Small Scale, High Security: Developing Multi-Agent Cyber Threat Detection Framework for SMEs

Karan Goel
School of Computing and Information Technology
University of Wollongong
kg956@uowmail.edu.au

***Abstract*—Small and Medium-Sized Enterprises (SMEs) are increasingly vulnerable to sophisticated cyber threats due to limited cybersecurity resources and awareness. This research aims to develop a robust, multi-agent cyber threat detection framework tailored specifically for SMEs. Despite the advancements in cybersecurity technologies such as next-generation firewalls, intrusion detection systems, and machine learning-based solutions, these tools remain underutilized by SMEs due to their complexity and high resource demands. This proposal addresses this gap by designing a framework that simplifies the implementation of cybersecurity measures, optimizes resource use, and provides customized security plans based on industry-specific risks. By leveraging a multi-agent system approach, this framework will enhance the detection, response, and management of cyber threats, ultimately improving the security posture and resilience of SMEs against cyber attacks. The expected outcomes include accessible, cost-effective cybersecurity solutions that empower SMEs to make informed decisions and maintain robust defenses in an increasingly digital landscape.**

I. Background

Day by day, as enterprise security technologies advance, cybercriminals counter with ever more sophisticated attack tools. In a world rapidly evolving with social networks, online transactions, cloud computing, and automated processes, cybercrime also progresses. Cybercriminals persistently develop new attack types, tools, and techniques, enabling them to infiltrate increasingly complex and tightly controlled environments, inflict more significant damage, and in some cases, remain untraceable [1].

Recent examples of such attacks include the Ticketmaster breach, which compromised the data of 560 million users [2]. Another significant incident was the Medibank cyber attack, which severely impacted the privacy of 9.7 million Australians [3]. Cybercrime is even predicted to cost the world approximately $10.5 trillion annually by 2025 [4].

While large organizations may have the tools to fend off these challenges, it is often observed that small and medium-sized enterprises (SMEs) are the ones most vulnerable to cyber attacks. Research indicates that nearly half of all small and medium businesses were victims of cyberattacks, a sharp increase from 2011 when only 15% reported breaches [5]. Cybercriminals often target SMEs, viewing them as easier targets due to their lack of sophisticated security tools. Alarmingly, 60% of smaller firms go out of business within six months of experiencing a breach. This vulnerability underscores the critical need for enhanced cybersecurity measures tailored to the resources and risks faced by smaller businesses.

A. Cybersecurity in SMEs

In their survey report, Chidukwani et al. [6] emphasize the urgent need for enhanced cybersecurity measures within small-to-medium enterprises (SMEs). They highlight the disproportionate vulnerability of SMEs to cyber threats, primarily due to inadequate security implementations and a significant gap in targeted research that addresses their unique needs.

Further compounding these issues, another survey by Shaikh et al. [7] presents a similar view, underscoring that the costs of technology and infrastructure pose substantial hurdles. This study identifies the lack of technical skills, organizational support, and government assistance as major barriers that hinder SMEs' ability to adopt and effectively integrate advanced security technologies.

While technological deficits are a significant concern, Wilson et al. [8] also point to more fundamental reasons behind these challenges. They note a pervasive lack of cybersecurity awareness and a common underestimation of risk among SMEs. Many SMEs perceive themselves as unlikely targets for cyber-attacks, believing that cybercriminals primarily target larger corporations. This misconception often results in a lower priority being placed on cybersecurity measures within their business strategies, exacerbating their vulnerability to attacks.

Recent studies by Saha et al. [9] also emphasize the multifaceted challenges faced by SMEs, highlighting the urgent need for strategic realignment. These studies stress the importance of addressing the lack of adequate support from policymakers and industry groups, underscoring the need for a concerted effort to bolster cybersecurity measures within these smaller enterprises.

B. Current Techniques and Challenges

Recent advancements in cybersecurity technology have introduced a variety of sophisticated tools that SMEs can utilize to safeguard against cyber threats. Key developments include next-generation firewalls (NGFWs), intrusion detection systems (IDS), and machine learning-based solutions designed for real-time threat detection. Furthermore, tools such as endpoint detection and response (EDR) and security information and event management (SIEM) systems play a crucial role in providing comprehensive security solutions that actively monitor, detect, and respond to incidents on SME networks. While these technologies are generally effective, they require significant time for full integration and continuous maintenance. Often, a single tool may not be sufficiently adaptive to address the multifaceted cyber threats that SMEs face, leading to their underutilization. This gap not only challenges the deployment and effective use of these tools but also exposes SMEs to ongoing cyber threats despite the availability of advanced solutions.

