Open Access Research Journal of
Science and Technology
Journals home page: https://oarjst.com/
ISSN: 2782-9960 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

Machine learning for preventing cyber-attacks on entrepreneurial crowdfunding platforms

Blessing Austin-Gabriel [1, *], Adeoye Idowu Afolabi [2], Christian Chukwuemeka Ike [3] and Nurudeen Yemi Hussain [4]

[1] *Montclair State University, Montclair, New Jersey, USA.*
[2] *CISCO, Nigeria.*
[3] *Globacom Nigeria Limited.*
[4] *Department of Computer Science, Texas Southern University, Texas, USA.*

Open Access Research Journal of Science and Technology, 2024, 12(02), 146-154

Publication history: Received on 09 November 2024; revised on 22 December 2024; accepted on 24 December 2024

Article DOI: https://doi.org/10.53022/oarjst.2024.12.2.0148

Abstract

Entrepreneurial crowdfunding platforms have become a vital component of modern finance, connecting entrepreneurs with potential investors and enabling the flow of significant financial transactions. However, these platforms are increasingly vulnerable to cyber threats, including fraud, identity theft, and data breaches. Machine learning (ML) offers a dynamic solution to these challenges, providing real-time detection, prevention, and mitigation of cyberattacks. This paper reviews the role of machine learning in enhancing the security of crowdfunding platforms, focusing on specific ML algorithms suited for fraud detection, identity verification, and transaction monitoring. It also explores the integration of ML-based security tools into existing platform architectures, real-time detection mechanisms, and the challenges of implementing ML in cybersecurity, such as ethical concerns and limitations in addressing sophisticated attacks. The paper concludes by discussing future trends, including advanced AI models, collaborative defense systems, and cross-platform threat intelligence sharing, as crucial elements for improving the cybersecurity of entrepreneurial crowdfunding platforms.

Keywords: Machine Learning; Cybersecurity; Crowdfunding Platforms; Fraud Detection; Identity Verification

1. Introduction

Entrepreneurial crowdfunding platforms have revolutionized the way startups and small businesses access funding. These platforms allow entrepreneurs to raise capital by connecting with a large pool of investors or backers online. Platforms such as Kickstarter, Indiegogo, and GoFundMe have enabled businesses to secure investments quickly and efficiently without relying on traditional financial institutions (Yasar, 2021). As a result, crowdfunding has become a critical component of modern finance, democratizing access to capital and fostering innovation. However, as these platforms grow in popularity, they also become attractive targets for cybercriminals seeking to exploit vulnerabilities for personal gain (Block, Groh, Hornuf, Vanacker, & Vismara, 2021).

Cybersecurity risks on crowdfunding platforms are diverse and include various forms of fraud, phishing attacks, and data breaches. Fraud can occur when malicious actors pose as legitimate entrepreneurs to collect funds without delivering on their promised projects (Saxena, 2021). Another common threat is phishing attacks, in which cybercriminals trick users into disclosing sensitive information, such as login credentials. Data breaches, in which unauthorized individuals gain access to user data, can have severe consequences, compromising both financial and personal information. These risks are compounded by the fact that many crowdfunding platforms handle significant amounts of money and sensitive user data, making them prime targets for cyberattacks (Zabyelina & Thachuk, 2022).

* Corresponding author: Blessing Austin-Gabriel.

The increasing reliance on technology to manage these platforms has led to a growing interest in using machine learning (ML) to enhance cybersecurity. Machine learning, a subset of artificial intelligence, involves the development of algorithms that can learn from data and make predictions or decisions without being explicitly programmed. In the context of cybersecurity, ML has shown significant potential in detecting and mitigating various cyber threats. ML algorithms can analyze vast amounts of data to identify patterns and anomalies that may indicate fraudulent behavior or potential security breaches. These models can also adapt and improve over time, making them highly effective in addressing evolving threats (Shah, 2021).

This paper aims to explore how machine learning can be leveraged to improve the security of entrepreneurial crowdfunding platforms. It aims to identify common cybersecurity risks faced by these platforms and examine how ML-based solutions can be applied to detect and prevent cyberattacks. Additionally, the paper discusses the challenges and limitations of implementing ML in the cybersecurity landscape and offers insights into future trends in the field. By providing an in-depth review of machine learning applications in this context, the paper seeks to contribute to the ongoing efforts to safeguard crowdfunding platforms and protect both entrepreneurs and investors from cyber threats.

