DOI: https://doi.org/10.4038/jdrra.v2i2.53

The Journal of Desk Research Review and Analysis, Vol. 2, Issue 1, 2024, 249-250

SYSTEMATIC LITERATURE REVIEW ON DEVELOPING AN AI FRAMEWORK FOR SME CYBERSECURITY IDENTIFICATION AND PERSONALISED RECOMMENDATIONS

HMTN Jayathilaka[1] and J Wijayanayake[2]

Abstract

Small and medium-sized enterprises (SMEs) are adopting digital solutions faster, which exposes them to cyber risks. This study aims to develop a framework for SME identification in the context of cybersecurity and fine-tuning an AI model for personalised security recommendations. The literature was systematically identified, screened, and selected following the PRISMA guidelines to ensure comprehensive topic coverage. The study also outlines the factors affecting SME cybersecurity, including limited resources, low knowledge, and complications of cybersecurity products. This research-based framework will help to overcome these challenges by identifying SMEs by their cybersecurity requirements and offering recommendations based on a fine-tuned AI model. The findings suggest that personalised security recommendations can significantly improve SMEs' capacity to proactively manage risks and safeguard their digital assets. This research adds value to the known knowledge by solving a significant problem that SMEs encounter. This framework, integrated with the fine-tuned AI model, will enhance the cybersecurity of SMEs and offer a customisable solution that can be applied to various settings.

Keywords: AI, Cybersecurity, Framework, Recommendations, SMEs

[1] Department of Industrial Management, University of Kelaniya, Sri Lanka

Email: tharindunaveen9@gmail.com https://orcid.org/0009-0004-5027-9609

[2] Professor, Department of Finance, University of Kelaniya, Sri Lanka.

Email janaka@kln.ac.lk https://orcid.org/0000-0002-9523-5384

Received date: 31.07.2024
Accepted date: 22.10.2024

Introduction

Background of the Study

The present situation in cybersecurity, especially for SMEs, is practised with the following issues primarily due to scarcity of resources and limited knowledge. A study has found that most small-level enterprises display lower risk appreciation towards cyber risks and consequently have weak protection (Armenia et al., 2021; Benz & Chatterjee, 2020). According to research by Symantec in 2016, 43% of cyber-attacks are aimed at SMEs, proving the associated risks. Moreover, as per the (Sarker et al., 2021) data report, in 2020, 28% of data breaches involved small, related businesses, indicating that the problem persists. Other scholars have also noted several difficulties in the SMEs about implementing a sound cybersecurity policy that may include lack of funding, inadequate human resources that possess the right skills, and ignorance of threats (Atoum & Otoom, 2017; Shojaifar & Järvinen, 2021).

Expanding on improving SMEs' cybersecurity, efforts have been made to increase awareness and ensure training. For example, campaigns by government departments and associations for industries aim to create awareness of basic cybersecurity measures among SME businesses (Rea-Guaman et al., 2020). Still, these initiatives are usually not very useful because the strategies are general, and the kind of SMEs to be dealt with is not considered. Hence, there is a greater demand for cybersecurity and a need to enhance it by making it more particular (Shojaifar et al., 2020).

Also, there is a need to advance cybersecurity, and the role of AI has been suggested as the solution with features including threat recognition, risk assessment, and mitigation (Goyal et al., 2023; Naumov et al., 2019; Perozzo et al., 2022). In this way, using AI for Security analysis allows it to process large amounts of data and identify patterns that indicate suspicious actions or events. This enables it to put up an equally fitting fight as the threats arise and give users assistance that meets their needs (Van Haastrecht et al., 2021).

Existing AI-based security has been examined in various situations and has indeed been effective up to now. For example, with a machine-learning approach, the probability of an attack can be estimated considering previous attacks and historical and current behaviours (Lin et al., 2023; Ozkan & Spruit, 2019). For example, IBM's Watson for Cyber Security involves natural language processing where cyber analysts can have high-level automated analysis of unstructured data that humans could otherwise not analyse (Erdogan et al., 2023; Li et al., 2023).

It is crucial to understand that the use of AI in the cybersecurity context for SMEs is still in its early stages. Security solutions that employ artificial intelligence are typically targeted at large-scale organisations with complex and costly implementations that are beyond the reach of SMEs (Walid & Hariri, n.d.). This gap reveals the lacuna from the absence of AI models for the domain of SMEs, which generally have limited resources at their disposal. Therefore, This research aims to identify the best approach to using AI in cybersecurity to provide specific and appropriate security measures that SMEs can adopt (Dai et al., 2023).

Research Problem

Small and medium-sized enterprises (SMEs) increasingly integrate digital technologies, enhancing their efficiency and exposing them to significant cybersecurity threats such as data breaches, ransomware, and phishing attacks. Despite the importance of cybersecurity, many SMEs show low levels of

awareness and preparedness due to limited resources, lack of specialised personnel, and the high cost of comprehensive security solutions.

Current cybersecurity frameworks and models often fail to meet the specific needs of SMEs. They are typically complex, static, and designed for larger enterprises with greater resources and technical expertise. This results in SMEs struggling to implement these models effectively, leading to reliance on costly external consultants or inadequate security measures.

Furthermore, the dynamic nature of cybersecurity threats requires adaptable and user-friendly frameworks that can evolve with changing threats. There is a significant gap in the literature and practical applications for frameworks explicitly tailored for SMEs and easily implemented without extensive technical knowledge.

