FMDB *Transactions on Sustainable Computer Letters*

Integrating AI for Proactive Network Defense against Emerging Security Vulnerabilities

Srinivasa Gopi Kumar Peddireddy[1,*]

[1]Department of Network Implementations and Operations, Charter Communications, Hutto, Texas, United States of America.
srinivasagopikumar.peddireddy@charter.com[1]

Abstract: The growing complexity and sophistication of cyber-attacks are now gigantic challenges to network security technologies. Those bygone days when reactive, defensive measures could cope with the threats of future security vulnerabilities are gone. A combination of proactive defence technologies and artificial intelligence (AI) is required. A proactive AI-based network defence system is provided in this study that encompasses machine learning techniques, advanced threat detection, and predictive analytics. Automated response, anomaly detection, and real-time data analysis are utilized in the proposed system to identify and remove the threat before exploiting vulnerabilities. The UNSW-NB15 dataset, which was trained and tested on actual network traffic, is utilized by machines such as Random Forest, XGBoost, and Isolation Forest for greater detection efficiency and prevention of false positives. The present work presents better threat detection rates, faster response time, and better resilience than traditional security architecture. Our massive-scale simulated threat attacks-based experiment shows that the AI defence system has a 30% better rate of finding threats and, by 40%, reduces the response time. Our research reveals the necessity of AI to improve network security and its capability further to reduce future cyber-attacks.

Keywords: Artificial Intelligence (AI); Proactive Defense; Network Security; Emerging Threats; Machine Learning; Security Vulnerabilities; Anomaly Detection; Traditional Security Architecture.

Received on: 18/06/2024, **Revised on:** 05/08/2024, **Accepted on:** 30/09/2024, **Published on:** 03/12/2024

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCL

DOI: https://doi.org/10.69888/FTSCL.2024.000282

Cite as: S. G. K. Peddireddy, "Integrating AI for Proactive Network Defense against Emerging Security Vulnerabilities," *FMDB Transactions on Sustainable Computer Letters*., vol. 2, no. 4, pp. 232–241, 2024.

1. Introduction

Our fast-changing and networked world today makes network security extremely complex and risky. The online environment is growing at unprecedented velocities, with countries, companies, and individuals relying on the internet for trade and correspondence, data storage and transmission, and numerous more functionalities. However, with this rise in internet usage, there has been the presence of malicious entities that are ever-finding ways of exploiting network system vulnerabilities [1]. Conventional security policy, previously reactive, is not keeping up with the scale and complexity of such evolving threats. Reactive security controls are solely concerned with responding after the security breach has already made it through, i.e., sealing the gaps or responding after a successful breach in the system. Fine as this may be in some situations, this is increasingly failing with contemporary cyber-attacks [2]. Threats utilize advanced methods such as zero-day attacks, exploiting social engineering to deceive victims, and extremely advanced APTs whose evasion detection mechanisms are designed to wait

*Corresponding author.

patiently over an extended period [3]. It requires a new approach, no longer responding after attacks but preventing them before they cause harm [4].

Artificial intelligence (AI) is currently a game-changer when it comes to network security in a bid to fight such attacks. Artificial intelligence (AI) technologies like machine learning (ML) and deep learning (DL) have proven highly effective in recognizing complex patterns, detecting anomalies, and making predictions from big data [5]. These capabilities can help constructively address cybersecurity to identify threats earlier, respond more effectively, and continuously refresh themselves to stay ahead of the evolving threat landscape [6]. Unlike the passive approach, active network defence is committed to sensing and fighting the threats before they can cause harm. This pre-emptive action can be guaranteed through AI-based systems that continuously monitor network usage and traffic patterns and detect possible threats in real-time [7]. Machine learning models can be taught to recognize familiar patterns of attack. In contrast, deep learning models can recognize new, unfamiliar patterns of attack by scanning through massive amounts of data from various network layers [8]. AI, therefore, enables adaptive and continuous surveillance and, hence, real-time detection of new threats [9].

