World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Advanced Detection Techniques to neutralize Supply Chain Cyber-attacks on small and medium businesses in the United States: The Machine Learning and AI Approach.

John Oluwafemi Ogun [1,*] and Segun Philip Olupinla [2]

[1] *Baylor University, Information Systems and Business Analytics, Hankamer School of Business, Waco, Texas, United States.*
[2] *International College of Research and Data Sciences, Head Research and Evaluation, Ilorin, Kwara State, Nigeria.*

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 662–671

Publication history: Received on 16 August 2024; revised on 28 September 2024; accepted on 30 September 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0459

Abstract

Cyber-attacks targeting supply chains represent a significant and increasing risk for small and medium-sized businesses (SMBs) in the United States. This paper examines the role of machine learning (ML) and artificial intelligence (AI) in detecting and mitigating these cybersecurity threats. Key challenges faced by SMBs include high implementation costs, a shortage of skilled personnel, inadequate data quality, and the complexity of integrating advanced technologies into existing systems. Despite these hurdles, the paper identifies strategic approaches that can empower SMBs to effectively leverage ML and AI, including affordable solutions, targeted training, and improved data management practices. It emphasizes the importance of addressing privacy and usability concerns to facilitate successful technology adoption. Recommendations include pursuing cost-effective, subscription-based AI and ML models, utilizing government incentives, and enhancing workforce skills through training and partnerships. Additionally, collaboration with larger organizations can improve data management and system efficacy. By implementing robust protective measures and increasing awareness through educational initiatives, SMBs can strengthen their cybersecurity posture and better navigate the evolving landscape of cyber threats.

Keywords: Supply Chain Cyber-attacks; Small and Medium-sized Businesses (SMBs); Machine Learning; Artificial Intelligence; and Cybersecurity.

1. Introduction

According to Hasan et al., (2024), small and medium-sized businesses (SMBs) are the backbone of the economy in the United States, providing more American jobs than any other single source and driving its economic growth. As much as the business operations incorporate digitalization, so have those same enterprises become cybercriminals' favorite targets regarding supply chain attacks. These attacks exploit vulnerabilities within the interlinked networks of suppliers, vendors, and contractors, leading to enormous financial and reputational damage (Pandey et al., 2020). Cyber threats are gaining in complexity, increasing the need for advanced methods of detection that can find and neutralize a threat before consequences can be realized. In that respect, the integration of Machine Learning and Artificial Intelligence has turned out very promising in delivering effective tools to SMBs to improve their security measures around supply chains because of sophisticated attacks (Ganesh & Kalpana, 2022).

1.1. Problem statement

Small and medium-sized businesses, due to their high number all over America, offer the largest chunk of all American jobs while fueling their economic growth (Johnson, 2022). On the contrary, with business activities finding increasing

* Corresponding author: John Oluwafemi Ogun

space that integrates into the cyber world, these companies have turned out to be cybercriminals' favorite targets in attacks such as supply chain attacks. Whereas machine learning and artificial intelligence have already shown some bright promise in detecting and neutralizing cyber-attacks, there is little real understanding of how well these techniques perform within the specific context of an SMB (Haletska, 2022). Most of the research and commercial approaches are pointed toward larger organizations. As a result, very little is known about the way that advanced techniques could be effectively tailored to the situation of an SMB. As this gap stands between SMBs and the use of current state-of-the-art technologies that are rapidly applied to protect supply chains, it increases cyber risk exposure for such organizations.

There is a requirement for the development of a special framework by which to implement ML- and AI-based detection systems, tailored to the needs and capabilities unique to U.S.-based SMBs (Broadbent, 2021). A framework should account for the financial constraints, operational scale, and technical expertise of these enterprises in a way that makes sure that such advanced approaches have been effective and feasible for small business entities. Unless there is a well-designed framework, very difficult may be the adoption and its ramifications by integrating ML and AI solutions into existing cybersecurity strategies at SMBs.

Furthermore, what remains blurred is the cost-effectiveness and scalability of ML- and AI-based threat detection techniques for SMBs. One strongly feels the imperative for any new solution to be viable within the tight budgets characteristic of SMBs. There is an urgent requirement to assess whether these technologies can pay back an investment made by an SMB or if they can scale with such small businesses as they get bigger.