The advent of artificial intelligence (AI) offers an opportunity to enhance cybersecurity for SMEs. However, the potential of AI to provide tailored cybersecurity solutions, such as customised security guidelines and recommendations, remains underexplored.

Research Objectives/Questions

The primary objective of this research is to develop a comprehensive and adaptable framework for identifying and assessing the cybersecurity needs of small and medium-sized enterprises (SMEs) and fine-tune an AI model (such as ChatGPT) to deliver personalised cybersecurity guidelines. The research aims to empower SMEs with accessible and cost-effective tools to manage their cybersecurity effectively and independently. The study aims to achieve the following specific objectives:

- Examine the factors that affect the cybersecurity status of SMEs.
- Examine the constraints and difficulties that SMEs encounter in implementing proper cybersecurity measures.
- Create a unique framework that identifies SMEs according to their cybersecurity requirements.
- Fine-tune an AI model to give SMEs tailored security recommendations based on their specific circumstances and needs.
- Assess the extent to which the AI model has improved the cybersecurity posture of SMEs.

The research seeks to answer the following questions:

RQ1: What are the primary cybersecurity challenges faced by SMEs?
RQ2: How can SMEs be identified based on their cybersecurity needs?
RQ3: In what ways can an AI model (Large Language Model such as ChatGPT) be fine-tuned to provide personalised cybersecurity guidelines for SMEs?
RQ4: How can the proposed solution improve cybersecurity awareness and preparedness among SMEs?

Methodology

This study employs the PRISMA methodology to systematically review the literature on SME cybersecurity and AI-based personalised security recommendations. The PRISMA approach involves four phases: identification, screening, eligibility, and inclusion.

Identification: Relevant papers on SME cybersecurity and AI security recommendations are searched using databases like Google Scholar, IEEE Xplore, and ResearchGate. Additional sources include references from initial articles and non-conventional sources like corporate reports. Initial search for relevant studies using terms like 'SME cybersecurity', 'AI recommendations', and 'cybersecurity frameworks' as well as more specific queries ("Small and Medium Enterprises" OR "SMEs") AND ("cybersecurity" OR "cyber security") AND ("Artificial Intelligence" OR "AI") AND ("security recommendations")

Table 1: Search Results Distribution Across Primary Sources for Each Search Term

Search Term	Google Scholar	IEEE Xplore	ResearchGate	Total Count
SME cybersecurity	28,800	6,458	17,994	**39,652**
AI recommendations	9,830	1,652	12,303	**23,785**
Cybersecurity frameworks	220,000	4,657	15,721	**240,378**
Complete search string	106	22	46	**174**

1. **Screening**: Duplicates are removed, and studies are filtered based on titles and abstracts using predefined inclusion and exclusion criteria. Inclusion criteria focus on studies involving SMEs, cybersecurity, and AI applications published in the last ten years. Exclusion criteria include non-English studies and irrelevant literature.
2. **Eligibility**: Full texts of remaining studies are reviewed for relevance and quality. This includes evaluating research techniques, data collection, analysis methods, and generalisation to SME cybersecurity and AI recommendations.
3. **Inclusion**: Key findings are extracted and categorised. A meta-analysis of the extracted data identifies trends, patterns, and research gaps, which inform the development of an SME cybersecurity framework and an AI-based model.

Using the PRISMA flowchart, 43 high-quality articles are selected, ensuring comprehensive and reliable findings.

