AI-DRIVEN STRATEGIES OF MITIGATING CYBERSECURITY THREATS IN U.S. SMALL AND MEDIUM ENTERPRISES (SMES)

Kemisola Kasali [1], Precious Orekha [2], Oluwaseun John Bamigboye [3], Afolabi Sabur Ajao [4], Peter O. Alawiye [5], Adeola Noheemot Raji [6]

[1] Department of Management, Marketing, and Technology, University of Arkansas at Little Rock, USA
[2] Department of Information Science, College of Computing and Informatics, Drexel University, Philadelphia, Pennsylvania, USA
[3] Department of Computer Science, California Miramar University, San Diego, California, USA
[4] Management Science, Kellogg School of Management, Northwestern University, Chicago, IL, USA
[5] Department of Business Administration, New Mexico Highlands University, Las Vegas, New Mexico, USA
[6] Pompea College of Business, University of New Haven, West Haven, Connecticut, USA

ABSTRACT

Small and Medium Enterprises (SMEs) in the United States face escalating cybersecurity threats including phishing, ransomware, and data breaches, yet lack resources for robust defense mechanisms. This qualitative exploratory research employs thematic content analysis of secondary data from peer-reviewed academic literature, industry reports from NIST and OECD, and documented case studies to examine AI-driven cybersecurity strategies for SMEs. The study identifies cost and lack of expertise as primary AI adoption barriers, with retail and financial services demonstrating higher adoption levels compared to manufacturing and education. A structured three-component framework focusing on threat detection, response automation, and compliance monitoring is developed for resource-constrained SME environments. Findings reveal critical gaps in SME-specific AI frameworks, with healthcare, retail, and financial services sectors showing vulnerability to cyberattacks and potential cyber resilience improvement. The research concludes that scalable AI methodologies tailored for smaller businesses and public-private collaboration are essential to strengthen cyber defenses across this vulnerable sector, addressing implementation costs and skilled personnel requirements.

KEYWORDS

Cybersecurity, SMEs, Artificial Intelligence, Threat Detection, Predictive Analytics

1. INTRODUCTION

Small and medium-sized businesses (SMBs) in the United States face unprecedented cybersecurity challenges. SMEs are dynamic business entities with fewer than 500 employees, limited resources, and a focus on driving substantial economic growth and innovation through agility, personalized customer service, a local market focus, and a flexible structure[1]. These businesses, which form the backbone of the U.S. economy has become prime targets for

cybercriminals due to their typically limited security resources and capabilities[2]. The increasing sophistication and frequency of cyber threats, which range from malware and ransomware to phishing attacks, pose significant financial, operational, and reputational risks to SMEs that often lack robust defense mechanisms[3]. Cyber incidents rank as the top business risk for companies globally, with SMEs particularly vulnerable[4]. This vulnerability is highlighted by the devastating consequences of successful attacks: significant financial losses, business disruption, compromised customer data, and diminished stakeholder trust[3]. Traditional security approaches are increasingly insufficient against evolving threats, creating an urgent need for innovative, cost-effective security solutions[5].

Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity, which offers SMEs powerful tools to enhance their security posture despite resource constraints[3]. AI- enabled solutions enable proactive threat detection, automated incident response, and continuous security monitoring by leveraging machine learning algorithms, behavior-based analysis, and predictive analytics[6,7]. These capabilities allow smaller businesses to identify anomalies, predict potential attacks, and respond to threats in real-time, that significantly improve their cyber resilience[3,6]. The integration of AI in cybersecurity enables SMEs to address their unique challenges through several mechanisms. First, AI-driven predictive analytics can anticipate potential threats based on historical data patterns to facilitate proactive security measures[3,8]. Second, automated threat detection using behavioral analytics establishes baselines of normal network activities which flag deviations that may indicate security breaches[3,9]. Third, AI streamlines incident response through automated prioritization and remediation recommendations that minimizes breach impact and recovery time[9].

To understand the specific cybersecurity challenges SMEs face, it is essential to examine the threat landscape in which they operate. SMEs, with limited resources and staff, are particularly vulnerable to cyberattacks, making it crucial to identify the sectors most at risk and the prevalent types of threats they encounter. Figures 1, 2, and 3 offer a detailed analysis of these aspects, shedding light on the sectors most frequently targeted and the types of cyber threats SMEs are most likely to experience.

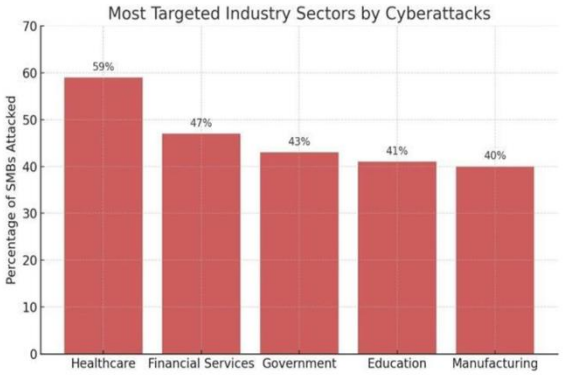
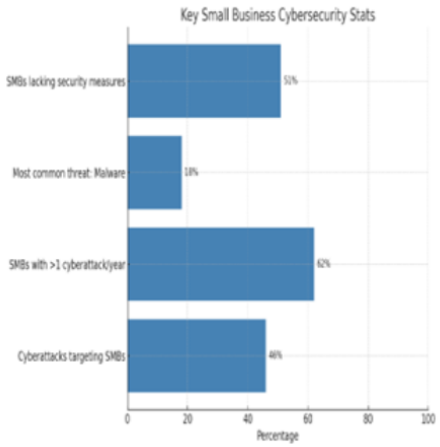


Fig 1 Most targeted sectors by cyberattacks

Figure 1 reveals the sectors most vulnerable to cyberattacks, which provides crucial context for understanding SMEs' exposure to cybersecurity risks. Industries with high exposure, such as healthcare, retail, and financial services, are shown to be prime targets for cybercriminals due to the sensitivity of the data they handle. This data underscores the need for targeted security approaches tailored to specific sectors' vulnerabilities and requirements. Similarly, **Figures 2 and 3** offer a detailed analysis of these aspects, which shed light on the sectors most frequently targeted, and the types of cyber threats SMEs are most likely to experience.