C. Research Proposal

To mitigate cybersecurity risks more effectively, SME IT leaders must adopt a systematic approach centered on pivotal inquiries:

- Where are our most significant cybersecurity vulnerabilities?
- What is the tolerable level of risk for our operations?
- How do our cybersecurity practices measure up against industry benchmarks?

Discovering a suitable methodology for cybersecurity risk assessment remains a significant challenge. Several information security governance frameworks are accessible, including ISO, CIS, PCI DSS, and COBIT. However, these frameworks can be intricate and costly to implement. For example, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, detailed over 55 pages, outlines an extensive process for implementation, presenting a formidable challenge for SMEs with limited resources and expertise. Furthermore, this framework does not offer specific risk-reduction strategies tailored to an organization's identified vulnerabilities [10].

Outsourcing cybersecurity management could be an alternative; however, it often results in over-reliance on external consultants and diminishes in-house capabilities. There is evidence to suggest that external vendors may not provide the level of customized care that a dedicated, in-house team can offer [11].

Another common approach is for IT leaders to continue purchasing and implementing security products in response to newly perceived threats or recent cybersecurity incidents. Yet, these reactive measures are generally ineffective if not part of a well-thought-out strategic framework [12]. Such reactive solutions may overlook critical vulnerabilities or represent suboptimal resource allocation. Without a robust, formalized cybersecurity governance approach, such reactivity is often counterproductive [13].

This research proposal aims to build upon the existing cybersecurity framework (CSF) to develop a tool that evaluates, recommends, and assists SMEs in enhancing their cybersecurity posture.

II. Literature Review

To address the cybersecurity vulnerabilities of small and medium-sized enterprises (SMEs), we conducted a comprehensive systematic literature review. This review focuses on recent advancements and strategic approaches to enhance cybersecurity measures specifically for SMEs. Drawing from a wide range of academic databases and journals, the review is structured into two main sections: theoretical frameworks and practical methods.

A. Cybersecurity Frameworks

Cybersecurity frameworks define best practices that SMEs can follow to manage cybersecurity risk, establish a common language internally and externally, standardize service delivery, and improve efficiency [14].

NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF) to enhance the security measures of critical infrastructure organizations [10]. The CSF is a voluntary framework that synthesizes existing standards, guidelines, and practices, informed by contributions from both industry and government sectors. It provides organizations with a structured approach to assess and enhance their capabilities to prevent, detect, and respond to cyber-attacks. While the CSF was initially tailored for critical infrastructure, its adaptable nature has made it applicable and beneficial to a variety of organizations [15].

ASD Essential Eight: The Australian Signals Directorate (ASD) has formulated a set of cybersecurity strategies known as the "Essential Eight" [16]. These strategies are designed to fortify the defenses of information systems against cyber-attacks, particularly from adversaries employing malicious software and tactics. The Essential Eight is recommended for all organizations aiming to secure their systems comprehensively. The core objective of these strategies is to mitigate the risk of data breaches, unauthorized access, and system compromises.

ISO 27001: ISO 27001 is an internationally recognized standard for managing information security [17]. Published by the International Organization for Standardization (ISO) in partnership with the International Electrotechnical Commission (IEC), it provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The standard emphasizes a risk management process that involves people, processes, and IT systems, thereby providing a holistic approach to information security. ISO 27001 is applicable to organizations of any size and type, including public and private companies, government entities, and non-profits.

PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) [18] establishes a set of security protocols aimed at safeguarding cardholder data. Developed by the Payment Card Industry Security Standards Council (PCI SSC), this standard is crucial for companies that handle credit card information, whether they process, store, or transmit it. The primary goal of PCI DSS is to reduce the risk of fraud and unauthorized access to sensitive data.

B. Cybersecurity Methods

Ensuring compliance with cybersecurity frameworks requires a robust set of methods designed to monitor, manage, and enforce security policies effectively. These methods not only help in maintaining security standards but also provide necessary documentation and reports for compliance audits.

Intrusion Detection: Since their first introduction by Denning et al. [19], Intrusion Detection Systems (IDS) have been a significant part of network security. Modern researchers are leveraging AI and ML techniques to enhance IDS capabilities for preventing advanced threats. For instance, Kumar et al. [20] applied IDS with deep residual convolutional neural networks, while Ullah et al. [21] utilized transformer-based models achieving high accuracy. Researchers have also applied swarm-based techniques for intrusion detection, as mentioned by Reddy et al. [22] in his review.