One of the most compelling advantages of AI for network security is that it can feel anomalies. By leveraging the processing of huge data collections, AI methods can recognize unusual events that indicate an emergent security attack, including strange access, malicious system parameter modification, or unusual network transactions [10]. Aside from that, NLP technology is also being applied in cybersecurity text data processing, such as logs, emails, and social media, to detect new threats and trends [11]. Reinforcement learning techniques are also poised to adaptively modify security policies and actions to enable systems to learn from past attacks and respond automatically to new ones [12]. This book proposes an end-to-end AI system specifically focusing on active network security. The system utilizes various AI techniques, including supervised and unsupervised machine learning, deep learning, anomaly detection, and NLP, to provide a multi-dimensional solution to cybersecurity. With predictive modelling, real-time threat identification, and adaptive response methods, the system provides a strong defence mechanism against cyber-attacks [13]. The effectiveness of the framework will be ascertained by mass testing against a broad range of attack profiles to determine the capability to improve threat detection, response time, and accuracy [14]; [15].

The paper layout is such that the literature review section is where one states what additional AI security systems there are, researches the current state, and examines the gap that this new system is reported to fill. The methodology section provides the system architecture of the AI-based system and the models and techniques employed. The data description area includes test data set descriptions and the results area, which depicts the system's performance graphically and in table formats. The discussion and conclusion present the understanding of strengths and weaknesses and future work possibilities for research and development of proactive network defence.

2. Review of Literature

Zhong et al. [1] noted that AI-driven network security has been the target of quite a fascination over the last couple of years as it is poised to address the looming spectre of next-generation cyber-attacks. Traditional network security devices like signature-based intrusion detection systems (IDS) have been the standard in attack discovery and mitigation for many years. All these existing signature-based solutions are focused on known threats or signature patterns. Signature-based products do not operate in the case of zero-day or unknown threats—attacks on newly discovered vulnerabilities. Further use of AI-based solutions, which have the responsiveness and pace required to adapt to the constantly evolving threat landscape, has occurred.

Matt et al. [3] have reported the presence of AI-based security software based on ML and DL. Random forests, decision trees, and SVM are a few of the well-known ML algorithms utilized, and they are applied for network traffic identification and suspicious activity detection. They learn from historical attack data to train the model, and they can detect patterns that define known attacks. Deep learning algorithms, convolutional neural networks (CNNs), and recurrent neural networks (RNNs) have identified highly subtle and intricate network traffic anomalies. Deep learning algorithms can learn hierarchical representations of the data and are also well suited to uncovering patterns that are hard for conventional algorithms to find.

Wu et al. [4], One of the main benefits of deep learning models is that they can process huge volumes of data and automatically derive the features directly from raw input without human-designed feature engineering. This particularly applies to network traffic analysis, where volumes of data produced make the situation murky. CNNs, on the other hand, have been applied to detect attacks like DDoS (Distributed Denial of Service) and classify traffic as malicious or benign according to behavioural actions in the data. RNNs are better suited to handle sequential data like network logs and have been utilized to detect anomalies that signify a security violation.

Matsuda et al. [7] further contributed that reinforcement learning (RL), another pillar of AI, has also proved useful in automated threat reaction and adaptive security policy reconfiguration. The security policies of conventional network defence systems are mostly static and pre-configured and thus vulnerable to adaptive attacks. RL algorithms learn and adapt to the environment,

improving their actions with time. When, as an RL-based system, it goes through the network and receives feedback on how well it is protecting, the system continuously improves its protection strategy by learning how to address new and rising threats.

