Intelligent Risk Management Systems for Cybersecurity in Enterprises.

Abstract:

With the rising complexity and frequency of cyber threats, enterprises require intelligent, proactive systems that can detect and mitigate risks in real time to safeguard critical infrastructure and data. This paper presents an attack taxonomy of the proposed system, mimicking real-world attacks such as Denial of Service (DoS), Man-in-the-Middle (MitM) scenarios, and insider attacks. Some of the principal components in the system architecture include the Intrusion Detection System (IDS), the decision-making system, and the response regimen. The outputs measured in throughput, latency, packet loss, detection accuracy, and resource utilization are used to formulate simulation KPIs. Outcomes show how the system can detect, counter, and prevent risks successfully and efficiently in the overall network. Some of the evident findings involve using AI in making decisions that would eliminate false positives and increase the detection percentage. Hence, the study recommends using easily scalable artificial intelligence models to support cybersecurity frameworks and expanding simulations in the real environment.

Keywords:

Enterprise cybersecurity, intelligent risk management, AI-driven decision-making, NS3 simulation, intrusion detection, threat mitigation.

1 Introduction

1.1 Background and Motivation

The adoption of digital technologies has presented enterprises with more evens of risk in the area of cybersecurity. The rise of advanced cyber threats such as ransomware, Distributed Denial-of-Service (DDoS) attacks, and data breaches has significantly intensified security challenges for enterprises, leading to operational disruptions, financial losses, and reputational damage, particularly among small- and medium-sized enterprises (SMEs) with limited cybersecurity infrastructure (AL-Dosari and Fetais, 2023).These risks have to be controlled effectively to secure operations and enable the continuation of business, to protect data as well as to maintain public confidence in online services. While current approaches to cybersecurity can be described as well, they are usually reactive, meaning that significant losses are suffered before countermeasures are taken(Gaikwad et al., 2023). Such a tactical approach outlines the need for aa proactive and smart risk management framework that will be able to sense and counter threats in the real-time environment.

Some of the technologies that should be employed in an effective risk management system include AI, ML, and simulation-based technologies. Of these tools, the NS3 simulator has turned out to be a formidable modelling tool and used widely as a means of mimicking different attack simulations(Ambreen et al., 2023). It enables the researcher and practitioners to try out security measures and to analyze the effectiveness of these measures under simulated conditions, making it appropriate for enterprise cyber security study(Cheimonidis and Rantos, 2023). Combining NS3 simulations with techniques in artificial intelligence can further improve the possibility of an enterprise to forecast and counter cyber threats, creating a preventive cybersecurity approach.

1.2 Research Problem and Objectives

Current enterprises face a lack of intelligence in risk management, even with the increased adoption of cybersecurity technologies(Kalinin et al., 2021). While numerous existing solutions exist, these are either too niche or not very flexible and create disjointed responses to security threats(Riley and Henderson, 2010). Also, enterprises resort to having standalone tools where the components are not integrated or do not interact with each other in any way, which means the entire system can be incapable of detecting multiple level attacks.

The main concern of this research is the designing and evaluation of an Intelligent Risk Management System (IRMS) for the cybersecurity of enterprises, that are based on the NS3 simulator. Using NS3 simulation, the system models an enterprise network, identifies threats, and addresses them through smart risk mitigation involving AI and ML. The primary objectives of this research are:

- To design an intelligent risk management system using NS3 for enterprise cybersecurity.
- To simulate enterprise network environments and evaluate system performance against common cybersecurity threats like DDoS, phishing, and malware attacks.
- To develop a decision-making model that leverages AI and ML for dynamic threat detection and risk mitigation.
- To evaluate the system's effectiveness using performance metrics such as detection accuracy, response time, and false positive rates.

1.3 Contributions of the Study

This study contributes on the field of enterprise cybersecurity and intelligent risk management immensely by providing a system design that combines NS3 simulations and AI

risk management procedures("Ns-3," 2024). It performs experiments on simulation based on different attack profiles and consequent system response. A decision support system built with AI makes it easy to identify threats, respond to them, and prevent them, improving efficiency. Proper performance assessment includes measures such as the accuracy of a solution, its capacity, as well as resource utilization. Furthermore, the study is useful for improving understanding of the use of NS3 simulations in cybersecurity and suggesting possible ideas for its implementation.

1.4 Paper Structure

This paper comprises six (6) sections. Section 2 overviews current cybersecurity risk management methods with primary focus on NS3 research on network security and AI driven threat detection supplemented with the outline of the research voids. Section 3 presents the design of the proposed system in terms of detection, threat analysis, decision making, and the automated response tools together with an NS3 simulation model. Experiment scenarios of Section 4 are specified as simulation, metrics, and visual data representation outcomes. Section 5 presents results obtained in this study, effectiveness of the proposed system, study limitations, and its practical applicability. Section 6 provides a summary of the study and recommends areas of future research.

2 Literature Review

This section presents an overview of the lifecycle of cybersecurity risk management, intelligent systems for threat detection, and network simulation tools. These elements are crucial to attain for the advancement of security framework in enterprises, since the enterprises' security environment is not shrinking – instead it is growing ever complex. The review is structured into four main subsections: cyber security risk analysis in enterprise

organizations, intelligent systems on cyber security, use of network emulation tools, and NS3 in cyber security studies.