2. Cybersecurity Threats in Crowdfunding Platforms

2.1. Identification of Common Cyber Threats in Crowdfunding Platforms

Crowdfunding platforms face an array of cyber threats that can compromise the security of both users and the platform itself. Among the most pervasive is phishing, a deceptive practice where cybercriminals trick users into divulging sensitive information, such as passwords, credit card numbers, or personal details. Attackers often impersonate legitimate platform administrators or campaign creators, sending emails or messages designed to look authentic. Once users fall victim to these schemes, their accounts can be hijacked, enabling attackers to drain funds, steal identities, or carry out fraudulent activities (Nguyen et al., 2021).

Another prevalent threat is fraudulent campaigns. Cybercriminals exploit crowdfunding platforms' open and trusting nature by setting up fake campaigns that promise products or services but fail to deliver. These malicious actors lure in backers with attractive offers or emotionally charged causes, only to disappear with the collected funds. Such campaigns damage the credibility of the platform and deter future participation by legitimate entrepreneurs and backers (Karthikeyan, 2020).

Additionally, data breaches pose a significant risk to crowdfunding platforms. Attackers who successfully infiltrate the platform's database can gain access to sensitive user information, including financial details, personal identities, and communication histories (Ali, Mijwil, Buruga, & Abotaleb, 2024). Breached data can be sold on the dark web or used to carry out identity theft, further complicating the security landscape for crowdfunding platforms. Furthermore, distributed denial-of-service (DDoS) attacks, where attackers overwhelm the platform's servers with traffic, can cause significant disruption, rendering the platform temporarily unusable and undermining user trust (Valiante, 2023).

2.2. Analysis of Attack Vectors and Vulnerabilities in Crowdfunding Systems

The vulnerabilities of crowdfunding platforms arise from several factors, including the high volume of transactions, the openness of the platform, and the rapid turnover of users and campaigns. Weak security measures, human error, or outdated software systems often enable attack vectors on these platforms. One of the primary attack vectors is inadequate authentication. Many crowdfunding platforms still rely on basic password authentication, which can be easily compromised through phishing, brute force attacks, or credential stuffing. A lack of multifactor authentication (MFA) leaves users particularly vulnerable, as attackers only need to obtain a single set of credentials to gain access to an account. Once inside, they can change account details, initiate fraudulent transactions, or impersonate the account owner (Wee, Chekole, & Zhou, 2024).

Another common vulnerability is insufficient data encryption. Platforms that do not implement strong encryption protocols for data storage and transmission expose user information to potential interception by malicious actors. This risk is particularly high for smaller platforms that may lack the resources to implement sophisticated encryption methods. Attackers can exploit these weaknesses to steal user data during transactions or while it is stored on the platform's servers (Tolbert, 2021).

Moreover, insider threats present a growing challenge for crowdfunding platforms. Employees, contractors, or even platform administrators with access to sensitive data may intentionally or unintentionally compromise platform

security. Malicious insiders might sell user information or sabotage the platform, while unintentional breaches can occur when insiders unknowingly click on phishing links or fail to follow proper security protocols (Ali et al., 2024).

The technical infrastructure of crowdfunding platforms also plays a significant role in determining their susceptibility to attacks. Platforms that rely on outdated software or lack regular security updates are prime targets for attackers. Cybercriminals often exploit known vulnerabilities in software to gain unauthorized access to systems. Platforms that fail to perform routine security audits or patch known vulnerabilities leave themselves exposed to these attack vectors (Araujo & Taylor, 2020).

2.3. The Financial and Reputational Impact of Cyber-attacks on Platform Owners and Users

The financial impact of cyberattacks on crowdfunding platforms can be catastrophic. When attackers gain unauthorized access to user accounts or platform systems, they can siphon off funds, potentially leading to significant financial losses for both users and the platform. Entrepreneurs who fall victim to cyberattacks may lose not only the capital they've raised but also the trust of their backers, making it difficult to secure future funding. For backers, losing money to fraud or stealing their personal financial information can deter them from participating in future crowdfunding efforts (Sharma, 2022).