Lastly, there exist strong difficulties in adopting ML and AI technologies to enhance the supply chain cybersecurity of SMBs. These include not only financial problems but also technical issues, organizational friction due to reluctance against change, and a lack of awareness or understanding of the benefits these technologies have for their use. The identification of these barriers is, therefore, very critical to ensure that SMBs can effectively make use of ML and AI for cybersecurity; such must be followed through with useful recommendations to facilitate its adoption and integration.

It is in this regard that this study embarks on the critical need for developing tailored, cost-effective, and scaled-up ML- and AI-based solutions to improve supply chain cybersecurity for U.S.-based SMBs. Precise challenges of the SMBs will be identified, the efficacy of modern detection techniques will be tracked, a framework by which to implement will be structured, measures for cost-effectiveness and scalability assessed, and action-driven moves recommended to enable SMBs to better protect their supply chains against cyberattacks.

1.2. Scope

This research will focus on the current status of detection and evaluation about state-of-the-art using Machine Learning and Artificial Intelligence to deter supply chain cyberattacks, specifically against Small and Medium Businesses within the United States. It particularly researches the following:

Identification of Cybersecurity Challenges: This study will try to identify and analyze what exactly the cybersecurity challenges are that U.S.-based SMBs face within their corresponding supply chains. This would also be inclusive of how deep an understanding is required in terms of the nature and frequency of cyber threats, vulnerabilities that exist within the supply chain network, and how these attacks are detrimental to the operation and profitability of SMBs.

Evaluation of ML and AI-Based Detection Techniques: This paper will evaluate the various techniques based on ML and AI previously applied or having applicability in detection and mitigation against supply chain cyber-attacks. This includes extant technologies and growing approaches, assessment of their effectiveness, precision, and adaptability to the SMB context.

1.3. Significance

The overall significance of the study is that it will facilitate holistic, action-enabling approaches toward strengthening cybersecurity for SMBs in the United States, a typically under-protected but very vital sector of this great nation's economy. The various key contributions and significance of this study research are as follows: This research is focused on enhancing the information security of one of the most critical gaps in the cybersecurity landscape. SMBs usually do not have the resources and competencies to protect themselves from sophisticated attacks as compared to large enterprises. Cost-effective and scalable ML and AI-based techniques for the detection of threats in SMBs are expected to be the developed outcome of this research, thereby enhancing their defense mechanisms. This work will also help reduce the economic losses linked to the supply chain cyberattack on SMBs by providing effective techniques of detection and neutralization. The research work will make its contribution to the development of ML and AI

technologies related to cybersecurity. The study will narrow the gap between the most advanced technological developments and practical applications by reviewing frameworks relevant to SMBs and further developing them so that they are suitable for the area under investigation. The results of this research can help policymakers and regulators understand the special needs of SMBs in terms of cybersecurity, eventually coming up with policies and support mechanisms that are much more effective in promoting the diffusion of advanced detection technologies. The research will add value to the body of knowledge within academia and industry on the application of ML and AI in cybersecurity, particularly within an area as critical as SMBs. That will be very useful for future research and for practitioners who want to push the boundaries of cybersecurity in their organizations.

1.4. Research Questions

- What problems does the modern world expose an SMB in the United States to in terms of detecting and some ways of neutralizing supply chain cyber-attacks?
- What are the various machine learning and AI-based techniques for effectiveness in detecting and neutralizing such supply chain cyber-attacks?
- What could be the barriers to the implementation of ML and AI solutions in supply chain cybersecurity for SMBs and how such can be mitigated?

1.5. Objectives

- To identify challenges that U.S-based SMBs face in managing supply chain cyber risks.
- To examine the various Machine Learning and AI-based techniques for effectiveness in the detection and neutralization of supply chain cyber-attacks.
- To assess the barriers to the implementation of ML and AI solutions in supply chain cybersecurity for SMBs and how such can be mitigated.

2. Methodology Research design

The approach will be a qualitative case study, supplemented by an in-depth literature review focused on U.S.-based small and medium-sized businesses (SMBs). This case study will further make it possible to look into practical scenarios of supply-chain cyber-attacks against SMBs within the United States, coupled with how ML and AI techniques are utilized in their detection and neutralization. This literature review will delineate the challenges, solutions, and effectiveness of these techniques in the context of U.S. SMBs.

2.1. Data collection method

Primary sources in this research will be peer-reviewed academic articles, industry reports, government publications, and case studies related to supply chain cybersecurity, ML, and AI in the U.S. context.

