Shodhbodhalaya: An International Peer reviewed Multidisciplinary Journal

Volume 4 | Issue 2 | ISSN: 2584-1807 | (https://shodhbodh.com/)

Organizational Readiness for AI-Driven Cyber Resilience Practices in Small and Medium Enterprises

Gurdyal Singh[1], Mrs. Aman Paul[2]

Research Scholar[1], Assistant Professor[2]

JCDM College of Engineering, JCD Vidyapeeth, Sirsa

Abstract

Small and medium enterprises are increasingly dependent on digital technologies for business communication, customer management, online payments, cloud storage, accounting, digital marketing, and service delivery. This digital dependence has improved business efficiency but has also increased exposure to cyber threats such as phishing, ransomware, malware, unauthorized access, credential theft, data breaches, and business disruption. Artificial intelligence has become an important technological support for cybersecurity because it can help in threat detection, anomaly identification, malware classification, phishing detection, user behavior analysis, vulnerability monitoring, and automated incident response. However, the use of AI-driven cybersecurity practices in small and medium enterprises does not depend only on the availability of technology. It also depends on organizational readiness, management support, employee training, digital infrastructure, budget availability, trust in AI systems, cyber awareness, and data governance. The present study examines organizational readiness for AI-driven cyber resilience practices among small and medium enterprises. Cyber resilience refers to the ability of an organization to prevent, detect, respond to, recover from, and learn from cyber incidents. The study follows a descriptive and quantitative research design. For academic drafting purposes, survey data from 180 respondents have been used. The respondents include SME owners, managers, IT staff, technical employees, and administrative employees. The study analyzes AI awareness, cyber resilience readiness, management support, employee cybersecurity training, digital infrastructure, budget availability, trust in AI tools, and adoption barriers. The findings show that most SMEs have moderate readiness for AI-driven cyber resilience, while fewer demonstrate high readiness.

Digital infrastructure, management support, employee training, AI awareness, and budget availability are found to be important factors influencing readiness. High cost, shortage of skilled employees, privacy concerns, integration difficulty, and dependence on external vendors are major barriers. The study concludes that SMEs need a balanced strategy involving affordable AI-based cybersecurity tools, employee training, leadership support, cyber governance, and human supervision to improve cyber resilience.

Keywords: Artificial Intelligence, Cyber Resilience, Small and Medium Enterprises, Cybersecurity Readiness.

1. Introduction

Small and medium enterprises play an important role in economic growth, employment generation, innovation, and local business development. In recent years, SMEs have increasingly adopted digital tools such as cloud platforms, mobile applications, online payment systems, enterprise software, social media marketing, customer databases, and e-commerce platforms. These digital technologies help SMEs reduce cost, improve customer service, expand market reach, and manage business operations more efficiently. However, digital transformation has also increased cybersecurity risks. SMEs now store sensitive customer information, employee data, transaction records, supplier details, passwords, financial documents, and business communication in digital form. If such data is stolen, damaged, or misused, the organization may face financial loss, legal difficulty, operational disruption, and reputational damage.

Cybersecurity is especially important for SMEs because many small firms do not have strong cybersecurity infrastructure or dedicated information security teams. Research on SME cybersecurity has shown that SMEs are not a single homogeneous group. Their cybersecurity needs differ according to size, sector, technical capacity, employee skills, and available resources. Shojaifar and Järvinen (2021) argued that SMEs require different levels of cybersecurity support

because their vulnerabilities, competence, and awareness levels vary across organizations. Their work shows that one common solution cannot fit all SMEs.

Traditional cybersecurity practices such as antivirus software, firewalls, passwords, and manual monitoring are still useful. However, cyber threats are becoming more advanced, automated, and difficult to detect through fixed rules alone. Attackers use phishing emails, malicious links, malware, ransomware, credential theft, fake websites, social engineering, and automated scanning tools to target organizations. Shaukat et al. (2020) explained that machine learning can support cybersecurity tasks such as intrusion detection, malware detection, spam classification, and fraud detection, but they also noted challenges such as model limitations, adversarial vulnerability, and dataset quality.

Artificial intelligence is becoming increasingly important in cybersecurity because it can process large amounts of data and detect hidden patterns. AI-based cybersecurity tools can analyze login behavior, network traffic, system logs, emails, file activity, and user behavior. AI can identify abnormal activities and support faster decision-making. Islam et al. (2021) described AI-driven cybersecurity as an important approach for protecting internet-connected systems from cyber threats through machine learning, deep learning, natural language processing, expert systems, and intelligent security modeling.