1.1. Problem Statement

Small and medium-sized enterprises face several cybersecurity challenges that leave them vulnerable to cyber threats. While AI-driven cybersecurity solutions have shown promise, SMEs often encounter significant obstacles in adopting these technologies. Key barriers include high costs, lack of in-house expertise, and privacy concerns, all of which hinder effective implementation. Understanding these barriers is crucial for ensuring that SMEs can successfully integrate AI tools to mitigate cybersecurity risks and enhance their defense mechanisms:



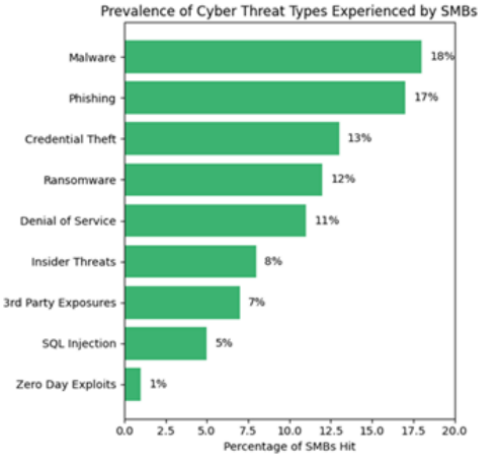


Fig 2 Most Targeted Industry Sectors by SMBs Fig 3 Breakdown of Cyber Threat Types Experienced by SMBs

The data presented in **Figure 2 and 3** points out the urgent need for targeted cybersecurity interventions for SMEs. The sectors identified as most vulnerable to cyberattacks show a clear pattern, which suggests specific areas where enhanced protection measures are needed. Furthermore, the prevalence of various cyber threats highlighted in the figures emphasizes the importance of adopting specialized AI-enabled solutions. These tools must be tailored to address the most common and severe types of threats, thereby helping SMEs to improve their resilience against cyber incidents. To better understand these challenges, **Figure 4** below illustrates the primary barriers SMEs face when adopting AI- powered defense mechanisms.

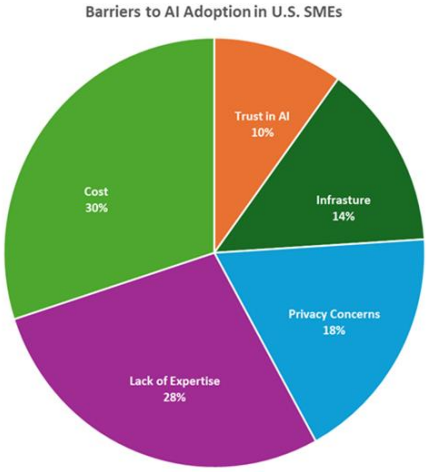


Fig 4 showing barriers to AI adoption in U.S. SMEs

Figure 4 reveals cost and lack of expertise as the primary obstacles SMEs face in adopting AI for cybersecurity which highlights the operational limitations SMEs must navigate when implementing AI-based security tools. Privacy concerns, while also significant, are less impactful than cost and expertise. Studies also show that SMEs are faced with regulatory compliance issues, which are exacerbated by industry-specific hurdles such as legacy systems, and handling large volumes of sensitive data[5,11]. The data underlines the need for cost-effective solutions that can be implemented without extensive in-house knowledge. Addressing these barriers will be essential for increasing AI adoption and enhancing cybersecurity in SMEs.

1.2. Research Objectives

1. Explore the different use cases of AI in cybersecurity across various industries.
2. Assess the current level of AI adoption in cybersecurity within Small and medium-sized enterprises.
3. Identify the unique challenges faced by small businesses in adopting AI solutions in cybersecurity.
4. Develop a structured framework for the adoption of AI-driven security tools in SMEs.
5. Provide recommendations for overcoming these challenges to enhance AI adoption in SMEs.

2. LITERATURE REVIEW

SMEs in the U.S. are increasingly vulnerable to cyber threats, including ransomware, phishing, and data breaches, due to limited cybersecurity resources and expertise[8,12]. The growing frequency and sophistication of these attacks have necessitated the adoption of advanced security measures, with artificial intelligence (AI) emerging as a critical tool for threat detection, prevention, and response[8]. AI-powered cybersecurity solutions offer SMEs the ability to automate threat analysis, enhance anomaly detection, and improve incident response times, addressing key challenges such as budget constraints and a shortage of skilled personnel[13]. However, while AI presents significant opportunities, debates persist regarding its effectiveness, ethical implications, and practical implementation for SMEs [14,15].