The data collection process for this study will involve:

Literature Search: Relevant literature shall be identified through a systematic search of IEEE Xplore, Google Scholar, and JSTOR, using the following keywords: "supply chain cyber-attacks," "SMBs in the U.S.," "Machine Learning," "Artificial Intelligence," and "cybersecurity."

Case Study Selection: Priority will first be given to case studies that deal specifically with supply chain cyber-attacks within the U.S. Case studies will provide information to answer questions about the nature of such attacks, the problems SMBs face in countering them, and how ML and AI mitigate this kind of threat.

2.2. Data analysis

The themes with these emphases shall be applied in the thematic analysis of the collected literature. Literature review of common challenges that U.S. SMBs face in the management of cyber risk in their supply chains. Again, the literature shall be consulted about the effectiveness of different techniques using ML and AI to detect and paralyze supply chain cyber-attacks on U.S. SMBs. Also, the literature will be explored to identify the barriers to adopting ML and AI technologies for enhancing supply chain cybersecurity among U.S. SMBs, along with associated recommendations on how to overcome them.

3. Result

3.1. Objective 1: To identify specific issues relating to the management of US-based SMB supply chain cyber risks.

Under this objective, 3 cases were used to position the specific issues relating to the management of US-based SMBS. The first is the Target Corporation Data Breach, 2013.

One of the most famous landmark cases of the early years of this decade is the 2013 Target data breach, which described the weak points in large enterprise supply chains and the consequences to small suppliers (Syed et al., 2022). In Target's case, a third-party vendor, a small to medium-sized HVAC company, was breached. The instance further reinstated that most of the SMBs have poor cybersecurity measures against the same, lack of awareness, and thereafter correspondingly less skilled workforce; all these can easily convert into one big vulnerability within the supply chain. It is stated further that cybercriminals often approach small vendors as an entryway to crack into larger organization networks. The second case is, the SolarWinds cyberattack which debuted new several critical challenges given the cyber supply chain risks facing SMBs (Melnyk et al., 2022). Most of the SMBs within the case were indirect victims due to their dependency on Orion Software by SolarWinds. One example, this serves as a case study of dependencies upon third-party vendors and how a cyberattack on such vendors could be cascading. Thus, strategies for risk management were more robust in SMBs, as recommended by Mandiant in 2020 (Nolan & Fixler, 2021).

The third case is the Colonial Pipeline ransomware attack, in 2021. This attack took fuel supplies offline across the United States, quite literally exposing weaknesses in critical infrastructure. While the Colonial Pipeline organization itself is not an SMB, the implication was rampant for many SMBs reliant on the fuel supplies disrupted by the attack (Vikash, 2022). More than anything else, this case study stands for the supply chains becoming interdependent and the level of difficulty faced by an SMB in mitigating risks because of an attack on bigger entities up the chain.

From these cases, the following specific challenges relating to the management of US-based SMB supply chain cyber risks were derived:

- Vulnerability Due to Poor Cybersecurity Measures: The Target Corporation breach of 2013 showed that many SMBs like the HVAC company involved lack adequate security measures. Largely, they do not have tight security measures and hence become easily susceptible to hackers who use them as a gateway to bigger organizations. Larger enterprises are in the supply chain with the SMBs having bad cybersecurity hence they can be used by the aggregator to penetrate even the large enterprises.
- Lack of Cybersecurity Awareness and Skilled Workforce: The Target breach also learned that SMBs have a low level of awareness of the risks of cyber threats and correspondingly, have a less skilled human resource to mitigate these threats. This lack of knowledge and skills that they possess worsens their situation since they cannot even detect, much less prevent or mitigate cyber threats to the supply chain hence amplifying risk in the process.
- Dependency on Third-Party Vendors: This means that SMBs are rather indirect victims of state-sponsored cyber activity that they cannot influence, for example, as a result of being impacted by cyberattacks targeting third parties such as SolarWinds' Orion software. This makes these third-party applications vulnerable and risky since an attack on them threatens the operation and security of SMBs.
- Challenges in Mitigating Risks from Interdependent Supply Chains: The Colonial Pipeline incident proved that SMBs are now integrated into supply chain networks in which disruptions in larger players, such as the pipeline firm, have a ripple effect on other organizations. There are several challenges that SMBs experience in managing cyber risks because many of them are downstream from more extensive upstream parties. In case of an attack targeting the critical infrastructure or a major supplier, it leads to disastrous consequences that are beyond the capacity of SMBs to manage on their own.
- Inadequate Risk Management Strategies: It was also revealed that the SolarWinds attack highlighted the fact that most SMBs do not have such well-developed approaches to risk management as are outlined by cybersecurity professionals, such as Mandiant. That is why, in contrast to large companies, SMBs cannot avoid critical impact from supply chain cyber risks because they have inadequate practices for risk management and are not ready for such scenarios in advance.