Security Information and Event Management: Security Information and Event Management (SIEM) systems are essential for the real-time analysis of security alerts generated by applications and network hardware. Uccello et al. [23] showcased how rule-based SIEM can be integrated with AI systems using deep learning approaches. Recent works, such as those by Yue et al. [24] and Xiao et al. [25], demonstrate how these systems can be used to develop advanced APT detection techniques using provenance graphs. The work of Mees et al. [26] highlights that these systems can also be implemented using multi-agent or swarm-based approaches.

Vulnerability Management: The Common Vulnerability Scoring System (CVSS) [27] was introduced by the National Infrastructure Advisory Council (NIAC). This system was one of the first methods for assessing and communicating the severity of software vulnerabilities. The framework was first released in 2005 as part of a broader initiative to enhance cybersecurity by providing a common language and metric for evaluating vulnerabilities, which could be used by various stakeholders, including security professionals, software developers, and organizations. Walkowski et al. [28] demonstrated how scoring systems can be used to manage vulnerabilities effectively. Modern vulnerability management tools incorporate AI to predict and prioritize vulnerabilities based on potential impact and exploitability, thereby enhancing the efficiency and effectiveness of vulnerability remediation efforts.

Compliance Management: In 2005, Solms [29] discussed the distinction between Information Security Operational Management and Information Security Compliance Management, arguing that for effective Information Security Governance, these two aspects should be managed separately. Today, AI-driven compliance management software offers automated risk assessments, continuous compliance monitoring, and the generation of audit-ready reports. Tang et al. [30] and Sun et al. [31] reviewed the possibility that swarm intelligence can be used to handle compliance management using automated agents.

Identity and Access Management: Identity and Access Management (IAM) systems control who is authorized to access specific resources within an organization, a core requirement in virtually all security standards. Advanced IAM solutions [32] now use AI to provide adaptive authentication, risk-based access control, and automated identity governance. Zhang et al. [33] showcased that IAM models can be improved using blockchain-based identity management models, providing better security and access.

III. Critical Analysis

The frameworks and methods discussed in this review provide a multi-faceted approach to enhancing cybersecurity for SMEs. Each framework offers distinct advantages, but also comes with certain limitations:

a) Framework::

- The NIST Cybersecurity Framework is highly adaptable and widely applicable, making it suitable for a variety of organizations. However, its compex and voluntary nature may result in inconsistent adoption among SMEs.
- The ASD Essential Eight is specifically designed to address common threats, but its Australian origin might limit its perceived relevance to SMEs outside Australia.
- ISO 27001 provides a comprehensive and globally recognized framework for information security management. However, the complexity and resource requirements for implementation can be a significant barrier for SMEs.
- PCI DSS is crucial for businesses handling credit card information, but the stringent requirements may pose challenges for smaller enterprises with limited resources.

b) Methods::

- Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems leverage advanced AI and ML techniques, offering robust security measures. However, the integration of these technologies requires significant technical expertise, which may not be readily available in SMEs.
- Vulnerability Management systems using CVSS offer a standardized approach to evaluating and prioritizing vulnerabilities. The use of AI enhances their effectiveness, but SMEs might struggle with the initial setup and ongoing management of such systems.
- AI-driven compliance management and Identity and Access Management (IAM) systems offer automated solutions that can greatly enhance efficiency and reduce the administrative burden. However, the initial cost of these solutions and the need for continuous updates and monitoring can be a hurdle for SMEs.

The results of the review are summarized in Table I.

IV. Research Problem

Based on the analysis in previous sections, it is evident that small and medium-sized enterprises (SMEs) are particularly vulnerable to cybersecurity threats due to a combination of factors. This section outlines the specific challenges faced by SMEs and the rationale for developing a new framework and recommendation system to enhance their cybersecurity posture.