The application of AI in cybersecurity is grounded in several foundational theories, which include machine learning (ML) and deep learning (DL) models that enable real-time threat detection and behavioral analysis[16]. Machine learning algorithms, particularly supervised and unsupervised learning techniques, allow SMEs to identify unusual network activity and potential intrusions without relying solely on manual monitoring[17]. Deep learning further enhances these capabilities by using neural networks to detect complex attack patterns, including zero-day exploits that traditional security systems might miss[18]. Beyond technical models, behavioral theories such as the Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) provide insights into how employees' security practices influence organizational cybersecurity[19]. AI can reinforce positive security behaviors by automating training programs and alert systems, reducing human error, a leading cause of breaches[20]. Furthermore, AI plays a crucial role in risk management by automating vulnerability assessments and optimizing resource allocation, ensuring that SMEs prioritize the most critical security gaps[21–23]. Cryptographic security also benefits from AI, as advanced algorithms can detect weaknesses in encryption methods and improve data protection[24,25].

Despite these advantages, debates surrounding AI's role in SME cybersecurity highlight several challenges. One major concern is the potential over-reliance on AI, which may lead to

complacency and a false sense of security[14,26]. AI systems are not infallible; they can produce false positives and negatives, requiring human oversight to validate alerts and make critical decisions[27]. Another significant debate revolves around the cost and complexity of AI implementation. While AI can reduce long-term security expenses, the initial investment in technology, infrastructure, and training may be prohibitive for SMEs with tight budgets[28]. Furthermore, integrating AI with existing IT systems demands technical expertise, which many small businesses lack[21,29]. Ethical considerations also come into play, particularly regarding data privacy, algorithmic bias, and regulatory compliance[14,30]. SMEs must navigate these challenges carefully, ensuring that AI deployments align with legal standards such as GDPR and CCPA while maintaining transparency in automated decision-making[21,31].

The existing literature on AI-driven cybersecurity for SMEs reveals several gaps that warrant further research. First, most AI cybersecurity frameworks are designed for large enterprises, which leave small businesses without tailored solutions that account for their unique constraints, such as limited IT staff and financial resources[21,32]. Empirical studies on AI's real-world effectiveness in SME environments are also scarce, with much of the available research focusing on theoretical models rather than practical applications[14]. Furthermore, while ethical concerns are frequently acknowledged, there is a lack of clear guidelines for SMEs on implementing AI responsibly, particularly regarding data handling and bias mitigation[33]. Finally, employee training remains an underexplored area, despite its importance in ensuring that staff can effectively use AI-powered security tools[33]. Future research should prioritize the development of SME-specific AI frameworks, conduct more case studies on successful implementations, and establish best practices for ethical AI adoption in small business settings[21,34]. AI offers transformative potential for enhancing SME cybersecurity, but its adoption must be approached with careful consideration of cost, usability, and ethical implications. While AI can automate threat detection and improve risk management, human oversight remains essential to ensure accuracy and accountability[14,35]. Small and medium-sized enterprises must balance technological innovation with practical constraints, seeking scalable and affordable AI solutions that align with their security needs[21,34]. Addressing the current gaps in research, particularly in SME-specific frameworks, empirical validation, and ethical guidelines, will be crucial in maximizing AI's benefits while minimizing risks. As cyber threats continue to evolve, AI-powered strategies will play an increasingly vital role in safeguarding SMEs, provided they are implemented thoughtfully and sustainably[15].

2.1. AI Use Cases in SMEs

AI applications in cybersecurity present significant potential for small businesses. As SMEs face a wide range of cybersecurity challenges, different industries are increasingly adopting AI tools to address sector-specific obstacles. These challenges include regulatory compliance, budget constraints, and data sensitivity. A closer look at how AI tools are utilized across various industries helps to understand their role in strengthening cybersecurity frameworks within SMEs. Table 1 provides an overview of AI adoption levels and the unique challenges faced by SMEs in different sectors.

Table 1: AI Cybersecurity Use Cases in SMEs – Industry Comparison

Industry	**AI Use Cases in Cybersecurity**	**Adoption Level**	**Unique Challenges**
Healthcare	Patient data protection, anomaly detection	Moderate	Strict regulatory compliance (e.g., HIPAA)
Retail	Transaction monitoring, phishing detection	High	Handling large PII volumes
Manufacturing	IoT security, predictive failure alerts	Low to Moderate	Limited IT staff, legacy systems
Financial Services	Fraud detection, behavior profiling	High	Data sensitivity, auditability
Education/EdTech	Access control, anti-cheating tools	Low	Budget constraints, student data privacy

Sources: Buczak & Guven (2016); Ahmad et al. (2022); Tawalbeh et al. (2023)

Table 1 reveals industries such as retail and financial services with high adoption levels of AI tools due to the need for ongoing monitoring of sensitive data. In contrast, sectors like manufacturing and education encounter barriers like legacy systems, limited resources and IT staff, and regulatory complexities that hinder AI adoption. These challenges highlight the importance of understanding sector-specific needs when implementing AI strategies in SMEs.

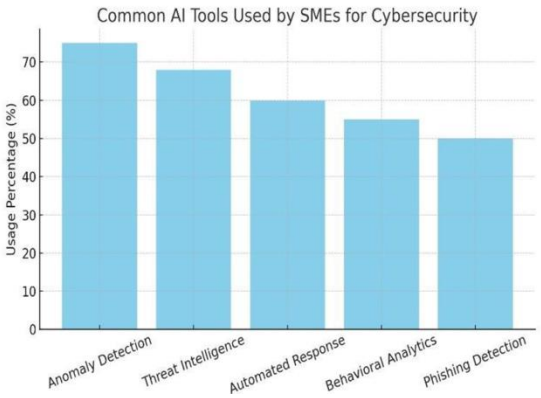


Fig 5 showing common AI tools used by SMEs for cybersecurity

Figure 5 illustrates the most common AI tools used by SMEs to mitigate cybersecurity threats.