These issues underscore the urgency of SMBs improving their cybersecurity posture, raising cybersecurity literacy, and decreasing reliance on third parties prone to cyber threats as well as the necessity of improving their techniques of managing cyber risks and fortifying their supply chains against cyber threats.

3.2. Objective 2: Examine the various machine learning and AI-based techniques for effectiveness in detecting and neutralizing such supply chain cyber-attacks.

Three cases help capture this objective. First, Darktrace Cyber Security is a cyber-security firm that caters to companies and organizations offering elite cyber defense services based on the employment of AI for the identification of threats and subsequent elimination (Jahankhani, 2020). Darktrace was founded in 2013 and it has quickly risen to be the world leader in autonomous cybersecurity, especially for the protection of supply chains.

Darktrace works with the use of its AI engine called the "Enterprise Immune System" which is self-learning and monitors the behaviors within an organization in the same way we observe the functions of users, devices, and networks before identifying the deviant ones. This enables it to be able to detect any anomaly which may hint at a cyber threat. Such patterns include assessing the kind of traffic flowing within the network or the activities of any user across the network in real time to look for any anomaly that may go unnoticed in large and complex supply chain networks. The uniqueness of the strategy and approach of Darktrace also lies in its autonomous response with the help of Antigena (Piconese et al., 2020). This system offers the capability to control threats by applying measures like quarantine of affected assets and blocking potentially malicious actions without human involvement. This is especially crucial in supply chain protection because it may take only a few minutes to disseminate a virus leak or breach.

Darktrace's AI is self-educating, which implies that it learns from new threats and is thus very efficient in today's dynamic threat environment (Katiyar, 2023). It also has enhanced visual capabilities that help the security team to gauge how such menaces are changing thus helping them to be a step ahead in prevention. On the effectiveness criterion, it was evident that Darktrace is effective in the identification of early detection of anomalies especially in supply chain cyberattacks. By using proactive threat mitigation capability one can easily control threats to minimize the effect they have on the integrity of the supply chain. In particular, its ability makes it possible to detect and counter even such threats that can be labeled as complex and refined. Darktrace also covers all the areas of the supply chain and keeps track of all the possible weak points so that the attacks can be prevented soon (Qumer & Ikrama, 2022).

Second is, IBM Watson for Cyber Security which is a sophisticated AI-based tool for improving the detection of cyber threats and investigation as well as their prevention (K. Hasan et al., 2019). This technology augments cognitive computing, machine learning, and natural language processing which help in the analysis of structured and unstructured data including security blogs and research papers that would help the technology to determine newly detected threats that simple tools like SIEM couldn't detect let alone identifying them within the supply chain security framework. Watson has a link with Ibm's X-Force Exchange to identify global cyber threat data to determine whether it poses risks to the supply chain and the actions to take to contain them. Among them, one of the most useful is the feature to automate the work on investigation of security incidents. Once a threat is identified Watson is capable of studying the context, and the level of threat and even suggests or takes actions to avoid cyber threats, thus minimizing the time needed to respond to such threats (Perwej et al., 2021).

The NLP feature of Watson helps the system to analyze large volumes of unstructured data and come up with analytics to help identify potential threats and recommend appropriate countermeasures. It also works in conjunction with other security solutions, allowing customers to have a holistic vision of possible supply chain threats and well-coordinated actions. Again, being an adaptive learning platform, Watson makes enhancements to its algorithms from the data it handles and the threats that it experiences. That makes it particularly useful in the continuing environment of supply chain security where threat types can evolve swiftly. Watson is valuable in assessing the risks because it can amalgamate information from various sources and give a complete outlook on possible threats when perused in the context of supply chain management (Fawcett et al., 2012).

- Deducing from these cases the following are different techniques for detecting and fighting cyberattacks on SMBs:

  i. Self-Learning AI (Enterprise Immune System): Self-Learning AI (Enterprise Immune System): Always stays active and gets trained with users' behavior, devices, and networks within an organization with a view of finding out when something weird of which may hint at a cyber threat is afoot.
- *ii. Anomaly Detection:* It is a technology that analyses the current activity on a network or with a user to look for a sharp change from the norm, that could be a result of an attempted cyber-attack.
- *iii. Autonomous Response (Antigena):* Isolation of affected assets and prevents such moves by reminding threats without approaching users to limit threats.
- *iv. Proactive Threat Mitigation:* Analyzes threats and prevents them from likely affecting the supply chain flow in the organization.