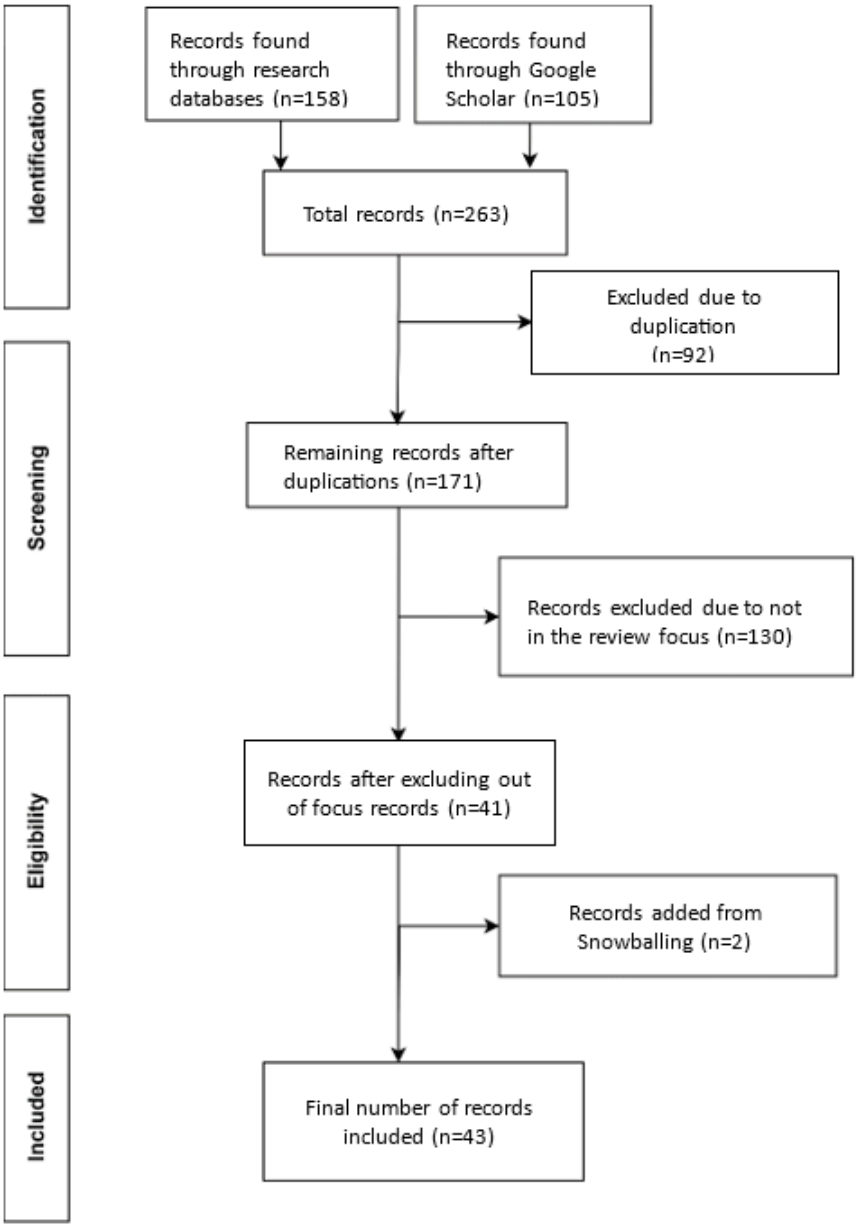

Fig 3: PRISMA Flow Diagram

Results and Discussion

Findings of the Study

Identification of Key Cybersecurity Challenges for SMEs

According to the results of the studies, it can be concluded that a few challenges hinder SMEs in their cybersecurity efforts, which are mainly attributed to the limited financial and human resources available to such companies (A. et al., 2021a). Another helpful observation would be that most SMEs often fail to finance the acquisition of elaborate software and security professionals. This financial issue means that they employ outdated or insufficient security measures; thus, they face today's cyber threats. However, the current studies also highlighted that the SME employees and their managerial staff had little cybersecurity training and awareness knowledge, meaning that human error would always prevail and present an opportunity for hackers (Cruzado et al., 2022).

Resource Limitations and Awareness Gaps

Small businesses may not have dedicated IT personnel to tackle cybersecurity either by outsourcing it from other experts or by having non-IT personnel with multiple functions in the company (Mahfuri et al., 2024). This again affects its enforcement and freedom from specialised knowledge, not to mention the delayed capability in identifying any threats. The same study also shows the inability to adequately guard against a threat that evolves as quickly and diversely as cybercrime often does since SMEs might struggle to properly employ and maintain the newest protective tools and measures (Kavakli et al., 2022).

Tailored Cybersecurity Needs

This research develops a context that defines SMEs' security needs and vulnerabilities within the cybersecurity environment. It includes characteristics such as the nature of the industry in which they operate, the size of the business, and the type of digital assets managed by the SME (Fleron et al., 2023). For instance, SMEs operating in the financial sector or those entities that collect and process personal data would require an entirely different set of security measures. This categorisation is beneficial in developing specific and relevant security recommendations or advisories for clients (A. A. Alahmari & Duncan, 2021b).

Practical Implications and Comparisons with Previous Research

The findings of this research support previous studies that have defined SMEs as a special group vulnerable to different cyber risks and the necessity of specialised security methods. (Rodriguez-Baca et al., 2022). Still, it is worth mentioning that this research fills the gaps in previous studies by including AI to reduce the lack of individualised, easily implementable and affordable solutions. The findings from this study indicate that, with the help of the resulting framework and AI model, the cybersecurity situation in SMEs can be enhanced and the probability of cyber-attacks minimised.

In-depth Analysis and Interpretation

Financial and Resource Constraints

The analysis also reveals that financial and resource constraints influence the most difficulty in preventing SMEs from implementing efficient cybersecurity strategies. Constraints such as inadequate funding, lack of priority, and lack of personnel or time are inherent barriers to cybersecurity in SMEs (Laato et al., 2020). This short-term-oriented approach means that companies and organisations use outdated tools and security systems that hackers regularly break into. Some of the issues that affect this area include. There is little or no indication of having specific IT personnel or cybersecurity specialists when SMEs use general workers who cannot implement robust cybersecurity measures (Jawhar et al., 2024b).

Awareness and Training Deficiencies

This raises a vital issue about cybersecurity in SMEs, particularly around the awareness and engagement of employees and management. This lack of awareness is problematic because the human factor that is the subject of security breaches is one of the leading causes (Ali et al., 2024; Jawhar et al., 2024a). Most SMEs do not engage in exercises such as training the employees on safety measures and other security measures such as conducting mock attacks and many other forms of security difficulties; the employees become vulnerable to quickly getting pretty through phishing, social engineering and other kinds of cyber threats (Nour & Said, 2024; Oh & Shon, 2023). This paper shows that SMEs' cybersecurity level can be significantly enhanced by increasing awareness and training in the sector.