2.1 Cybersecurity Risk Management in Enterprises

Cyber security risk management refers to the process of identifying potential threats faced by an organization to secure its enterprise networks. It comprises of evaluation and managing of risks common in security(Alahmari and Duncan, 2020). Increasingly as companies integrate digital processes into their workflow, their networks also become larger and offer hackers additional opportunities to infiltrate the systems. Cybersecurity threats have been expanded considerably due to the digitalization of enterprises(Alahmari and Duncan, 2020). Rather than relying on rules and/or user-directed processes, which are typical of conventional cybersecurity architectures, current Advanced Persistent Threats are way beyond their capabilities.

An enterprise network is always at risk of being attacked through a number of malicious techniques that include data theft, ransomware, phishing, and even DDoS attacks(Romanosky and Petrun Sayers, 2024). One of the highlighted problems of organizations is threat development since the attackers are constantly changing their strategies to avoid traditional security measures. For instance, a firewall may avoid recognized threats and attacks such as polymorphic, malware may easily go past these systems by changing their characteristics(Romanosky and Petrun Sayers, 2024). Furthermore, current business structures require cloud arrangements, mobile devices, and Internet of Things (IoT) systems that elevate the attack ground and leave traditional protection models insufficient.

This has enhanced the need for enhanced active automated risk management systems which in turn have been designed to make use of advanced technologies(Sukumar et al.,

2023). The primary use of such systems is to extend the capacity for threat identification and deliver quick responses to security threats in the process of their formation. However, the efficiency of these systems demands the inclusion of real-time tracking, risk assessment models, and automated countermeasures(Sukumar et al., 2023). There is the need for the enterprises to address challenges which include limited resource, as well as skilled personnel. Of course, modern tools can support the risk management process, but even today, many companies cannot systematically approach risk management because of high costs, inadequate knowledge, or confusing security concepts.

2.2 Intelligent Systems for Cybersecurity

AI and ML with progressively interfering in cybersecurity by allowing anticipation of threats, implementing interactive actions, and using statistical predictions(Kaur et al., 2024). With steadily increasing Enterprise networks complexity, there is need for fully automated system which can detect and selectively retaliate against threats independently.

One of the most important applications of AI among the cybersecurity domain is Anomaly Detection(Mohamed, 2023). Traditional systems are preprogramed with rules, which are no use if facing an unknown entity. On the other hand, AI systems learn from data that there are normal behavior patterns and there are anomalous behavior patterns of the network. This makes it easier for them to identify other activities for example attempts at unauthorized access or data leakage.

Intrusion detection systems (IDS) also incorporate AI models that analyze network traffic, alert the system of possible incursion and learn about attacks(Nair et al., 2024). Another reason for using machine learning is that it improves the accuracy of IDS by detecting such weak and intricate patterns as may not easily be detected by analysts. Also,

forward analysis involves using past attack data to forecast future attacks that are vital for organizations to prevent.

However, AI application for cybersecurity has its challenges. To train an ML model, the data required must be top-notch because the model mirrors normal and malicious activity. Therefore, it is very important that the data is available abundant, clean, and diverse for the best performance to be observed(Jada and Mayayise, 2024). In addition, interpretability is a problem once again. The degree of complexity in the models that AI uses might cause some events to be highlighted as malicious, restricting the use of automated decision-making systems by other people. Achieving effectiveness of AI in cybersecurity and at the same time, transparency is another important area of consideration that deserves careful examination.

2.3 Network Simulation Tools in Cybersecurity Research

The use of network simulation tools has emerged as a critical technology in cyberspace research. These tools enable a researcher to replicate actual networks in real environments with actual threats and to test its security systems in conditions free from actual risk(Gomez et al., 2023). It is possible to use simulation to show how an organization's system will react when a specific attack is performed, all this with no risk of affecting the actual network.

There are many network simulation tools available to researchers and practitioners. Cisco offers Packet Tracer as a simple tool useful for configuring applied switches as well as for basic network settings creation(Veksler et al., 2018). Although using full packet capture, it is more suitable for that than Packet Tracer, this is still far from being suitable for highly complex security analysis. GNS3 is comparatively more effective for creating networks and enables users to simulate enterprise-class networks and develop extensive security configurations based on that.

There are numerous powerful simulation platforms of which NS3 is a popular open-source network simulator used for research purposes(Lee et al., 2023). This makes NS3 suitable for complex cybersecurity education since it allows for the customization of large protocols as well as the size of the network. Because the wireless simulator is open source, the researchers are free to alter the structure and architecture to fit their enhanced models, new attack models, new security measures and new routing protocols.

The part that simulation tools play in the model's assessment of cybersecurity systems is essential under various attack scenarios. They also make it possible to perform a trial of intrusion detection systems, firewalls, as well as other security arrangements, with little threat of being compromised(Ficco et al., 2017). Moreover, simulations help the researchers investigate the impact of scalability of security solutions in large and dynamic networks(Ficco et al., 2017). Fortunately, there is a group of researchers that through security lab and experimentations they can evaluate the level of security system in recognizing, prevent, contain, and healing from an array of simulated cyber threats helping them to determine its efficiency.