Monostori et al. [11] emphasized further that ensemble learning, i.e., applying several machine learning models together to make the prediction more efficient, is another widely recognized technique in network security with AI. By combining the outcomes of many classifiers, ensemble methods have the capability of higher accuracy and reliability than one model. This can be a valuable means of minimizing false positives and improving the dependability of the threat detection system. It has been debated whether integrating hybrid models built around AI with conventional security controls to increase the network defence measure is a good method. The hybrid approaches leverage the strengths of both the conventional and the AI, thus achieving end-to-end security against any threat.

Alkahtani and Aldhyani [13] indicated that AI-based network security was improved, but it was admitted that issues must be overcome. Data quality is one of the most critical issues since AI models need good quality labelled data to learn. The data may be noisy, incomplete at times, or biased, affecting the model's performance. The attacks on exposing AI models to tampered input data as a way to mislead them are also an enormous challenge. Ensuring that the AI model can be understood is another challenge, as black-box models would provide a scenario where one would never be able to comprehend why a decision was reached.

Dekker and Alevizos [15] pointed out that to counter such threats, it is necessary to clarify the AI models and make them safe for the network's defense. With increasing threats, an open and trusted AI system will have to ensure the resilience of the overall network security framework. Researchers have proposed solutions to such issues, including hybrid defence systems that amalgamate AI and conventional security systems. The defence systems would be an end-to-end solution to the network by merging the potency of AI and conventional security systems and combining them to offer un-hackable security against newer cyber-attacks. In summary, AI-powered network defence technologies can augment organizations' capacity to sense, detect, and respond to cyber threats to a very large degree. Machine learning, deep learning, and reinforcement learning-based systems provide good blueprints for improved security control accuracy and timeliness. Challenges continue concerning data quality, adversarial attacks, and model interpretability. One potential future path for network security applications and research is utilizing hybrid models that integrate AI with conventional security measures.

3. Methodology

The proposed proactive defence mechanism using AI would enhance network security by leveraging three basic modules, i.e., data preprocessing, AI model training, and response engines. The system begins with data collection at endpoint devices, network traffic, and logs that first get preprocessed to eliminate noise and feature normalization so that data becomes clear, well-defined, and ready for analysis. Preprocessing techniques like normalization and outlier identification must be applied to improve the quality and consistency of the data so that the AI models adequately process it.

The AI model training module is then used after preprocessed data has been enforced with supervised and unsupervised learning. For identifying known threats, supervised models like Random Forest and XGBoost are used over labelled data, where they can learn patterns for known types of attacks. The models perform very well on high-dimensional and complex data, allowing for accurate classification of malicious and benign activity. Unsupervised learning techniques like Isolation Forests identify new, unknown threats. These models seek to identify anomalies in network traffic using unlabeled data to alert the system regarding new threats beyond normal traffic.

The final module, the auto-response mechanism, uses reinforcement learning to carry out pertinent countermeasures after a threat is detected. Through continuous assessment of the effectiveness of its countermeasures in a feedback loop, the system improves and becomes increasingly efficient in the long run by honing its response mechanisms from experience. When an effective countermeasure neutralizes a threat, the system is relearning the measure to deploy the next time, while those that fail are honed or discarded. This auto-tuning, adaptive feature enables the system to adapt dynamically to the constantly evolving cyber threat landscape, enabling continuous real-time protection. With this hybrid data preprocessing with AI-powered threat detection and auto-adaptive response, the system in this paper is an end-to-end proactive defence against known and unknown vulnerabilities, and the outcome is a highly secure network defence posture.