Current State of Cybersecurity in SMEs

The status of cybersecurity in SMEs can be described as the space where businesses do not have a sufficient defence against cyber threats because of a lack of sufficient funds and experience. Most SMEs are ignorant of their danger, having a widely believed notion that they are safe from cyber-attacks (Van Haastrecht et al., 2021). From the findings of the current study, even as awareness in SMEs rises, 50% of them have poor cybersecurity plans. This lack of preparedness means they are at risk of data loss, ransomware and email phishing among other cyber hazards (Atoum & Otoom, 2017). This paper has also established that SMEs must improve their awareness of cybersecurity issues and take initial steps to protect against threats.

Existing Frameworks and Their Limitations

The existing literature on cybersecurity readiness highlights the necessity for tailored cybersecurity frameworks that address the unique challenges SMEs face. Various models and frameworks have been developed to help SMEs effectively manage their cybersecurity risks. For example, the CyberSecurity Readiness Model for SMEs (CRMM-SME) emphasises a socio-technical approach, integrating technical and social aspects to enhance cybersecurity readiness. This model addresses the gap in the existing literature by focusing on the specific needs of SMEs and proposing a comprehensive strategy that includes both technological and human factors (Perozzo et al., 2022).

Similarly, frameworks such as AVARCIBER and SME Cyber Risk Assessment (SMECRA) offer structured methodologies for assessing and managing cybersecurity risks specific to SMEs. These frameworks provide detailed guidelines and tools for SMEs to evaluate their cybersecurity posture, identify vulnerabilities, and implement appropriate measures to mitigate risks. However, despite their usefulness, these models often lack practical implementation strategies and may be difficult for SMEs to adopt without external support (Erdogan et al., 2023).

The NIST Cybersecurity Framework (CSF) is among the most respected and widely used standard cybersecurity methodologies. Developed by the National Institute of Standards and Technology, the CSF provides a comprehensive structure to guide organisations in managing and reducing cybersecurity risk. It is designed to be flexible and applicable to organisations of all sizes, including SMEs. (National Institute of Standards and Technology, 2024).

Fig 4: Steps for creating and using a CSF Organizational Profile

Source: (National Institute of Standards and Technology, 2024)

However, the NIST CSF has several limitations. It is not a trivial effort to undertake. For example, it requires learning an entirely new vocabulary described in a detailed 55-page guidebook (National

Institute of Standards and Technology, 2024). The framework is also very complicated to comprehend and implement. While the NIST CSF allows IT leaders to rate themselves on each stated standard, it does not specify acceptable ratings for those standards. Organisations cannot gauge the effectiveness of implementing the recommended security policies and procedures without comparative data. The NIST CSF does not provide best practices or specific recommendations for improvement, requiring each organisation to set its target based on its environment (Abraham et al., 2019; Lord, 2018).

Moreover, many existing frameworks are static and fail to account for the dynamic nature of cybersecurity threats. They often emphasise compliance and technical assessments without adequately addressing the social and organisational aspects of cybersecurity. As a result, there is a critical need for more holistic and adaptable frameworks that SMEs can easily implement and tailor to their specific needs and constraints (Atoum & Otoom, 2017).

Framework for SME identification

The first key finding of this research is the development of a general conceptual framework that targets SME organisations. The framework can be applied by identifying the SMEs by the type of industry, company size, and nature of assets involved in digitisation, and it provides guidance on how to protect the assets. For example, financial systems must ensure SMEs employ identity management and check-ups while manufacturing SMEs must focus on supply chain and terminal security. This is made more accessible, bearing in mind that the approach enables the determination of the most applicable and feasible security measures to adopt for each category of SMEs (Paul et al., 2024).

Integration of AI and Cybersecurity for SMEs

The advent of artificial intelligence (AI) and machine learning (ML) technologies has opened new avenues for enhancing cybersecurity measures. AI-driven cybersecurity solutions offer real-time threat detection, automated response mechanisms, and personalised security recommendations, significantly improving the efficiency and effectiveness of cybersecurity practices (Sarker et al., 2021). Studies have demonstrated the potential of AI models, such as ChatGPT, to be fine-tuned for specific applications, including personalised recommendation systems and cybersecurity guidance (Li et al., 2023).

For instance, AI-driven solutions can provide SMEs with cost-effective tools to manage their cybersecurity needs independently. AI models can analyse vast amounts of data to detect patterns and anomalies indicative of cyber threats, allowing quicker and more accurate responses (Naumov et al., 2019). Integrating AI technologies in cybersecurity practices has improved real-time threat detection and automated response mechanisms and provided personalised security recommendations (Goyal et al., 2023).

Suitability of Generative AI for Cybersecurity Recommendations in SMEs

Generative AI, particularly Large Language Models (LLMs) like ChatGPT, are increasingly seen as a powerful tool for building recommendation systems, including those aimed at cybersecurity. The strength of generative AI lies in its ability to analyse vast amounts of unstructured data, generate human-like responses, and provide personalised recommendations based on the specific needs of users. This ability to deliver tailored, context-aware recommendations is critical for SMEs as they often lack the in-house expertise to manage their cybersecurity infrastructure effectively (Dai et al., 2023).

Generative AI models like ChatGPT excel at processing natural language, meaning they can interpret human input flexibly and meaningfully, helping SMEs understand complex cybersecurity recommendations. These models can distil detailed security policies into actionable steps, helping

SMEs, who often struggle with technical jargon, better comprehend and apply the advice provided (Naumov et al., 2019).