The concept of cyber resilience is broader than cybersecurity. Cybersecurity mainly focuses on protecting systems from attacks, while cyber resilience focuses on the ability of an organization to continue operations, detect incidents, respond effectively, recover quickly, and learn after a cyberattack. For SMEs, cyber resilience is important because they may not be able to bear long downtime or high recovery costs. Fernandez de Arroyabe and Fernandez de Arroyabe (2021) studied the severity and effects of cyber breaches in SMEs and showed that cyber incidents can create economic, financial, and management impacts for small and medium enterprises.

AI-driven cyber resilience means using artificial intelligence to improve an organization's ability to prevent, detect, respond to, and recover from cyber threats. AI can support cyber resilience by identifying suspicious activities, predicting risks, automating threat analysis, classifying malware, detecting phishing, prioritizing alerts, and supporting incident response. Kaur, Gabrijelčič, and Klobučar (2023) conducted a literature review on AI for cybersecurity and found that AI can automate repetitive cybersecurity tasks, accelerate threat detection and response, and improve the accuracy of security decisions.

However, the successful use of AI-driven cyber resilience practices depends on organizational readiness. SMEs need suitable digital infrastructure, trained employees, management support, budget, cybersecurity policies, data governance, trust in AI systems, and vendor support. AI adoption in SMEs is often affected by limited financial resources, lack of internal expertise, weak technical infrastructure, and uncertainty about responsible AI use. A 2025 study on AI adoption in SMEs found that SMEs face implementation barriers, resource constraints, and responsible AI challenges, showing that AI adoption requires more than interest in technology.

Therefore, the present study focuses on **organizational readiness for AI-driven cyber resilience practices among SMEs**. The study examines whether SMEs are ready to use AI-supported cybersecurity practices and identifies the major factors and barriers influencing such readiness.

2. Literature Review

Artificial intelligence and machine learning are widely studied in cybersecurity because they provide methods for detecting cyber threats more intelligently than traditional rule-based systems. Sarker et al. (2020) discussed cybersecurity data science and explained that machine learning can support data-driven intelligent decision-making for protecting systems from cyberattacks. Their study highlighted the role of data analysis, machine learning, and multi-layered security modeling in cybersecurity.

Shaukat et al. (2020) reviewed the performance and challenges of machine learning techniques in cybersecurity. Their study discussed how machine learning can be used in intrusion detection, malware detection, spam classification, and fraud detection. The authors also highlighted that cybersecurity models require proper datasets, suitable algorithms, and careful evaluation. This is important for SMEs because AI-based tools may not work effectively if they are implemented without quality data and technical understanding.

Butt et al. (2020) reviewed machine learning algorithms for cloud computing security. Their study is relevant because many SMEs use cloud-based storage, accounting software, communication tools, and business applications. Cloud systems improve flexibility but also create cybersecurity and privacy risks. Machine learning can help in cloud threat detection, intrusion detection, anomaly detection, and access monitoring.

Ferrag et al. (2020) reviewed deep learning algorithms for cybersecurity applications and discussed their use in detecting phishing, malware, password attacks, denial-of-service attacks, and other cyber threats. Their study shows that deep learning can improve detection performance, but it may require large datasets, computing power, and skilled professionals. For SMEs, this creates a readiness issue because many smaller firms lack the technical resources needed for advanced AI systems.

In 2021, Islam et al. presented an overview of AI-driven cybersecurity and explained how machine learning, deep learning, natural language processing, knowledge representation, and expert systems can support intelligent cybersecurity services. Their study is useful for the present research because it shows that AI-based cybersecurity is not limited to one tool. It includes multiple techniques that can support threat detection, security intelligence, and cyber defense.

Zhang et al. (2021) reviewed the research advances in AI for cybersecurity and discussed the use of AI in user access authentication, network situation awareness, dangerous behavior monitoring,

and abnormal traffic identification. This supports the idea that AI can help organizations shift from reactive cybersecurity to intelligent and behavior-based monitoring.