- *v. Visual Threat Analysis:* Offers better visualization facilities that would enable the security personnel to better track and comprehend the dynamic nature of threats.
- *vi. Machine Learning:* Adapts and changes its algorithms on the input data and the threats that it identifies and eradicates thereby enhancing its efficiency in doing so.
- *vii. Natural Language Processing (NLP*): Process and filter through large amounts of data that has not been earmarked for any particular use giving it a good perspective of threat.
- *viii. Global Threat Intelligence Integration (X-Force Exchange):* This Makes use of cyber threat information from all around the world to evaluate the risks and apply corresponding protection strategies within the supply chain.

3.3. Objective 3: to assess the barriers to the implementation of ML and AI solutions in supply chain cybersecurity for SMBs and how such can be mitigated.

In the context of cybersecurity, an impediment to Machine Learning (ML) and Artificial Intelligence (AI) solutions can be described as a factor that can oppose or slow down the integration of Machine Learning and Artificial Intelligence in the SMBs' cybersecurity frameworks as well as restrict their efficient application (Ozkan-Ozay et al., 2024). These may be financial, technical, or organizational ones or stem from cultural perspectives and can thus substantially slow down or even hinder the implementation of state-of-the-art cybersecurity solutions based on ML and AI.

3.4. Barriers to Implementation

3.4.1. Cost Constraints

Small and medium-sized businesses (SMBs) often operate with limited budgets, making the high upfront costs associated with implementing AI and ML solutions in cybersecurity a significant barrier. The costs include purchasing software, acquiring necessary hardware, and training staff to effectively use these technologies. To mitigate this, SMBs can explore cost-effective AI and ML solutions that offer scalable pricing models, such as subscription-based services or cloud-based platforms. Additionally, governments and industry bodies can offer subsidies, grants, or tax incentives to encourage adoption (Dalton, n.d., SMALL, n.d., Mburu, 2023).

Lack of Skilled Workforce: AI and ML technologies require specialized skills in data science, machine learning, and cybersecurity, which are often in short supply among SMBs (Rawindaran et al., 2021). This skill gap can prevent SMBs from effectively implementing and managing these advanced technologies. This can be overcome if SMBs can invest in training and upskilling their current workforce through partnerships with educational institutions, online courses, or industry certification programs. Collaboration with third-party cybersecurity providers who offer managed services can also help bridge the skill gap.

Data Quality and Quantity: The effectiveness of AI and ML solutions depends heavily on the quality and quantity of data available for training the algorithms (Rawindaran et al., 2021). SMBs may struggle with limited or poor-quality data, which can hinder the performance of these technologies. This will be best managed if SMBs should focus on improving their data collection and management practices, possibly by adopting standardized data formats and protocols. They can also explore partnerships with larger organizations or industry consortia to access shared data pools, enhancing the quality and volume of data available for AI and ML applications.

Cybersecurity Awareness and Understanding: Most SMBs have low awareness levels about possible cyber threats they can be exposed to and the possible uses of AI and ML in providing protection (Chidukwani et al., 2022). This lack of understanding can cause some businesses to be slow in the adoption of new technologies. For this, ultimately, SMBs are more likely to recognize the need to invest in AI and ML for cybersecurity when there is a flow of information through campaigns, workshops, and seminars. Another method of increasing the SMB's willingness to adopt the technologies is through the use of case studies and success stories of other SMBs that have adopted the technologies.

The complexity of Implementation: AI and ML solutions are not easy to deploy because they may require the integration of new systems into legacy IT environments, may require fine-tuning to reflect the needs of particular organizations, and may require ongoing support. SMBs can find this complexity challenging to deal with especially if they have few professionals in this field. AI and ML solutions that are easy to implement in SMBs are available in the market and these systems also have catchy interfaces as well as good vendors' support. Another way is to involve external consultants or work with technology vendors who can also help in implementing the solution.

Security and Privacy Concerns: Applications of AI and ML involve training and employing algorithms on huge volumes of data that contain personal information hence creating the issue of data protection, and security of these systems (Chio

& Freeman, 2018). AI and ML solutions could pose some risks on SMBs' data, and the firms want to minimize such risks. To alleviate all these risks, SMBs must ensure that the AI and ML solutions they implement meet data privacy standards (e.g., GDPR) and data security controls such as encryption and access controls. The same concern should apply to the vendors proposing AI and ML solutions and they should ensure direct opacity of their approaches and guarantee data safety.

