ORION
SCHOLAR JOURNALS

International Journal of Scientific Research Updates

Journal homepage: https://orionjournals.com/ijsru/

ISSN: 2783-0160 (Online)

Int. J. Sci. Res. Updates
International Journal of Scientific Research Updates
Orion Scholar Journals
PHILIPPINES

(REVIEW ARTICLE)

# Machine learning-driven cybersecurity for social media data protection in entrepreneurial ventures

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.*

International Journal of Scientific Research Updates, 2024, 08(02), 175-184

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

Article DOI: https://doi.org/10.53430/ijsru.2024.8.2.0070

## Abstract

This review paper explores the application of machine learning-driven cybersecurity solutions to enhance social media data protection, with a specific focus on entrepreneurial ventures. Social media platforms are integral to business operations, especially for startups, but they pose significant cybersecurity risks, including phishing, malware, and data breaches. Machine learning offers innovative approaches to detecting and mitigating these threats through real-time anomaly detection, deep learning, and AI-driven threat intelligence. However, challenges such as evolving cyber threats, privacy concerns, and the high implementation costs present barriers for small businesses. This paper examines the current cybersecurity landscape, the role of machine learning in addressing these risks, and provides recommendations for startups to enhance social media data protection. Emerging trends, such as the use of deep learning and AI-driven threat intelligence, are also discussed, alongside best practices for entrepreneurial ventures in adopting scalable and effective ML solutions.

**Keywords:** Machine Learning; Cybersecurity; Social Media; Entrepreneurial Ventures; Data Protection; Deep Learning

## 1 Introduction

In the digital age, social media has become an integral tool for entrepreneurial ventures, providing a platform for brand building, customer engagement, and marketing. However, as entrepreneurs increasingly rely on social media for business operations, they face various cybersecurity threats (Park, Kim, Jeong, & Minshall, 2021). These threats, ranging from data breaches to malicious attacks, can lead to significant financial and reputational damage. Startups and small businesses are particularly vulnerable due to their limited resources and lack of advanced cybersecurity defenses. The rapid pace of technological advancements also means that new threats emerge frequently, making it harder for businesses to keep up (Jahankhani, Meda, & Samadi, 2022).

Machine learning (ML), a subset of artificial intelligence, has emerged as a powerful tool in the fight against these cybersecurity threats (Shah, 2021). ML-driven systems can analyze vast amounts of data, identify patterns, and detect anomalies in real-time, allowing businesses to mitigate potential risks before they cause harm. For entrepreneurial ventures, machine learning offers a scalable and effective solution to protecting sensitive data and ensuring the security of their online presence (Okoli, Obi, Adewusi, & Abrahams, 2024).

[*] Corresponding author: Blessing Austin-Gabriel

The protection of social media data is particularly critical for startups, as their growth and customer relationships often depend heavily on these platforms. A single data breach can lead to the loss of sensitive information and erode the trust of customers and stakeholders. Thus, entrepreneurial ventures need to invest in robust cybersecurity strategies that leverage machine learning.

The objectives of this paper are threefold: (1) to explore the current cybersecurity threats faced by entrepreneurial ventures on social media platforms, (2) to examine how machine learning can enhance data protection in this context, and (3) to discuss the challenges and future directions of machine learning-driven cybersecurity solutions for startups and small businesses.

## 2 Cybersecurity Threat Landscape in Social Media

### 2.1 Types of Cybersecurity Threats Targeting Social Media Platforms

Social media platforms are vulnerable to a wide range of cybersecurity threats, some of which are more prevalent than others (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin, 2023). One of the most common threats is phishing, a technique used by attackers to trick individuals into revealing sensitive information such as usernames, passwords, or financial details. Phishing attacks on social media typically involve the use of fake messages or websites that mimic legitimate platforms, luring users into clicking malicious links or downloading malware (Alabdan, 2020). Entrepreneurs, who often manage their own social media accounts without the support of a dedicated IT team, are particularly vulnerable to these deceptive tactics (Alkhalil, Hewage, Nawaf, & Khan, 2021).