2.4 NS3 Simulator for Cybersecurity Applications

NS3 has fast established itself as easily the most flexible and amply adopted network simulators by researcher and academicians(Kumar et al., 2013). Its sound design facilitates the representation of different networking entities, such as routers, switches, wireless networks, and security systems. Another major strength of NS3 is its application in emulating realistic traffic and intricate attack models – critical to evaluating state-of-the-art security protocols.

Specifically for cybersecurity context, NS3 can be used to model different forms of cyber threats such as DDoS, malware and data theft(Campanile et al., 2020). Scientists are

able to replicate such attacks to study their consequences for the network, the reaction of the defense measures, and risks within enterprise systems(Abraham and Riley, 2012).Similar to NS2, NS3 can also simulate security features such as SSL/TLS, IPsec and firewalls whereby academic researchers can test their efficiency in preventing certain threats.

Nonetheless, work with NS3 has its difficulties. The above analysis shows that the simulation needs expertise in programming languages like C++ and Python, which is a cone to beginners. Moreover, when small-world models are used to perform large-scale simulations, the observer may face significant computational difficulties and may need to retrieve computing resources of a higher level(Conway, 2016). However, these restraints do not deter the fact that NS3 offers an immense amount of flexibility and reliability to model and evaluate multiple cybersecurity scenarios in all types of enterprise uses.

3 Methodology

In this chapter, the authors specify the approach to designing and assessing an IRS for enterprise cybersecurity. The approach would include using an NS3 simulator through which the actual networks can be emulated, several types of security threats can be modelled, and the impact of intelligent security systems can be judged. Our approach is divided into several key stages: The structures of the communication network, the setup of the communication network model, the definition of attack scenarios, the integration of security solutions, the performance indexes, and the assessment of the communication network and system performance.

3.1 Network Design and Simulation Setup

In the first process of the high-level, generic framework for developing a cybersecurity risk management system, there is a need to create a network as a replica of the typical

environment of an enterprise. This network must consider the shapes of the organization's structure and how information flows through this structure. In the present simulation, our main objective is to design a small to midsize enterprise network interconnecting routers, switches, servers, workstations, and other connected devices such as IoT and mobile host devices.

First, the researcher established the enterprise network in the NS3 simulator by specifying the network topology. This includes defining the kind of nodes, their connection, and the protocols these constituents communicate. The topology may vary depending on the specific use case, but for this research, a generic enterprise network topology is used, which includes:

- Core and edge routers: These form the network's core; they transport data within the organization.
- Firewalls float on strategic nodes of the network to ensure the protection of outside threats (Bedford and Sanchez, 2021).
- Intrusion Detection Systems (IDS): Embedded in various network regions for early detection of untoward events.
- Server farms and workstations: This captures critical applications and end usage within an enterprise, i.e., critical applications using the endpoints within an enterprise (Kokovin et al., 2021).

The NS3 simulator offers the simulative tools required to deploy such a network arrangement. It also works with several network protocols, such as TCP/IP, HTTP, and SSL/TLS, which are useful in realistic enterprise-level emulation(Elucidate Education, 2024). In addition, thanks to NS3, users can develop scripts that determine the behavior of the

network elements, which introduces a high degree of freedom while setting up each node and the overall traffic flow.

3.2 Modelling Cybersecurity Attacks

Once the network design is complete, the next critical step is to model various cybersecurity attacks to evaluate the effectiveness of the intelligent risk management system. As often the circumstances as enterprise threats change, the possibility of identifying new attacks in real-time and responding to them is critical in order to maintain network security. NS3 offers some modules to simulate key attacks observed in the network. Telecommunications Denial of Service (DoS) attacks involve bombarding a network with traffic, and Distributed Denial of Service (DDoS) can be simulated using multiple malicious nodes creating synthetic traffic (Serru et al., 2022). This approach only exercises the fuel on large-scale attacks, which is an ideal model for penetrating server online space.

Another active attack is a Man-in-the-Middle (MitM) attack that attacks the exchange of network communication and can also be emulated in NS3. Packet interception and modification are also allowed to assess the efficiency of some encryption protocols, for instance, SSL and TLS, in protecting information transactions (Fritz and Zhang, 2018). While NS3 cannot mimic human-targeted phishing attacks, it can mimic the impact of a malware attack. This involves undifferentiated data leakage or theft and events that are incongruous with the device or application usage, for instance, helping identify malware detection and mitigation. Further, an inside attacker threat from the insider, an employee, can be demonstrated by mimicking internal nodes and indulging in evil deeds. This facilitates the evaluation of the possible breaches resulting from trusted insiders entering the network. Altogether, all these simulations improve the system's readiness for cyber threats.

3.3 Integration of Intelligent Security Mechanisms

After the attacks are modelled, the next stage incorporates the first intelligent security measures into the network. The idea is to use security tools capable of detecting the given simulated attacks and responding to them in real-world scenarios, leaving the enterprise network secure (El Khoury et al., 2009). The analyzed intelligent systems are created using machine learning and AI, which allow the enhancement of capabilities depending on new threats evolving in the future.