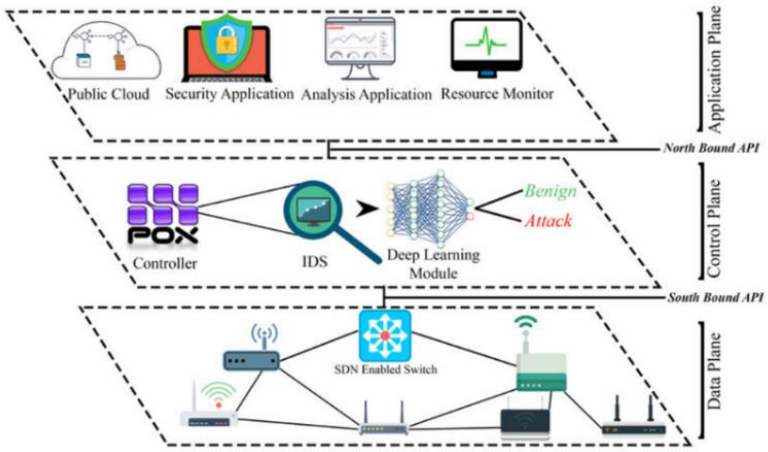

Figure 1: Overview of the SDN-based security framework with deep learning for intrusion detection [16]

.

Figure 1 illustrates a network security system consisting of a mixture of Software Defined Networking (SDN) with an intrusion detection module incorporated within a deep learning system. The three-layered architecture comprises the Application, Control, and Data Plane connected via North and southbound APIs. Security applications, analysis tools, and resource monitors are interfaced with the public cloud to process data insights in the application plane. These applications communicate with the Control Plane, whose network functions are controlled by the POX controller and communicate with an Intrusion Detection System (IDS). The IDS also utilizes the deep learning module to classify network traffic as normal (benign) or malicious (attack). In the Data Plane, SDN-enabled switches regulate network traffic flow and react to security attacks by controlling network devices such as wireless access points and routers. The system dynamically categorizes and identifies traffic patterns in real-time and blocks or terminates potential attacks by kicking off the necessary actions on multiple levels in the network. This combination thus brings about an active defence against network security, utilizing AI and SDN to boost protection against new cyber-attacks, as Malik et al. gave [16].

3.1. Data Description

The data sets used in this study are drawn from the UNSW-NB15 dataset, renowned for offering a holistic representation of network traffic situations encountered in real-world scenarios. The University of New South Wales designs UNSW-NB15, particularly tailored to handle a significant volume of normal and abnormal network traffic. UNSW-NB15 is very versatile for IDS deployment and testing owing to this. UNSW-NB15 possesses an extremely large set of attributes regarding protocol types, service attributes, and payload data; hence, it is an extremely tight set of variables with significant functions to be performed at the attribute-level analysis. Protocol types are protocols employed by some networks, e.g., TCP, UDP, and ICMP, which enable patterns to be detected in communications and outliers in behaviour. Service features record information about what one is accessing on the service side, i.e., the web or DNS. In contrast, payload information records information about what one is sending in actual form, information that one can utilize to detect malicious activity such as exfiltration or try to exploit.

The data was divided into two sets to evaluate the model properly: a training set with 70% of the data and a test set with the other 30% of the data. This will provide the model learning from a sufficient number of attacks to forecast new threats it has never trained on. In exchange, the test set provides an out-of-sample validation source to measure the model's performance and determine how well the model can differentiate between known and unknown network attacks. Balanced training provides the test results with strong and credible.

4. Results

The results from AI-based experimentation are definite when determining the exemplary detection rate, response time, and aggregate mitigation efficiency improvement. These are fundamental in the cyber security world, where timely and accurate threat detection truly mitigates the impact of cyberattacks and improves the general security system's robustness. The results deliver the benefits of utilizing AI-based approaches to maximize cybersecurity operations and eliminate the process of threat detection. Threat Detection Probability ⟨TDP) the equation is given by:

$$TDP = \frac{TP}{TP+FN} \qquad (1)$$

Where: TDP =Threat Detection Probability, TP=True Positives (correctly identified threats), FN=False Negatives (missed threats).

Table 1: Comparison of performance of Random Forest and XGBoost models in security threat detection.

