Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
May 2024 12(5), 108–123

TOWARDS IMPROVED THREAT MITIGATION IN DIGITAL ENVIRONMENTS: A COMPREHENSIVE FRAMEWORK FOR CYBERSECURITY ENHANCEMENT

Hewa Balisane [1], Ehigiator Iyobor Egho-Promise [2], Emmanuel Lyada [3], Folayo Aina [4]

[1] Business School, The University of Law, United Kingdom
[2] ICT department, Faculty of CreaTech, City of Oxford College and University Centre, United Kingdom
[3] Learning Content Developer, ISBAT University, Kampala, Uganda
[4] Department of Computing, School of Engineering and Computing, University of Central Lancashire, United Kingdom

Received 12 April 2024
Accepted 16 May 2024
Published 14 June 2024

Corresponding Author

Ehigiator Iyobor Egho-Promise, eghopromise@yahoo.com

DOI
10.29121/granthaalayah.v12.i5.2024.5655

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

In today's digital landscape, cybersecurity has become a critical concern due to the increasing sophistication of cyber threats. Traditional cybersecurity measures are often inadequate against evolving attacks, necessitating the development of comprehensive and adaptive threat mitigation frameworks. This study aims to address this gap by proposing a robust cybersecurity framework that integrates advanced technologies such as artificial intelligence (AI), machine learning (ML), and blockchain to enhance threat detection, response, and recovery capabilities. The framework adopts a layered defense mechanism, real-time monitoring, and proactive threat hunting to provide a holistic approach to cybersecurity. By examining current methodologies and identifying their limitations, this research highlights the necessity for enhanced threat mitigation strategies. Through a mixed-methods approach involving online surveys and literature review, the study develops a flexible, scalable, and adaptive framework capable of countering sophisticated cyber threats. Key recommendations include adopting advanced technologies, continuous training, enhancing threat intelligence sharing, implementing a layered defense strategy, and conducting regular security audits. This comprehensive framework aims to improve organizational resilience, ensuring the safety and integrity of digital environments in the face of an ever-evolving cyber threat landscape.

Keywords: Cybersecurity, Threat Mitigation, Digital Transformation, Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Risk Management, Cybersecurity Framework, Cyber Threat Detection, Cyber Resilience, Cybersecurity Strategy

How to cite this article (APA): Balisane, H., Egho-Promise, E. I., Lyada, E., and Aina, F. (2024). Towards Improved Threat Mitigation in Digital Environments: A Comprehensive Framework for Cybersecurity Enhancement. *International Journal of Research - GRANTHAALAYAH, 12*(5), 108–123. doi: 10.29121/granthaalayah.v12.i5.2024.5655

1. INTRODUCTION

1.1. BACKGROUND

In today's rapidly evolving digital landscape, cybersecurity has become a critical concern for individuals, organizations, and governments worldwide. The increasing reliance on digital technologies and the internet has exposed users to a wide array of cyber threats, ranging from malware and phishing attacks to sophisticated state-sponsored cyber espionage and ransomware. These threats have significant implications, including financial losses, data breaches, disruption of critical infrastructure, and erosion of trust in digital systems.

As cyber threats become more complex and pervasive, traditional cybersecurity measures are often insufficient to protect against the evolving landscape of digital attacks. This necessitates the development of more comprehensive and adaptive frameworks for threat mitigation. The complexity of modern cyber threats requires an integrated approach that combines technological, organizational, and human factors to enhance the overall security posture.

The cybersecurity policies are required to a certain extent because the number of cyber threats has increased in the last several years. Since everything that transpires in an organization is potentially susceptible to internal and external threats, prevention measures are required more than ever Mishra et al. (2022). In the contemporary landscape, the use of information technologies in the modern world, such as digitalization, has become an inseparable part of people's lives Verma & S. Sangle (2023). This phenomenon, widely known as Digital Transformation (DT), explains the integration of various digital abilities into traditional processes, thereby revolutionizing how different businesses, governments, and individuals operate. Although DT presents the possibility of drastic increases in productivity and an innovative future for convenience, it simultaneously intertwines various entries that put the key infrastructures at risk.

However, Kaloudi & Li (2020) found that one of the issues of greatest concern within this framework is the increasing threat landscape of cybersecurity.

As organizations strive to embrace the benefits of the digitalization trend, the threat vector for cyber threats expands exponentially. The connectivity of devices, the continuous emergence of smart devices, the uses of cloud technology, and advent of IoT devices has led to the creation of a sophisticated environment, where security breaches have far-reaching consequences Schiller et al. (2022). New trends like remote work and the decentralization of data storage further increase cybersecurity personnel's difficulties. In this context, defining and describing the multifaceted challenges that appear due to the symbiotic relationship between digitalization and cybersecurity becomes crucial. However, modern threat actors struggle with the high volume of cyber threats, while smart utilities, ICSs, and SCADA systems remain vulnerable to the attacks Knapp (2024). It is still among those few crucial infrastructures that can easily be noted or play important roles. Therefore, the research data gathered so far is of immense value in supporting the development of a comprehensive cybersecurity framework.

Furthermore, Alsirhani et al. (2023) proposed another framework for exposure of the vulnerabilities of smart grid. Imaging with feature-based methods and deep learning algorithms is introduced in one part of the strategy with the AVOA-DBN-LSTM model. Hossain et al. (2023) also pointed out the increasing demand for ML in enhancing cybersecurity in today’s Smart Grids. By including the evaluated approaches of the different machine learning, the experts recommend developing attack prediction models. Deep transfer learning (DTL) performance in an ICS environment was discussed in research conducted by Gao et al. (2023). Researchers were able to look at the current developments with this approach and at possible future directions that could be considered hot topics.