Another prevalent threat on social media is malware, which involves installing malicious software on a user's device. Malware can be distributed through social media posts, direct messages, or even advertisements, making it easy for unsuspecting users to fall victim to these attacks. Once malware is installed, it can steal sensitive data, monitor user activity, or even lock users out of their accounts until a ransom is paid. The consequences of a malware attack can be devastating for entrepreneurial ventures that rely heavily on social media for business operations (Atanassov & Chowdhury, 2021).

In addition to phishing and malware, data breaches are a significant concern for businesses using social media. A data breach occurs when unauthorized individuals gain access to a company's sensitive information, such as customer data, financial records, or proprietary business insights. Social media platforms store vast amounts of personal information, making them prime targets for hackers seeking to exploit this data for financial gain. For startups and small businesses, the impact of a data breach can be particularly severe, leading to financial losses, regulatory fines, and damage to the company's reputation (Jain, Sahoo, & Kaubiyal, 2021).

Account takeovers represent another serious threat on social media. In these attacks, cybercriminals gain unauthorized access to a business's social media account, allowing them to post malicious content, steal information, or communicate directly with customers. Account takeovers can cause significant damage to a company's brand and credibility, particularly if the attacker uses the compromised account to defraud customers or spread misinformation (Wilbanks, 2020). For entrepreneurial ventures, the loss of control over their social media accounts can result in a severe loss of trust from their audience. Finally, social engineering attacks are a growing concern on social media platforms. These attacks involve manipulating individuals into divulging sensitive information or performing actions that compromise their security. Unlike traditional hacking methods that rely on technical vulnerabilities, social engineering attacks exploit human psychology. Cybercriminals may impersonate trusted individuals or organizations on social media to deceive users into sharing confidential information. Startups, which often have limited cybersecurity training, are especially susceptible to these kinds of attacks (Hijji & Alam, 2021).

### 2.2 Specific Risks and Vulnerabilities Faced by Entrepreneurial Ventures Using Social Media

Entrepreneurial ventures face unique challenges when it comes to cybersecurity on social media. Unlike large corporations with dedicated cybersecurity teams and advanced defenses, startups and small businesses often operate with limited budgets and technical expertise (Blum, 2020). As a result, they are more likely to fall victim to cyberattacks, and the impact of these attacks can be far more damaging. One of the most significant vulnerabilities for entrepreneurial ventures is the lack of dedicated cybersecurity resources. Many startups do not have the financial capacity to invest in advanced cybersecurity tools or hire professionals to manage their online security. Instead, business owners or small teams often manage their social media accounts, leaving them exposed to cyber threats they may not fully understand. This lack of expertise can make it difficult for entrepreneurs to detect and respond to potential threats promptly (Kramer, Teplinsky, & Butler, 2022).

Another risk is the tendency of startups to rely on third-party tools and platforms for managing their social media presence. Many entrepreneurs use social media management tools, scheduling apps, and analytics platforms to streamline their marketing efforts. While these tools can be valuable, they also introduce additional cybersecurity risks. If a third-party service is compromised, it can provide hackers with a backdoor into the company's social media accounts, leading to data breaches or account takeovers (Gupta, Rubalcaba, Gupta, & Pereira, 2024).

The rapid growth and scalability of entrepreneurial ventures also present cybersecurity challenges. As startups expand their social media presence to reach a wider audience, the volume of data they generate increases. This growth makes monitoring and securing all interactions and data exchanges on social media platforms more difficult. Furthermore, as a company's social media following grows, it becomes a more attractive target for cybercriminals, who see the potential for larger financial gains or more significant reputational damage (Oyeyemi et al., 2024).

The high level of public visibility associated with social media also creates risks for entrepreneurial ventures. Many startups rely heavily on social media to build their brand and connect with customers, making their online presence a critical part of their business strategy (Troise, Dana, Tani, & Lee, 2022). However, this visibility also makes them more vulnerable to cyberattacks, as any breach or incident on social media is likely to be highly publicized. For a small business, the public fallout from a cybersecurity incident can be difficult to recover from, potentially leading to a loss of customers and long-term damage to the brand (Netecha, 2024).