4. Summary of the Findings

SMBs are experiencing increasing risks of cyber threats, especially to their supply chain, while current techniques such as ML and AI are focused on large firms. Through this study, the authors seek to propose a framework for the adoption of ML- and AI-based cybersecurity solutions for SMBs that are cost-efficient, generic, and effective for implementation amid the critical constraints to the SMBs, including financial, technical, and organizational factors. This research aims to analyze the extent of using Machine learning and artificial intelligence in the prevention of the supply chain cyberattacks on SMBs in USA. It aims to outline major cybersecurity threats that such businesses encounter and analyze the effectiveness of the current ML and AI-based detection approaches to determine their applicability to SMBs. This research aims to establish the cybersecurity threats affecting the U.S.-based SMBs, especially supply chain attacks. Its purpose is to determine threats that such businesses have, analyze the appropriateness of the use of ML and AI, and consider the challenges of integration. The research uses qualitative case study and literature review approaches for the following reasons: This study thus used scientific research materials such as peer-reviewed articles and literature review, government reports, and case studies. The data collection process will entail a systematic search of the literature and qualitative analysis, which will focus on challenges, effectiveness assessment of ML and AI, costs and scalability analysis, and barriers to its adoption. The study identified key challenges U.S.-based SMBs face in managing supply chain cyber risks, based on three case studies: including the 2013 Target Corporation's data breach, the SolarWinds cyber-attack incident, and the 2021 Colonial Pipeline ransomware attack. These cases pointed to specific problems like; weak cybersecurity protocols, lack of insight and human capital, reliance on high-risk third parties, and problems with risk from complex supply chain relationships. Also, the protection policies of SMBs remain flimsy, and most of them do not have a proper risk management strategy that increases the vulnerability of the business to cyber threats.

The study underscores the fact that SMBs need to enhance their cybersecurity knowledge, lessen their reliance on third parties, and enhance their cybersecurity risk management strategies to mitigate the risks of cyber threats affecting their supply chain. Darktrace employs a self-learning AI system known as the Enterprise Immune System and this analyzes behaviors within an organization with a view of identifying patterns that suggest cybersecurity threats. Some of its features include an autonomous response system known as Antigena which can isolate infected assets while preventing further actions at the same time without the intervention of humans. Darktrace is most effective in the identification of threats right at the initial stages as well as the prevention of such threats especially for intricate supply chain management. IBM Watson for Cyber Security utilizes advanced features including Artificial intelligence, Machine learning, and natural language processing in assessing cyber security big structured and unstructured data. It improves threat identification, creates security incidents, and investigates them, and uses cyber threat intelligence from around the world (with the help of IBM X-Force Exchange). It takes into consideration new threats and offers a wide view of risks; therefore, it is relevant in evaluating the supply chain risks. Such derived techniques are self-learning AI, anomaly detection, autonomous response, proactive threat, visual threat analysis, machine learning, NLP, and threat intelligence global integration. All these approaches assist SMBs in identifying, avoiding, and neutralizing cyber threats within supply chains. Applying principles of Machine Learning (ML) and Artificial Intelligence (AI) to small and medium enterprises (SMBs) presents the following major challenges. The implementation of these technologies presents one significant issue, which is the cost: the costs of licenses for this software, investments in appropriate hardware, and training for employees assigned to work in connection with these technologies. To this end, SMBs could look at options that are cheap or else get the government to provide incentives to help lighten the costs.

Another challenge is the current scarcity of talents specializing in data science, machine learning, or cybersecurity. This skills deficit may hamper the efficient usage of AI and ML. These issues can be mitigated by SMBs by training their employees and outsourcing to providers that offer managed services. Issues include data quality and quantity of data credibility and availability. One of the key factors about all the AI and ML solutions is that they need vast amounts of high-quality data to operate. SMBs must enhance their data management capabilities and think about tie-ups with bigger organizations or industry groups for better data access. Lack of information on the threats from cyber criminals and knowledge on how AI and ML are advantageous in an organization may slow down the adoption of the two technologies. It is recommended to support SMBs through awareness-raising campaigns, workshops, and demonstrations of success stories of the application of these technologies in other companies. One of the challenges of AI and ML adoption is the level of difficulty involved in bringing in new systems and incorporating them with other IT systems. SMBs can derive value from solutions that are easy to understand and utilize, especially backed up by good

vendor support or consulting services. Lastly, the application of AI and ML means processing information that may be sensitive and personal, thus causing questions about privacy protection. SMBs must make sure that their solutions meet the data protection regulations and that security to risks has been incorporated.