Moreover, Ferrag & Maglaras (2023) explore the benefits of integrating Blockchain technology into administering intrusion detection systems (IDS) employing federated learning over IoT networks. This research paper seeks to discover the varied areas of cybersecurity threats in the digital transformation era. By synthesizing the current literature, empirical data, and case studies, the study aims to provide a comprehensive overview of the evolving threat landscape

1.2. AIM AND OBJECTIVES

This study is aimed at developing a robust cybersecurity framework that utilizes state-of-the-art threat mitigation techniques to enhance digital defense mechanisms and its objectives of are: -

1) To examine the current cybersecurity frameworks and identify their limits in mitigating modern cyber threats.
2) To Change a structured framework encompassing proactive measures for threat detection, response, and recovery.

1.3. PROBLEM STATEMENT

Despite efforts in cybersecurity, existing threat mitigation strategies often fall short of addressing the evolving nature of cyber threats. Old-fashioned approaches, such as firewalls and antivirus software, are no longer sufficient to protect against modern attacks. The nature and intensity of the threat landscape necessitate enhanced strategies that can adapt and respond to real-time threats Kayode-Ajala (2023). It is also important to properly organize the concept and make it as flexible and easy to implement as possible due to the fast-changing character of cyber threats. However, the idea of an ecosystem remains inconsequential in shaping an architectural approach towards cybersecurity. The rush to increase cybersecurity's intensity is paramount and necessary because the current security measures cannot effectively neutralize sophisticated attackers. This is so because the existing substitutes are inadequate in some ways for offering the much-needed safeguards.

2. LITERATURE REVIEW

2.1. EXISTING LITERATURE ON THREAT MITIGATION APPROACHES, FRAMEWORKS, AND TECHNOLOGIES

The robust cyber security measure can't be overstated in the rapidly evolving landscape of digital environments. With the increasing sophistication and complexity of cyber threats, there is a need to enhance existing threat mitigation approaches, technologies, and frameworks. This literature review aims to comprehensively examine current methodologies, evaluate their weaknesses and strengths, and identify gaps in the research study that present opportunities for improvement.

2.1.1. PROACTIVE AND REACTIVE MEASURES

Hider & Shabir (2024) provide an extensive overview of cybersecurity threats and mitigation techniques, emphasizing the importance of a dual approach comprising proactive and reactive measures. The proactive measures aim to prevent cyber threats before they occur. This incorporates predictive analytics and machine learning to monitor traffic and user activity to predict attacks that might arise by spotting patterns or weird network movements Mazhar et al. (2023). As such, machine learning algorithms may be adjusted according to the historical data websites and could, in turn, detect early signals of a hacking attempt, such as atypical login patterns or data transfers to strange locations. Of course, they are part of the early warning system for airborne attacks and misled the chance of success. Furthermore, these systems often require vast RAM space and complicated programming skills to be utilized Jimmy (2024). Some difficulties in smoothly conducting them are the amount of memory and the high level of programming skills needed.

2.1.2. HYBRID APPROACHES

As noted by Safitra et al. (2023), using hybrid solutions that prevent various types of destruction plays the most important role among the different prevention methods. These approaches combine different detection methods, such as signature-based, anomaly-based, and behaviour-based detection, to enhance overall security. Signature-based detection includes comparing the incoming data against a database of known malware signatures, making it highly efficient in dealing with known threats. However, it falls short in detecting new or unknown threats, where anomaly-based and behaviour-based detections come into play.

The anomaly-based technique identifies deviations from normal behaviour patterns within a system or the network, thus introducing a new form of threat detection Hajj et al. (2021). Behaviour-based detection analyses the actions of applications and users to identify malicious activities based on deviations from legitimate behaviours. By introducing these methods, hybrid approaches incorporate the advantages of each technique, improving the detection accuracy and fewer false positives.

2.1.3. NIST FRAMEWORK

The National Institute of Standards and Technology (NIST) framework for improving critical infrastructures cybersecurity, updated in 2018, remains a cornerstone in cybercrime. The NIST framework advocates for a risk-based cybersecurity approach, emphasizing the need for organizations to manage and reduce cybersecurity risk cost-effectively. The framework is structured around five core functions: Identify, Protect, Detect, Respond, and Recover Saritac et al. (2022). The Identify function means obtaining the obscure portrait that indicates networking systems, data, facilities, and capabilities analyzed. Its functions comprise the following: asset management, risk analysis and governance. The Protect function involves deploying adequate security measures to ensure the critical infrastructure's operation is exploited to acquire the right information, including access control, data, and maintenance. The Detect function is to designate the scheduled observation of cybersecurity incidents events, constant monitoring and performing of the detection procedures and events, and events management organization Kordestani & Saif (2021).

The case study presented by Hemberg et al. (2024) underscores the continuous learning and adapting concept of Cybersecurity by emphasizing advances in AI, analytics, threat discovery, vulnerability and mitigation knowledge, hunting, and simulations. They establish that the evolutionary feature of cyber threats necessarily requires constant improvement and modification of strategies for detecting threats and mitigation. According to Kinyua & Awuah (2021), advanced analytics and simulation software are crucial in mitigating and responding to threat detection and response capabilities. Cyber analytics involves using big data techniques to analyze vast amounts of security data, identifying patterns and correlations that may indicate a threat. In addition, Ukwandu et al. (2020) found that virtual experiments, like cyber range drills, are the techniques that would simulate attacks and verify how well organizations would be able to face the challenge, helping to discover the hidden problems and improve their response.