3.3.1 Intrusion Detection and Prevention Systems (IDPS)

Intrusion detection systems (IDS) are important components of any organization's information security. For the context of this research, we will be incorporating an ML-based IDS with the NS3 simulated network (Khan et al., 2024). The IDS will be looking for suspicious activity that might signify an attack is imminent on the network. Once trained, the IDS uses information from past attacks and normal traffic and thus can quickly identify new attacks. Furthermore, the IDS can also be integrated with other features to detect anomalies in the network, where the machine learning algorithms establish a baseline for the behaviors of the network and learn the changes occurring in the network (Khan et al., 2024). It may be malware or an ongoing DDoS attack for cases when the system can escalate to alert or when it can block more malicious traffic.

3.3.2 Firewall Configurations and Traffic Filtering

Firewalls have remained very important in screening traffic and protecting the access of any systems within an enterprise (Chen, 2020). As for this study, the architecture of the intelligent firewalls is designed with a system for automatically generating rules based on traffic analysis. This can be easily done as the firewall has always integrated the capability to

dynamically decide on the best filtering policy based on the flow of traffic across the network as well as the threats that are being seen by it in that particular period.

The firewall can also use machine learning models to automatically calibrate the filtering of threat streams. For instance, while conducting a DDoS attack, the firewall would trigger a rate of limitations or IP restrictions. These automated responses are how the network sustains its functionality amid these threats.

3.3.3 Encryption and Secure Communication

In contained attacks like Man-in-the-Middle and data exfiltration, the network nodes must be protected with connection ports/sockets (Kotsias et al., 2023). It enshrines efficient security properties that can offer a strong antithesis to packet interception when incorporating SSL/TLS encryption. The technical potential of the NS3 simulator is that it enables researchers to perform simulations and study the outcome of applied encryption protocols on the network and its security.

3.4 Evaluation Metrics

[Table 1 near here]

3.5 Performance Analysis

The described intelligent risk management system includes several AI and ML approaches into the process of cybersecurity that has been divided into detection, classification, and response. These algorithms improve the system capability to identify, forecast and respond to threats in real time.

Anomaly detection is performed by use of unsupervised learning algorithms including K-Means clustering and autoencoder(Daah et al., 2025). These models monitor traffic in a

given network and are able to detect anomalous behavior of the traffic, thus will be able to alert the system even when faced with new kinds of attacks.

For threat classification we use supervised learning techniques like SVM, Random Forest, MLP. These models are trained fractioned sets that contain examples of normal traffic and malicious traffic and known to help the system discern between harmless and damaging activities accurately.Recurrent Neuronal Networks and Long Short-Term Memory Networks in the field of predictive analytics are used to gather relevant attack data through historical lens to predict future threats(Prabowo et al., 2023). Further, Bayesian networks are statistical models, which offer prognosis of future events based on the observed network events.

The system's intrusion response automation applies the reinforcement learning models. Of these, the proactive models modify the defensive tactics based on multiple past encounters, providing the best answer to new threats while also focusing on stinginess of materials and time.

3.6 Comparison Analysis

It is obvious that the proposed intelligent risk management system provides major improvements compared to existing cybersecurity approaches. There are old and well-known models of Internet Security like IDS, firewalls, and SIEM, which are mostly based on the use of rules and detection of known signatures (Bedford and Sanchez, 2021). These systems are adequate in extruding known threats but are weak against zero-day attacks and when confronted with complex adversarial techniques since they are typically rigid and require human intervention.

However, the proposed system employs artificial intelligence and machine learning algorithms to learn the new threats emanating from the network at a given time. There is the unique capability of using an internal anomaly-based detection method that can detect new

dangerous forms of attacks, compared to purely pattern-based approaches (Kokovin et al., 2021). Compared with the prior frameworks that can have long response times due to programmatic configurations, the proposed system offers immediate threat management with decisions made automatically.

Flexibility of operation is listed as one of the major strategic advantages. The system uses reinforcement learning enabling it adapt the threat response strategies effectively, and in a more efficient manner, than program based on rules only. It also has efficiency in terms of resources, it is smart enough to increase or decrease its operations according to the threat level, without adding extra computations.

The incorporation of NS3 simulation with self-learning analytics has not been attempted before. This allows for totality in experimenting on many types of attacks, allowing the systems to be tuned up before actual implementation (Fritz and Zhang, 2018). These capabilities combined make a statement the system is robust, adaptive and scalable cybersecurity solution suitable for the constantly changing nature of threats in the enterprise space as depicted in the following figure.

4 Results

Implementing the proposed intelligent risk management system was tested against several attack scenarios, including DoS, DDoS, MitM, malware, and insider attacks. The metrics mainly include the index of throughput, latency, packet loss, detection rate, and false positives, as well as resource consumption. It highlights metrics that are integral in determining the level of threat management and, at the same time, the ability to preserve the efficiency of the network.

4.1 Throughput Analysis

Throughput can be described as the number of messages sent over the network in time and space (Daah et al., 2025). Figure 1 illustrates how the throughput is affected by the roles and responsibilities of the models involved in each of the mentioned scenarios. The system sustains a constant throughput of 95 Mbps if normal traffic volumes are present. Nonetheless, throughput is noticeably lowered in the same environment when the site undergoes a DDoS attack, mainly due to the excessive network traffic; throughput plummets to 40Mbps at the worst part of the attack. The intelligent risk management system introduced prevents the attack, and throughput is returned to 87 Mbps, proving the system's efficiency in maintaining the integrity of the network.