5. Conclusion

Specifically, the use of ML and AI in SMBs has some unique difficulties they will face, which are high costs, lack of human resources, quality of data, and the complexity of the task implementation, but these challenges can be criticized by the help of some specific and effective strategies. Solutions in this regard entail affordable ones, better training, efficient data handling, and higher awareness that can solve this problem. Lastly, the ease of use of the technology and strict measures that need to be taken regarding the security of the data are essential factors in the implementation of the model, and thus are some of the barriers that have to be addressed. It is crucial to address these barriers to help SMBs realize the potential of AI and ML in strengthening cybersecurity systems.

5.1. Recommendation

Based on the conclusion, the following recommendations can be made for small and medium-sized businesses (SMBs) seeking to integrate Machine Learning (ML) and Artificial Intelligence (AI) into their cybersecurity frameworks:

- Explore Cost-Effective Solutions: SMBs should seek affordable AI and ML options, such as subscription-based or cloud-based services, and take advantage of government subsidies and incentives to manage initial costs.
- Invest in Workforce Training: To address the shortage of skilled professionals, SMBs should invest in training programs for their existing employees and consider partnerships with educational institutions or third-party providers offering specialized training.
- Enhance Data Management Practices: SMBs should improve their data collection and management to ensure high-quality and sufficient data for AI and ML applications. Collaborating with larger organizations or industry consortia can also provide access to better data resources.
- Increase Awareness and Simplify Implementation: To facilitate adoption, SMBs should engage in educational campaigns, workshops, and case studies to raise awareness about AI and ML benefits. Additionally, they should choose user-friendly technologies and seek support from vendors or consultants to simplify the implementation process.
- Prioritize Security and Privacy: SMBs must ensure that their AI and ML solutions comply with data protection standards and incorporate robust security measures to safeguard sensitive information and address privacy concerns.

Compliance with ethical standards

Disclosure of conflict of interest

There is no known conflict of interest.

References

[1] Broadbent, M. (2021). What's Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence. Center for Strategic and International Studies (CSIS). Available at: Http://Www. Jstor. Org/Stable/Resrep30085 [Accessed 14.05. 2021].

[2] Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access, 10, 85701–85719.

[3] Chio, C., & Freeman, D. (2018). Machine learning and security: Protecting systems with data and algorithms. " O'Reilly Media, Inc."

[4] Dalton, C. (n.d.). Effects of Artificial Intelligence Adoption on Small and Medium Business Cyber Security Risk Management.

[5] Fawcett, S. E., Fawcett, A. M., Watson, B. J., & Magnan, G. M. (2012). Peeking inside the black box: toward an understanding of supply chain collaboration dynamics. Journal of Supply Chain Management, 48(1), 44–72.

[6] Ganesh, A. D., & Kalpana, P. (2022). Future of artificial intelligence and its influence on supply chain risk management–A systematic review. Computers & Industrial Engineering, 169, 108206.

[7] Haletska, S. (2022). Cyberattacks on Ukraine, classification and prediction attempt.

[8] Hasan, K., Shetty, S., & Ullah, S. (2019). Artificial intelligence empowered cyber threat detection and protection for power utilities. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), 354–359.

[9] Hasan, R., Chy, M. A. R., Johora, F. T., Ullah, M. W., & Saju, M. A. B. (2024). Driving Growth: The Integral Role of Small Businesses in the US Economic Landscape. American Journal of Industrial and Business Management, 14(6), 852–868.

[10] Jahankhani, H. (2020). Cyber Security Practitioner's Guide. World Scientific.

[11] Johnson, C. (2022). Rethinking how to grow a small business. Strategic Finance, 103(7), 50–56.

[12] Katiyar, S. (2023). 8 Cyber Security Using Artificial Intelligence. Cyber Security Using Modern Technologies: Artificial Intelligence, Blockchain and Quantum Cryptography, 111.

[13] Mburu, M. (2023). CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES.

[14] Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162–183.

[15] Nolan, C., & Fixler, A. (2021). The economic costs of cyber risk. Foundation for Defense of Democracies.

[16] Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access.

[17] Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103–128.