Comparing Generative AI Models for Personalized Cybersecurity Recommendations

While several generative AI models are available today, ChatGPT stands out as a superior option for delivering personalised cybersecurity recommendations for SMEs. Below is a comparison between ChatGPT and other prominent generative AI models, such as Google's Bard, Meta's LLaMA, and Gemini AI (Soman & Ranjani, 2023; Caramancion, 2023)

Criteria	ChatGPT (OpenAI)	Google Bard	Meta's LlaMA	Gemini AI
Pretrained on Extensive Data	Pretrained on a vast dataset covering diverse domains, enabling it to handle various cybersecurity scenarios effectively.	Pretrained on web data focusing on real-time information but lacks comprehensive domain-specific training like ChatGPT.	It is designed for research, not optimised for general-purpose recommendations, and lacks extensive conversational training.	Trained on broad datasets, focusing on AI safety and real-world applications, but lacks the deep fine-tuning capabilities ChatGPT offers for specific cybersecurity needs.
Conversational & Contextual Understanding	Excels in engaging multi-turn conversations, refining answers based on user input, ideal for clarifying complex cybersecurity issues.	They have good conversational abilities but are focused on integrating live web access, making it less suitable for in-depth multi-step inquiries.	It is not optimised for conversational tasks but is primarily used for research.	It is designed to be safe and general but may not handle technical, in-depth cybersecurity discussions as effectively as ChatGPT.
Fine-Tuning Capabilities	Easily fine-tuned for specific domains like SME cybersecurity, enabling personalised recommendations.	It does not offer extensive fine-tuning for domain-specific needs, relying more on real-time data retrieval.	Fine-tuning is possible but requires advanced technical resources, making it less accessible for SMEs.	Focuses on broader applications, it currently lacks the same level of domain-specific fine-tuning available in ChatGPT.
Real-Time Adaptability	It can be updated periodically without requiring live web	Excels in real-time adaptability via live web	Open source but requires manual updates; not	It focuses on real-time updates and safety but

	access, allowing adaptability to emerging cybersecurity threats.	access but lacks deep fine-tuning capabilities.	suited for real-time recommendations.	may not offer highly specialised or technical updates without fine-tuning.
User-Friendliness & Accessibility	Designed for ease of use, with the ability to explain complex cybersecurity concepts in simple terms, making it accessible for non-technical users.	User-friendly but may overwhelm SMEs with real-time data rather than consistent, clear recommendations.	Not user-friendly for non-technical users; mainly a research tool for developers and researchers.	User-friendly with safety as a focus but may not provide in-depth technical guidance as required for specialised fields like cybersecurity.

Table 2: Generative AI Models Comparison Table

AI-Driven Personalized Cybersecurity Recommendations

This research establishes that SME cybersecurity can be improved by using an individual customisation approach with the fine-tuned AI model suggested as the solution. Using the data from history and general tendencies, estimated for each SME, using an AI model can indicate relative risks and suggest specific measures for their mitigation. It also enhances the capacity for identifying threats and mitigating them while providing certainty that the recommended strategies can be implemented within the framework of the SME (Bountouni et al., 2023; Squillace et al., 2024). The model also has the advantage of providing (timely) information and can be modified to include new risks that may exist in the SMEs.

Proposed Automated SME Cybersecurity Recommender System

The current Cybersecurity Evaluation Tool (CET) methodology for SMEs, as illustrated in Figure 3, involves several manual steps that require significant time and expertise. This process begins with an online survey, followed by an evaluation engine that compares the responses to best practices and averages and culminates generating a report card and recommendations. The final steps involve recognising risks and implementing recommendations to improve cybersecurity maturity (Benz & Chatterjee, 2020).

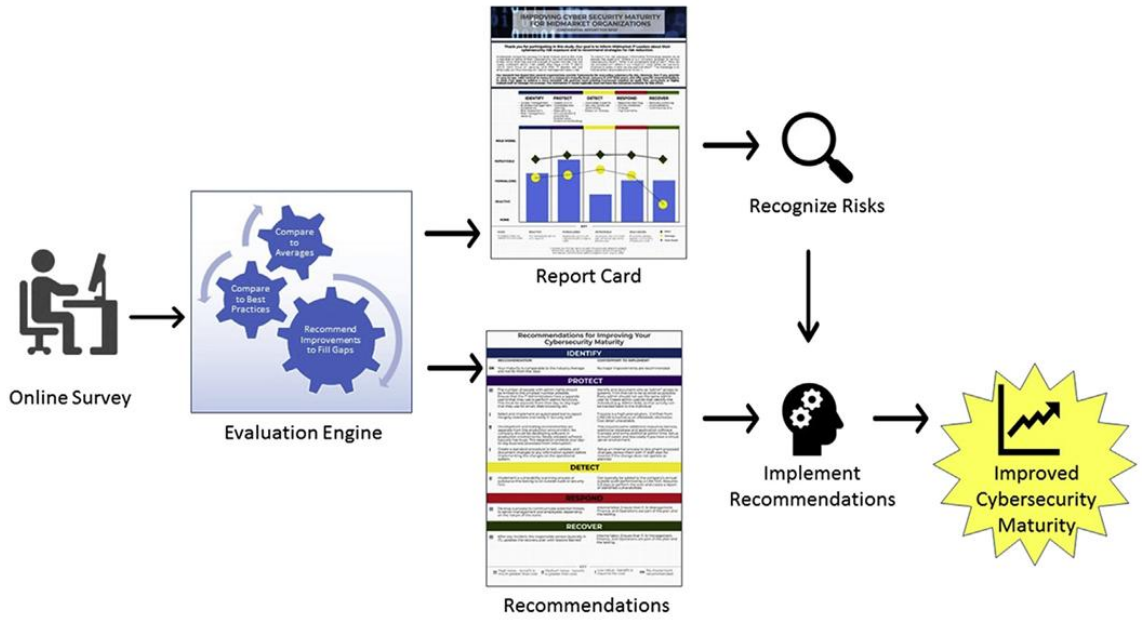

Figure 5: SME cybersecurity evaluation tool (CET) methodology
Source: (Benz & Chatterjee, 2020)