2.2. LIMITATIONS, STRENGTHS AND WEAKNESS OF CYBER-ATTACKS

Despite the literature's variety, some shared pros and cons of the emerging technologies to the present threat mitigation systems can be identified. The primary techniques discussed models include signature-based detection, anomaly-based detection, behavior-based detection, and hybrid approaches. Each method from this category would possess particular advantages and restrictions that would affect their efficiency differently in various cybersecurity situations.

Signature-based detection is one of the oldest and quite conventional approaches compared to others and is widely deployed in Cybersecurity Applebaum et al. (2021). This method utilizes a database with recorded malware signatures, consisting of code fragments or even strings of code known to be unique for each malicious software. By doing that way, when incoming data suits an identifiable signature, the system marks it as a threat. The main strength of signature-based detection is a very high level of accuracy when distinguishing known threats. It is considered efficient, easy to implement and can scan and compare large numbers of data against the signature database.

According to Debas et al. (2024), the anomaly-based detection technique addresses some of the limitations of situational-based approaches by focusing on discovering the system's anomaly or network behaviour. Such surveillance implicates creating a normal baseline of activity and then identifying any leaks that might signify a potential danger in time. The main advantage of anomaly-based detection is that it can discover new and unidentified threats, including advanced or previously unseen attacks, by recognizing unknown threats or behaviors that may signify abnormal patterns or behaviors Zoppi et al. (2021).

However, anomaly-based detection does not come without challenges, even when it is so effective. As per Ortega Vázquez et al. (2023), another problem worth noting is an overestimated rate of false positives. Normal network activities are likely to vary greatly, and not each departure from the base of record points exclusively on approaching a computer threat. Such deviation-related systems often trigger wrong alarms that confuse the benign behaviors and become suspicious threats, which may lead to burned alerts and distraction to security teams only to real threats Martins et al. (2022). Moreover, this process necessitates fine-tuning to the degree that it can identify if the anomaly is a normal deviation or a proven threat. Such expertise needs ongoing adjustment.

Behaviour-based monitoring stretches out anomaly detection rules set to respond only to abnormal actions of applications and users Borgi (2021). This approach involves looking for things that the expected pattern should never exceed, such as app executing and user activities not happening from normal procedural behaviour. Behavior-based detection is particularly against advanced persistent threats (APTs) and other malicious attacks which are being correlated to unconventional models.

To mitigate the weaknesses of individual detection methods, many cybersecurity professionals and teams should follow the same path of hybrid method detection that combines several detection techniques. Hybrid systems leverage signature-based, anomaly-based, and behaviour-based detection strengths to enhance robustness and accuracy Jeffrey et al. (2023). For instance, a hybrid system might use signatory-based detection systems for known threats, anomalous intrusion systems to uncover peculiar traffic patterns and user activity-monitoring intrusion systems.

Hybrid approaches not only reveal increases in the detection precision but also reduce false positives. By cross-referencing various detection approaches, hybrid systems can provide a more comprehensive view of potential threats, increasing the likelihood of identifying genuine attacks while minimizing false alarms Ahmad et al. (2024).

2.3. GAPS AND RESEARCH OPPORTUNITIES

In the era of unending new technology breakthroughs, there are still some sectors where research gaps persist in the cybersecurity landscape. Yet, the most important part of building a mechanism that can save lives is to make it incredibly accurate in spotting potential threats in real-time and working well under complex circumstances, as per Talaat & ZainEldin (2023). The problem nowadays is adversaries have dramatically increased their capacity to carry out attacks since normal processors of modern cyber threats currently cannot react promptly and adaptably against them. Hence, security issues arise when they need to respond to these threats. Moreover, high false-positive rates become a significant threat, specifically for anomaly- or behaviour-based detection methods Jeffrey et al. (2024). Such false alarms will invoke a higher workload on security staff as they shift their attention from actual security cues to higher non-issue alerts, and the systems have a higher chance of missing a serious issue.

Indeed, cybercrime threats continue to evolve in complexity and sophistication; there is a demand for an adaptable and scalable approach to threat mitigation solutions Aslan et al. (2023). As more networks are scaled, the existing frameworks will experience challenges. Such challenges include the increased sizes and complexities caused by the expansion of nodes, highlighting the need for innovative approaches to ensure effectiveness across diverse environments. However, Jamshed et al. (2022) found that while these technologies can hold the key to sustainable use of wireless sensor networks, their abilities must be considered. This can be done by studying emerging technologies like artificial intelligence, blockchain, and quantum computing that can address the security frameworks' diverse needs and enhance the existing security systems. Integrating such technologies can revolutionize real-time monitoring of threats, but future research is still needed to fully understand their practical applications and implications.

Yet, the priority is to find methods to prevent conformity threats, considering all data protection rules and privacy laws particularities Aslan et al. (2023). It is so hard to find the right balance between the asymmetric cyber security strategy and the privacy of the general public people which becomes an ever more complicated issue to solve. However, it demands multidimensional work and nice approaches to problems.

2.4. OPPORTUNITIES FOR IMPROVEMENT

According to Catal et al. (2023), several new strategies can be developed to cover cybersecurity knowledge gaps. Firstly, by using the advancements in machine learning and artificial intelligence and placing on more efficient and accurate risk alerting models. Such models will automatically adapt to evolving threats in real time, reducing the false positives and maximizing the effectiveness of the cybersecurity mechanisms. In addition, sharing intelligence and data among organizations can improve cybersecurity resilience at the collective level Nova (2022). The community members pool their information findings and share them in the system. Whereby the cyber network is diagnosed effectively, with the rise in resilience of a cyber network as a whole.