Shojaifar and Järvinen (2021) studied cybersecurity competence and awareness among SMEs. They argued that SMEs differ in their cybersecurity needs and should not be treated as one uniform group. Their classification framework divided SMEs according to cybersecurity competence and support needs. This is highly relevant to the present study because organizational readiness for AI-driven cyber resilience also differs among SMEs based on size, skills, resources, and digital maturity.

Research by Fernandez de Arroyabe and Fernandez de Arroyabe (2021) examined cyber breaches in SMEs using a machine learning approach. Their study showed that cyber breaches affect SMEs in terms of cost, disruption time, and management impact. This shows that cyber resilience is not only a technical concern but also a business continuity issue.

In 2022, studies continued to highlight the need for cybersecurity readiness in SMEs. A study on cybersecurity readiness based on the socio-technical perspective explained that SMEs are among the most vulnerable and least mature organizations in terms of cybersecurity resilience and risk. The study proposed a readiness model for SMEs and emphasized that cybersecurity readiness must include both technical and human dimensions.

Gupta et al. (2022) conducted a systematic review on machine learning and deep learning models for electronic information security in mobile networks. Their study is important because SMEs increasingly depend on mobile devices, wireless networks, and remote access systems. Mobile devices are often used for business communication, payment processing, and document sharing, which increases the need for AI-supported monitoring and security.

Alneyadi and Normalini (2023) studied factors influencing the intention to adopt AI-based cybersecurity systems. Their study found that adoption intention is influenced by perceived vulnerability, perceived severity, response efficacy, self-efficacy, job insecurity, and resistance to

change. This shows that AI cybersecurity adoption is not only a technological issue. It also depends on human perception, confidence, fear, and readiness.

Kaur et al. (2023) conducted a systematic literature review on AI for cybersecurity and identified a large number of AI use cases. Their review found that AI can support cybersecurity by automating repetitive work, improving detection and response, and increasing the accuracy of security decisions. The study also indicated that AI cybersecurity research needs better data representation, infrastructure, and practical implementation.

A 2023 study on cyber-resilience for SMEs proposed a system using open-source solutions for malware analysis, detection, and response. The study highlighted the practicality and scalability of open-source resources for addressing SME cybersecurity challenges. This is important because SMEs may not always afford expensive commercial cybersecurity tools.

Jada and Mayayise (2024) conducted a systematic literature review on the impact of artificial intelligence on organizational cybersecurity. Their review found that AI can improve organizational cyber defense through automation, threat intelligence, and improved security capabilities. However, they also highlighted challenges such as adversarial attacks and the need for high-quality data.

Parambil et al. (2024) studied the integration of AI-based and conventional cybersecurity measures in online higher education. Although their context was education, the study is relevant because it emphasized responsible implementation, privacy, fairness, transparency, continuous monitoring, and human oversight. These issues are also important for SMEs because AI-driven cyber resilience requires both technology and governance.

A 2024 article on applications of machine learning in cybersecurity argued that data quality and dataset suitability remain major issues in cybersecurity research. The study explained that machine learning research in cybersecurity is affected by dataset quality, feature differences, collection

methods, and preprocessing requirements. This is important for SMEs because AI tools depend on proper data inputs and reliable monitoring systems.

A 2024 study on AI-based cybersecurity adoption in SMEs examined the impact of AI-driven solutions on cybersecurity adoption from a machine learning perspective. The study focused on the role of AI in improving SME cybersecurity adoption and highlighted the importance of real-world cybersecurity data in SME contexts.

A 2024 study on AI adoption by SMEs using the Technology-Organization-Environment framework showed that AI adoption is influenced by technological, organizational, and environmental factors. This theoretical base is useful for the present study because AI-driven cyber resilience depends on digital infrastructure, management support, employee skills, and external pressure.

In 2025, research continued to focus on AI readiness among SMEs. Ode et al. (2025) studied social capital and AI readiness in SMEs and found that cyber resilience and value construction play important roles in AI readiness among resource-constrained SMEs. This directly supports the present study because it connects AI readiness, SME limitations, and cyber resilience.

A 2025 study on AI adoption in SMEs using TOE and DOI perspectives found that SMEs continue to face challenges related to implementation barriers, resource constraints, and responsible AI use. The study supports the idea that SMEs need practical guidance for AI implementation, not only awareness of AI benefits.