To enhance efficiency and accuracy, we propose an automated system that integrates a framework for SME identification integrated with a fine-tuned AI model to provide personalised cybersecurity recommendations. This system aims to address the limitations of the existing CET methodology by streamlining the evaluation process and offering tailored advice based on the specific needs of each SME.

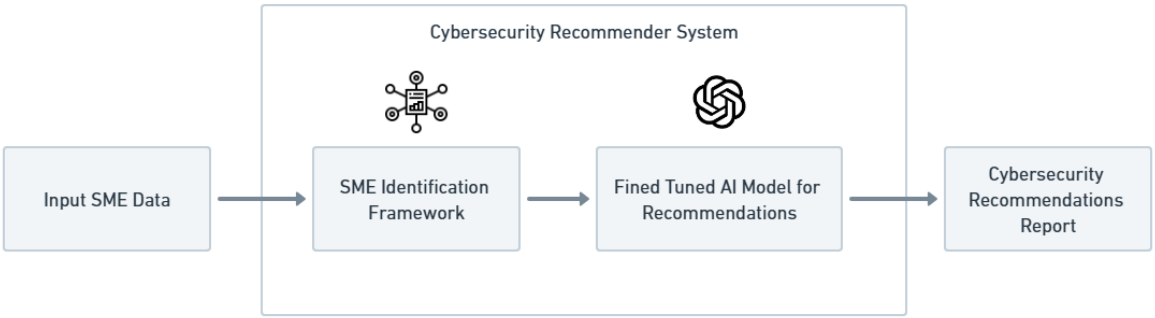

Fig 4: Architecture diagram for the proposed recommender System

Significance and Implications

The significance of this research is that it has aimed to explore a new way of combating cybersecurity challenges within SMEs. This research offers an applicable resolution to a significant problem of generating security options according to SMEs' needs and establishing which among them are qualified for the plan by recognising SMEs based on their needs and utilising AI to produce personally tailored security recommendations.

Comparison with Previous Research

Extending from research that argues SMEs are vulnerable to cybersecurity threats and the need for differential security approaches, this paper proves that. Another stream of research has also revealed that organisational aspirations, resources, and knowledge about security are often compromised in SMEs (Aalborg university et al., n.d.; Zawaideh et al., 2023). With the current line of products and

technologies, the cybersecurity adopted by SMEs is quite costly and complicated to integrate from the currently available, more extensive enterprise-security technologies.

On the other hand, this research contributes to the literature by developing a framework appropriate for SMEs, given their specific limitations and needs. Unlike previous studies that grouped SMEs into one category, this study segments SMEs based on industry, size, and the sensitivity of their digital assets to develop practical and feasible recommendations.

Also, using AI to offer customised security recommendations is another new development in earlier research. Although the use of AI in cybersecurity has been discussed (Hu, 2011; Saudi et al. et al., 2019), AI has mainly been geared towards large enterprises. This research shows that AI can provide effective, efficient and SME-appropriate security solutions for the future, addressing a gap highlighted in the literature review.

Conclusion

Key Findings

The research demonstrates a significant advancement in addressing the cybersecurity challenges small and medium-sized enterprises (SMEs) face. Due to limited resources, expertise, and awareness, SMEs are particularly susceptible to cybersecurity threats. These constraints make it challenging for SMEs to implement robust cybersecurity measures, leaving them vulnerable to cyber-attacks. Common threats SMEs face include data breaches, ransomware attacks, and phishing attempts, which can devastate their operations and reputations. The lack of dedicated IT security personnel and inadequate training further exacerbates their vulnerability, making it crucial for SMEs to adopt effective and accessible cybersecurity solutions.

Existing cybersecurity frameworks often fall short of addressing the specific needs of SMEs. Many of these frameworks are static and do not adapt to the rapidly evolving nature of cyber threats. They are typically designed for larger organisations with more resources and technical expertise, making them complex and costly for SMEs to implement effectively. The high cost and complexity of these frameworks present significant barriers for SMEs, leading to inadequate security measures and increased reliance on external consultants, which may not always provide the necessary level of protection.

The research aim to developed a conceptual framework that identifies SMEs based on industry type, company size, and the nature of digital assets managed and with a fined tuned AI model like ChatGPT give specific and relevant security recommendations, enhancing the overall cybersecurity posture of SMEs. Additionally, this system aims to improve threat identification and mitigation, making cybersecurity more accessible and practical for SMEs.

Suggestions for Further Research

Future research should refine the AI model to improve its accuracy and expand its applicability to various SME contexts. Longitudinal studies are recommended to assess the long-term effectiveness of the proposed framework and AI model in enhancing SME cybersecurity. Additionally, exploring the integration of this system with existing cybersecurity policies and regulatory frameworks could provide a more comprehensive approach to safeguarding SME digital assets.