Anomaly detection, threat intelligence, and automated response tools are widely adopted due to their ability to enhance real-time threat monitoring and provide quick responses during incidents. AI applications like these are particularly critical for sectors that handle large amounts of sensitive data and need to maintain high security levels. Automated response tools are particularly beneficial in managing security incidents without extensive human intervention, thus addressing staffing challenges many SMEs face. Industries with complex security needs, such as healthcare and financial services, benefit significantly from these AI tools in managing emerging cybersecurity threats.

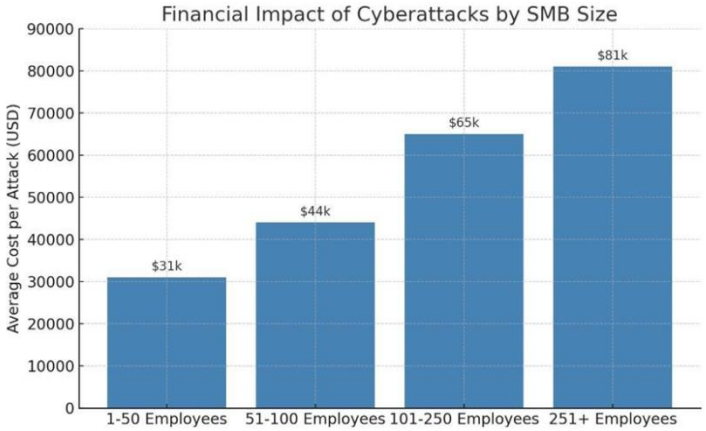


Fig 6 showing financial impact of cyber-attacks by SMB size

The financial impact of cyberattacks on SMBs varies by company size, with larger organizations incurring significantly higher costs per attack. In **Figure 6**, the average cost of a cyberattack increases with the size of the organization, with companies employing over 250 employees facing the highest financial burdens. Smaller SMBs, such as those with 1-50 employees, experience lower costs, but these expenses still represent a significant financial strain. This data underlines the need for targeted cybersecurity measures based on company size to mitigate financial losses. Larger SMBs with more employees face heightened exposure to cyber threats, further emphasizing the necessity of robust, scalable cybersecurity frameworks.

3. METHODOLOGY

This study adopts a qualitative, exploratory research design to investigate how U.S. SMEs are utilizing AI-powered tools to mitigate cybersecurity threats. The complexity of AI technologies, along with the contextual differences between SMEs and larger enterprises, makes a qualitative approach ideal for this study which allows for a deeper understanding of the strategies, outcomes, and challenges faced by SMEs in adopting AI-based cybersecurity solutions. The research is not focused on making statistical generalizations, but instead aims to analyze trends, patterns, and best practices drawn from existing data and literature. The primary goal is to identify how AI is being applied in cybersecurity, the effectiveness of these applications, and the barriers SMEs face in adoption.

Data for this research was exclusively sourced from secondary research due to the challenges of accessing primary data from small business cybersecurity infrastructures. The sources included peer-reviewed academic literature, industry reports, documented case studies, and government publications. This broad range of sources ensures that the research covers a comprehensive spectrum of the AI cybersecurity landscape for SMEs. Specific sources include peer-reviewed journals and technical articles such as IEEE Security & Privacy, and Journal of Cybersecurity Research and Computers & Security reports from organizations such as Proofpoint, VC3, NIST and OECD; documented case studies of AI implementations by SMEs or their vendors as well as government publications, guidelines and frameworks issued by Small Business Administration (SBA) and U.S. Chamber of Commerce. This combination of sources ensures a robust and well-rounded understanding of the current AI cybersecurity landscape for SMEs.

The research analysis involved using a thematic content analysis approach to identify recurring themes, patterns, and insights across literature and case studies. Key themes such as AI

applications (e.g., anomaly detection, predictive analytics, automated incident response) were coded and categorized. A comparative analysis was conducted to highlight how AI strategies in SMEs differ from those in large corporations and assess the scalability of these strategies for smaller operations. Furthermore, triangulation was used to validate recurring findings, particularly challenges related to cost and data privacy. The study also applied relevant frameworks, that include the AI Risk Management Framework by NIST and the Ethical AI Guidelines by ENISA, to evaluate the governance and effectiveness of AI adoption in smaller businesses. SMEs face unique challenges when adopting AI-enabled cybersecurity solutions, which makes it essential to offer a structured method for incorporating AI technologies effectively. This approach aims to help SMEs overcome key barriers such as cost, lack of expertise, and privacy concerns. It focuses on three critical components: threat detection, response automation, and risk mitigation and compliance monitoring.

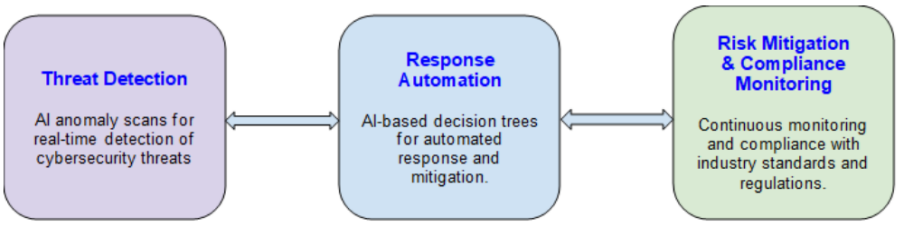


Fig 7 showing AI adoption framework for SME cybersecurity

The proposed framework addresses the primary challenges SMEs face in adopting AI-driven mitigation strategies. AI anomaly scans enable real-time detection of cybersecurity threats. SMEs can proactively identify and address vulnerabilities before they escalate. AI-based decision trees automate response and mitigation efforts, which streamlines the process and reduces the need for extensive IT expertise. This automation enhances efficiency for SMEs with limited technical resources. Continuous monitoring and adherence to industry standards ensure that SMEs remain compliant while effectively managing cyber risks. This component also addresses privacy concerns, which fosters trust in AI tools and ensures that data protection remains a priority. The approach is cost-efficient, making AI adoption feasible for SMEs with limited budgets. It eliminates the need for specialized knowledge and allows businesses to benefit from AI-enabled cybersecurity solutions. Integrating monitoring and compliance features addresses privacy concerns, which promotes broader adoption and confidence in AI technologies.