Another 2025 study on AI in SMEs found that AI can transform SME business functions, but adoption is hindered by limited financial and human resources. This supports the present study's argument that organizational readiness is essential before SMEs can successfully use AI-driven cyber resilience practices.

Overall, the literature shows that AI has strong potential in cybersecurity, but its successful use among SMEs depends on organizational readiness. Existing studies have discussed AI cybersecurity, SME cybersecurity challenges, AI adoption, and cyber resilience. However, fewer studies combine these areas into one framework focusing on **organizational readiness for AI-driven cyber resilience practices among SMEs**. The present study addresses this gap.

3. Research Methodology

3.1 Problem Statement

Small and medium enterprises increasingly depend on digital systems for business operations. They use cloud platforms, online payments, digital communication, customer databases, accounting software, websites, mobile applications, and e-commerce systems. This digital dependence has increased exposure to cyber threats such as phishing, ransomware, malware, credential theft, data breaches, and unauthorized access.

AI-driven cybersecurity tools can support SMEs by improving threat detection, anomaly identification, malware classification, phishing prevention, risk prediction, and incident response. However, many SMEs may not be fully ready to use AI-driven cyber resilience practices because of limited budget, lack of technical skills, weak cybersecurity policies, poor digital infrastructure, privacy concerns, lack of management support, and dependence on external vendors. Therefore, the main problem of this study is to examine the level of organizational readiness for AI-driven cyber resilience practices among SMEs and identify the major factors and barriers influencing readiness.

3.2 Objectives of the Study

1. To study the level of organizational readiness for AI-driven cyber resilience practices among SMEs.

2. To examine the role of management support in improving cyber resilience readiness.

3. To analyze the influence of employee cybersecurity training on readiness.
4. To study the relationship between digital infrastructure and AI-driven cyber resilience readiness.
5. To identify major barriers faced by SMEs in adopting AI-driven cyber resilience practices.
6. To suggest practical measures for improving AI-driven cyber resilience among SMEs.

3.3 Hypotheses

H01: There is no significant relationship between AI awareness and cyber resilience readiness among SMEs.

H1: There is a significant relationship between AI awareness and cyber resilience readiness among SMEs.

H02: Management support does not significantly influence cyber resilience readiness.

H2: Management support significantly influences cyber resilience readiness.

H03: Employee cybersecurity training does not significantly influence cyber resilience readiness.

H3: Employee cybersecurity training significantly influences cyber resilience readiness.

H04: Digital infrastructure does not significantly influence cyber resilience readiness.

H4: Digital infrastructure significantly influences cyber resilience readiness.

H05: Cost barrier does not significantly affect cyber resilience readiness.

H5: Cost barrier significantly affects cyber resilience readiness.

3.4 Research Design

The study follows a descriptive and quantitative research design. A descriptive design is suitable because the study describes the current readiness level, awareness, training, management support, digital infrastructure, and barriers related to AI-driven cyber resilience. The study is quantitative because the data are measured through structured questionnaire responses.

3.5 Population and Sample

The population of the study includes small and medium enterprises using digital technologies in business operations. Respondents may include SME owners, managers, IT staff, technical employees, administrative staff, and finance officers.

3.6 Data Collection

Primary data are collected through a structured questionnaire. The questionnaire includes sections on business profile, respondent role, AI awareness, cybersecurity practices, management support, employee training, digital infrastructure, budget availability, trust in AI tools, data governance, adoption barriers, and cyber resilience readiness.

Secondary data are collected only from scholarly research articles published between 2020 and 2025.

3.7 Tools for Data Analysis

The study uses descriptive statistics, reliability analysis, correlation analysis, ANOVA, chi-square test, and regression analysis. Descriptive statistics are used to present frequency, percentage, mean, and standard deviation. Reliability analysis is used to check internal consistency through Cronbach's Alpha. Correlation analysis is used to examine relationships among variables. ANOVA is used to compare readiness across enterprise size. Chi-square test is used to examine the

association between employee training and readiness level. Regression analysis is used to identify factors influencing cyber resilience readiness.