A. Vulnerability of SMEs

1) SMEs as Easy Targets: SMEs are often seen as easy targets by cybercriminals for several reasons:

Method	Adaptabile	Complex	Usefull	Ease of Implement
NIST Framework	✓	✓	✓	✗
ASD Eight	✗	✗	✓	✓
ISO 27001	✗	✓	✓	✗
PCI DSS	✗	✓	✓	✗
Intrusion Detection Systems (IDS)	✓	✗	✓	✗
Security Information and Event Management (SIEM)	✓	✓	✓	✗
Vulnerability Management (CVSS)	✓	✓	✓	✗
Compliance Management	✗	✓	✓	✗
Identity and Access Management (IAM)	✓	✗	✓	✗

TABLE I
ADVANTAGES AND LIMITATIONS OF CYBERSECURITY FRAMEWORKS AND METHODS FOR SMES

- **Limited Cybersecurity Measures**: Many SMEs lack robust cybersecurity measures, making them easier targets compared to larger organizations with more sophisticated defenses.
- **Valuable Data**: Despite their smaller size, SMEs often hold valuable data, including customer information, financial records, and intellectual property, which can be highly attractive to attackers.
- **Low Detection Rates**: SMEs may not have the necessary tools or expertise to detect and respond to cyber threats promptly, resulting in prolonged breaches and increased damage.
- **Supply Chain Vulnerability**: SMEs often serve as suppliers or partners to larger organizations, and attackers may target SMEs as a means to infiltrate more significant networks.

2) Resource Constraints: SMEs typically operate with constrained resources, impacting their ability to maintain robust cybersecurity defenses:

- **Financial Limitations**: Budget constraints can limit SMEs' ability to invest in advanced cybersecurity tools and services. This often leads to reliance on basic security measures that may not be sufficient to thwart sophisticated attacks.
- **Lack of Expertise**: SMEs may not have dedicated cybersecurity staff. Often, IT responsibilities are managed by general IT personnel who may lack specialized training in cybersecurity.
- **Time Constraints**: The limited workforce in SMEs means that employees often juggle multiple roles, leaving little time for the implementation and maintenance of comprehensive cybersecurity measures.

B. Challenges in Maintaining Cybersecurity Tools

Implementing and maintaining cybersecurity tools can be particularly challenging for SMEs:

- **Complexity of Tools**: Many cybersecurity tools and frameworks, including those based on the NIST Cybersecurity Framework (CSF), can be complex to implement and manage. This complexity can overwhelm SMEs, leading to suboptimal usage or non-implementation.
- **Ongoing Management**: Cybersecurity requires continuous monitoring, updating, and management. The dynamic nature of cyber threats means that tools need regular updates and patches, which can be resource-intensive for SMEs to manage.
- **Integration Issues**: SMEs often use a mix of legacy and modern systems. Integrating new cybersecurity tools with existing infrastructure can be technically challenging and costly.

C. Limitations of the NIST Cybersecurity Framework for SMEs

While the NIST CSF offers a comprehensive approach to managing cybersecurity risks, it does not fully meet the needs of SME IT leaders:

- **Voluntary Nature**: As a voluntary framework, adoption among SMEs can be inconsistent. Without regulatory pressure or sufficient internal motivation, SMEs may not fully implement the CSF.
- **Generalization**: The NIST CSF is designed to be broadly applicable across various sectors and organization sizes. This generality can result in recommendations that are not sufficiently tailored to the specific threats and operational realities of SMEs.
- **Resource Demands**: The framework assumes a certain level of resource availability that may not exist in SMEs, making full compliance difficult to achieve without significant adjustments.

Despite these limitations, the NIST CSF provides a strong foundation for developing a more tailored evaluation and recommendation system that can better serve the needs of SMEs.

V. OBJECTIVES

The primary objective of this research is to develop a new framework and a software system that build on the existing NIST Cybersecurity Framework (CSF) to better address the specific cybersecurity needs of small and medium-sized enterprises (SMEs). This framework and system will be designed to help SMEs make informed cybersecurity decisions and prevent cyber attacks more effectively. The specific objectives of this research are outlined as follows:

A. Objective 1: Simplified Implementation

To simplify the implementation process of cybersecurity measures for SMEs, the new framework will:

- **Create User-Friendly Guidelines**: Develop straightforward guidelines and checklists that SMEs can follow without requiring extensive cybersecurity expertise.
- **Provide Step-by-Step Instructions**: Offer detailed, step-by-step instructions to guide SMEs through the implementation of essential cybersecurity practices.

B. Objective 2: Resource Efficiency

To accommodate the resource constraints typical of SMEs, the framework will prioritize measures that offer the highest security impact for the lowest cost and effort:

- **Leverage Affordable Technologies**: Identify and recommend affordable technologies and tools that can enhance security without necessitating significant financial investments.
- **Automate Security Processes**: Incorporate automated tools and solutions to reduce the manual effort required for maintaining cybersecurity measures.