3.1. Ethical Considerations

The research is based solely on secondary data to ensure no human subjects were involved. Ethical concerns such as algorithmic bias, privacy implications, and transparency in decision-making are considered and all sources used are publicly available or properly cited. The study adheres to established ethical guidelines, particularly regarding data privacy, responsible use of AI in cybersecurity, and ensuring the confidentiality of proprietary information. Potential biases in the secondary data sources are acknowledged, and the importance of AI governance and accountability in automated cybersecurity decision-making is emphasized.

3.2. Case Studies

The implementation of AI-driven strategies to bolster cybersecurity is not merely theoretical. Several real-life case studies highlight the effective application of these technologies in SMEs. This section explores two notable examples that demonstrate the practical benefits of AI in mitigating cybersecurity threats within the SME sector. Cylance, acquired by BlackBerry, shows

a successful AI-enabled approach to cybersecurity tailored for SMEs. Cylance's AI-based platform uses machine learning algorithms to predict and prevent cyber threats before they execute. This proactive approach offers a cost-effective solution for organizations that lack extensive IT resources. Cylance analyzes the characteristics of files and applications, assessing whether they pose a potential threat. This pre-execution analysis prevents malicious files from running, significantly reducing the risk of zero-day attacks, which are particularly challenging for SMEs due to their limited resources. For example, a medium-sized manufacturing company implemented Cylance to secure its industrial control systems. Prior to the adoption of Cylance, the company frequently faced severe disruptions and financial losses due to cybersecurity incidents. However, after adopting Cylance, the company successfully thwarted a targeted malware attack that could have crippled production lines. The AI-powered solution not only strengthened the company's defense mechanisms but also allowed it to reallocate some of its limited resources more effectively, which shows the practicality and efficiency of AI in a real-world SME setting.

IBM Watson for Cyber Security exemplifies AI's role in enhancing human intelligence to detect and respond to emerging cyber threats. IBM Watson processes vast volumes of unstructured data, which draws insights from various sources such as blogs, research papers, and news articles. This capability is particularly beneficial for small businesses, which often struggle with managing large datasets due to limited personnel and budgetary constraints. A global financial services firm, for instance, utilized IBM Watson to combat a complex phishing campaign targeting its employees. By integrating Watson into its existing security architecture, the firm was able to improve its threat detection accuracy. Watson's ability to correlate external intelligence with internal data allowed the organization to identify vulnerabilities and implement actionable interventions before sensitive customer data was compromised. The successful integration of Watson into the firm's cybersecurity framework illustrates how AI can significantly augment existing systems, which makes SMEs more resilient to sophisticated cyber threats and reinforces the importance of adopting AI in the SME sector.

3.3. Limitations of the Study

This study primarily relies on secondary data from existing literature, industry reports, and case studies, which limits its ability to capture real-time implementation feedback and firsthand experiences from U.S. SMEs. As the research focuses on published information, it may not fully reflect the dynamic, evolving nature of AI- powered cybersecurity practices in SMEs. The lack of primary data, such as interviews or surveys with SME stakeholders, means that some of the practical challenges and insights faced by organizations in adopting AI solutions may not be adequately represented. In addition, the study's reliance on case studies may not account for the diverse contexts and operational differences across SMEs, particularly those in various stages of AI adoption. The findings are also constrained by the availability and scope of secondary sources, which may not encompass the latest technological advancements or the most up-to-date regulatory changes affecting small business. Therefore, future research incorporating primary data collection could provide a more inclusive understanding of the real-world barriers, opportunities, and outcomes of AI integration in SME cybersecurity.

4. FINDINGS AND DISCUSSION

The research reveals significant cybersecurity vulnerabilities across U.S. SMEs, with Figure 4 demonstrating that cost and lack of expertise represent the most substantial barriers to AI adoption in cybersecurity frameworks. High-risk sectors such as healthcare, retail, and financial services exhibit moderate to high AI adoption levels according to Table 1, while manufacturing

and education sectors demonstrate lower adoption rates due to legacy system constraints and limited IT resources. Figure 6 illustrates that the financial impact of cyberattacks increases proportionally with company size, with larger SMBs experiencing significantly higher costs per incident. These vulnerability patterns directly correlate with the implementation challenges observed in AI adoption, where financial constraints and technical expertise gaps prevent effective cybersecurity enhancement.

Building on these vulnerability findings, the literature review identifies substantial gaps in current AI cybersecurity frameworks, which reveals that most existing solutions target large enterprises rather than addressing the unique constraints faced by SMEs. This enterprise-focused approach creates operational challenges where smaller businesses cannot effectively implement sophisticated AI models designed for larger organizational environments. The practical implications of these gaps manifest in the tools SMEs actually adopt: Figure 5 shows that anomaly detection, threat intelligence, and automated response tools represent the most commonly adopted AI applications among SMEs. Despite higher adoption rates shown in Table 1, retail and financial services still encounter regulatory compliance challenges, which demonstrates that even leading implementation sectors face significant obstacles. The case studies of Cylance and IBM Watson provide evidence of practical AI applications but reinforce these implementations barriers through documented challenges related to system integration and technical expertise requirements.