[Figure 1 near here]

4.2 Latency Evaluation

The next parameter is latency, which represents the delay data goes through before reaching the next nodal point (Prabowo et al., 2023). This is normally the case throughout the experiment, as seen from the figure where the latency hovers around 10 ms (Figure 2). However, the latency significantly increases during a DDoS attack to between 100-200 ms level due to a high traffic volume, most of which is malicious. With the help of such mechanisms, the latency time is lowered to approximately 30 ms; this shows once again how the system can quickly identify attacks with high latency, and at the same time, it does not harm the normally expected latency for other legitimate traffic.

[Figure 2 near here]

4.3 Packet Loss

The other important measure is packet loss, especially against attack conditions like DDoS, since the congestion level in the network causes packets to be dropped (De Souza et al., 2020). During normal communications, the percentage of lost packets is small (1%). This was reflected in Figure 3, which showed that packet loss increased to as high as 60% during a DDoS attack. The mitigation system reduces the packet loss rate to 12%, thus proving the data transmission's stability and the attacks' adverse effects.

[Figure 3 near here]

4.4 Detection Rate and False Positives

Detection Rate and False Positives parameters provide information on the Intrusion Detection System (IDS) performance [34]. Specifically, the system yielded satisfactory security measurement results with 95% DDoS, 90% MitM, and 92% malware attacks, as depicted in Figure 4 below. The false positive rates were fairly good, at 5%, 8%, and 7% individually. This shows that not only can the system effectively identify threats, but it also does not produce high volumes of alarms that are not required.

[Figure 4 near here]

4.5 Resource Utilization

In order to determine the effectiveness of the risk management system under different resource constraints, input and output ratios such as CPU and memory were collected for analysis [35]. Normal operation of the system involved using 20 % CPU and 25 %memory. However, in attack conditions, the resource consumption is much higher, specifically over the quad-core CPU usage, which is about 80%, and the memory usage is about 75%. With

mitigation, resource utilization was controlled to such an extent that CPU had gone down to 45% and memory usage down to 50%, suggesting that the system could work optimally with available resources.

[Figure 5 near here]

4.6 Limitations and Future Improvements

Even though the above-proposed system seems to accrue several advantages, it also has certain limitations. The success of the implemented system depends significantly on the nature and the amount of data used for training the AI models (Yaokumah et al., 2023). Additional studies may target more complex intelligent technologies, including deep learning models, that might increase identification effectiveness for emerging or complex risks. Further, the simulations on real-world conditions would give more possibilities if the system was applicable, workable, and scalable.

5 Discussion

The results described in the previous section prove that the intelligent risk management system designed in this paper efficiently mitigates different types of cyber threats, such as DoS, DDoS, MitM, phishing, malware, and insider threats. It is crucial in contemporary enterprise environments for a system integrating these layers to be capable of identifying, managing, and combating these threats while preserving the performance of networks. In this chapter, the meaning of all these results will be explained, and the strengths and limitations of the proposed system will be suggested. In addition, recommendations for further enhancement of the system will be provided.

5.1 Effectiveness in Threat Detection and Mitigation

Automated intelligent learning-based risk management systems has shown high performance in a number of works dealing with different cyber threats, thus raising the probability of integrating these systems in enterprise networks. Throughput, Latency, Packet Loss, Detection Rate, FP as for KPI's are significant in evaluating the ability of the system to protect it from cyber threats.

5.1.1 Throughput Performance

Actual end-to-end throughput represents the defense of the network against cyber-attacks while forwarding genuine data traffic. During performance evaluation based on simulations, the system was still able to achieve throughput of 95 Mbps under normal load, which is characteristic of most enterprise networks. Through information during the testing phase, throughput was established to reduce to 40 Mbps during the DDoS attack as a result of high bogus traffic. Large scale attack mitigation by the system mechanisms brought back the throughput to 87 Mbps proving the efficiency of the system. Implementing of this system in actual data centers as well as cloud infrastructure may save a business from network freezing and preserve it consequently emphasizing on its importance in enterprise environment where any disruption of operations may cause critical losses.

5.1.2 Latency and Packet Loss

High availability is preferred in applications that have low tolerance for delay in transactions, voice-conference calls, and industrial processes. In normal circumstances voluntary motion was sustained at approximately 10ms latency which is ideal for enterprise applications. While responding to a DDoS attack emulation, the latency as high as 200ms because the networks got congested but, the system was able to reduce it to 30ms. In real-world scenarios it can

facilitate assure the operation of these latency-sensitive applications such as Video Conferencing, Online Banking, Tele-medicine etc.

Packet loss another important parameter as far as the quality of the conversation is concerned was at 1% under normal circumstances and then spiked up to 60% during the DDoS attack. Packets were lost at only 12 percent, from the intelligent system's adaptive response mechanisms. Based on this performance, it is perhaps testament that real-world applications like media streaming, VoIP services and cloud-based storage could stand to gain from reduced packet loss rates implying higher packet data integrity and quality of service.

5.1.3 Detective Rate and False Positive

It is therefore important that intrusions detection systems (IDS) achieve high value of detection rate and lower false positive rate for it to be effective in real world. According to the results obtained, the system had a success rate of 95% in detecting DDoS attacks, 90% in detecting MitM and 92% in detecting malware attacks. These numbers provide information that the system is a successful in identifying and combating various kinds of cyber threats. In corporate networks or government infrastructures where data is often an object of virus attacks, such a system may help to protect from serious damage as the virus is recognized within the first few hours after its penetration.