C. Objective 3: Customization and Relevance

To ensure the new framework is relevant to the specific needs and threats faced by SMEs, it will include:

- **Industry-Specific Guidelines**: Develop guidelines tailored to the unique vulnerabilities and compliance requirements of different types of SMEs.
- **Risk Assessments**: Provide method for conducting self-assessments to identify and prioritize specific risks relevant to the SME's industry and operational context.
- **Customized Security Plans**: Enable SMEs to generate and follow customized cybersecurity plans based on their unique needs and circumstances.

D. Framework and Recommendation System Development

The development of the new framework and recommendation system will involve a comprehensive process, leveraging a multi-agent approach [26] [22] [31] [30] to enhance functionality and scalability. The process includes:

- **Needs Assessment**: Conduct surveys, interviews, and workshops with SME IT leaders to identify their specific challenges and requirements.
- **Framework Design**: Develop the structure and components of the new framework, ensuring it aligns with existing standards while being tailored to the SME context.
- **System Development Using Multi-Agent Approach**: Create a software system that embodies the framework, utilizing multiple autonomous agents to perform specific tasks. This system will feature intuitive interfaces, automation capabilities, and customization options.
  - **Autonomous Agents**: Develop agents specialized in various aspects of cybersecurity, such as risk assessment, threat detection, compliance checking, and vulnerability management.
  - **Coordination and Integration**: Ensure seamless coordination among agents to provide a comprehensive and cohesive cybersecurity solution.

VI. Methodology

The methodology for developing a new cybersecurity framework and system tailored to the needs of small and medium-sized enterprises (SMEs) will involve a systematic approach divided into several key phases. This section outlines the steps and processes involved in the research and development of the proposed framework and tool, leveraging a multi-agent approach to enhance efficiency and effectiveness.

A. Phase 1: Needs Assessment (Exploratory and Qualitative Research)

The first phase involves understanding the specific cybersecurity challenges and requirements of SMEs:

- **Surveys and Interviews**: Administer surveys and conduct interviews with SME IT leaders and cybersecurity professionals to gather firsthand insights into their challenges, resource constraints, and specific security needs. This step involves both exploratory and qualitative research methods to gather detailed information.
- **Workshops and Focus Groups**: Organize workshops and focus groups with SME stakeholders to discuss and validate findings from the surveys and interviews, and to explore potential solutions and requirements in depth. These activities further employ qualitative research methods.

B. Phase 2: Framework Design (Descriptive and Qualitative Research)

Based on the insights gathered in Phase 1, the next step is to design the new cybersecurity framework:

- **Define Objectives and Scope**: Clearly define the objectives and scope of the framework, ensuring it addresses the unique needs of SMEs while aligning with existing standards such as the NIST CSF. This involves descriptive research to articulate the framework's goals.
- **Develop Framework Structure**: Create a structured framework that includes simplified guidelines, checklists, and step-by-step instructions tailored to SMEs. This is a part of the qualitative research process.
- **Incorporate Customization**: Ensure the framework allows for customization based on industry-specific needs, risk assessments, and the operational context of SMEs.
- **Prioritize Cost-Effective Measures**: Identify and include cybersecurity measures that offer high impact at low cost, making them feasible for SMEs to implement.

C. Phase 3: Tool Development Using Multi-Agent Approach (Scientific and Quantitative Research)

The development of an accompanying tool will leverage a multi-agent approach to enhance its functionality and effectiveness:

- **Tool Design and Prototyping**: Design and develop a prototype of the software tool that embodies the framework. This tool will utilize multiple autonomous agents to perform specific tasks, enhancing scalability and responsiveness. This phase includes scientific research to develop and test the tool.
- **Automated Assessments**: Integrate functionalities for automated assessments of an SME's current cybersecurity posture. Different agents will specialize in various aspects of security evaluation, such as vulnerability scanning, risk assessment, and compliance checking. This involves quantitative research methods.
- **Continuous Monitoring and Reporting**: Develop agents dedicated to continuous monitoring and reporting. These agents will ensure real-time detection of threats and provide regular updates to the framework based on emerging cybersecurity trends.
- **User Testing and Feedback**: Conduct usability testing with a sample of SME users to gather feedback on the tool's functionality, ease of use, and overall effectiveness. This feedback will be used to refine the agents' behaviors and interactions. This step involves both qualitative and quantitative research methods.