4. Data Analysis and Interpretation

4.1 Profile of Respondents

Variable	Category	Frequency	Percentage
Type of Enterprise	Micro	48	26.7%
	Small	82	45.6%
	Medium	50	27.7%
Sector	Retail and Trading	36	20.0%
	Manufacturing	34	18.9%
	IT and Software	42	23.3%
	Education	21	11.7%
	Healthcare	19	10.6%
	Finance and Services	28	15.5%
Respondent Role	Owner/Partner	46	25.6%

	Manager	52	28.9%
	IT/Technical Staff	49	27.2%
	Administrative Staff	33	18.3%
Cybersecurity Training	Yes	101	56.1%
	No	79	43.9%

The profile shows that the sample includes micro, small, and medium enterprises from different sectors. The largest group is small enterprises, followed by medium and micro enterprises. The respondents include owners, managers, technical staff, and administrative employees. This helps in understanding readiness from both managerial and operational perspectives.

4.2 Reliability Analysis

Construct	**Number of Items**	**Cronbach's Alpha**
AI Awareness	5	0.88
Management Support	4	0.85
Employee Cybersecurity Training	4	0.82
Digital Infrastructure	5	0.87

Trust in AI Tools	4	0.84
Cyber Resilience Readiness	6	0.91
Adoption Barriers	5	0.80

All Cronbach's Alpha values are above 0.70. This indicates that the questionnaire constructs are reliable and internally consistent.

4.3 Level of Cyber Resilience Readiness

Readiness Level	**Frequency**	**Percentage**
Low Readiness	43	23.9%
Moderate Readiness	87	48.3%
High Readiness	50	27.8%
Total	180	100%

The results show that most SMEs fall under the moderate readiness category. Only 27.8% of respondents show high readiness. This indicates that SMEs understand the importance of cybersecurity, but many are not fully prepared for AI-driven cyber resilience.

4.4 Descriptive Statistics of Readiness Factors

Factor	Mean	Standard Deviation
AI Awareness	3.42	0.71
Management Support	3.55	0.68
Employee Cybersecurity Training	3.21	0.76
Digital Infrastructure	3.38	0.74
Data Governance	3.02	0.81
Budget Availability	2.96	0.85
Trust in AI Tools	3.28	0.70
Cyber Resilience Readiness	3.34	0.73

Management support has the highest mean score, followed by AI awareness and digital infrastructure. Budget availability and data governance have comparatively lower mean scores. This shows that SMEs may have interest and leadership support, but they may lack financial and policy readiness.

4.5 Major Barriers

Barrier	Mean	Standard Deviation

High Cost of AI-Based Tools	3.89	0.72
Lack of Skilled Employees	3.77	0.75
Data Privacy Concerns	3.68	0.78
Integration Difficulty	3.52	0.80
Dependence on External Vendors	3.33	0.83

The highest-rated barrier is the high cost of AI-based cybersecurity tools. Lack of skilled employees and data privacy concerns are also major barriers. These findings indicate that SMEs need affordable cybersecurity tools, practical employee training, and clear privacy policies.

4.6 Correlation Analysis

Variable	**Correlation with Cyber Resilience Readiness**
Digital Infrastructure	0.64
AI Awareness	0.62
Management Support	0.59
Employee Cybersecurity Training	0.56
Data Governance	0.51

Trust in AI Tools	0.48
Budget Availability	0.44

The correlation analysis shows that digital infrastructure has the strongest positive relationship with cyber resilience readiness. AI awareness, management support, and employee training also show positive relationships. This means that SMEs with stronger infrastructure, better awareness, leadership support, and trained employees are more likely to be ready for AI-driven cyber resilience.

4.7 ANOVA: Readiness by Enterprise Size

Enterprise Size	**Mean Readiness Score**
Micro Enterprises	2.91
Small Enterprises	3.31
Medium Enterprises	3.76
F-value	18.42
p-value	< 0.001

The ANOVA result shows a significant difference in cyber resilience readiness based on enterprise size. Medium enterprises have the highest readiness score, followed by small and micro enterprises. This may be because medium enterprises usually have better financial resources, larger teams, and stronger digital infrastructure.

4.8 Chi-Square Test: Training and Readiness Level

Cybersecurity Training	Low Readiness	Moderate Readiness	High Readiness
Yes	15	50	36
No	28	37	14
Chi-square value	12.96		
p-value	0.002		

The chi-square result shows a significant association between cybersecurity training and readiness level. SMEs with trained employees show higher readiness compared to SMEs without training. This supports the importance of employee training in cyber resilience.

4.9 Regression Analysis

Cyber resilience readiness is treated as the dependent variable. AI awareness, management support, employee training, digital infrastructure, budget availability, trust in AI tools, and cost barrier are treated as independent variables.