### 2.3 Examples of Notable Cybersecurity Incidents Affecting Small Businesses

Several high-profile cybersecurity incidents have demonstrated the severe impact of social media attacks on small businesses. One such example is the 2020 Twitter hack, where attackers gained access to the accounts of numerous high-profile individuals and businesses through a social engineering attack (Aldawood & Skinner, 2020). While this attack targeted prominent figures, it underscored the vulnerabilities in social media platforms and the ease with which cybercriminals can exploit them. For small businesses, such an attack could have catastrophic consequences, leading to a loss of customer trust and significant financial losses (Witman & Mackelprang, 2022).

Another notable incident occurred when Facebook experienced a data breach in 2018, exposing the personal information of over 50 million users. Although Facebook is a large corporation, the breach highlighted the vulnerabilities inherent in social media platforms and the potential for widespread data exposure (Daswani, Elbayadi, Daswani, & Elbayadi, 2021). Small businesses using Facebook for marketing and customer engagement were indirectly affected, as users became more cautious about sharing personal information on the platform, reducing engagement and trust (Nwaimo, Adegbola, & Adegbola, 2024b; Okoli et al., 2024).

These examples illustrate the diverse range of cybersecurity threats that can affect small businesses on social media platforms. The consequences of these incidents, whether through direct attacks or broader breaches of trust, can have long-lasting effects on entrepreneurial ventures that rely on social media for their operations (Zhang et al., 2022).

## 3 Machine Learning in Cybersecurity

### 3.1 Introduction to Machine Learning and Its Applications in Cybersecurity

Machine learning is a branch of AI that focuses on the development of algorithms capable of learning from data and making predictions or decisions without being explicitly programmed for every task. In the context of cybersecurity, machine learning systems analyze vast datasets, often too large for human operators to handle, to identify patterns and behaviors that indicate a potential security threat. This data-driven approach allows machine learning models to recognize known threats and detect new or evolving ones (Sarker et al., 2020).

One of the primary challenges in cybersecurity is that many attacks, especially on social media platforms, evolve quickly. New vulnerabilities and attack vectors are constantly emerging, and machine learning offers a way to keep up with these changes. Instead of relying solely on pre-programmed rules or signature-based detection methods, ML systems can learn from historical data, identify normal and abnormal behavior patterns, and adapt their responses accordingly. This adaptability makes machine learning particularly useful in the fast-paced world of social media, where threats such as phishing, malware, and account takeovers can spread rapidly across platforms (Apruzzese et al., 2023).

Machine learning has broad applications in cybersecurity, ranging from threat detection to incident response and even prediction of future attacks. In social media, ML can help detect suspicious activity, prevent unauthorized access, and protect sensitive data from breaches. For entrepreneurial ventures that rely heavily on social media for marketing and customer engagement, the use of machine learning in cybersecurity provides a scalable, cost-effective solution to safeguard their digital presence (Dasgupta, Akhtar, & Sen, 2022).

### 3.2 Key Machine Learning Techniques Used to Detect and Mitigate Threats

Several machine learning techniques are commonly employed in cybersecurity, each offering unique advantages in identifying and mitigating threats. These techniques include anomaly detection, supervised learning, unsupervised learning, and reinforcement learning, all of which contribute to a more robust cybersecurity framework (Ahsan et al., 2022).

Anomaly detection is one of the most widely used ML techniques in cybersecurity. This method involves training a model to recognize normal behavior patterns in a system or network. Once the model has a baseline of what constitutes normal activity, it can flag any deviations or anomalies that may indicate a security threat. In the context of social media, anomaly detection can be used to monitor user behavior, flagging unusual login patterns, unexpected account activity, or suspicious posts that may signal a phishing attempt or account takeover. Anomaly detection is particularly effective because it does not rely on predefined attack signatures; instead, it can detect previously unknown threats by identifying behaviors that fall outside the norm (Elmrabit, Zhou, Li, & Zhou, 2020).