The innovative use of blockchain technology is considered another opportunity for improvement. By forming secure and tamper-proof network activities, blockchain can be important in tracking potential hazards increasing transparency and accountability in cybersecurity operations. Moreover, a tremendous passion for quantum-resistant algorithms formation is a must for dealing with future issues caused by quantum computing How & Cheah (2023). With the accelerating development of quantum computing, the existing cryptographic methods may no longer be secure, as hackers might use quantum technology to attack the system. As a result, the quantum era must be prepared, requiring much more robust encryption technology. Implementing the opportunities presented by this issue, the society of cyber security professionals will be able to expand the quality of threat mitigation efforts and prevent the noxious impact of digital environments from emerging cyber threats worldwide Nova (2022). Collaboration, innovation, and the readiness to keep perfecting the systems will be important for creating tough and relaxed cyberspace setups where routine and achievable goals will be met in the future.

3. THEORETICAL FRAMEWORK

The theoretical framework is the main factor for understanding and addressing the cyber threat in the digital environment. It integrates key concepts from three primary domains: Cybersecurity, risk management, and threat intelligence. This integrated approach provides a comprehensive understanding of the threat landscape and effective mitigation strategies.

3.1. CYBERSECURITY

Cybersecurity encompasses a vast bundle of different approaches, methods, tools, and procedures applied to protect systems, networks, and data from a wide spectrum of cyber threats that constantly threaten the digital environment. Cyber security is tooled with several fundamentals that defend against uninvited access, data breaches, and other cyber threats Shaikh et al. (2021). The Confidentiality, Integrity and Availability Triad, or the CIA Triad, is one of the first principles to follow, comprising the elements above. Confidentiality provides the private information sanctity only to the authorized person, and is protected from unauthorized disclosure or access. This can be achieved through encryption, access control, and strong authentication. Integrity involves managing data with accuracy and completeness throughout its lifecycle Duggineni (2023). It prevents data alteration by creating data integrity processes, such as hash function, digital signature and checksums, to detect and prevent unauthorized modifications. Availability is the ability of the authorized person who needs this information and resources to get it whenever and wherever it is. This will give a lesser chance of downtime, making the critical services smoother and smooth functioning. Introducing redundancy, load-balancing, and selecting an appropriate distributed denial-of-service (DDoS) shield are crucial in maintaining increased availability.

3.2. RISK MANAGEMENT

Risk management in Cybersecurity is a systematic process involving diagnosing risks, evaluating their effects, addressing the most pressing issues, and implementing controls to preclude mishaps. It offers a risk management framework for treating uncertainty, which helps avoid any threat from exploitation of the organizational assets. Risk assessment lies in the first position in risk management, as it involves the determination of potential threats to information assets, evaluating their probability of occurrence and the association of possible impacts of each threat with an objective measure Landoll (2021). The phase of the process includes asset identification, when an organization identifies and evaluates the fundamental assets critical to the successful running and purposes of the organization; threat analysis, which involves understanding and identifying the different types of threats that could lead to an unexpected loss for these assets; vulnerability assessment identifies weaknesses which could potentially be exploited; and risk estimation that entails combining the likelihood and impact to prioritize the risks. As per Xie et al. (2021), technologies and methodologies like risk matrices, heat maps and quantitative risk analysis models are usually introduced as supporting systems to assist decision-making.

After the risks have been identified and assessed, Risk Mitigation Strategies are formed to mitigate any further risks in the accepted level range. The solutions might include technical control, administrative control, and physical control. Devising an effective approach to risk minimization is based on either the reduction of the probability of a risk happening or the reduction of its influence Benami et al. (2021). This involves using different security controls, such as preventive, detective and corrective controls, which have been used to remediate vulnerabilities.

3.3. THREAT INTELLIGENCE

According to Zhao et al. (2020), threat intelligence involves collecting, analyzing, and disseminating data on present attacks and future threats to the organization. These procedures are key in allowing the organization to make well-calculated decisions to prevent cyber-attacks. Such choices, especially those which are actionable, are based on the "threat trend landscape. The threat landscape is the unstable and constantly changing extent of threats that a company is exposed to. Understanding the threat landscape involves following all the new threats spread, the techniques, tactics, and procedures used by the attackers, and the overall trends of cyber threats Kaloudi & Li (2020). This knowledge is considered necessary for the arranging of response and prevention measures. The threat intelligence feeds, security reports, and threat databases can act as the compass for an organization to stay on track of the latest developments in the cybercrime scene.

Indicators of Compromise (IOCs) are forensic data such as logs or hashes that could hint at a compromise to a system. IOCs involve traffic patrols, file patterns, bizarre IP addresses, and abnormal login activities. Monitoring and identifying IOCs enables the detection of incidents more rapidly and early, which limits the damage a cyberattack can cause. Additionally, Asiri et al. (2023) found that IOCs are useful hints that indicate the emergence of harmful intrusion activities promptly in the attack lifecycle.

The theoretical framework underpinning the dissertation research, "Towards Improved Threat Mitigation in Digital Environments: A Comprehensive Framework for Cybersecurity Enhancement," is a cornerstone that influences all the research components. Through Cybersecurity, risk management, and threat intelligence concepts, this framework supplies a broad approach that wraps problem-solving around cybersecurity consequences in the digital environment.

3.4. MAPPING THREATS TO CONTROLS

According to Ullah et al. (2021), at the fundamental level of the framework, there is an ability to match identified threats with security controls and risk management strategies. It includes the threat intelligence acquisition to gain insight into the constantly changing threat landscape. Through data monitoring and analysis of threat data, organizations can identify new threats, understand their tactics and techniques, and align the correct security controls to mitigate them Kunduru (2023). To illustrate, if a threat actor is found to use a specific weakness within a particular software, organizations can go ahead with further patching or updating the respective operating system, considering the preventive measures. Risk management in Cybersecurity involves mapping the threats towards controls; hence, an approach is put into place targeting issues and resources are judiciously allocated to address the critical challenges.