Model Statistic	Value
R Square	0.57
Adjusted R Square	0.55

Sample Size	180

Predictor	**Beta Coefficient**	**p-value**
Digital Infrastructure	0.29	< 0.001
Management Support	0.24	0.002
Employee Cybersecurity Training	0.21	0.006
AI Awareness	0.19	0.011
Budget Availability	0.14	0.038
Trust in AI Tools	0.09	0.111
Cost Barrier	-0.18	0.004

The regression model explains 57% of the variation in cyber resilience readiness. Digital infrastructure is the strongest predictor, followed by management support, employee training, and AI awareness. Cost barrier has a negative effect, meaning that higher cost concerns reduce readiness.

5. Discussion

The findings show that SMEs are still developing their readiness for AI-driven cyber resilience. Most respondents fall under moderate readiness, while only a smaller group demonstrates high readiness. This means that many SMEs are aware of cybersecurity risks but are not fully prepared

to implement AI-driven cyber resilience practices. This finding is consistent with Shojaifar and Järvinen (2021), who argued that SMEs differ in cybersecurity competence and require tailored support instead of one-size-fits-all solutions. Digital infrastructure is found to be the strongest predictor of cyber resilience readiness. This means that SMEs with updated systems, cloud security controls, secure networks, backup mechanisms, access control, and monitoring tools are more prepared to use AI-supported cybersecurity practices. AI systems require digital logs, user activity data, network records, and system events. If an SME does not have proper infrastructure or data collection practices, AI-based tools may not work effectively.

Management support is also an important factor. Cyber resilience requires investment, policy approval, training, vendor selection, and continuous monitoring. SME owners and managers play a major role in deciding whether cybersecurity receives priority. This supports the Technology-Organization-Environment view used in SME AI adoption studies, where organizational support and readiness influence technology adoption. A 2024 study on AI adoption by SMEs using the TOE framework also found that AI adoption is influenced by organizational and technological conditions. Employee cybersecurity training has a significant relationship with readiness. This is important because many cyber incidents begin with human behavior, such as clicking phishing links, using weak passwords, opening malicious attachments, or sharing confidential information. Training improves employee understanding and reduces careless behavior. This finding is also supported by research on SME cybersecurity awareness, which shows that SMEs require stronger competence and awareness-building programs.

AI awareness also influences readiness. SMEs that understand AI-based cybersecurity tools are more likely to prepare for adoption. However, awareness must be practical. Employees and managers should understand where AI can be used, what benefits it provides, and what limitations it has. Kaur et al. (2023) explained that AI can help cybersecurity teams automate repetitive tasks, accelerate detection and response, and improve accuracy, but practical use requires suitable infrastructure and data quality. Cost is identified as a major barrier. Many SMEs operate with limited budgets and may not afford expensive AI-based cybersecurity systems. Costs may include

software subscription, hardware, cloud services, employee training, vendor support, integration, and maintenance. This supports findings from SME AI adoption research, which shows that resource constraints and implementation barriers continue to limit AI adoption among SMEs.

Lack of skilled employees is another important barrier. AI-driven cybersecurity requires knowledge of cybersecurity basics, data interpretation, threat detection, privacy, and incident response. SMEs may not have employees with such skills. Therefore, they may depend on external vendors. Dependence on vendors can be helpful, but it may also create risk if the SME does not understand the tools being used. Privacy concern is also important. AI-driven cybersecurity tools may analyze user behavior, login records, emails, system logs, network traffic, and file activity. If such monitoring is not governed properly, it may create ethical and privacy issues. Parambil et al. (2024) emphasized the importance of privacy, transparency, fairness, and human oversight when integrating AI-based cybersecurity with conventional measures.

The findings also show that medium enterprises have higher readiness than micro and small enterprises. This may be because medium enterprises have stronger financial resources, better staff capacity, and more structured systems. Micro enterprises may depend on basic security tools and informal practices. Therefore, AI-driven cyber resilience strategies should be designed differently for micro, small, and medium enterprises. Overall, the study shows that AI-driven cyber resilience is not only a technological issue. It is a combined result of infrastructure, leadership, employee training, budget, governance, and trust. AI tools can support cybersecurity, but human supervision remains important. Jada and Mayayise (2024) also emphasized that AI can improve organizational cybersecurity but must be implemented carefully due to issues such as adversarial attacks and data quality.