Incident is always a non-trivial problem throughout the cybersecurity process since they produce false alarms and take time. Overall, the system was able to generate minimal false positives of 5% for DDoS, 8% for MitM and 7% for malware attacks. This is especially useful in the real world today where IT security teams are often overwhelmed by numerous alerts that are not very accurate most of the time. Applying this system, in large enterprises, could help make the security processes operational less cluttered while eliminating noise about false alarms that only obscure real threats.

5.1.4 Real-World Deployment

The models inherent to the proposed self-learning risk management system, derived from artificial intelligence, allow the system to learn by analyzing past occurrences and solving the problem of refining the detection algorithms. This continuous improvement process is especially good for implementation in cloud computing systems, smart city systems, and industrial systems where new dangers are constantly being developed. When it becomes embedded in critical systems ranging from power and energy, transportation, and financial sectors, it can complement national cybersecurity architectures.

As a potential application, the resulting system of automated and real-time threat detection and prevention in the presented framework could become the basis for managed security services and enterprise Security Operation Centers (SOCs). By its capacity to deliver high network performance, low packet loss rates, low latency, and low false positives, it is ideal for massive scalability, and where system downtimes and unauthorized access costs businesses financially, and tarnishes their reputation.

5.2 Resource Utilization and Efficiency

Among the effective cybersecurity measures, the question of their resource utilization is one of the most important. Several cybersecurity controls, such as AI and machine learning, can be complex and computationally expensive. High use of the scheme can lead to network degradation, which is not good for enterprise-class networks where resource conservation is important (Nisa et al.,2024).

In normal operating conditions, the system consumes 20% of the CPU and 25% of the server's memory. These levels of resource consumption are characteristic of a system running with the highest efficiency. However, during an attack, the usage of resources in the system was greatly augmented. For instance, CPU usage was 80%, and memory usage was 75%

during DDoS attacks. Higher usage of resources is quite reasonable in times of traffic peak since the system has to navigate through vast amounts of data to find that it is under attack.

The known fact is the system patent's remarkable capacity to adjust resource throughput during the attack. After implementing risk management measures, CPU usage decreased to 45% and memory usage to 50%, even during a DDoS attack. This proves that the system accomplishes the integration of the computing resources in a way that optimizes the security mechanisms without burdening the network with a slowdown. Effective resource management must be maintained to keep a network's overall health without compromising security mechanisms as a potential chokepoint.

5.3 System Limitations

Even though the intelligent risk management system highlighted the far-reaching advantages of identifying and containing cyber-attacks, the following limitations were identified. A major drawback is the fact that the operational capabilities of the system are directly proportional to the amount of training data fed into the machines that learn algorithms. Traditional intrusion detection techniques rely on large volumes of high-quality data to properly function machine learning-based IDS (Nisa et al., 2024). If the training data is inadequate or contains attacks that are not close to real-life attacks, the system's performance goes down, and the system may either give out a lot of false alarms or fail to detect actual attacks.

Moreover, even though the system is extremely successful in identifying existing threats, the scheme's effectiveness in identifying inventive, new, and unseen patterns of attacks may be low (Nisa etal., 2024). The existing system may consist of well-acknowledged attack types like DDoS, MitM, and malware; however, deep learning may improve the

achievement of the system and the likelihood of learning the unknown and advanced attacks that can merely be spotted with the earlier learning.

The last challenge is the explainability of various AI models incorporated into the system. The problem with complex machine learning is that as the models get more diverse, a question like 'Why did the system categorize this particular event as malicious?' becomes difficult to answer (Nagarajan andSvn, 2025). This lack of transparency may be a disadvantage when it comes to trusting the system that makes security decisions, and the security teams may only be partially dependent on this system to make major decisions. The interpretability of the constructed models remains a problem in cybersecurity systems using AI, and potential investigations could enhance the explainability of the models for better comprehension of threats detected by security teams.

5.4 Future Directions

Future research and development of the presented intelligent risk management system may include the application of other innovative technologies including deep learning, quantum cryptography, blockchain and others to improve the system’s resilience to new types of cyber threats.

5.4.1 Integration of Deep Learning

We suggest to extend the functionality of the system with deep learning models, especially recurrent neural networks (RNNs) and convolutional neural networks (CNNs) that would enhance the detection of previously unknown sophisticated cyber threats. These models are capable of handling high amounts of traffic data from the network and identifying subtle patterns and deviations which suggest new attack methods(Campanile et al., 2020). For example, extending the use of long short-term memory (LSTM) networks could improve the

system's capability in the detection of persistent and complex attacks such as the Advanced Persistent Threats that may take many days to complete. Further work can look at the practical applicability of these models for real-time threat identification systems, including the questions of their scalability and performance.

5.4.2 Application of Quantum Cryptography

The use of quantum cryptography can be incorporated in the data transfer communication system in the event that the system required high level of security against interceptions and or alterations. Quantum Key Distribution (QKD) will help in making the keys for encrypting information exchanged in such a way that data transmission is almost impenetrable to eavesdropping(Bedford and Sanchez, 2021). Applying this technology in the proposed system could improve its adaption to critical data transmission environment, which is characteristic of financial and governmental networks. One idea for future work is the construction of field experiments concerning the feasibility of including QKD into conventional enterprise information security systems.