Supervised learning is another key technique used in machine learning-based cybersecurity systems. In supervised learning, the model is trained on a labeled dataset, where the input data (e.g., network traffic or user behavior) is paired with corresponding labels that indicate whether the data is associated with normal behavior or a specific type of threat. The model uses this training data to learn how to classify future inputs as either benign or malicious. In social media security, supervised learning can be applied to detect known threats such as phishing or malware by identifying patterns that match those of previously encountered attacks (Dasgupta et al., 2022).

Unsupervised learning differs from supervised learning in that it does not rely on labeled data. Instead, the model is trained to find patterns or clusters within the data without knowing what constitutes a threat. This makes unsupervised learning particularly valuable for detecting unknown or emerging threats (Guo, Zhang, Jiang, Li, & Zhou, 2020). For example, in social media security, unsupervised learning can be used to analyze large datasets of user interactions, identifying clusters of suspicious behavior that may indicate coordinated attacks or automated bot activity. Because unsupervised learning can detect new attack vectors without needing to be trained on specific threat signatures, it offers a powerful tool for dealing with evolving cyber threats (Van Engelen & Hoos, 2020).

Reinforcement learning is a more advanced ML technique that involves training a model to make decisions based on feedback from its environment. In cybersecurity, reinforcement learning can be used to develop systems that learn how to respond to security threats dynamically. For instance, a reinforcement learning model could be used to optimize the response to a detected attack, choosing the most effective countermeasures based on previous outcomes (Singh, Kumar, & Singh, 2022). In social media security, reinforcement learning could help automate the defense process, allowing the system to respond to threats more effectively while minimizing disruptions to legitimate users (Miao et al., 2021).

### 3.3 Advantages of Machine Learning for Real-Time Threat Detection and Response in Social Media Data Protection

One of the most significant advantages of using machine learning in cybersecurity, particularly for social media data protection, is its ability to provide real-time threat detection and response. Traditional cybersecurity systems often rely on predefined rules or signatures to identify threats, which can be slow and ineffective against novel attacks. On the other hand, machine learning can analyze data in real-time, detecting threats as they emerge and responding immediately to mitigate potential damage (Nassar & Kamal, 2021).

The ability to automate threat detection and response through machine learning is invaluable for entrepreneurial ventures, which often operate with limited resources. Instead of relying on human operators to monitor social media activity and respond to security incidents, machine learning models can continuously analyze data and take action as needed. This reduces the burden on small businesses and ensures that potential threats are addressed promptly, before they can cause significant harm (Shah, 2021).

In addition to its speed and adaptability, machine learning offers a higher degree of accuracy in detecting threats. Traditional methods often struggle with false positives (incorrectly identifying benign activity as a threat) or false negatives (failing to detect actual threats). Machine learning models, particularly those that are well-trained and regularly updated with new data, can achieve higher precision in distinguishing between normal and malicious activity.

This is especially important in social media environments, where large volumes of data are generated, and distinguishing between legitimate and malicious interactions can be challenging (Wazid, Das, Chamola, & Park, 2022).

Another advantage of machine learning is its ability to scale. Social media platforms generate vast amounts of data every second, making it impractical for traditional security systems to keep up with the sheer volume of activity (Balaji, Annavarapu, & Bablani, 2021). Machine learning, however, excels at handling large datasets, making it an ideal solution for businesses that rely on social media for their operations. As entrepreneurial ventures grow and expand their online presence, machine learning can scale alongside them, providing continuous protection without requiring significant additional resources (Lwakatare, Raj, Crnkovic, Bosch, & Olsson, 2020).

Finally, machine learning offers the potential for predictive cybersecurity, where models are used to detect and respond to existing threats and anticipate future attacks. By analyzing historical data and identifying trends in cybercriminal behavior, machine learning systems can predict which areas of a network or social media account are most likely to be targeted next. This allows businesses to take proactive measures to secure vulnerable points before an attack occurs, further enhancing the overall security of their social media presence (Nassar & Kamal, 2021).