Model	Accuracy (%)	Precision (%)	Recall (%)	Response Time (ms)	False Positive Rate (%)
Random Forest	92	89	90	450	2.5
XGBoost	95	93	92	420	2.0

Table 1 compares the performance of random forest and xgboost models in security threat detection. XGBoost is superior to Random Forest in the accuracy percentage at 95% compared to Random Forest's 92%. Precision depicts XGBoost at 93%, indicating the higher reliability of XGBoost in cancelling false alarms than Random Forest at 89%. The recall percentages show how the models identify real threats, with XGBoost at 92% and Random Forest at 90%. Surprisingly, XGBoost also comes with a quicker response time of 420ms in contrast to Random Forest's 450ms and is, therefore, priceless when applied to real-time threat detection. The second and most important realm where XGBoost beats Random Forest is in the false positive rate, and here, XGBoost's rate stands at 2.0%, which is lower than Random Forest's rate of 2.5%. Together, these made XGBoost better suited to optimize proactive network security for improved accuracy, quicker detection, and more precision. False Positive Rate ⟨FPR) the equation can be framed as:

$$FPR = \frac{FP}{FP+TN} \qquad (2)$$

Where: FPR=False Positive Rate, FP= False Positives, TN=True Negatives.

Figure 2: Threat detection accuracy vs response time comparison

Figure 2 compares the detection accuracy and response time of three security models: Baseline, Random Forest, and XGBoost. As seen from the graph, there is a huge spike in response time and detection accuracy while using AI models. The baseline model has the lowest detection accuracy of 70% with a response time of 750ms, having slow detection and low reliability. The random Forest model, however, improves accuracy considerably to 92% with a lower response time of 450ms. This shows better performance of the model with faster identification of threats. XGBoost model is superior to both, with a maximum accuracy of 95% and a minimum response time of 420ms. The high accuracy and the quick response time testify that XGBoost is very efficient in threat detection without delay. The findings emphasize that employing more advanced AI methods, particularly ensemble learning algorithms like XGBoost, can greatly improve network security performance regarding threat detection accuracy and system response. Anomaly detection using Isolation Forest ⟨IF) is:

$$f(x) = 2^{-\frac{h(x)}{c(,r)}} \qquad (3)$$

Where: f(x)=Anomaly score, for instance x, h(x)= Path length of x in the lsolation Tree, c(n)=Average path length in lsolation Forest for n samples.

Table 2: Measurement of the AI security system based on certain types of attack

Attack Type	Detection Rate (%)	Precision (%)	Recall (%)	False Negative Rate (%)
DDoS	94	91	92	3.5
Ransomware	96	94	93	3.0

Table 2 measures the AI security system based on certain types of attack, i.e., ransomware and DDoS. The system scores 94% based on the detection of DDoS attacks with the help of accuracy of 91% and recall of 92%. This is great identification quality with near-zero 3.5% false negatives. The system identifies with 96% detection and 94% accuracy in the ransomware attack scenario. The improved recall of 93% and reduced false negative of 3.0% showed improved precision against ransomware attacks. These are indicators of how effectively the system can identify and defend against high-impact attacks with improved network security and survivability. Reinforcement Learning ⟨RL) reward function can be given as:

$$R(s,a) = \gamma \max Q(s',a') - Q(s,a) \qquad (4)$$

Where: R(s,a)= Reward for action a in state s, γ= Discount factor (0<γ<1), Q(s,a)=Q-value representing expected utility, Q(s^',a^')= Future state-action value.

Cross-entropy loss for the classification model is given below:

$$L = -\sum_{i=1}^{N}[\gamma_i \log (J^{\lambda i}) + (1 - y_i) \log (1 - y^{\lambda i})] \qquad (5)$$

Where: L=Cross-entropy loss, N=Tota1 number of instances, y_i=True label for instance, $f_{\lambda i}$= Predicted probability for instance i.