References

Aalborg University, Institute of Electrical and Electronics Engineers, & Institute of Electrical and Electronics Engineers. Denmark Section. (n.d.). *2019 12th CMI Conference on Cybersecurity and Privacy (CMI) : Aalborg University Copenhagen, Copenhagen, Denmark, 28-29 November 2019.*

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons, 62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Alahmari, A. A., & Duncan, R. A. (2021a). Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs. *2021 IEEE International Conference on Computing, ICOCO 2021*, pp. 115–121. https://doi.org/10.1109/ICOCO53166.2021.9673554

Alahmari, A. A., & Duncan, R. A. (2021b, July 1). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. *Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2021*. https://doi.org/10.1109/ECAI52376.2021.9515166

Ali, A., Ahmed, S., Hussain, M., Bhutta, T. A., Raza, A., Nadeem, M. W., Jadoon, Y. K., & Ali, F. (2024). The Synergy of Artificial Intelligence and Cybersecurity. *2nd International Conference on Cyber Resilience, ICCR 2024*. https://doi.org/10.1109/ICCR61006.2024.10532953

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*. https://doi.org/10.1016/j.dss.2021.113580

Atoum, I., & Otoom, A. (2017). A Classification Scheme for Cybersecurity Models. *International Journal of Security and Its Applications*, *11*(1), 109–120. https://doi.org/10.14257/ijsia.2017.11.1.10

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Bountouni, N., Koussouris, S., Vasileiou, A., & Kazazis, S. A. (2023). A Holistic Framework for Safeguarding of SMEs: A Case Study. *2023 19th International Conference on the Design of Reliable Communication Networks, DRCN 2023*. https://doi.org/10.1109/DRCN57075.2023.10108247

Caramancion, K. M. (2023). News verifiers showdown: A comparative performance evaluation of ChatGPT 3.5, ChatGPT 4.0, Bing AI, and Bard in news fact-checking. *ArXiv*. https://arxiv.org/abs/2311.10821

Cruzado, C. F., Rodriguez-Baca, L. S., Huanca-Lopez, L. G., & Acuna-Salinas, E. I. (2022). Reference framework "HOGO" for cybersecurity in SMEs based on ISO 27002 and 27032. *Proceedings of the Confluence 2022 - 12th International Conference on Cloud Computing, Data Science and Engineering*, 35–40. https://doi.org/10.1109/Confluence52989.2022.9734116

Dai, S., Shao, N., Zhao, H., Yu, W., Si, Z., Xu, C., Sun, Z., Zhang, X., & Xu, J. (2023). Uncovering ChatGPT's Capabilities in Recommender Systems. *Proceedings of the 17th ACM Conference on Recommender Systems, RecSys 2023*, 1126–1132. https://doi.org/10.1145/3604915.3610646

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023). Cybersecurity Awareness and Capacities of SMEs. *International Conference on Information Systems Security and Privacy*, 296–304. https://doi.org/10.5220/0011609600003405

Fleron, C. N., Jorgensen, J. K., Kulyk, O., & Paja, E. (2023). Towards a Basic Security Framework for SMEs - Results From an Investigation of Cybersecurity Challenges in Denmark.

Proceedings - 31st IEEE International Requirements Engineering Conference Workshops, REW 2023, 230–233. https://doi.org/10.1109/REW57809.2023.00046

Goyal, S. B., Rajawat, A. S., Solanki, R. K., Zaaba, M. A. M., & Long, Z. A. (2023). Integrating AI With Cyber Security for Smart Industry 4.0 Application. *6th International Conference on Inventive Computation Technologies, ICICT 2023 - Proceedings*, 1223–1232. https://doi.org/10.1109/ICICT57646.2023.10134374

Hu, H. L. (2011). The research on SMEs' adoption of B2B E-market. *Proceedings - 2011 4th International Conference on Business Intelligence and Financial Engineering, BIFE 2011*, pp. 299–302. https://doi.org/10.1109/BIFE.2011.138

Jawhar, S., Miller, J., & Bitar, Z. (2024a). AI-Based Cybersecurity Policies and Procedures. *2024 IEEE 3rd International Conference on AI in Cybersecurity, ICAIC 2024*. https://doi.org/10.1109/ICAIC60265.2024.10433845

Jawhar, S., Miller, J., & Bitar, Z. (2024b). AI-Driven Customized Cyber Security Training and Awareness. *2024 IEEE 3rd International Conference on AI in Cybersecurity, ICAIC 2024*. https://doi.org/10.1109/ICAIC60265.2024.10433829

Kavakli, E., Loucopoulos, P., & Skourtis, Y. (2022). Capability-oriented RE for Cybersecurity and Personal Data Protection: Meeting the challenges of SMEs. *Proceedings of the IEEE International Conference on Requirements Engineering*, pp. 244–249. https://doi.org/10.1109/REW56159.2022.00053

Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020). AI in cybersecurity education systematic literature review of studies on cybersecurity moocs. *Proceedings - IEEE 20th International Conference on Advanced Learning Technologies, ICALT 2020*, 106–108. https://doi.org/10.1109/ICALT49669.2020.00009

