions not only in trials, but also in real-world implementations. Tian et al. (2024) warn that the mismatch between the speed of innovation and the slowness of the legislative process can be a major obstacle to the effective implementation of ML technology. They suggest a risk-based regulation approach, where policies are customized based on the risk and complexity of the technology being used. This approach would allow regulators to be more agile in handling innovation without having to stifle the creativity of industry players. In this context, they also suggest a national collaborative platform that brings together stakeholders from the technology, legal and public sectors. In a previous study, Tian et al. (2023) also highlighted the need for solid data and computing infrastructure, especially for complex ML models such as Graph Neural Network (GNN). They stated that the ability of a country or institution to adopt a GNN-based fraud detection system is highly dependent on the adequacy of information technology resources and network architecture that enables fast and secure data processing. Therefore, regulations should not only facilitate, but also encourage investment in the development of supporting technology ecosystems. Furthermore, Psychoula et al. (2021) analyzed the legal consequences of implementing ML-based automated systems, particularly within the framework of the General Data Protection Regulation (GDPR) in Europe. They emphasized the importance of algorithm interpretability as a condition for the legality of automated decisions, such as loan denials or account blocking. The application of Explainable AI (XAI) techniques such as SHAP and LIME is mandatory in this context, so that consumers have the right to understand and challenge system decisions. These findings are highly relevant for the development of similar legal frameworks in developing countries, including Indonesia.

From a local perspective, Lee et al. (2025) emphasized the need for an evidence-based policy approach to accommodate the development of ML technology in Indonesia. They suggest a joint task force between OJK, BI, BSSN, academia, and industry to design technical guidelines, audit models, and cross-agency data-based early warning mechanisms. With this approach, policies will be more grounded, responsive, and not solely rely on a top-down approach. Fildansyah (2024) strengthens this argument by emphasizing the importance of a cyber resilience framework that relies not only on technology, but also on organizational readiness in responding to attacks and anomalies. He also highlighted the need for specialized education and training for human resources in the financial sector to manage ML systems, from data processing, results interpretation, to risk governance. Competent human resources are an important element in bridging technology and regulation. Chy (2024) underlined that security is not enough from the technical side, but must also be accompanied by integrated risk governance. He suggests a three lines of defense approach, where technology teams, internal audit, and regulators work together to ensure that ML systems are secure, transparent, and accountable. If not accompanied by risk mitigation policies and consumer education, ML technology can be a double-edged sword that endangers the financial system itself. From various studies that have been reviewed, it can be concluded that the successful application of machine learning in improving the security of the fintech system is not only determined by the sophistication of the algorithm, but also depends on the alignment between regulations, technological infrastructure, human resource capacity, and process transparency. Rigid and slow regulations will make it difficult to adapt to innovation, while a weak technology ecosystem will hinder the implementation of complex systems. Therefore, a holistic approach that integrates pro-innovation regulations, cross-sector collaboration, human resource training, and digital infrastructure investment is required. Thus, the implementation of ML in fintech can take place effectively, ethically, and sustainably, addressing future challenges while maintaining public trust in the digital financial system.

Conclusion

This literature review confirms that machine learning (ML) technology has a strategic role in improving transaction security in the financial technology (fintech) sector, especially in Indonesia. ML-based approaches have proven effective in detecting and preventing fraudulent activities automatically, adaptively, and in real-time. Various algorithms such as Random Forest, Support Vector Machine (SVM), Neural Network, to Graph Neural Network (GNN) have been tested in the context of financial transactions, and show promising results in recognizing anomalous patterns and minimizing fraud losses. However, the application of ML is not free from

challenges. Issues such as data imbalance, concept drift, black box models, and limited technological infrastructure are significant obstacles. In addition, model interpretability, regulatory compliance, and the availability of human resources who understand both the technical and ethical sides of AI are crucial to support a successful implementation. Studies also show that the success of ML in the fintech context is highly influenced by data quality, feature selection process, and integration with internal control systems. In the Indonesian context, there are growing efforts to adapt the technology to local needs, through model testing on domestic transaction data as well as fraud simulations based on public datasets. Although most of the research is still at the experimental stage, there are strong signals that the adoption of ML can be a key solution to build a safe, efficient, and reliable digital financial system. Therefore, a multidisciplinary approach is needed that includes collaboration between industry players, regulators, academics, and the public. Adaptive regulations, model transparency through explainable AI, infrastructure investment, and cyber education are important foundations in building a fintech ecosystem that is resilient to future security threats.

References

Al-Hashedi, A., & Magalingam, P. (2021). *Financial fraud detection applying data mining techniques: A comprehensive review*. Computer Science Review, 39, 100402.

Sadgali, M., Sael, N., & Benabbou, A. (2019, March). *Performance of machine learning techniques in the detection of financial frauds*. In 2019 International Conference on Smart Systems and Data Science (ICSSD) (pp. 1-8). IEEE.

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). *Follow the trail: Machine learning for fraud detection in fintech applications*. Sensors, 21(5), 1594.

Tian, Y., Guo, S., & Yu, X. (2024). *Machine learning in internet financial risk management: A systematic literature review*. PLOS ONE, 19(2), e0300195.

Zandler, H., Faryabi, S. P., & Ostrowski, S. (2022). *Contributions to satellite-based land cover classification, vegetation quantification and grassland monitoring*. Frontiers in Environmental Science, 10, 684589.

Chy, M. K. H. (2024). *Proactive fraud defense: Machine learning's evolving role in protecting against online fraud*. World Journal of Advanced Research and Reviews, 23(3), 1580-1589. https://doi.org/10.30574/wjarr.2024.23.3.2811

Fildansyah, R. (2024). *Optimization of machine learning algorithms for fraud detection in electronic financial transactions*. Eastasouth Proceeding of Nature, Science, and Technology. https://asj.eastasouth-institute.com/index.php/epnst

Lee, C.-W., Fu, M.-W., Wang, C.-C., & Azis, M. I. (2025). *Evaluating machine learning algorithms for financial fraud detection: Insights from Indonesia*. Mathematics, 13(600). https://doi.org/10.3390/math13040600

Psychoula, I., Gutmann, A., Mainali, P., Lee, S. H., Dunphy, P., & Petitcolas, F. A. P. (2021). *Explainable machine learning for fraud detection*. IEEE Computer Society (To appear). arXiv:2105.06314. https://arxiv.org/abs/2105.06314

Tian, Y., Liu, G., Wang, J., & Zhou, M. (2023). *Transaction fraud detection via an adaptive graph neural network*. arXiv:2307.05633. https://arxiv.org/abs/2307.05633