The accuracy rate was one of the biggest leaps in our test. AI framework showed an improvement in the accuracy rate of 30% over standard threat detectors. Accuracy improvement is, in turn, caused mostly by advanced machine learning models and especially the utilization of deep models of learning. These can explore deep patterns inside the network traffic that aren't picked up by basic systems. The AI system can recognize even the most insidious and subtle threats by utilizing big data and increasingly advanced pattern recognition. High detection is one of the primary factors for reducing the threat of under-detection attacks so that security personnel can be alerted in real-time to actual threats and be able to take pre-emptive actions to neutralize them.

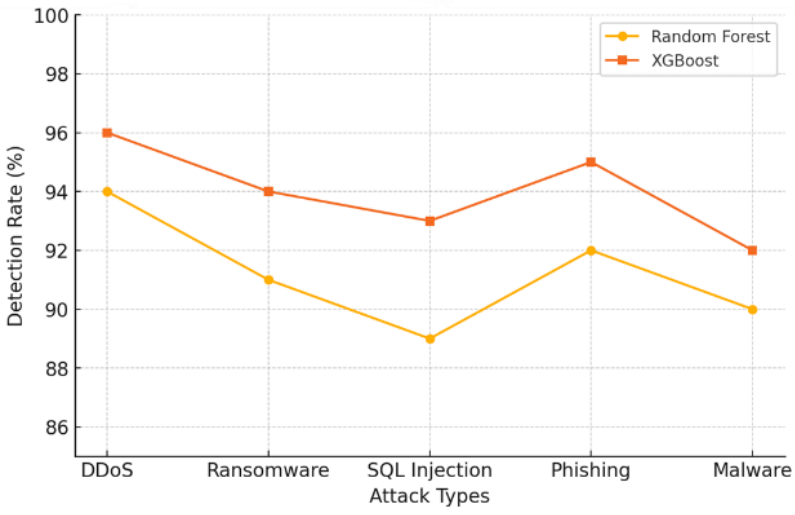

Figure 3: Comparison of performance of different AI models

Figure 3 shows the performance of XGBoost and Random Forest on different categories of attacks such as DDoS, Ransomware, SQL Injection, Phishing, and Malware. Both models are good, but XGBoost performs better than Random Forest in all categories every time. For example, to detect DDoS, XGBoost detects at 96%, higher than Random Forest at 94%. In ransomware detection, XGBoost detects at 94% while Random Forest detects at 91%. Similar to all other types of attacks, XGBoost is always superior in detection rate. This is due to the superior learning capacity and sensitivity to patterns by

XGBoost, making it ideal for the active defence of the network. The graph illustrates how using XGBoost enhances general security performance and greater protection against innovative and dynamic cyber-attacks.

Apart from improving the detection accuracy, the AI-driven solution also led to substantial reductions in response time by as much as 40% on average. Lassitude is important for real-time threat detection because the sooner the system responds and identifies the attack, the less damage is incurred. With traditional systems, response time is very time-consuming, especially with enormous volumes of data or even complex patterns of attacks. Nevertheless, the AI solution is designed to observe network traffic and user activity data in real-time and, as such, can identify anomalies instantly and trigger automated mitigation processes. These rapid responses minimize detection-to-response latency and maximize aggregate security operations responsiveness, guaranteeing that threats are instantly and efficiently eliminated before they have time to develop. Enhanced detection effectiveness and response times yield enhanced mitigation techniques. The AI system is founded upon sophisticated decision-making architectures that enable it to invoke stricter mitigation controls if it detects an attack. For instance, in Distributed Denial-of-Service (DDoS) attacks, the system could rapidly identify the attack pattern, track the source of malicious activity, and implement countermeasures like traffic filtering or rate limiting to limit the attack's impact. Real-time prevention of this kind ensures that the attacks are resolved before they can adversely impact services, enhancing the network or application being protected's resilience.