The financial repercussions extend beyond immediate losses. Crowdfunding platforms may face substantial costs in the aftermath of a cyberattack, including legal fees, compensation to affected users, and investment in stronger security measures. In some cases, platforms may also be subject to fines or regulatory penalties if it is found that they did not implement adequate security measures to protect user data. For smaller platforms, these costs can be crippling and may even lead to the platform's collapse (Nwaimo, Adegbola, & Adegbola, 2024b; Okoli, Obi, Adewusi, & Abrahams, 2024).

Beyond the direct financial costs, the reputational impact of a cyber-attack can be equally, if not more, damaging. Loss of trust is perhaps the most significant consequence of a cybersecurity breach on a crowdfunding platform. These platforms thrive on the goodwill and trust of users, both entrepreneurs and backers, who expect their personal and financial information to be secure. A successful cyber-attack can shatter this trust, leading to a decline in user engagement, fewer campaigns, and decreased backer participation. Rebuilding a platform's reputation after a breach is a long and difficult process, often requiring extensive public relations efforts and the demonstration of improved security practices (Al-Turjman & Salama, 2021).

The ripple effects of cyber-attacks can also extend to the broader crowdfunding ecosystem. If a major platform suffers a breach, it may create fear and uncertainty across the industry, prompting users to avoid crowdfunding altogether or migrate to platforms perceived as more secure. This erosion of confidence can hinder the growth of the crowdfunding sector, reducing the availability of alternative financing for entrepreneurs and small businesses (Karthikeyan, 2020).

3. Machine Learning in Cybersecurity

3.1. Overview of Machine Learning Techniques Used in Cybersecurity

Machine learning techniques employed in cybersecurity primarily revolve around anomaly detection and predictive modeling. These methods leverage the inherent ability of ML algorithms to learn from historical data, recognize patterns, and make decisions without explicit programming (Dasgupta, Akhtar, & Sen, 2022).

Anomaly detection is a widely used technique in cybersecurity, particularly in environments like crowdfunding platforms where normal user behavior is relatively well-defined. This technique involves the identification of deviations from established patterns of behavior. For instance, if a user typically logs into their account from the same geographic location at regular intervals, an ML model trained on this data would flag a login attempt from a different location or at an unusual time as a potential threat. Anomaly detection helps identify a range of cyber-attacks, including unauthorized access, account takeovers, and fraudulent activities. The advantage of anomaly detection is that it can operate in real time, providing immediate alerts to security teams when suspicious behavior is identified (Apruzzese et al., 2023).

Predictive modeling, another important technique in machine learning, allows cybersecurity systems to anticipate future threats based on past data. Using historical records of cyber-attacks, ML models can identify patterns and trends that suggest the likelihood of future attacks. This is particularly useful in detecting evolving threats, such as phishing campaigns or malware attacks, which often follow identifiable patterns. Predictive models can forecast potential vulnerabilities in a system, allowing administrators to take preventive measures before an attack occurs. This proactive

approach is essential in cybersecurity, where the ability to prevent an attack is often more valuable than merely responding to it (Sarker, 2023).

Another ML technique that is gaining traction in cybersecurity is behavioral analysis. This involves creating profiles of user behavior over time and identifying discrepancies that may indicate malicious intent. For example, suppose a crowdfunding platform user suddenly begins making large transactions at a faster rate than usual or interacting with unfamiliar campaigns. In that case, ML models can detect these deviations and flag the account for further investigation. Behavioral analysis can detect fraud and other insider threats that might not trigger traditional security measures (Nassar & Kamal, 2021).

3.2. How Machine Learning Models Can Detect, Prevent, and Mitigate Cyber-attacks

Machine learning models are uniquely suited to detect, prevent, and mitigate cyber-attacks because they can process large datasets and identify hidden patterns that human analysts may overlook. In crowdfunding platforms, ML models can be trained to recognize users' specific behaviors and transaction patterns, making them particularly effective in identifying abnormal or malicious activities (Shah, 2021).