D. Phase 4: Pilot Testing and Refinement (Descriptive, Diagnostic, and Hypothesis-Testing Research)

Before the full-scale deployment, the framework and tool will undergo pilot testing:

- **Select Pilot SMEs**: Identify and collaborate with a diverse group of SMEs across different industries to test the framework and tool in real-world scenarios.
- **Implementation Support**: Provide support and guidance to pilot SMEs during the implementation process to ensure accurate feedback and data collection. This involves descriptive and diagnostic research.
- **Evaluate Effectiveness**: Assess the effectiveness of the framework and tool based on predefined metrics such as ease of use, improvement in security posture, and user satisfaction. This phase involves hypothesis-testing research.
- **Gather Feedback**: Collect detailed feedback from the pilot SMEs regarding any challenges faced, suggestions for improvement, and overall experience with the framework and tool.
- **Refine Framework and Tool**: Based on the feedback and evaluation, refine and enhance the framework and tool to address any identified issues and improve usability and effectiveness.

E. Phase 5: Deployment and Support (Causal Research and Quantitative Research)

Following successful pilot testing and refinement, the final phase involves deploying the framework and tool to a broader audience:

- **Launch Framework and Tool**: Officially launch the refined framework and tool, making them available to SMEs through various channels such as industry associations, cybersecurity consultants, and online platforms. This involves causal (explanatory) research to understand the impact of the deployment.
- **Provide Training and Resources**: Develop and distribute training materials, user manuals, and online tutorials to help SMEs understand and implement the framework and tool effectively.
- **Ongoing Support and Updates**: Establish a support system to provide ongoing assistance to SMEs, including helpdesk services, community forums, and regular updates to keep the framework and tool current with evolving cybersecurity threats.
- **Monitor Adoption and Impact**: Continuously monitor the adoption and impact of the framework and tool, collecting data to assess improvements in SMEs' cybersecurity posture and making further adjustments as needed. This phase utilizes quantitative research methods.

VII. Expected Outcomes

The methodology aims to develop a practical and effective cybersecurity framework and tool that SMEs can easily adopt and maintain. The expected outcomes include:

- **Enhanced Security Posture**: SMEs will have access to tailored, actionable cybersecurity measures that enhance their overall security posture.
- **Increased Resilience**: By implementing the framework and tool, SMEs will be better equipped to detect, respond to, and recover from cyber attacks.
- **Cost-Effective Solutions**: The framework and tool will provide cost-effective solutions that are feasible for SMEs with limited resources.
- **Empowered SMEs**: SMEs will be empowered with the knowledge and tools needed to make informed cybersecurity decisions, ultimately fostering a more secure and resilient business environment.

VIII. Research Plan

The research plan outlines the steps and timeline for developing and implementing a new cybersecurity framework and tool tailored for small and medium-sized enterprises (SMEs). This plan includes key milestones, activities, and deliverables to ensure the successful completion of the project.

In Phase 1 (Weeks 1-6), a comprehensive needs assessment will be conducted through a literature review (Weeks 1-2) to identify gaps in existing frameworks, followed by surveys and interviews with SME IT leaders (Weeks 1-4) to gather insights into their challenges. Workshops and focus groups (Weeks 5-6) will validate these findings and explore potential solutions, culminating in a Needs Assessment Report (Week 7).

Phase 2 (Weeks 8-11) involves designing the framework, starting with defining objectives and scope (Weeks 8-9) to ensure alignment with existing standards like the NIST CSF. The framework structure will be developed (Weeks 8-9) with simplified guidelines, and customization and prioritization will be addressed (Weeks 10-11) to tailor the framework to industry-specific needs. The deliverable for this phase is a draft of the new cybersecurity framework (Week 11).

In Phase 3 (Weeks 12-18), the tool will be developed using a multi-agent approach. This includes tool design and prototyping (Weeks 12-13) with intuitive interfaces and automation capabilities. Automated assessments and continuous monitoring functionalities will be integrated (Weeks 14-15). Usability testing and feedback (Weeks 16-17) will refine the tool, with the final deliverable being a prototype and user feedback report (Week 18).

Phase 4 (Weeks 19-21) focuses on pilot testing and refinement. A diverse group of SMEs will be selected for pilot testing (Week 19). Support will be provided during implementation (Weeks 19-20), and the framework's effectiveness will be evaluated (Week 20). Feedback will be gathered and used to refine the framework and tool (Week 21), resulting in a refined framework and pilot testing report.