3.5. INFORMED DECISION-MAKING

A proper work environment with risk management aspects embedded into its framework guides the organization's decision-making processes. Through the assessment of and the quantified risks based on their possible impact and probability, risk management provides information for educated decisions regarding the strategy of risk mitigation Ganesh & Kalpana (2022). Enterprises can set agendas considering the level of risk for each threat and funnel their resources where the high-risk threats may have a critical impact on their activity. Such a risk-assessment approach guarantees that limited resources are used for risky areas to increase the efficiency of mitigation efforts. In addition, risk management practices furnish an organized procedure for assessing the cost-benefit risk area using various mitigation strategies, thus enabling organizations to make well-informed decisions according to their strategic objectives Zeng et al. (2023).

3.6. PROACTIVE THREAT MITIGATION

One of the main features of the integrated theoretical framework is the emphasis on the complex strategy of threat mitigation. By combining cybersecurity defences with proactive threat intelligence capacities, organizations can be proactive against Cybersecurity and intercept and prepare for potential threats before they appear McCall Jr (2022). Threat intelligence has a role in security controls and risk management processes, hence facilitating enterprises to pinpoint the emergence of threats in their operations, analyse the operating principle of the threats and develop preventive measures. Thus, this timely approach enables organizations to stay on the step of the adversaries, so their vulnerability is reduced, and the consequences of security incidents will be reduced Kalla & Kuraku (2023). In addition, risk preventive measures promote the organization's resilience as they make possible up-to-date threat detection and response, thus preventing wide-ranging damage or disruption of normal operations.

4. HOLISTIC FRAMEWORK FOR ENHANCING THREAT MITIGATION IN DIGITAL ENVIRONMENTS

The framework's structure is built on a holistic approach that interconnects various cybersecurity segments to stand against a unified and cohesive strategy for threat mitigation Domínguez-Dorado et al. (2022). By combining risk management, threat intelligence, and incident response, the framework ensures that all cybersecurity aspects are addressed synergistically. As for the meaning of risk management, it is stated that risk management seeks to know its risks and provide a means to assess the risks so that actions can be taken in advance. Threat intelligence informs users of new threats and attack vectors, enabling informed and timely decision-making. The incident response ensures that when a threat does materialize, the organization can react promptly and effectively to mitigate and contain the damage.

This framework also contains a layered defense mechanism, which incorporates multiple security measures layers to prevent different types of threats. These measures guard the network, for instance, firewalls and intrusion alarms, endpoint protection like antivirus software and device management, and data security practices such as encryption and access controls Kumar & Somani (2022). However, by implementing these layers, the framework ensures comprehensive coverage, making it difficult for the attacker to penetrate the defenses. Each layer acts as a barrier, and if one layer is crossed, there are still more layers, which would ensure that some operations are not likely to occur, diminishing the chances of attacks massively.

In addition, the framework is flexible and expandable; also, it is considered capable of upgrading capacity according to the existing and new threats. Due to the increasing emergence of new threats that relate to cybercrime, the framework needs to enhance the aspect by responding to some of the changes Tsakalidis et al. (2019). This adaptability is the major focus of the security measures put in place and constantly monitored for improvements using the existing technologies and intelligence. Also, it is an adaptable framework since it is malleable to encompass any organization's structure and size. As with a small business or a big enterprise, one needs to understand that the framework can be easily scaled up or scaled down to maintain some levels of protection without losing the effectiveness of its functioning. This scalability makes it possible for the framework to be responsive to the ever-evolving organizations' size and challenging digital landscapes, making them capable of effectively responding to cyber threats.

5. CONCLUSION

In this research, we have thoroughly examined the complexities of the modern cybersecurity landscape and the pressing need for enhanced threat mitigation strategies. Our comprehensive framework, "Towards Improved Threat Mitigation in Digital Environments: A Comprehensive Framework for Cybersecurity Enhancement," seeks to address the shortcomings of existing cybersecurity measures and propose robust solutions that leverage advanced technologies and methodologies.

The background and problem statement highlighted the inadequacies of traditional cybersecurity measures in combating sophisticated and evolving cyber threats. The study underscored the necessity of integrating technological, organizational, and human factors to develop a more adaptive and comprehensive approach to cybersecurity.

Through a detailed literature review, we explored various threat mitigation approaches, including proactive and reactive measures, hybrid detection methods, the NIST framework, and continuous learning and adaptation. We identified the strengths and weaknesses of these methodologies and recognized the need for a multifaceted approach to effectively address modern cyber threats.

Our proposed comprehensive framework integrates key concepts from cybersecurity, risk management, and threat intelligence, emphasizing a layered defense mechanism, real-time monitoring, and proactive threat hunting.