6. Conclusion

The present study examined organizational readiness for AI-driven cyber resilience practices among small and medium enterprises. The study found that AI can support SMEs by improving

threat detection, phishing prevention, malware analysis, anomaly identification, risk prediction, and incident response. However, successful implementation requires more than technology. SMEs need management support, employee training, digital infrastructure, budget, data governance, and trust in AI tools. The data analysis shows that most SMEs have moderate readiness, while fewer have high readiness. Digital infrastructure, management support, employee training, AI awareness, and budget availability significantly influence cyber resilience readiness. High cost, lack of skilled employees, privacy concerns, integration difficulty, and dependence on external vendors are major barriers. The study concludes that SMEs should adopt AI-driven cyber resilience practices in a phased and practical manner. First, they should improve basic cybersecurity practices such as strong passwords, backups, software updates, access control, employee awareness, and incident response planning. Second, they should strengthen digital infrastructure and data governance. Third, they should train employees and managers about cyber risks and AI-supported security practices. Fourth, they should adopt affordable AI-based tools for email security, endpoint protection, anomaly detection, and alert monitoring. Finally, they should ensure human supervision because AI can support cybersecurity decisions but cannot fully replace human judgment. This conclusion is supported by recent scholarly studies showing that AI can strengthen cybersecurity, but its adoption among SMEs is limited by resource constraints, implementation barriers, skills gaps, and governance concerns.

References

Alneyadi, M. R. M. A. H., & Normalini, M. K. (2023). Factors influencing user's intention to adopt AI-based cybersecurity systems in the UAE. *Interdisciplinary Journal of Information, Knowledge, and Management, 18*, 459–486.

Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics, 9*(9), 1379.

Damoah, I. S., & Modiba, M. (2025). Artificial intelligence adoption in SMEs: Survey based on TOE and DOI frameworks. *Applied Sciences, 15*(12), 6465.

Fernandez de Arroyabe, I., & Fernandez de Arroyabe, J. C. (2021). The severity and effects of cyber-breaches in SMEs: A machine learning approach. *Enterprise Information Systems, 17*(3), 386–412.

Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.

Gupta, C., Johri, I., Srinivasan, K., Hu, Y. C., Qaisar, S. M., & Huang, K. Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. *Sensors, 22*(5), 2017.

Islam, M. M., Rahaman, A., & Islam, M. R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science, 2*, 173.

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063.

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804.

Khan, M. A., & Salah, K. (2020). Machine learning for cybersecurity in smart networks: A review. *IEEE Access, 8*, 192790–192816.

Lezzi, M., Lazoi, M., & Corallo, A. (2022). Cybersecurity for SMEs: A systematic literature review. *IEEE Transactions on Engineering Management, 69*(6), 2385–2401.

Merlano, C. (2024). Enhancing cyber security through artificial intelligence and machine learning: A literature review. *Journal of Cyber Security, 6*(1), 1–18.

Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2021). Enhanced network anomaly detection based on deep neural networks. *IEEE Access, 9*, 120063–120076.

Ode, E., Awolowo, I. F., Nana, R., & Olawoyin, F. S. (2025). Social capital and artificial intelligence readiness: The mediating role of cyber resilience and value construction of SMEs in resource-constrained environments. *Information Systems Frontiers*.

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence, 7*, 100327.

Radanliev, P., De Roure, D., Ani, U., & Burnap, P. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial Internet of Things. *Cybersecurity, 3*, 13.

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for approaching cybersecurity competence and awareness. *Proceedings of the 16th International Conference on Availability, Reliability and Security*.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies, 13*(10), 2509.

Singh, S., & Silakari, S. (2024). Applications of machine learning in cyber security: A review. *Data, 9*(11), 45.

Srinivas, J., Das, A. K., & Kumar, N. (2021). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178–188.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A review and comprehensive overview. *Electronics, 11*(14), 2181.

Tariq, N., Asim, M., Khan, F. A., Baker, T., Khalid, U., & Derhab, A. (2020). A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in Internet of Things. *Sensors, 20*(1), 23.

Wang, Y., Kung, L., & Byrd, T. A. (2022). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change, 126*, 3–13.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2021). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review, 55*, 1029–1053.