5.4.3 Blockchain on Threat Intelligence Sharing

It is suggested that blockchain technology might be used to establish a distributed and immutable threat intelligence sharing platform. Whenever an attack signature or threat reports are captured on the distributed ledger, organizations can share live TIP that is secure and easily accessible(Khan et al., 2024). This would allow the system to tap on a larger source of threat information and therefore would improve the predictive analysis and response of the system. While the use of blockchain for protecting a nation's critical infrastructure is presented in Mahmoodi and Rial's article, the authors are right to suggest that more significant research into real-world applicability of blockchain and its integration with the

current cybersecurity architecture would be needed if one is to apply their concept in practice.

5.5 Future Research Directions

For the further validation of the system performance in terms of the given parameters under real-world scenarios, it is recommended to extend the simulation space and design it based on the enterprise-level network environments(Wakili et al.,2024).This would draw attention to how fast the data intensive computations are, how much resources are used, and how well the computational system scales up. Moreover, threat intelligence data amalgamation across networks firewalls, IPS and end-point devices could be another form of an ensemble threat detection framework. A single chain of processing the obtained information using the big data frameworks like Apache Kafka or Apache Spark might be employed for the immediate identification and elimination of attacks.

6 Conclusion

This paper discusses the design, implementation, and assessment of an integrated intelligent risk management system for enterprise networks. It considers its effectiveness in identifying and preventing cyber threats such as DDoS, MitM, malware, phishing, and insider threats. The measurement criteria used to evaluate the system included throughput, latency, packet loss, detection rate, false positive, and resource usage. The results indicated the system's ability to effectively mitigate threats to an enterprise network while keeping the network performance fairly tolerable across the board.

Throughput and latency analysis showed that overall, the system could handle DDoS attacks and successfully brought throughput back to normal while controlling the latency and minimizing the packet drops. This is well illustrated by the high detection rates and low false positive rates of the intrusion detection system, which portrays the extent of success of this

system in detecting anti-social activities. Also, it further showcased that it was resource-friendly – the system leveraged the available resources with little compromise of the network throughput during the attack phases.

However, while the system has brought impressive results, there are restrictions: the requirement for high-quality training datasets and the issues of using machine learning to act as an 'oracle.' However, I recognize that there are areas where future work can especially focus on overcoming present limitations, such as the incorporation of artificial intelligence, the simulation of the system in actual environments, and the collection of more informative data from other sources to enhance its threat assessment.

7 Acknowledgement

The author would like to express sincere gratitude to his supervisor and co-author for valuable guidance, insightful comments, and continuous academic support throughout the development of this research. The author also gratefully acknowledges the financial support provided by the funding bodies that made this study possible.

Special thanks are extended to friends and colleagues who provided helpful discussions, constructive feedback, and encouragement during the writing and revision of this manuscript.

Finally, the author would like to express heartfelt appreciation to his girlfriend for her patience, understanding, and unwavering emotional support throughout the research and writing process.

8 Funding

This work was supported by the Excellent Scientific Research and Innovation Team Support Project of Universities and Colleges in Anhui Province [grant number 2022AH010054], and the Major National Social Science Fund Project [grant number 22ZDA112]. The funding

sources had no involvement in the study design, data collection, analysis and interpretation of data, writing of the report, or the decision to submit the article for publication.

9 References

Abraham, J., Riley, G., 2012. Simulator-Agnostic ns-3 Applications. Brussels: ICST Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, pp. 391–396.

Al-Dosari, K., Fetais, N., 2023. Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. Electronics 12 (17), 3629.

Alahmari, A., Duncan, B., 2020. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In: Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE, Dublin, pp. 1–5.

Ambreen, L., Jain, M., Yadav, R.K., Loonkar, S., 2023. Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. Multidisciplinary Reviews 6, e2023ss080.

Bedford, D., Sanchez, T.W., 2021. Network structures and components. In: Working Methods for Knowledge Management. Emerald Publishing Limited, Leeds, pp. 21–32.

Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., Mastroianni, M., 2020. Computer network simulation with ns-3: A systematic literature review. Electronics 9 (2), 272.

Chen, X., 2020. A security integration model for private data of intelligent mobile communication based on edge computing. Computers & Communications 162, 204–211.

Cheimonidis, P., Rantos, K., 2023. Dynamic risk assessment in cybersecurity: A systematic literature review. Future Internet 15 (10), 324.

Conway, A.E., 2016. A cloud-based service for generating ns-3 network simulation programs. In: Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS). IEEE, Montreal, pp. 1–8.

Daah, C., Qureshi, A., Awan, I., Konur, S., 2025. Simulation-based evaluation of advanced threat detection and response in financial industry networks using zero trust and blockchain technology. Simulation Modelling Practice and Theory 138, 103027.

De Souza, E., Ardakanian, O., Nikolaidis, I., 2020. A co-simulation platform for evaluating cyber security and control applications in the smart grid. In: Proceedings of the IEEE International Conference on Communications (ICC). IEEE, Dublin, pp. 1–7.