6. FUTURE WORK

To ensure the successful implementation and continual improvement of the proposed comprehensive framework, we recommend the following actions: Adopt Advanced Technologies; Continuous Training and Awareness Programs; Enhance Threat Intelligence Sharing; Implement a Layered Defense Strategy; Regularly Update Security Policies and Procedures; Invest in Proactive Threat Hunting; Conduct Regular Security Audits and Assessments; Promote a Culture of Cybersecurity; Utilize Simulation and Testing and Stay Informed of Regulatory Changes: Organizations should stay informed of regulatory changes and ensure compliance with relevant cybersecurity laws and standards. Adapting to new regulations promptly can prevent legal repercussions and enhance the organization’s overall security posture.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Ahmad, S., Mehfuz, S., Urooj, S., & Alsubaie, N. (2024). Machine Learning-Based Intelligent Security Framework for Secure Cloud Key Management. Cluster Computing, 1-27. https://doi.org/10.1007/s10586-024-04288-8

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-Threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice. Computers & Security. https://doi.org/10.1016/j.cose.2023.103352

Alsirhani, A., Alshahrani, M.M., Hassan, A.M., Taloba, A.I., Abd El-Aziz, R.M., & Samak, A.H. (2023). Implementation of African Vulture Optimisation Algorithm Based on Deep Learning for Cybersecurity Intrusion Detection. Alexandria Engineering Journal, 79, 105-115. https://doi.org/10.1016/j.aej.2023.07.077

Alsmadi, I. (2023). The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics. Springer Nature. https://doi.org/10.1007/978-3-031-21651-0

Applebaum, S., Gaber, T., & Ahmed, A. (2021). Signature-Based and Machine-Learning-Based Web Application Firewalls: A Short Survey. Procedia Computer Science, 189, 359-367. https://doi.org/10.1016/j.procs.2021.05.105

Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A Review of Intrusion Detection Systems using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. Electronics, 9(7), 1177. https://doi.org/10.3390/electronics9071177

Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding Indicators of Compromise Against Cyber-Attacks in Industrial Control Systems: A Security Perspective. ACM Transactions on Cyber-Physical Systems, 7(2), 1-33. https://doi.org/10.1145/3587255

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Beck, C.T. (2019). Secondary Qualitative Data Analysis in the Health and Social Sciences. Routledge. https://doi.org/10.4324/9781315098753

Benami, E., Jin, Z., Carter, M.R., Ghosh, A., Hijmans, R.J., Hobbs, A., Kenduiywo, B., & Lobell, D.B. (2021). Uniting Remote Sensing, Crop Modelling and Economics for Agricultural Risk Management. Nature Reviews Earth & Environment, 2(2), 140-159. https://doi.org/10.1038/s43017-020-00122-y

Borgi, M.A. (2021). Behavior Profiling-Based Approach for the Security of Smart Home Systems.

Brannen, J. (2017). Combining Qualitative and Quantitative Approaches: An Overview. Mixing Methods: Qualitative and Quantitative Research, 3-37. https://doi.org/10.4324/9781315248813-1

Braun, V., & Clarke, V. (2019). Reflecting on Reflexive Thematic Analysis. Qualitative Research in Sport, Exercise and Health, 11(4),589-597. https://doi.org/10.1080/2159676X.2019.1628806

Bryman, A., & Buchanan, D.A. (2018). Unconventional Methodology in Organisation & Management Research. Oxford University Press. https://doi.org/10.1093/oso/9780198796978.001.0001

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of Cyber Security Knowledge Gaps Based on Cyber Security Body of Knowledge. Education and Information Technologies, 28(2), 1809-1831. https://doi.org/10.1007/s10639-022-11261-8

Cybersecurity, C.I. (2018). Framework for Improving Critical Infrastructure Cybersecurity. CSWP, 4162018, 7. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST

Dastane, D.O. (2020). The Effect of Bad Password Habits on Personal Data Breach. International Journal of Emerging Trends in Engineering Research, 8(10). https://doi.org/10.30534/ijeter/2020/538102020

Davidson, E., Edwards, R., Jamieson, L., & Weller, S. (2019). Big Data, Qualitative Style: A Breadth-&-Depth Method for Working with Large Amounts of Secondary Qualitative Data. Quality & quantity, 53(1), 363-376. https://doi.org/10.1007/s11135-018-0757-y

Debas, E., Alhumam, N., & Riad, K. (2024). Similarity Learning; Siamese Networks; MCESTA; Triplet Loss; Similarity Metrics. International Journal of Advanced Computer Science & Applications, 15(3). https://doi.org/10.14569/IJACSA.2024.01503137

Domínguez-Dorado, M., Carmona-Murillo, J., Cortés-Polo, D., & Rodríguez-Pérez, F.J. (2022). CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity from Tactical and Operational Levels. IEEE Access, 10, 122454-122485. https://doi.org/10.1109/ACCESS.2022.3223440

Dufour, I.F., & Richard, M.C. (2019). Theorizing from Secondary Qualitative Data: A Comparison of two Data Analysis Methods. Cogent Education, 6(1). https://doi.org/10.1080/2331186X.2019.1690265

Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. Science and technology, 13(2), 29-35.

Ferrag, M. A., & Maglaras, L. (2023). DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. IEEE Transactions on Engineering Management, 67(4), 1285-1297. https://doi.org/10.1109/TEM.2019.2922936

Ganesh, A.D., & Kalpana, P. (2022). Future of Artificial Intelligence and its Influence on Supply Chain Risk Management-A Systematic Review. Computers & Industrial Engineering, 169. https://doi.org/10.1016/j.cie.2022.108206

Gao, X., Wen, Z., & Hu, J. (2023). A Survey of Security Challenges in Cloud-Based SCADA Systems. Sensors, 21(4). https://doi.org/10.3390/s21041234

George, A.S., George, A.H., & Baskar, T. (2023). Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats. Partners Universal International Innovation Journal, 1(4), 155-172. https://doi.org/10.5040/9781350033061.ch-8

Habeeb, R.A.A., Nasaruddin, F., Gani, A., Hashem, I.A.T., Ahmed, E., & Imran, M. (2019). Real-Time Big Data Processing for Anomaly Detection: A Survey. International Journal of Information Management, 45, 289-307. https://doi.org/10.1016/j.ijinfomgt.2018.08.006

Hajj, S., El Sibai, R., Bou Abdo, J., Demerjian, J., Makhoul, A., & Guyeux, C. (2021). Anomaly-Based Intrusion Detection Systems: The Requirements, Methods, Measurements, and Datasets. Transactions on Emerging Telecommunications Technologies, 32(4). https://doi.org/10.1002/ett.4240

Hemberg, E., Turner, M.J., Rutar, N., & O'reilly, U.M. (2024). Enhancements to Threat, Vulnerability, and Mitigation Knowledge for Cyber Analytics, Hunting, and Simulations. Digital Threats: Research and Practice, 5(1), 1-33. https://doi.org/10.1145/3615668

Hider, B., & Shabir, G. (2024). Cybersecurity Threats and Mitigation Strategies in the Digital Age: A Comprehensive Overview.