Li, X., Zhang, Y., & Malthouse, E. C. (2023). *Exploring Fine-tuning ChatGPT for News Recommendation*. http://arxiv.org/abs/2311.05850

Lin, J., Dai, X., Xi, Y., Liu, W., Chen, B., Zhang, H., Liu, Y., Wu, C., Li, X., Zhu, C., Guo, H., Yu, Y., Tang, R., & Zhang, W. (2023). *How Can Recommender Systems Benefit from Large Language Models: A Survey*. http://arxiv.org/abs/2306.05817

Mahfuri, M., Ghwanmeh, S., Almajed, R., Alhasan, W., Salahat, M., Lee, J. H., & Ghazal, T. M. (2024). Transforming Cybersecurity in the Digital Era: The Power of AI. *2nd International Conference on Cyber Resilience, ICCR 2024*. https://doi.org/10.1109/ICCR61006.2024.10533072

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

Naumov, M., Mudigere, D., Shi, H.-J. M., Huang, J., Sundaraman, N., Park, J., Wang, X., Gupta, U., Wu, C.-J., Azzolini, A. G., Dzhulgakov, D., Mallevich, A., Cherniavskii, I., Lu, Y., Krishnamoorthi, R., Yu, A., Kondratenko, V., Pereira, S., Chen, X., … Smelyanskiy, M. (2019). *Deep Learning Recommendation Model for Personalization and Recommendation Systems*. http://arxiv.org/abs/1906.00091

Nour, S. M., & Said, S. A. (2024). Harnessing the Power of AI for Effective Cybersecurity Defense. *6th International Conference on Computing and Informatics, ICCI 2024*, pp. 98–102. https://doi.org/10.1109/ICCI61671.2024.10485059

Oh, S., & Shon, T. (2023). Cybersecurity Issues in Generative AI. *2023 International Conference on Platform Technology and Service, PlatCon 2023 - Proceedings*, pp. 97–100. https://doi.org/10.1109/PlatCon60102.2023.10255179

Ozkan, B. Y., & Spruit, M. (2019). Cybersecurity standardisation for SMEs: The stakeholders' perspectives and a research agenda. In *International Journal of Standardization Research* (Vol. 17, Issue 2, pp. 41–72). IGI Global. https://doi.org/10.4018/IJSR.20190701.oa1

Paul, S., Vijayshankar, S., & Macwan, R. (2024). Demystifying Cyberattacks: Potential for Securing Energy Systems With Explainable AI. *2024 International Conference on Computing, Networking and Communications (ICNC)*, pp. 430–434. https://doi.org/10.1109/ICNC59896.2024.10556212

Perozzo, H., Zaghloul, F., & Ravarini, A. (2022). CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective. *Complex Systems Informatics and Modeling Quarterly*, *2022*(33), 53–66. https://doi.org/10.7250/csimq.2022-33.04

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: A framework for assessing cybersecurity risks. *Cluster Computing*, *23*(3), 1827–1843. https://doi.org/10.1007/s10586-019-03034-9

Rodriguez-Baca, L. S., Larrea-Serquen, R. L., Cruzado, C. F., Alarcon-Diaz, M., Garcia- Hernandez, S. E., & Pebe-Espinoza, J. (2022). Business Cybersecurity. Case study in Peruvian and Mexican SMEs. *2022 3rd International Conference for Emerging Technology, INCET 2022*. https://doi.org/10.1109/INCET54531.2022.9824900

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. In *SN Computer Science* (Vol. 2, Issue 3). Springer. https://doi.org/10.1007/s42979-021-00557-0

Saudi Computer Society., Institute of Electrical and Electronics Engineers. Saudi Arabia Section, Institute of Electrical and Electronics Engineers. Region 8, & Institute of Electrical and Electronics Engineers. (2019). *2nd International Conference on Computer Applications & Information Security (ICCAIS 2019) : 01-03 May 2019 Riyadh, Kingdom of Saudi Arabia*.

Shojaifar, A., Fricker, S. A., & Gwerder, M. (2020). *Automating the Communication of Cybersecurity Knowledge: Multi-Case Study*.

Shojaifar, A., & Järvinen, H. (2021). *Classifying SMEs for Approaching Cybersecurity Competence and Awareness*.

Soman, S., & Ranjani, G. (2023). Observations on LLMs for telecom domain: Capabilities and limitations. *ArXiv*. https://arxiv.org/abs/2305.04637

Squillace, J., Cappella, J., & Sepp, A. (2024). User Vulnerabilities in AI-Driven Systems: Current Cybersecurity Threat Dynamics and Malicious Exploits in Supply Chain Management and Project Management. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2024*, 1760–1765. https://doi.org/10.1109/ICETSIS61505.2024.10459480

Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021, August 17). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3469199

Walid, H., & Hariri, W. (n.d.). *Unlocking the Potential of ChatGPT: A Comprehensive Exploration of Its Applications, Advantages, Limitations, and Future Directions in Natural Language Processing*. https://www.researchgate.net/publication/369771657

Zawaideh, F. H., Abu-Ulbeh, W., Mjlae, S. A., El-Ebiary, Y. A. B., Al Moaiad, Y., & Das, S. (2023). Blockchain Solution For SMEs Cybersecurity Threats In E-Commerce. *2023 International Conference on Computer Science and Emerging Technologies, CSET 2023*. https://doi.org/10.1109/CSET58993.2023.10346628