Phase 5 (Weeks 22-24) involves deployment and support. The framework and tool will be launched to a broader audience (Weeks 22-23). Training materials, user manuals, and tutorials will be provided (Weeks 23-24), along with ongoing support and updates. The adoption and impact of the framework will be continuously monitored (Week 24), culminating in a final deployment report, including adoption metrics and impact analysis (Week 24).

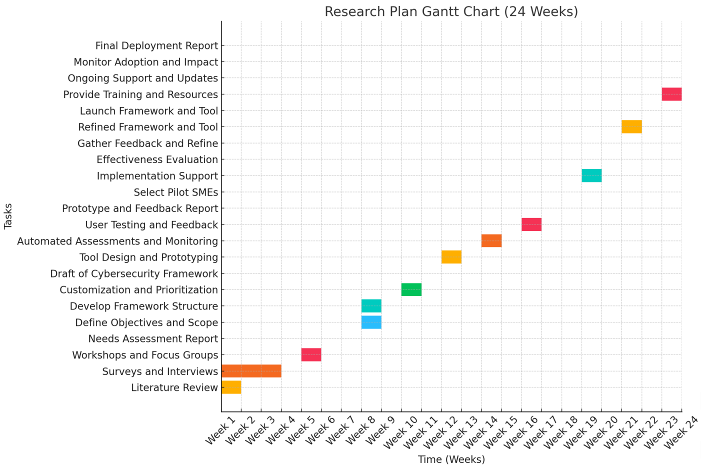

Fig. 1. Research Plan Gantt Chart (24 Weeks)

IX. Conclusion

In conclusion, the cybersecurity landscape for small and medium-sized enterprises (SMEs) presents unique challenges that necessitate tailored solutions. The proposed research aims to address these challenges by developing a new cybersecurity framework and tool, building on the strengths of the existing NIST Cybersecurity Framework (CSF) while specifically catering to the needs and constraints of SMEs. This research highlights key insights such as the vulnerability of SMEs due to limited resources and the perception of being easy targets, the limitations of current frameworks in terms of complexity and resource demands, and the potential benefits of leveraging a multi-agent approach to enhance functionality, scalability, and responsiveness.

The new framework and tool will simplify implementation by providing straightforward guidelines and step-by-step instructions, enhance resource efficiency by prioritizing cost-effective solutions and leveraging automation, offer industry-specific guidelines and customizable security plans, and ensure continuous improvement through regular updates, ongoing support, and continuous monitoring. The expected impact includes reducing vulnerabilities by helping SMEs identify and address specific cybersecurity risks, improving resilience by enabling effective detection, response, and recovery from cyber attacks, and empowering decision-making by providing the necessary knowledge and tools for informed cybersecurity decisions.

References

[1] A. Bendovschi, "Cyber-attacks–trends, patterns and security countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24–31, 2015.

[2] "Australians among 560 million users around the world caught in ticketmaster hack," *ABC News*, 05 2024. [Online]. Available: https://www.abc.net.au/news/2024-05-29/ticketmaster-hack-allegedlyshinyhunter-customers-data-leaked/103908614

[3] "Huge potential fines on the table as medibank sued over 2022 data breach," *ABC News*, 05 2024. [Online]. Available: https://www.abc.net.au/news/2024-06-05/medibank-taken-to-federal-court-over-cyber-attack/103936664

[4] R. Naveenan and G. Suresh, "Cyber risk and the cost of unpreparedness of financial institutions," in *Cyber Security and Business Intelligence*. Routledge, 2023, pp. 15–36.

[5] R. Sinex, "Small and medium businesses are drawing the attention of cybercriminals," Ph.D. dissertation, Utica College, 2017.

[6] A. Chidukwani, S. Zander, and P. Koutsakis, "A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations," *IEEE Access*, vol. 10, pp. 85 701–85 719, 2022.

[7] D. A. A. Shaikh, M. A. Kumar, D. A. A. Syed, and M. Z. Shaikh, "A two-decade literature review on challenges faced by smes in technology adoption," *Academy of Marketing Studies Journal*, vol. 25, no. 3, 2021.

[8] M. Wilson, S. McDonald, D. Button, and K. McGarry, "It won't happen to me: surveying sme attitudes to cyber-security," *Journal of Computer Information Systems*, vol. 63, no. 2, pp. 397–409, 2023.

[9] B. Saha and Z. Anwar, "A review of cybersecurity challenges in small business: The imperative for a future governance framework," *Journal of Information Security*, vol. 15, no. 01, pp. 24–39, 2024.