ML models continuously analyze incoming data to detect cyber-attacks, comparing it against the learned behavior of users and systems. By doing so, they can flag anomalies such as unusual login attempts, strange transaction patterns, or irregular campaign activity. For example, suppose a malicious actor attempts to launch a phishing campaign or manipulate the platform through fake accounts. In that case, the ML model can detect inconsistencies in account behavior and trigger an alert. This real-time detection capability is crucial in crowdfunding platforms, where rapid transactions and the transfer of large amounts of money can make traditional security measures too slow to respond effectively (Sarker, 2021).

When it comes to preventing attacks, machine learning models use predictive capabilities to anticipate potential vulnerabilities and respond proactively. Based on previous incidents and patterns, predictive models can forecast future cyber threats, such as the likelihood of a phishing attack targeting a particular group of users or the appearance of fraudulent campaigns during a certain time period. Armed with this knowledge, platform administrators can implement targeted security measures, such as increased monitoring or the use of two-factor authentication, to preemptively thwart these attacks (Rani).

In terms of mitigation, machine learning models can automate responses to cyber threats, significantly reducing the time between detection and resolution. Once a threat is detected, ML systems can immediately suspend suspicious accounts, block transactions, or isolate compromised systems. This automated response mitigates the damage caused by cyber-attacks and reduces the burden on human security teams, allowing them to focus on more complex tasks. Additionally, machine learning models can learn from these incidents, refining their algorithms to better detect similar threats in the future, further enhancing the platform's security posture (Sarker, 2023).

3.3. Strengths and Limitations of ML in Dynamic Environments

While machine learning offers several advantages in cybersecurity, particularly in dynamic environments like crowdfunding platforms, it is not without its limitations. Understanding both the strengths and weaknesses of ML in this context is essential for leveraging its full potential. One of the primary strengths of machine learning in cybersecurity is its ability to adapt to new threats. Traditional rule-based security systems often struggle to keep pace in crowdfunding platforms where user behavior and transaction patterns can change rapidly. Machine learning models, on the other hand, continuously learn from new data, allowing them to adapt to emerging attack vectors. This adaptability is particularly valuable in the ever-evolving landscape of cybercrime, where attackers are constantly developing new tactics to exploit vulnerabilities (Aljuhani, 2021).

Another strength of ML is its scalability. Crowdfunding platforms handle large volumes of transactions and data exchanges, making it difficult for human security teams to monitor everything in real time. Machine learning models, however, can analyze vast amounts of data at high speeds, providing real-time detection and response capabilities that significantly enhance platform security. This scalability makes ML particularly effective in detecting large-scale fraud or coordinated attacks that might otherwise go unnoticed (Sarker, 2023).

Despite these strengths, machine learning also has several limitations. One of the most significant challenges is the need for high-quality data. Machine learning models are only as effective as the data they are trained on, and in dynamic environments like crowdfunding platforms, maintaining an accurate and comprehensive dataset can be difficult.

Suppose the data used to train the model is incomplete or biased. In that case, the model may generate false positives or negatives, undermining its effectiveness (Schwartz et al., 2022).

Additionally, machine learning models are vulnerable to adversarial attacks, where attackers deliberately feed misleading data into the system to manipulate the model's predictions. In the case of a crowdfunding platform, for instance, an attacker could create a series of fake accounts with normal-looking behavior, gradually "training" the ML model to accept fraudulent activities as legitimate. This type of attack can erode the platform's security over time and requires constant vigilance to detect and counter (Chishti, 2020). Lastly, while ML excels at detecting patterns and anomalies, it can struggle with contextual understanding. A machine learning model might flag a large transaction as suspicious simply because it deviates from the norm, without understanding that the user may be an entrepreneur launching a successful crowdfunding campaign. This lack of contextual awareness can lead to unnecessary disruptions for legitimate users, highlighting the need for human oversight in conjunction with ML systems (Akartuna, Johnson, & Thornton, 2022).