These implementation challenges reflect broader research limitations that perpetuate the SME vulnerability gap. The study establishes that current academic and industry research predominantly focuses on enterprise-level implementations, which leaves SMEs without tailored frameworks that address their specific operational and financial constraints. The theoretical foundations in machine learning and behavioral security models provide technical capabilities, yet practical implementation guidance remains limited and largely theoretical rather than actionable for smaller businesses. Privacy concerns, particularly regarding data handling and algorithmic transparency, compound these barriers by creating additional adoption obstacles that existing literature inadequately addresses for small business environments. These findings support the need for developing targeted AI frameworks that bridge the gap between technological capability and practical implementation feasibility for resource-constrained SMEs, directly informing the scalable, cost-effective solutions proposed in the recommendations section.

4.1. Recommendations and Future Directions

This study highlights the potential of AI to significantly enhance the cybersecurity posture of Small and medium-sized businesses, while also identifying critical barriers to its adoption. Based on the findings, several key recommendations emerge to facilitate the integration of AI-driven cybersecurity solutions in SMEs. The development of cost-effective, scalable AI solutions tailored to the unique needs of SMEs is essential. Many small businesses face financial constraints that prevent them from adopting cutting-edge cybersecurity tools. Future research should focus on the creation of modular AI systems that are both affordable and scalable, which enables SMEs to implement solutions based on their specific requirements and available resources. To address the shortage of in-house expertise, it is vital to design AI tools that require minimal technical knowledge for effective operation and maintenance. Research should explore the design of user-friendly AI platforms with intuitive interfaces, as well as the inclusion of comprehensive training and support resources for Small and medium-sized businesses. This would empower smaller businesses to manage AI tools with ease and reduce their reliance on external expertise.

Data privacy concerns remain a significant barrier for SMEs when adopting AI-enabled cybersecurity tools. The integration of AI with strict regulatory standards is critical. Future research should focus on AI solutions that are compliant with regulations like GDPR and CCPA, which ensure SMEs can adopt these tools without compromising data security. In addition, research into AI transparency, auditability, and ethical practices would foster trust and acceptance among SME owners and stakeholders. The combination of AI solutions with existing infrastructure is another challenge. Many SMEs operate on legacy systems, which makes it difficult to adopt new technologies without significant overhauls. Research should explore how AI-driven tools can be seamlessly integrated with these existing systems, minimizing the need for costly upgrades and reducing operational disruptions. This approach would allow small businesses to benefit from AI-powered solutions without the burden of a complete system overhaul.

Scalability must be a central focus when developing AI solutions for SMEs. As these businesses grow and evolve, their cybersecurity needs change as well. Future research should focus on ensuring that AI solutions can scale with the growth of SMEs, offering flexibility and adaptability to accommodate changing security needs as the business expands. Moreover, increased collaboration between government bodies, industry stakeholders, and academic institutions is crucial to supporting SMEs in adopting AI technologies. Research should investigate the potential for public-private partnerships and government incentives that could alleviate the financial and technical challenges small and medium-sized businesses face when implementing AI-enabled cybersecurity tools. Lastly, empirical studies involving primary data from small businesses would provide valuable insights into the real-world challenges and successes of AI adoption. Research should focus on case studies of SMEs that have successfully implemented AI solutions, which could serve as models for other businesses. These case studies would provide practical guidance and highlight the specific barriers that small and medium-sized businesses encounter in different industries. Future research efforts should aim to bridge the gap between AI technology and its practical application in SMEs, addressing the challenges identified in this study and promoting more effective and widespread adoption of AI for cybersecurity.

5. CONCLUSION

AI-driven cybersecurity strategies are crucial for Small and Medium Enterprises to address increasing cyber threats. The use of machine learning, predictive analytics, and automated threat detection offers significant advantages, such as cost reduction and improved security monitoring. However, SMEs face barriers such as high costs, lack of technical expertise, and privacy concerns that hinder effective AI adoption. Despite these challenges, AI tools can help SMEs enhance their cybersecurity posture and safeguard critical data. Tailored, cost-effective AI solutions are needed to overcome these barriers and enable SMEs to protect themselves against evolving cyber threats. The paper highlights the importance of addressing sector-specific vulnerabilities and the need for scalable AI technologies. Further research is required to assess the real-world impact of AI on SME cybersecurity and explore ethical considerations. Public-private partnerships could play a key role in facilitating AI adoption among small and medium-sized businesses. The findings stress the importance of practical, accessible, and adaptable AI solutions to strengthen SME cybersecurity. Overall, AI presents a powerful tool for small businesses to improve their resilience and ensure business continuity.

REFERENCES

[1] R. May, “2: Machine learning algorithms in cybersecurity,” LinkedIn. [Online]. Available: https://www.linkedin.com/pulse/2-machine-learning-algorithms-cybersecurity-rob-may-nbqje/. [Accessed: Apr. 3, 2025]

[2] Parthasarathy, "Leveraging AI for faster and smarter cyber incident management & response," LinkedIn. [Online]. Available: https://www.linkedin.com/pulse/leveraging-ai-faster-smarter-cyber-incident-response-parthasarathy-mat0c/. [Accessed: Apr. 4, 2025]

[3] Admin, "Cyber threats top global business risk concern for 2024: Allianz," Insurance Journal, Feb. 5, 2024. [Online]. Available: https://www.insurancejournal.com/magazines/mag-features/2024/02/05/759018.htm

[4] "Advanced tools and AI to combat human error in cybersecurity," Sangfor. [Online]. Available: https://www.sangfor.com/blog/cybersecurity/mitigating-human-errors-in-cybersecurity. [Accessed: May 6, 2025]