## 4 Challenges and Limitations of Machine Learning-Driven Cybersecurity

### 4.1 Limitations of Machine Learning Models in Handling Evolving Threats

One of the key limitations of machine learning in cybersecurity is its difficulty in handling rapidly evolving threats. Cyber attackers are constantly developing new techniques and exploiting previously unknown vulnerabilities. As these threats evolve, machine learning models must be continuously updated and retrained to remain effective. This process can be complex and time-consuming, as models trained on historical data may struggle to recognize emerging patterns or novel attack methods. For instance, while supervised learning models can be highly effective at detecting known threats, they are less capable of identifying zero-day attacks—those that exploit vulnerabilities not yet documented or understood (Bharadiya, 2023).

Moreover, machine learning models can be prone to adversarial attacks, where cybercriminals intentionally manipulate data to deceive the model. Attackers can exploit weaknesses in the model's learning process by introducing subtle alterations to the input data, causing it to misclassify or fail to detect a threat. For example, an attacker might disguise a phishing link to evade detection, knowing that the ML model will not recognize the altered link as malicious. This issue becomes particularly challenging on social media platforms, where attackers often modify their tactics to blend in with legitimate user activity, making it harder for machine learning systems to distinguish between benign and malicious behavior (Salem, Azzam, Emam, & Abohany, 2024).

Another limitation is the lack of contextual understanding in many machine learning models. While these models are excellent at detecting patterns in data, they cannot often comprehend the broader context in which an action occurs fully. For instance, a machine learning system might flag a particular user behavior as suspicious because it deviates from the norm, but without understanding the context (e.g., the user might be traveling and accessing their account from a different location), the model might generate false positives. In cybersecurity, excess false positives can overwhelm security teams, leading to alert fatigue and potentially causing real threats to go unnoticed (Strielkowski, Vlasov, Selivanov, Muraviev, & Shakhnov, 2023).

### 4.2 Privacy Concerns and Ethical Considerations

The use of machine learning in cybersecurity, particularly on social media platforms, raises significant privacy and ethical concerns. Social media platforms are repositories of vast amounts of personal data, including private messages, browsing habits, location data, and other sensitive information. When machine learning algorithms are applied to this data, they can analyze user behavior in ways that may infringe on individual privacy. The ability of machine learning models to scrutinize and profile users, even to improve cybersecurity, poses ethical questions about data collection, consent, and surveillance (Al-Mansoori & Salem, 2023).

One of the primary concerns is the potential misuse of data. While machine learning algorithms may be designed to detect threats, they also have the capacity to collect and process large amounts of personal information that may not be directly related to security risks. This raises questions about how this data is stored, who has access to it, and how long it is retained. Without stringent data protection measures in place, the use of machine learning in cybersecurity could inadvertently lead to the violation of user privacy, particularly if sensitive information is mishandled or exposed to unauthorized parties (Bhattacharya, Roy, Chattopadhyay, Das, & Shetty, 2023).

Another ethical consideration is the potential for bias in machine learning models. Machine learning systems are only as good as the data on which they are trained. Suppose the training data is biased or incomplete. In that case, the model may produce biased outcomes, unfairly targeting certain groups of users or failing to protect others. In the context of social media, this could lead to disproportionate scrutiny of certain user behaviors or demographics, raising concerns about discrimination and fairness. For example, a machine learning model trained on data from a specific region or demographic may not perform as well when applied to users from different cultural or geographic backgrounds (Bodini, Rivolta, & Sassi, 2021).

There are also concerns about transparency and accountability. Machine learning models, particularly those that use complex algorithms like deep learning, are often considered "black boxes" because it can be difficult to understand how they arrive at specific decisions. This lack of transparency can be problematic in cybersecurity, where it is important to understand why a particular action was flagged as a threat or why certain data was prioritized for protection. In the event of a data breach or security failure, the opacity of machine learning systems may make it difficult to assign responsibility or determine what went wrong, further complicating efforts to improve security (Buhrmester, Münch, & Arens, 2021).