4. ML-Based Solutions for Crowdfunding Platforms

4.1. Machine Learning Algorithms for Fraud Detection, Identity Verification, and Transaction Monitoring

Fraud detection, identity verification, and transaction monitoring are three key areas where machine learning can significantly enhance the security of crowdfunding platforms. By leveraging sophisticated algorithms, ML systems can continuously analyze vast amounts of user data to identify patterns and detect anomalies, providing a robust defense against cybercriminals. One of the most effective machine learning techniques for fraud detection is supervised learning, particularly algorithms like decision trees, random forests, and logistic regression. These algorithms are trained on labeled datasets that include both legitimate and fraudulent transactions, enabling them to distinguish between normal user behavior and suspicious activities (Afriyie et al., 2023). For instance, a random forest algorithm, which consists of multiple decision trees, can analyze various features of a transaction—such as the amount, location, and frequency of activity—to determine whether it is likely to be fraudulent. Over time, these models improve their accuracy as they learn from new data, making them highly effective in identifying even subtle fraud patterns that traditional rule-based systems might go unnoticed (Khatri, Arora, & Agrawal, 2020).

In identity verification, biometric authentication powered by machine learning is becoming increasingly popular. Techniques such as facial recognition, voice recognition, and fingerprint analysis can be integrated into crowdfunding platforms to verify user identities in real-time. For example, convolutional neural networks (CNNs), a type of deep learning algorithm, are widely used in facial recognition systems to detect and verify the unique features of a user's face. By comparing the facial data provided during login with the data stored in the system, these models can ensure that the individual attempting to access the account is indeed the legitimate owner. This adds an additional layer of security, making it much more difficult for cybercriminals to gain unauthorized access (Nwaimo, Adegbola, Adegbola, & Adeusi, 2024; Nwobodo, Nwaimo, & Adegbola, 2024).

Unsupervised learning techniques such as clustering and anomaly detection are particularly useful in terms of transaction monitoring. These algorithms do not rely on labeled data but instead seek to identify unusual behavior by grouping similar transactions and flagging those that deviate from the norm (Hilal, Gadsden, & Yawney, 2022). For example, clustering algorithms can group users with similar transaction patterns together, and any outlier—such as an unusually large transaction or a sudden change in behavior—would be flagged for further investigation. This approach is especially valuable in crowdfunding platforms, where the volume of transactions is high and manual monitoring is impractical. The ability to detect anomalies in real-time ensures that potentially fraudulent or malicious activities can be addressed before significant damage is done (Afriyie et al., 2023; Khatri et al., 2020).

4.2. Real-Time Detection and Response Mechanisms for Cyber Threats

One of the most significant advantages of machine learning in cybersecurity is its ability to operate in real-time, offering immediate detection and response to cyber threats. In the fast-paced environment of crowdfunding platforms, where millions of dollars may be transferred in seconds, the ability to react swiftly to an emerging threat is critical to minimizing damage (Abdul-Azeez, Ihechere, & Idemudia, 2024).

Real-time threat detection in machine learning is typically achieved through streaming analytics, which allows the continuous processing of data as it is generated. Machine learning models, particularly those using anomaly detection, monitor user behavior, login patterns, and transaction data in real-time, comparing each new data point against established patterns. When an anomaly is detected—such as an unusually large withdrawal or an unrecognized login

from a different geographic location—the system can immediately flag the activity and trigger a security response (Fang, Chen, & Xue, 2021).

Neural networks, particularly recurrent neural networks (RNNs) and long short-term memory (LSTM) networks, are particularly effective for real-time detection because they are designed to recognize sequences and temporal dependencies in data. These algorithms are well-suited for analyzing continuous streams of transactions or login attempts on crowdfunding platforms, where user behavior over time is often a critical indicator of fraud or malicious activity. RNNs can analyze sequences of actions and detect deviations that may signal an impending attack, enabling platform administrators to intervene before a threat escalates (Ghislieri, Cerone, Knaflitz, & Agostini, 2021).

The response mechanisms enabled by machine learning systems are also highly automated, allowing for instant action once a threat is identified. For example, if a fraudulent transaction is detected, the machine learning model can automatically block the transaction, freeze the account, or notify the user and administrators of the suspicious activity. This ability to respond autonomously and in real-time is particularly valuable in environments like crowdfunding, where delays in response can result in significant financial losses or data breaches (Khalifa, Mandic, & Sejdić, 2021).