[5] "AI powered cyber security for small business," iFeeltech, Oct. 2, 2024. [Online]. Available: https://ifeeltech.com/ai-security-small-business/

[6] National Institute of Standards and Technology, "AI risk management framework," NIST, 2021. [Online]. Available: https://www.nist.gov/itl/ai-risk-management-framework

[7] "Aligning AI ethics with privacy compliance: Why it matters for your business," TrustArc. [Online]. Available: https://trustarc.com/resource/ai-ethics-with-privacy-compliance/. [Accessed: May 6, 2025]

[8] S. G. Ayinaddis, "Artificial intelligence adoption dynamics and knowledge in SMEs and large firms: A systematic review and bibliometric analysis," Journal of Innovation & Knowledge, vol. 10, no. 3, p. 100682, 2025. [Online]. Available: https://doi.org/10.1016/j.jik.2025.100682

[9] "Case studies—AI in cyber defense success stories," Umetech, Sep. 3, 2024. [Online]. Available: https://www.umetech.net/blog-posts/successful-implementations-of-ai-in-cyber-defense

[10] C. Choudhury, "Role of AI in cybersecurity: Benefits of AI on security," Qualysec, Jan. 20, 2025. [Online]. Available: https://qualysec.com/ai-in-cybersecurity/

[11] P. A. Clark, "Small businesses face rising cyber threats, pleas to report attacks," Axios, Apr. 4, 2023. [Online]. Available: https://www.axios.com/2023/04/04/small-businesses-cybersecurity-attacks-cisa

[12] "How artificial intelligence helps SMEs overcome their challenges," Activdev. [Online]. Available: https://www.activdev.com/en/trashed-22/. [Accessed: May 6, 2025]

[13] "Cost-benefit analysis of AI implementation in SMEs (AI ROI)," ProfileTree, May 6, 2024. [Online]. Available: https://profiletree.com/cost-benefit-analysis-of-ai-implementation-in-smes/

[14] A. Sukumar, H. Amoozad Mahdiraji, and V. J. Sadeghi, "Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors," Risk Analysis, vol. 43, no. 10, pp. 2082–2098, 2023. [Online]. Available: https://doi.org/10.1111/risa.14092

[15] "Cybersecurity's AI tidal wave—eBook," Proofpoint, Mar. 22, 2024. [Online]. Available: https://www.proofpoint.com/us/resources/e-books/cybersecuritys-ai-tidal-wave

[16] J. Fattahi, "Machine learning and deep learning techniques used in cybersecurity and digital forensics: A review," arXiv, no. arXiv:2501.03250, 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2501.03250

[17] H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," Electronics, vol. 9, no. 10, p. 1684, 2020. [Online]. Available: https://doi.org/10.3390/electronics9101684

[18] A. Huang, "Cybersecurity for SMEs in the era of AI," SME Horizon, Mar. 27, 2025. [Online]. Available: https://www.smehorizon.com/cybersecurity-for-smes-in-the-era-of-ai/

[19] HUMAN, "AI in cybersecurity: Pros and cons," HUMAN Security, Jun. 13, 2024. [Online]. Available: https://www.humansecurity.com/learn/blog/ai-in-cybersecurity-pros-and-cons/

[20] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Computers & Security, vol. 31, no. 1, pp. 83–95, 2012. [Online]. Available: https://doi.org/10.1016/j.cose.2011.10.007

[21] "Incorporating AI into your cybersecurity strategy for small- to mid-sized businesses," Technology Advancement Center, Jan. 22, 2025. [Online]. Available: https://thetac.tech/incorporating-ai-into-your-cybersecurity-strategy-for-small-to-mid-sized-businesses/

[22] "Investigation of artificial intelligence in SMEs: A systematic review of the state of the art and the main implementation challenges," Management Review Quarterly. [Online]. Available: https://link.springer.com/article/10.1007/s11301-024-00405-4. [Accessed: May 6, 2025]

[23] Y. Jama, Adopting machine learning-based IDS systems in SMEs: Challenges and solutions, M.Eng. thesis, Metropolia University of Applied Sciences, Information Technology, Dec. 1, 2024

[24] N. Kshetri, M. M. Rahman, M. M. Rana, O. F. Osama, and J. Hutson, "algoTRIC: Symmetric and asymmetric encryption algorithms for cryptography — A comparative analysis in AI era," arXiv, no. arXiv:2412.15237, 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2412.15237

[25] "Leveraging AI for enhanced cybersecurity in SMEs," Treatydigital.com, Nov. 11, 2024. [Online]. Available: https://treatydigital.com/leveraging-ai-for-enhanced-cybersecurity-in-smes/

[26] J. F. MBA, "How to automate vulnerability management," PurpleSec, Mar. 4, 2024. [Online]. Available: https://purplesec.us/learn/vulnerability-management-automation/

[27] N. K. Reddy, K. Venkateswari, N. Veeralahari, M. Pavithra, and G. Thippanna, "The role of AI in improving encryption in data privacy: A hypothetical approach," International Journal of Engineering Technology and Management Sciences, vol. 9, no. 2, pp. 68–75, 2025. [Online]. Available: https://doi.org/10.46647/ijetms.2025.v09i02.012

[28] "Outshift | Exploring the potential of AI agents in combatting cyber threats," Outshift by Cisco. [Online]. Available: https://outshift.com/blog/exploring-the-potential-of-ai-agents-in-combatting-cyber-threats. [Accessed: May 6, 2025]

[29] N. Leo and O. Archie, "AI and cybersecurity for SMEs: Balancing ethical considerations and operational efficiency," ResearchGate, 2024. [Online]. Available: https://doi.org/10.13140/RG.2.2.33120.49923