### 4.3 Challenges Specific to Entrepreneurial Ventures

Adopting machine learning-driven cybersecurity solutions presents several unique challenges for entrepreneurial ventures, primarily related to cost, expertise, and scalability. Startups and small businesses often operate on tight budgets, making investing in advanced cybersecurity technologies like machine learning difficult. While larger organizations may have the resources to hire dedicated data scientists and cybersecurity experts, entrepreneurial ventures may lack the financial capacity to do so. As a result, they may be forced to rely on off-the-shelf solutions, which may not offer the same level of customization or effectiveness as more sophisticated systems (Nwaimo, Adegbola, Adegbola, & Adeusi, 2024; Nwobodo, Nwaimo, & Adegbola, 2024).

The lack of in-house expertise is another significant barrier for startups looking to implement machine learning in their cybersecurity strategies. Machine learning requires a deep understanding of both cybersecurity principles and data science techniques, which can be difficult for small businesses to acquire. Even if a startup can afford to invest in machine learning tools, they may not have the personnel to manage, train, and maintain these systems effectively. This gap in expertise can lead to suboptimal performance, with machine learning models failing to detect critical threats or generating a high volume of false positives that overwhelm small teams (Nwaimo, Adegbola, & Adegbola, 2024a).

Scalability is also a concern for entrepreneurial ventures. As a business grows and its social media presence expands, the data that needs protection increases dramatically. Machine learning systems must be able to scale alongside the business to ensure that they can continue to detect threats and protect sensitive data effectively. However, scaling machine learning models requires significant computational resources, which can be costly and difficult to manage for startups. Small businesses may struggle to protect their data as they grow without the infrastructure to support large-scale machine learning operations (Westerlund, 2020).

In addition to these technical challenges, there are regulatory hurdles that entrepreneurial ventures must navigate when applying machine learning to social media data. In many jurisdictions, strict regulations govern personal data collection, storage, and processing. Startups that wish to use machine learning for cybersecurity must ensure that their data practices comply with these regulations, such as the General Data Protection Regulation (GDPR) in the European Union. Failure to do so can result in significant legal and financial penalties, adding another layer of complexity to the implementation of machine learning-based cybersecurity solutions (Abdul-Azeez, Ihechere, & Idemudia, 2024; Adewusi et al., 2024).

## 5 Future Directions

### 5.1 Emerging Trends in Machine Learning for Cybersecurity

One of the most promising emerging trends in machine learning for cybersecurity is the integration of deep learning. Deep learning, a subset of ML that uses neural networks with multiple layers, can identify complex patterns in large datasets. This makes it particularly effective at detecting sophisticated cyber threats, such as those that involve subtle behavioral changes or highly targeted phishing attacks. Deep learning models have the potential to outperform traditional ML models by recognizing these intricate patterns and adapting to new types of attacks more quickly. As more social media platforms adopt deep learning for cybersecurity, the industry is likely to see improvements in the detection of advanced threats.

Another key trend is the rise of AI-driven threat intelligence, where machine learning is used to gather and analyze threat data in real-time. This approach enables cybersecurity systems to continuously monitor global cyber threat environments, providing up-to-date intelligence on emerging attack vectors. For social media platforms, AI-driven threat intelligence can help identify new vulnerabilities and anticipate the tactics of cybercriminals. This proactive approach allows businesses to defend their networks and social media accounts better before a threat materializes, enhancing overall cybersecurity resilience.

### 5.2 Best Practices for Entrepreneurial Ventures

For entrepreneurial ventures, implementing machine learning-based cybersecurity solutions requires a strategic approach. Data quality is critical to the success of any ML system. Startups must ensure they are feeding accurate, clean, and relevant data into their models to improve threat detection capabilities. This may involve working with cybersecurity providers or investing in tools that automatically clean and filter data.

Another best practice is to integrate machine learning with existing security tools. Rather than completely replacing traditional cybersecurity measures, startups should consider incorporating ML solutions into their infrastructure. This allows for a layered approach, where machine learning enhances threat detection and response without creating gaps in security coverage.

Entrepreneurial ventures should also prioritize scalability when choosing machine learning solutions. As businesses grow, so too does the volume of data that must be protected. Scalable ML models ensure that cybersecurity systems can evolve in tandem with the business, offering continued protection as social media and online operations expand.