4.3. Integration of ML Tools into Crowdfunding Platform Architectures

Integrating machine learning tools into existing crowdfunding platforms requires careful planning and consideration of both the platform's technological infrastructure and operational processes. The integration process involves ensuring that the machine learning models can seamlessly interact with the platform’s databases, transaction systems, and user interfaces while maintaining high levels of performance and scalability. One approach to integrating ML tools is through cloud-based solutions, which offer scalability and flexibility. By leveraging cloud platforms like Amazon Web Services (AWS) or Google Cloud, crowdfunding platforms can implement machine learning models without the need for significant on-premises infrastructure (Ahsan et al., 2022). Cloud services provide access to powerful machine learning frameworks, such as TensorFlow or PyTorch, enabling platforms to train and deploy models efficiently. These services also allow for real-time data processing, which is essential for detecting and responding to threats as they occur (Igbinidu-Uwuigbe, 2022).

Another important aspect of integration is the use of APIs (Application Programming Interfaces) to connect machine learning models with the platform’s core systems. APIs enable seamless communication between the ML models and the various components of the crowdfunding platform, such as the user database, transaction processor, and security systems. For example, an API can send real-time alerts to administrators when a potential threat is detected or trigger an automated response when suspicious activity is flagged (Zikopoulos, Bienko, Backer, Konarski, & Vennam, 2021).

Incorporating machine learning into the user experience is also crucial for ensuring that security measures do not disrupt the platform’s functionality. For instance, identity verification processes powered by machine learning, such as facial recognition or fingerprint scanning, should be designed to be both secure and user-friendly. Crowdfunding platforms must strike a balance between implementing robust security measures and maintaining a seamless user experience, ensuring that legitimate users are not inconvenienced by false positives or overly aggressive security protocols (Sarker, 2023).

Lastly, continuous model improvement is essential for maintaining the effectiveness of ML-based security systems. Cyber threats are constantly evolving, and machine learning models must be regularly updated and retrained to reflect new patterns of attack. This can be achieved by implementing feedback loops, where data from detected threats and successful interventions is fed back into the model to improve its accuracy and predictive capabilities. By continuously refining the models, crowdfunding platforms can stay ahead of emerging cyber threats and ensure the ongoing security of their users and transactions (Dasgupta et al., 2022).

5. Challenges and Future Directions

5.1. Ethical and Privacy Concerns

One of the primary challenges surrounding the use of ML in cybersecurity is the ethical and privacy implications. Crowdfunding platforms collect and process large amounts of personal data, ranging from financial information to user behavior patterns. The deployment of ML models to monitor and analyze this data raises concerns about how personal information is handled, stored, and protected. Users may feel that constant surveillance through behavioral tracking and anomaly detection invades their privacy, especially when these systems are designed to flag deviations in behavior (Nwaimo, Adegbola, & Adegbola, 2024a).

Additionally, the potential for bias in machine learning models is a significant ethical concern. If models are trained on biased data, they may produce skewed results that disproportionately affect certain user groups. For example, an ML algorithm designed to detect fraud may falsely flag transactions from a particular demographic or geographic region, leading to unfair account restrictions. Ensuring that ML models are both transparent and accountable is critical in addressing these ethical issues. More transparent algorithms and strict data governance policies will be necessary to balance the need for security with the preservation of user privacy.

While ML has demonstrated its effectiveness in identifying many cyber threats, it is not a panacea for all cybersecurity challenges. One of the main limitations of current ML approaches is their reliance on historical data to detect anomalies or predict attacks. Sophisticated cyber threats, such as zero-day attacks or advanced persistent threats (APTs), are often designed to bypass known patterns of behavior, rendering many ML models ineffective. As these attacks evolve, they exploit vulnerabilities in ways that existing models may not anticipate, creating a gap between detection and mitigation (Adewusi et al., 2024).

Moreover, machine learning models are susceptible to adversarial attacks, where cybercriminals manipulate input data to trick the system into misclassifying malicious activity as legitimate. For example, attackers can subtly alter data to fool ML models into overlooking malware or unauthorized access attempts. This highlights the need for robust and resilient models capable of adapting to new threats without relying solely on pre-existing data.