Hossain, M. S., Muhammad, G., & Guizani, N. (2023). Secure and Efficient Multiparty Data Aggregation for Smart Grid Communications in the Internet of Things. IEEE Transactions on Parallel and Distributed Systems, 30(12), 2819-2832. https://doi.org/10.1109/TPDS.2019.2926979

How, M.L., & Cheah, S.M. (2023). Business Renaissance: Opportunities and challenges at the Dawn of the Quantum Computing Era. Businesses, 3(4), 585-605. https://doi.org/10.3390/businesses3040036

Hughes, K., Frank, V.A., Herold, M.D., & Houborg, E. (2023). Data Reuse Across International Contexts? Reflections on New Methods for International Qualitative Secondary Analysis. Qualitative Research, 23(4), 1155-1168. https://doi.org/10.1177/14687941211052278

Islam, M.M., Hasan, M.K., Islam, S., Balfaqih, M., Alzahrani, A.I., Alalwan, N., Safie, N., Bhuiyan, Z.A., Thakkar, R., & Ghazal, T.M. (2024). Enabling Pandemic-Resilient Healthcare: Narrowband Internet of Things and Edge Intelligence for Real-Time Monitoring. CAAI Transactions on Intelligence Technology. https://doi.org/10.1049/cit2.12314

Jamshed, M.A., Ali, K., Abbasi, Q.H., Imran, M.A., & Ur-Rehman, M. (2022). Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review. IEEE Sensors Journal, 22(6), 5482-5494. https://doi.org/10.1109/JSEN.2022.3148128

Jawaid, S.A. (2022). Data Protection in Organization by the Implementation of Cyber Security. https://doi.org/10.20944/preprints202211.0371.v1

Jeffrey, N., Tan, Q., & Villar, J.R. (2023). A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. Electronics, 12(15). https://doi.org/10.3390/electronics12153283

Jeffrey, N., Tan, Q., & Villar, J.R. (2024). A Hybrid Methodology for Anomaly Detection in Cyber-Physical Systems. Neurocomputing, 568. https://doi.org/10.1016/j.neucom.2023.127068

Jimmy, F.N.U. (2024). Cyber Security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS), 2(1), 129-171. https://doi.org/10.60087/jaigs.vol03.issue01.p233

Kalla, D., & Kuraku, S. (2023). Advantages, Disadvantages and Risks Associated with ChatGPT and AI on Cybersecurity. Journal of Emerging Technologies and Innovative Research, 10(10). https://ssrn.com/abstract=4619204

Kaloudi, N., & Li, J. (2020). The Ai-Based Cyber Threat Landscape: A Survey. ACM Computing Surveys (CSUR), 53(1), 1-34. https://doi.org/10.1145/3372823

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V.P. (2020). IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process. EURASIP Journal on Information Security, 1-18. https://doi.org/10.1186/s13635-020-00111-0

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in its Adoption. Applied Research in Artificial Intelligence and Cloud Computing, 6(8), 1-21.

Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. Intelligent Automation & Soft Computing, 28(2). https://doi.org/10.32604/iasc.2021.016240

Knapp, E.D. (2024). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and other Industrial Control Systems. Elsevier.

Komasawa, N. (2024). Revitalizing Postoperative Pain Management in Enhanced Recovery After Surgery via Inter-Departmental Collaboration Toward Precision Medicine: A Narrative Review. Cureus, 16(4). https://doi.org/10.7759/cureus.59031

Kordestani, M., & Saif, M. (2021). Observer-Based Attack Detection and Mitigation for Cyberphysical Systems: A Review. IEEE Systems, Man, and Cybernetics Magazine, 7(2), 35-60. https://doi.org/10.1109/MSMC.2020.3049092

Kumar, A., & Somani, G. (2022). Security Infrastructure for Cyber Attack Targeted Networks and Services. In Recent Advancements in ICT Infrastructure and Applications. Singapore: Springer Nature Singapore, 209-229. https://doi.org/10.1007/978-981-19-2374-6_9

Kunduru, A.R. (2023). Industry Best Practices on Implementing Oracle Cloud ERP Security. International Journal of Computer Trends and Technology, 71(6), 1-8. https://doi.org/10.14445/22312803/IJCTT-V71I6P101

Landoll, D. (2021). The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. CRC Press. https://doi.org/10.1201/9781003090441

Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection.

Martins, I., Resende, J.S., Sousa, P.R., Silva, S., Antunes, L., & Gama, J. (2022). Host-Based IDS: A Review and Open Issues of an Anomaly Detection System in IoT. Future Generation Computer Systems, 133, 95-113. https://doi.org/10.1016/j.future.2022.03.001

Mazhar, T., Irfan, H.M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of Cyber Security Attacks and its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods. Future Internet, 15(2), 83. https://doi.org/10.3390/fi15020083

McCall Jr, G.C. (2022). Exploring a Cyber Threat Intelligence (CTI) Approach in the Thwarting of Adversary Attacks: An Exploratory Case Study (Doctoral Dissertation, Northcentral University).