### 5.3 Recommendations for Improving Social Media Data Protection

To improve social media data protection using machine learning, businesses should focus on continuous model training and updates. Given the constantly evolving nature of cyber threats, retraining machine learning models on new data is essential to keep them effective. Regular updates allow the models to recognize emerging attack patterns and respond to new vulnerabilities.

Another recommendation is to increase collaboration between social media platforms and cybersecurity providers. By sharing threat intelligence, businesses can benefit from a collective knowledge base, improving the overall effectiveness of machine learning systems. Social media platforms should also invest in user education, ensuring that individuals understand basic cybersecurity practices. This reduces the likelihood of human errors, such as falling victim to phishing attacks, which ML models can complement by detecting and mitigating risks.

## 6 Conclusion

This study underscores the critical role of machine learning (ML) in addressing cybersecurity challenges for entrepreneurial ventures leveraging social media platforms. By offering scalable and adaptive solutions, ML enables real-time detection and mitigation of threats, such as phishing, malware, and account takeovers, which are particularly detrimental to startups with limited resources. The integration of ML-driven tools, including anomaly detection, supervised learning, and AI-powered threat intelligence, has proven effective in protecting sensitive data and ensuring operational continuity for small businesses. Despite its potential, the study highlights significant challenges in implementing ML for cybersecurity, including high costs, technical complexity, and evolving threat landscapes. Privacy concerns and ethical issues further complicate the adoption of these technologies. For entrepreneurial ventures, overcoming these barriers requires a strategic approach, emphasizing collaboration with cybersecurity providers, continuous training of ML models, and adherence to stringent data protection regulations. Emerging trends, such as deep learning and AI-driven predictive analytics, offer promising avenues for enhancing social media data protection. Startups must adopt best practices, including integrating ML with existing security frameworks, prioritizing data quality, and ensuring scalability to accommodate growth. By doing so, entrepreneurial ventures can safeguard their digital presence while maximizing the benefits of social media for business expansion. Ultimately, this study provides a roadmap for startups to navigate the intersection of ML and cybersecurity, fostering a safer digital ecosystem. By addressing vulnerabilities on social media platforms, this research contributes to broader societal benefits, including enhanced consumer trust, economic resilience, and the sustainable growth of digital entrepreneurship. Future efforts should focus on refining ML models, fostering public-private partnerships, and promoting education on cybersecurity best practices to empower businesses and users in an increasingly connected world.

## 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] 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.

[4] Al-Mansoori, S., & Salem, M. B. (2023). The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations. International Journal of Social Analytics, 8(9), 1-16.

[5] Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future internet, 12(10), 168.

[6] Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. International Journal of Computer Applications, 177(30), 1-11.

[7] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

[8] 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.

[9] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

[10] Atanassov, N., & Chowdhury, M. M. (2021). Mobile device threat: Malware. Paper presented at the 2021 IEEE International Conference on Electro Information Technology (EIT).

[11] Balaji, T., Annavarapu, C. S. R., & Bablani, A. (2021). Machine learning algorithms for social media analysis: A survey. Computer Science Review, 40, 100395.

[12] Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. European Journal of Technology, 7(2), 1-14.

[13] Bhattacharya, M., Roy, S., Chattopadhyay, S., Das, A. K., & Shetty, S. (2023). A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges. Security and Privacy, 6(1), e275.

[14] Blum, D. (2020). Rational cybersecurity for business: the security leaders' guide to business alignment: Springer Nature.

[15] Bodini, M., Rivolta, M. W., & Sassi, R. (2021). Opening the black box: interpretability of machine learning algorithms in electrocardiography. Philosophical Transactions of the Royal Society A, 379(2212), 20200253.

[16] Buhrmester, V., Münch, D., & Arens, M. (2021). Analysis of explainers of black box deep neural networks for computer vision: A survey. Machine Learning and Knowledge Extraction, 3(4), 966-989.

[17] 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.

[18] Daswani, N., Elbayadi, M., Daswani, N., & Elbayadi, M. (2021). Facebook Security Issues and the 2016 US Presidential Election. Big Breaches: Cybersecurity Lessons for Everyone, 97-130.

[19] Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020). Evaluation of machine learning algorithms for anomaly detection. Paper presented at the 2020 international conference on cyber security and protection of digital services (cyber security).