5.2. Future Trends in ML and Cybersecurity

The future of ML in cybersecurity is promising, with several trends poised to overcome current limitations. Advanced AI models, including deep learning and reinforcement learning, are likely to play a more significant role in detecting and responding to complex cyber threats. These models, capable of learning from both structured and unstructured data, will improve the adaptability and accuracy of ML-based security systems.

Another future trend is the development of collaborative defense systems that involve multiple stakeholders, including platform operators, cybersecurity firms, and governmental agencies, working together to share threat intelligence. Cross-platform threat intelligence sharing will become increasingly important in preventing large-scale attacks across different sectors. By pooling resources and insights, platforms can enhance their ability to detect and respond to cyber threats more effectively than when operating in isolation. Finally, as the cyber threat landscape evolves, autonomous defense systems powered by AI will enable real-time responses without human intervention. These systems can continuously learn from new data and adjust their defenses dynamically, offering a more proactive and scalable approach to cybersecurity.

6. Conclusion

This study has highlighted the transformative potential of machine learning (ML) in mitigating cybersecurity threats faced by entrepreneurial crowdfunding platforms. By leveraging sophisticated ML algorithms for fraud detection, identity verification, and real-time transaction monitoring, platforms can significantly enhance their security postures against evolving cyber threats. The integration of ML tools into platform architectures not only enables real-time detection and automated responses but also ensures scalability and adaptability, critical for managing large volumes of transactions and dynamic user behaviors. However, the study also underscores the challenges of implementing ML in cybersecurity, including ethical concerns, data quality limitations, and susceptibility to adversarial attacks. Addressing these issues requires a multifaceted approach involving transparency in ML model development, continuous refinement of algorithms, and collaboration among stakeholders to share threat intelligence and develop robust countermeasures. Despite these challenges, ML remains a promising tool for addressing the ever-evolving landscape of cybercrime, offering a proactive and scalable defense mechanism. Future advancements in AI, including reinforcement learning and autonomous defense systems, will further enhance the ability of platforms to detect and mitigate complex threats with minimal human intervention. Moreover, fostering cross-platform collaboration and integrating ethical AI practices will ensure a more secure and inclusive digital ecosystem. By safeguarding crowdfunding platforms, this research contributes to the broader goal of promoting trust and innovation in the entrepreneurial finance sector. It ensures that these platforms continue to serve as vital engines of economic growth and opportunity, benefiting both entrepreneurs and investors. Moving forward, the integration of advanced AI models, ethical guidelines, and global threat-sharing frameworks will be pivotal in shaping the future of cybersecurity in crowdfunding.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdul-Azeez, O., Ihechere, A. O., & Idemudia, C. (2024). Digital access and inclusion for SMEs in the financial services industry through Cybersecurity GRC: A pathway to safer digital ecosystems. Finance & Accounting Research Journal, 6(7), 1134-1156.

[2] Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. World Journal of Advanced Research and Reviews, 21(1), 2263-2275.

[3] Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., . . . Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal, 6, 100163.

[4] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527-555.

[5] Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting and Social Change, 179, 121632.

[6] Al-Turjman, F., & Salama, R. (2021). Cyber security in mobile social networks. In Security in IoT Social Networks (pp. 55-81): Elsevier.

[7] Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A Comprehensive review on cybersecurity issues and their mitigation measures in FinTech.

[8] Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. Ieee Access, 9, 42236-42264.

[9] Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), 1-38.

[10] Araujo, F., & Taylor, T. (2020). Improving cybersecurity hygiene through JIT patching. Paper presented at the Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering.

[11] Block, J. H., Groh, A., Hornuf, L., Vanacker, T., & Vismara, S. (2021). The entrepreneurial finance markets of the future: a comparison of crowdfunding and initial coin offerings. Small Business Economics, 57, 865-882.

[12] Chishti, S. (2020). The AI book: the artificial intelligence handbook for investors, entrepreneurs and fintech visionaries: John Wiley & Sons.

[13] Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57-106.

[14] Fang, W., Chen, Y., & Xue, Q. (2021). Survey on research of RNN-based spatio-temporal sequence prediction algorithms. Journal on Big Data, 3(3), 97.