[30] M. Soudi and M. Bauters, "AI guidelines and ethical readiness inside SMEs: A review and recommendations," DISO, vol. 3, no. 3, 2024. [Online]. Available: https://doi.org/10.1007/s44206-024-00087-1

[31] I. Fidel-Anyana, E. G. Onus, U. Mikel-Olisa, and N. Ayanbode, "AI-driven cybersecurity frameworks for SME development: Mitigating risks in a digital economy," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 6, no. 1, pp. 982–988, 2025. [Online]. Available: https://www.researchgate.net/publication/388382166_AI-Driven_Cybersecurity_Frameworks_for_SME_Development_Mitigating_Risks_in_a_Digital_Economy

[32] P. Radadiya, "Automating AI in cybersecurity: A comprehensive literature review," Journal of Information Systems Engineering & Management, vol. 10, no. 28s, pp. 533–541, 2025. [Online]. Available: https://doi.org/10.52783/jisem.v10i28s.4354

[33] K. Kasali, "Developing scalable HR analytics platforms for SMEs with data-driven strategies to empower smaller businesses," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 4, pp. 2582–5208, 2025. [Online]. Available: https://doi.org/10.56726/IRJMETS71604

[34] "Privacy and data protection compliance in AI-driven SME platforms," ResearchGate. [Online]. Available: https://www.researchgate.net/publication/391274897_Privacy_and_Data_Protection_Compliance_in_AI-Driven_SME_Platforms. [Accessed: May 6, 2025]

[35] N. Yuhan and J. Hamilton, "Strengthening SMEs through cybersecurity and AI: A path to operational excellence," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/384443733_Strengthening_SMEs_through_Cybersecurity_and_AI_A_Path_to_Operational_Excellence. [Accessed: Apr. 3, 2025]

[36] G. A. D. Scientist, "AI cybersecurity for small businesses: Protecting data effectively," Generative AI Data Scientist, Feb. 23, 2025. [Online]. Available: https://generativeaidatascientist.ai/ai-cybersecurity-for-small-businesses-protecting-data-effectively/

AUTHORS

Kemisola is a People Data Analyst and Researcher specializing in data analytics, artificial intelligence, explainable AI, generative AI, machine learning, and workforce and business analytics. Her research integrates statistical modeling, organizational effectiveness, and the study of data-driven strategies shaping small and medium-sized enterprises as well as broader economic and social systems at national and international levels. She leverages advanced tools including Python, R, SQL, Tableau, Power BI, and SAS to develop models and insights that connect theory with practice, with a particular emphasis on explainable AI and its role in driving research and innovation. Beyond workforce and business analytics, she has authored and coauthored publications on healthcare, cybersecurity, disaster management, public safety, and supply chain resilience, with work spanning the United States and international contexts. She also serves as a reviewer and editorial board member for academic journals, further strengthening her contribution to

advancing ethical and impactful research.

Precious Orekha is a data scientist and researcher with expertise in machine learning, natural language processing, and applied analytics for business intelligence. He holds a master's degree in data science with a minor in Project Management from Drexel University, complemented by a background in Chemical Engineering. His research interests include model interpretability, predictive modeling, and the application of AI in domains such as healthcare, transportation, and financial systems. Precious has worked on projects involving explainable AI (XAI), advanced text analytics, and computer vision, focusing on real-world problems like fraud detection, clinical trial optimization, and human behavior analysis using deep learning. He has contributed to developing AI-driven solutions that improve decision-making, optimize workflows, and enhance security awareness. Passionate about bridging the gap between theory and practical application, Precious continues to explore innovative approaches to ethical and scalable AI systems.

Oluwaseun John Bamigboye is a researcher in the field of Computer Information Systems, specializing in artificial intelligence and data management, with focuses on designing intelligent systems that optimize data-driven decision-making, with interest in machine learning, data governance, and the ethical deployment of AI technologies. With a strong foundation in both theoretical and applied research, Oluwaseun has contributed to projects that enhance organizational efficiency and support scalable digital transformation. He is passionate about interdisciplinary collaboration and actively engages in mentoring and outreach to promote responsible innovation in the evolving landscape of intelligent information systems.

Afolabi Sabur Ajao, MBA, CISSP, is a cybersecurity and strategy professional with expertise in enterprise risk management, cloud migration, and ERP transformation for Fortune 100 companies. He has designed and delivered initiatives that improved security posture, accelerated digital transformation timelines, and optimized large-scale technology portfolios. His work emphasizes the integration of applied artificial intelligence into security strategy, where his current research explores AI-driven approaches to strengthening cybersecurity resilience in small and medium enterprises among others.

Peter O. Alawiye is an academic researcher with over a decade of expertise in human resources, digital banking, and organizational strategy, with a focus on artificial intelligence, data analytics, and cybersecurity. His research explores innovative approaches to workforce management, supply chain optimization, and organizational resilience within dynamic global markets. He combines practical industry experience with research-based inquiry, and his work contributes to knowledge on the intersection of human capital development, emerging technologies, and sustainable organizational performance.

Adeola Raji is data-driven analytics professional and researcher with over five years of experience in applying machine learning, artificial intelligence, and advanced data analytics to complex business and technology challenges. Her work emphasizes developing intelligent systems for cybersecurity, supply chain resilience, and healthcare innovation, with a focus on predictive modeling, anomaly detection, and adaptive risk management. Adeola has successfully led cross-functional projects translating business needs into scalable technical solutions, while also contributing to academic research on next-generation encryption, AI-driven communication models, and the economic implications of digital transformation. Her research interests lie in leveraging emerging technologies to enhance resilience, security, and stability across critical domains in the digital economy.