[20] Guo, L.-Z., Zhang, Z.-Y., Jiang, Y., Li, Y.-F., & Zhou, Z.-H. (2020). Safe deep semi-supervised learning for unseen-class unlabeled data. Paper presented at the International conference on machine learning.

[21] Gupta, V., Rubalcaba, L., Gupta, C., & Pereira, L. (2024). Social networking sites adoption among entrepreneurial librarians for globalizing startup business operations. Library Hi Tech, 42(3), 947-974.

[22] Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. Ieee Access, 9, 7152-7169.

[23] Jahankhani, H., Meda, L. N., & Samadi, M. (2022). Cybersecurity challenges in small and medium enterprise (SMEs). In Blockchain and Other Emerging Technologies for Digital Business Strategies (pp. 1-19): Springer.

[24] Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157-2177.

[25] Kramer, F. D., Teplinsky, M. J., & Butler, R. J. (2022). Cybersecurity for Innovative Small and Medium Enterprises and Academia: Atlantic Council, Scowcroft Center for Strategy and Security.

[26] Lwakatare, L. E., Raj, A., Crnkovic, I., Bosch, J., & Olsson, H. H. (2020). Large-scale machine learning systems in real-world industrial settings: A review of challenges and solutions. Information and software technology, 127, 106368.

[27] Miao, Y., Chen, C., Pan, L., Han, Q.-L., Zhang, J., & Xiang, Y. (2021). Machine learning–based cyber attacks targeting on controlled information: A survey. ACM Computing Surveys (CSUR), 54(7), 1-36.

[28] 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.

[29] Netecha, M. (2024). Digital marketing tendencies of Ukrainian business development at an international level (based on the "Business Media Network" case). Private Higher Educational Establishment-Institute "Ukrainian-American …,

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] Oyeyemi, O. P., Kess-Momoh, A. J., Omotoye, G. B., Bello, B. G., Tula, S. T., & Daraojimba, A. I. (2024). Entrepreneurship in the digital age: A comprehensive review of start-up success factors and technological impact. International Journal of Science and Research Archive, 11(1), 182-191.

[36] Park, H., Kim, S., Jeong, Y., & Minshall, T. (2021). Customer entrepreneurship on digital platforms: Challenges and solutions for platform business models. Creativity and Innovation Management, 30(1), 96-115.

[37] Salem, A. H., Azzam, S. M., Emam, O., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big data, 11(1), 105.

[38] Sarker, I. H., Kayes, A., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.

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

[40] Singh, B., Kumar, R., & Singh, V. P. (2022). Reinforcement learning in robotic applications: a comprehensive survey. Artificial Intelligence Review, 55(2), 945-990.

[41] Strielkowski, W., Vlasov, A., Selivanov, K., Muraviev, K., & Shakhnov, V. (2023). Prospects and challenges of the machine learning and data-driven methods for the predictive analysis of power systems: A review. Energies, 16(10), 4025.

[42] Troise, C., Dana, L. P., Tani, M., & Lee, K. Y. (2022). Social media and entrepreneurship: exploring the impact of social media use of start-ups on their entrepreneurial orientation and opportunities. Journal of Small Business and Enterprise Development, 29(1), 47-73.

[43] Van Engelen, J. E., & Hoos, H. H. (2020). A survey on semi-supervised learning. Machine learning, 109(2), 373-440.

[44] Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. ICT express, 8(3), 313-321.

[45] Westerlund, M. (2020). Digitalization, internationalization and scaling of online SMEs. Technology Innovation Management Review, 10(4).

[46] Wilbanks, L. R. (2020). Cyber risks in social media. Paper presented at the Social Computing and Social Media. Design, Ethics, User Behavior, and Social Network Analysis: 12th International Conference, SCSM 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part I 22.

[47] Witman, P. D., & Mackelprang, S. (2022). The 2020 Twitter Hack--So Many Lessons to Be Learned. Journal of Cybersecurity Education, Research and Practice, 2021(2).

[48] Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., & Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. International Journal of Information and Computer Security, 19(3-4), 402-442.