El Khoury, P., Hacid, M.-S., Sinha, S.K., Coquery, E., 2009. A study on recent trends on integration of security mechanisms. In: Studies in Computational Intelligence. Springer, Berlin, pp. 203–224.

Elucidate Education, 2024. Network components. Available at:https://www.elucidate.org.au/content/network-components (accessed 11 December 2024).

Ficco, M., Choraś, M., Kozik, R., 2017. Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. Journal of Computational Science 22, 179–186.

Fritz, R., Zhang, P., 2018. Modeling and detection of cyber attacks on discrete event systems. IFAC-PapersOnLine 51 (7), 285–290.

Gaikwad, A.P., Kakpure, K.B., Landge, A.A., Kulkarni, S.G., Jadhav, M.P., Tiwari, M., 2023. Cybersecurity risk management: A complete framework for IT enterprises. In: Proceedings of the IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). IEEE, Gautam Buddha Nagar, pp. 602–607.

Gomez, J., Kfoury, E.F., Crichigno, J., Srivastava, G., 2023. A survey on network simulators, emulators, and testbeds used for research and education. Computer Networks 237, 109993.

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

Kalinin, M., Krundyshev, V., Zegzhda, P., 2021. Cybersecurity risk assessment in smart city infrastructures. Machines 9 (4), 78.

Kaur, R., Gabrijelčič, D., Klobučar, T., 2024. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion 97, 101807.

Khan, B.U.I., Goh, K.W., Khan, A.R., Zuhairi, M.F., Chaimanee, M., 2024. Integrating AI and blockchain for enhanced data security in IoT-driven smart cities. Processes 12 (9), 1825.

Kokovin, V.A., Evsikov, A.A., Diagilev, V.I., Skvortsov, V.V., Uvaysov, S.U., Uvaysova, A.S., 2021. Design of functional networking components as elements of an industrial ecosystem. In: Proceedings of the International Seminar on Electron Devices Design and Production (SED). IEEE, Prague, pp. 1–5.

Kotsias, J., Ahmad, A., Scheepers, R., 2023. Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems 32 (1), 35–51.

Kumar, A.R.A., Rao, S.V., Goswami, D., 2013. NS3 simulator for a study of data center networks. In: Proceedings of the IEEE International Symposium on Parallel and Distributed Computing. IEEE, Bucharest, pp. 224–231.

Lee, D.-H., Kim, C.-M., Song, H.-S., Lee, Y.-H., Chung, W.-S., 2023. Simulation-based cybersecurity testing and evaluation method for connected car V2X application using virtual machine. Sensors 23 (3), 1421.

Mohamed, N., 2023. Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering 10 (2), 2272358.

Nagarajan, S., Svn, S.K., 2025. An intelligent sailfish optimization-based fault diagnosis and classification in wireless sensor networks. Peer-to-Peer Networking and Applications 18 (1), 1–22.

Nair, M.M., Deshmukh, A., Tyagi, A.K., 2024. Artificial intelligence for cyber security: Current trends and future challenges. In: Automated Secure Computing for Next-Generation Systems. Wiley, New Jersey, pp. 83–114.

Nisa, N., Khan, A.S., Ahmad, Z., Abdullah, J., 2024. TPAAD: Two-phase authentication system for denial of service attack detection and mitigation using machine learning in software-defined networks. International Journal of Network Management 34 (3), e2258.

Ns-3, 2024. Ns-3 network simulator. Available at: https://www.nsnam.org/ (accessed 11 December 2024).

Prabowo, W.A., Fauziah, K., Nahrowi, A.S., Faiz, M.N., Muhammad, A.W., 2023. Strengthening network security: Evaluation of intrusion detection and prevention systems tools in networking systems. International Journal of Advanced Computer Science and Applications 14 (9).

686 Riley, G.F., Henderson, T.R., 2010. The ns-3 network simulator. In: Modeling and Tools for
687 Network Simulation. Springer, Berlin, pp. 15–34

688 Romanosky, S., Petrun Sayers, E.L., 2024. Enterprise risk management: How do firms
689 integrate cyber risk? Management Research Review 47 (1), 1–17.

690 Serru, T., Nguyen, N., Batteux, M., Rauzy, A., 2022. Modelingcyberattack propagation and
691 impacts on cyber-physical system safety: An experiment. Electronics 12 (1), 77.

692 Sukumar, A., Mahdiraji, H.A., Jafari-Sadeghi, V., 2023. Cyber risk assessment in small and
693 medium-sized enterprises: A multilevel decision-making approach for small e-tailors. Risk
694 Analysis 43 (10), 2082–2098.

695 Veksler, V.D., Buchler, N., Hoffman, B.E., Cassenti, D.N., Sample, C., Sugrim, S., 2018.
696 Simulations in cyber-security: A review of cognitive modeling of network attackers,
697 defenders, and users. Frontiers in Psychology 9, 691.

698 Wakili, A., Bakkali, S., Alaoui, A.E.H., 2024. Machine learning for QoS and security
699 enhancement of RPL in IoT-enabled wireless sensors. Sensors International 5, 100289.

700 Yaokumah, W., Baidoo, C.Y.M., Owusu, E., 2023. Measuring throughput and latency of
701 machine learning techniques for intrusion detection. In: Advances in Computational
702 Intelligence and Robotics. IGI Global, Hershey, PA, pp. 27–49.

703