[18] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on cyber security. International Journal of Scientific Research and Management, 9(12), 669–710.

[19] Piconese, F., Hakkala, A., Virtanen, S., & Crispo, B. (2020). Deployment of Next Generation Intrusion Detection Systems against Internal Threats in a Medium-sized Enterprise.

[20] Qumer, S. M., & Ikrama, S. (2022). Poppy Gustafsson: redefining cybersecurity through AI. The Case for Women, 1–38.

[21] Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. Computers, 10(11), 150.

[22] SMALL, I. M. L. I. N. (n.d.). A CONCEPTUAL STRATEGIC FRAMEWORK FOR IMPLEMENTING MACHINE LEARNING IN SMALL AND MEDIUM-SIZED ENTERPRISES.

[23] Syed, N. F., Shah, S. W., Trujillo-Rasua, R., & Doss, R. (2022). Traceability in supply chains: A Cyber security analysis. Computers & Security, 112, 102536.

[24] Vikash, B. S. (2022). Exploring Challenges Faced by Information Technology Security Managers in Implementing Risk Management Framework to Protect Protected Health Information and Personally Identifiable Information. Northcentral University.

[25] Broadbent, M. (2021). What's Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence. Center for Strategic and International Studies (CSIS). Available at: Http://Www. Jstor. Org/Stable/Resrep30085 [Accessed 14.05. 2021].

[26] Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access, 10, 85701–85719.

[27] Chio, C., & Freeman, D. (2018). Machine learning and security: Protecting systems with data and algorithms. " O'Reilly Media, Inc."

[28] Dalton, C. (n.d.). Effects of Artificial Intelligence Adoption on Small and Medium Business Cyber Security Risk Management.

[29] Fawcett, S. E., Fawcett, A. M., Watson, B. J., & Magnan, G. M. (2012). Peeking inside the black box: toward an understanding of supply chain collaboration dynamics. Journal of Supply Chain Management, 48(1), 44–72.

[30] Ganesh, A. D., & Kalpana, P. (2022). Future of artificial intelligence and its influence on supply chain risk management–A systematic review. Computers & Industrial Engineering, 169, 108206.

[31] Haletska, S. (2022). Cyberattacks on Ukraine, classification and prediction attempt.

[32] Hasan, K., Shetty, S., & Ullah, S. (2019). Artificial intelligence empowered cyber threat detection and protection for power utilities. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), 354–359.

[33] Hasan, R., Chy, M. A. R., Johora, F. T., Ullah, M. W., & Saju, M. A. B. (2024). Driving Growth: The Integral Role of Small Businesses in the US Economic Landscape. American Journal of Industrial and Business Management, 14(6), 852–868.

[34] Jahankhani, H. (2020). Cyber Security Practitioner's Guide. World Scientific.

[35] Johnson, C. (2022). Rethinking how to grow a small business. Strategic Finance, 103(7), 50–56.

[36] Katiyar, S. (2023). 8 Cyber Security Using Artificial Intelligence. Cyber Security Using Modern Technologies: Artificial Intelligence, Blockchain and Quantum Cryptography, 111.

[37] Mburu, M. (2023). CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES.

[38] Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162–183.

[39] Nolan, C., & Fixler, A. (2021). The economic costs of cyber risk. Foundation for Defense of Democracies.

[40] Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access.

[41] Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103–128.

[42] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on cyber security. International Journal of Scientific Research and Management, 9(12), 669–710.

[43] Piconese, F., Hakkala, A., Virtanen, S., & Crispo, B. (2020). Deployment of Next Generation Intrusion Detection Systems against Internal Threats in a Medium-sized Enterprise.

[44] Qumer, S. M., & Ikrama, S. (2022). Poppy Gustafsson: redefining cybersecurity through AI. The Case for Women, 1–38.

[45] Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. Computers, 10(11), 150.

[46] SMALL, I. M. L. I. N. (n.d.). A CONCEPTUAL STRATEGIC FRAMEWORK FOR IMPLEMENTING MACHINE LEARNING IN SMALL AND MEDIUM-SIZED ENTERPRISES.

[47] Syed, N. F., Shah, S. W., Trujillo-Rasua, R., & Doss, R. (2022). Traceability in supply chains: A Cyber security analysis. Computers & Security, 112, 102536.

[48] Vikash, B. S. (2022). Exploring Challenges Faced by Information Technology Security Managers in Implementing Risk Management Framework to Protect Protected Health Information and Personally Identifiable Information. Northcentral University.