Mik-Meyer, N. (2020). Multimethod Qualitative Research. Qualitative Research, 5, 357-374.

Mishra, A., Alzoubi, Y.I., Anwar, M.J., & Gill, A.Q. (2022). Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations. Computers & Security, 120. https://doi.org/10.1016/j.cose.2022.102820

Nova, K. (2022). Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence. International Journal of Information and Cybersecurity, 6(1), 21-42.

Okunlaya, R.O., Syed Abdullah, N., & Alias, R.A. (2022). Artificial Intelligence (AI) Library Services Innovative Conceptual Framework for the Digital Transformation of University Education. Library Hi Tech, 40(6), 1869-1892. https://doi.org/10.1108/LHT-07-2021-0242

Ortega Vázquez, C., Vanden Broucke, S., & De Weerdt, J. (2023). A Two-Step Anomaly Detection Based Method for PU Classification in Imbalanced Data Sets. Data Mining and Knowledge Discovery, 37(3), 1301-1325. https://doi.org/10.1007/s10618-023-00925-9

Poth, C.N. (2019). Rigorous and Ethical Qualitative Data Reuse: Potential Perils and Promising Practices. International Journal of Qualitative Methods, 18. https://doi.org/10.1177/1609406919868870

Ruggiano, N., & Perry, T.E. (2019). Conducting Secondary Analysis of Qualitative Data: Should We, Can We, and How?. Qualitative Social Work, 18(1), 81-97. https://doi.org/10.1177/1473325017700701

Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, 15(18). https://doi.org/10.3390/su151813369

Saritac, U., Liu, X., & Wang, R. (2022). Assessment of Cybersecurity Framework in Critical Infrastructures. In 2022 IEEE Delhi Section Conference (DELCON). IEEE. 1-4. https://doi.org/10.1109/DELCON54057.2022.9753250

Saunders, M.N., Lewis, P., Thornhill, A., & Bristow, A. (2015). Understanding Research Philosophy and Approaches to Theory Development.

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT Security. Computer Science Review, 44. https://doi.org/10.1016/j.cosrev.2022.100467

Shaikh, A., Khan, A.A., Zebanaaz, S., Shaikh, S., & Akhter, N. (2021). Exploring Recent Challenges in Cyber Security and their Solutions. International Journal of Creative Research Thoughts, 9(12), 6.

Siwakoti, Y.R., Bhurtel, M., Rawat, D.B., Oest, A., & Johnson, R.C. (2023). Advances in IOT Security: Vulnerabilities, Enabled Criminal Services, Attacks and

Countermeasures. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2023.3252594

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry, 13(4), 597. https://doi.org/10.3390/sym13040597

Tahmasebi, M. (2024). Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. Journal of Information Security, 15(2), 106-133. https://doi.org/10.4236/jis.2024.152008

Talaat, F.M., & ZainEldin, H. (2023). An Improved Fire Detection Approach Based on YOLO-v8 for Smart Cities. Neural Computing and Applications, 35(28), 20939-20954. https://doi.org/10.1007/s00521-023-08809-1

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A Cybercrime Incident Architecture with Adaptive Response Policy. Computers & Security, 83, 22-37. https://doi.org/10.1016/j.cose.2019.01.011

Ukwandu, E., Farah, M.A.B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., & Bellekens, X. (2020). A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors, 20(24). https://doi.org/10.3390/s20247148

Ullah, F., Qayyum, S., Thaheem, M.J., Al-Turjman, F., & Sepasgozar, S.M. (2021). Risk management in Sustainable Smart Cities Governance: A TOE Framework. Technological Forecasting and Social Change, 167. https://doi.org/10.1016/j.techfore.2021.120743

Vanin, P., Newe, T., Dhirani, L.L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. Applied Sciences, 12(22). https://doi.org/10.3390/app122211752

Verma, P., & S. Sangle, P. (2023). Role of Digital Transformation in Inspection and Certification. In Handbook of Quality System, Accreditation and Conformity Assessment. Singapore: Springer Nature Singapore, 1-29. https://doi.org/10.1007/978-981-99-4637-2_28-1

Xie, S., Dong, S., Chen, Y., Peng, Y., & Li, X. (2021). A Novel Risk Evaluation Method for Fire and Explosion Accidents in Oil Depots Using Bow-Tie Analysis and Risk Matrix Analysis Method Based on Cloud Model Theory. Reliability Engineering & System Safety, 215. https://doi.org/10.1016/j.ress.2021.107791

Zeng, P., Fang, W., Zhang, H., & Liang, Z. (2023). Cost-Benefit Analysis of the Wuxikou Integrated Flood Management Project Considering the Effects of Flood Risk Reduction and Resettlement. International Journal of Disaster Risk Science, 14(5), 795-812. https://doi.org/10.1007/s13753-023-00520-y

Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., & Li, B. (2020). TIMiner: Automatically Extracting and Analysing Categorised Cyber Threat Intelligence from Social Data. Computers & Security, 95. https://doi.org/10.1016/j.cose.2020.101867

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic Defenses in Cyber Security: Techniques, Methods and Challenges. Digital Communications and Networks, 8(4), 422-435. https://doi.org/10.1016/j.dcan.2021.07.006

Zoppi, T., Ceccarelli, A., Capecchi, T., & Bondavalli, A. (2021). Unsupervised Anomaly Detectors to Detect Intrusions in the Current Threat Landscape. ACM/IMS Transactions on Data Science, 2(2), 1-26. https://doi.org/10.1145/3441140