[10] M. P. Barrett, "Framework for improving critical infrastructure cybersecurity version 1.1," 2018.

[11] R. D. Austin and J. C. Short, "ipremier (a): Denial of service attack (graphic novel version)," 2009.

[12] H. Conick, "Four things middle market companies must do to improve cybersecurity," in *American Marketing Association*, 2017.

[13] M. Benz and D. Chatterjee, "Calculated risk? a cybersecurity evaluation tool for smes," *Business horizons*, vol. 63, no. 4, pp. 531–540, 2020.

[14] "What is a cybersecurity framework?" 04 2021. [Online]. Available: https://reciprocity.com/resources/what-is-a-cybersecurity-framework/

[15] N. Hanacek, "Nist releases version 1.1 of its popular cybersecurity framework," *National Institutes of Standards and Technology (NIST) News*, 2018.

[16] G. Slocombe, "Cyber security: Australian signals directorate (asd) is in the defensive and offensive front-line," *Asia-Pacific Defence Reporter (2002)*, vol. 44, no. 9, pp. 34–36, 2018.

[17] J. Brenner, "Iso 27001 risk management and compliance." *Risk management*, vol. 54, no. 1, pp. 24–29, 2007.

[18] G. Ataya, "Pci dss audit and compliance," *Information security technical report*, vol. 15, no. 4, pp. 138–144, 2010.

[19] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on software engineering*, no. 2, pp. 222–232, 1987.

[20] G. S. C. Kumar, R. K. Kumar, K. P. V. Kumar, N. R. Sai, and M. Brahmaiah, "Deep residual convolutional neural network: An efficient technique for intrusion detection system," *Expert Systems with Applications*, vol. 238, p. 121912, 2024.

[21] F. Ullah, S. Ullah, G. Srivastava, and J. C.-W. Lin, “Ids-int: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic,” *Digital Communications and Networks*, vol. 10, no. 1, pp. 190–204, 2024.

[22] D. K. K. Reddy, J. Nayak, H. Behera, V. Shanmuganathan, W. Viriyasitavat, and G. Dhiman, “A systematic literature review on swarm intelligence based intrusion detection system: Past, present and future,” *Archives of Computational Methods in Engineering*, pp. 1–68, 2024.

[23] F. Uccello, M. Pawlicki, S. D’Antonio, R. Kozik, and M. Choraś, “Towards hybrid nids: Combining rule-based siem with ai-based intrusion detectors,” in *International Conference on Advances in Computing Research*. Springer, 2024, pp. 244–255.

[24] H. Yue, T. Li, D. Wu, R. Zhang, and Z. Yang, “Detecting apt attacks using an attack intent-driven and sequence-based learning approach,” *Computers & Security*, p. 103748, 2024.

[25] N. Xiao, B. Lang, T. Wang, and Y. Chen, “Apt-mmf: An advanced persistent threat actor attribution method based on multimodal and multilevel feature fusion,” *arXiv preprint arXiv:2402.12743*, 2024.

[26] W. Mees and T. Debatty, “Multi-agent system for apt detection,” in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*. IEEE, 2014, pp. 401–406.

[27] P. Mell, K. Scarfone, and S. Romanosky, “Common vulnerability scoring system,” *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[28] M. Walkowski, J. Oko, and S. Sujecki, “Vulnerability management models using a common vulnerability scoring system,” *Applied Sciences*, vol. 11, no. 18, p. 8735, 2021.

[29] S. B. Von Solms, “Information security governance–compliance management vs operational management,” *Computers & Security*, vol. 24, no. 6, pp. 443–447, 2005.

[30] J. Tang, G. Liu, and Q. Pan, “A review on representative swarm intelligence algorithms for solving optimization problems: Applications and trends,” *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 10, pp. 1627–1643, 2021.

[31] W. Sun, M. Tang, L. Zhang, Z. Huo, and L. Shu, “A survey of using swarm intelligence algorithms in iot,” *Sensors*, vol. 20, no. 5, p. 1420, 2020.

[32] S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye, and T. O. Oladoyinbo, “Ai for identity and access management (iam) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems,” *Authorization, and Access Control within Cloud-Based Systems (January 25, 2024)*, 2024.

[33] K. Zhang, C. K. Lee, and Y. P. Tsang, “Stateless blockchain-based lightweight identity management architecture for industrial iot applications,” *IEEE Transactions on Industrial Informatics*, 2024.