[15] Ghislieri, M., Cerone, G. L., Knaflitz, M., & Agostini, V. (2021). Long short-term memory (LSTM) recurrent neural network for muscle activity detection. Journal of NeuroEngineering and Rehabilitation, 18, 1-15.

[16] Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. Expert Systems with Applications, 193, 116429.

[17] Igbinidu-Uwuigbe, A. (2022). Agnet Object-Detection and Alert System with TensorFlow-Serving and Agnet-API.

[18] Karthikeyan, C. (2020). Crowdfunding. In.

[19] Khalifa, Y., Mandic, D., & Sejdić, E. (2021). A review of Hidden Markov models and Recurrent Neural Networks for event detection and localization in biomedical signals. Information Fusion, 69, 52-72.

[20] Khatri, S., Arora, A., & Agrawal, A. P. (2020). Supervised machine learning algorithms for credit card fraud detection: a comparison. Paper presented at the 2020 10th international conference on cloud computing, data science & engineering (confluence).

[21] Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning in Management, 5(1), 51-63.

[22] Nguyen, L. T., Hoang, T. G., Do, L. H., Ngo, X. T., Nguyen, P. H., Nguyen, G. D., & Nguyen, G. N. (2021). The role of blockchain technology-based social crowdfunding in advancing social value creation. Technological Forecasting and Social Change, 170, 120898.

[23] Nwaimo, C. S., Adegbola, A. E., & Adegbola, M. D. (2024a). Data-driven strategies for enhancing user engagement in digital platforms. International Journal of Management & Entrepreneurship Research, 6(6), 1854-1868.

[24] Nwaimo, C. S., Adegbola, A. E., & Adegbola, M. D. (2024b). Predictive analytics for financial inclusion: Using machine learning to improve credit access for under banked populations. Computer Science & IT Research Journal, 5(6), 1358-1373.

[25] Nwaimo, C. S., Adegbola, A. E., Adegbola, M. D., & Adeusi, K. B. (2024). Evaluating the role of big data analytics in enhancing accuracy and efficiency in accounting: A critical review. Finance & Accounting Research Journal, 6(6), 877-892.

[26] Nwobodo, L. K., Nwaimo, C. S., & Adegbola, A. E. (2024). Enhancing cybersecurity protocols in the era of big data and advanced analytics. GSC Advanced Research and Reviews, 19(3), 203-214.

[27] Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286-2295.

[28] Rani, L. Security Issues and Defense Mechanism Using IoMT. In Artificial Intelligence Technology in Healthcare (pp. 211-242): CRC Press.

[29] Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet of Things, 14, 100393.

[30] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, 10(6), 1473-1498.

[31] Saxena, A. (2021). Black Money and Economic Crimes: KK Publications.

[32] Schwartz, R., Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). Towards a standard for identifying and managing bias in artificial intelligence (Vol. 3): US Department of Commerce, National Institute of Standards and Technology.

[33] Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.

[34] Sharma, R. (2022). Cyber Security to Safeguard Cyber Attacks. International Journal of Information Security and Cybercrime (IJISC), 11(2), 50-63.

[35] Tolbert, M. (2021). Vulnerabilities of Multi-factor Authentication in Modern Computer Networks. UK: Worcester Polytechnic Institute Worcester.

[36] Valiante, D. (2023). Regulating Digital Platforms: the European Experience with Financial Return Crowdfunding. European Company and Financial Law Review, 19(5), 854-894.

[37] Wee, A. K., Chekole, E. G., & Zhou, J. (2024). Excavating Vulnerabilities Lurking in Multi-Factor Authentication Protocols: A Systematic Security Analysis. arXiv preprint arXiv:2407.20459.

[38] Yasar, B. (2021). The new investment landscape: Equity crowdfunding. Central Bank Review, 21(1), 1-16.

[39] Zabyelina, Y., & Thachuk, K. L. (2022). The Private Sector and Organized Crime: Criminal Entrepreneurship, Illicit Profits, and Private Sector Security Governance: Taylor & Francis.

[40] Zikopoulos, P., Bienko, C., Backer, C., Konarski, C., & Vennam, S. (2021). Cloud Without Compromise: " O'Reilly Media, Inc."