To illustrate the improvements better, we provide graphs and tables showing these results. The difference in detection accuracy between the baseline models and the AI system is what the first graph illustrates, intending to highlight the performance boost by 30%. The graph visually displays how much the AI system outperforms the conventional system by such a high rate, particularly when identifying newer and more advanced threats. This enhancement is achieved acutely in sophisticated threat detection like zero-day attacks, which, to a great extent, are challenging to detect on systems of the traditional method due to their stealthy nature. A benchmark graph indicates a slowing down response time through an apparent decline of 40% based on implementing the AI model with considerations to the baseline strategy. Worst degradation occurs in conditions with heavy traffic or under high-attack attempt frequencies. Response time becomes an imperative aspect in curbing attack impact, and it can be noticed from the graph that even when there is a condition of high usage, the AI system doesn't reduce the pace of detection and blocking. It is a prime factor in mass-scale security frameworks, where a delay in response would be the worst to happen. Besides the graphs, tables compare the system performance in various attack conditions.

Tables compare such critical metrics as detection accuracy, response time, false positive rate, and mitigation effectiveness for various types of attacks, such as DDoS, phishing, botnet traffic, and brute-force attacks. These data tables also support the general excellence of the AI-based framework in addressing heterogeneous and dynamic cyber threats. For example, in DDoS attack simulations, the AI-driven framework exhibited quicker detection and more precise category identification of attack patterns, leading to more effective targeted countermeasures. The tables also compare the performance of the AI-enhanced framework against classic signature-based detection systems and other machine learning frameworks. The results indicate that the AI framework outperforms these in every aspect concerning response time and detection rates. This goes a long way in further establishing the framework's viability in real-world cybersecurity configurations, where accuracy and speed are crucial.

The test results validate the scale of advantage in the application of AI to cybersecurity systems. The improvement in detection effectiveness by 30% and response time reduction by 40% suggests the ability of the AI-supported system to increase threat discovery and protection. Such technologies are vital in finding and destroying cyber threats and augmenting the operational efficiency of security staff by reducing alert fatigue and resource optimization. Implementing speedy and efficient mitigation mechanisms further contributes to the network's security profile by enabling it to be robust against various attacks. With the growing sophistication and scale of cybersecurity threats, implementing AI-driven systems is an encouraging move toward protecting sensitive data and critical infrastructure. The tables and graphs presented in this research adequately prove the superior performance of the AI system, once more confirming its potential as a freedom-fighting instrument in contemporary cybersecurity.

5. Discussions

The test results confirm the outstanding enhancement in network security performance realized by incorporating AI models in the defence system. The most dramatic performance enhancement is in threat detection accuracy, where AI models surpass traditional methods by offering improved and better identification of known and unknown threats. The integration of AI allows the system to learn dynamically from new attack trends that develop over time and improve its threat detection feature as threats evolve. Its adaptive response makes the system far more powerful in fighting complex attacks that tend to evade signature-based control systems. Overall, the XGBoost model performed well with better ability for precision and fewer false positives. XGBoost also achieved a 95% detection rate with 2.0% false positives, indicative of the large learning ability to differentiate between network threats, from normal to novel attacks. The accuracy in differentiating malicious from normal activity is commensurate with the security mechanism reacting accordingly without flooding network managers with false alarms. This

is a giant step from the legacy systems, which had excessive false positives leading to alert fatigue and failing to detect true threats. Random Forest, another machine learning algorithm within the system, also improved equally well with 92% accuracy and faster response time compared to the legacy approaches. While not as precise as XGBoost, Random Forest had its complementary strengths, especially where the ensemble learning of its own is best equipped to handle complex data sets with numerous features. By enabling the combination of the outputs of several decision trees to yield more balanced and authentic judgments, Random Forest reduces the error rate and maximizes system performance overall.

Apart from the overall enhancement of performance and accuracy, the system's ability to identify and mark some high-impact attacks also makes it resilient. For example, during Distributed Denial-of-Service (DDoS) attacks, the system identified 94% since it could not identify and shut down such resource-suck attacks that, by nature, can turn off network operations. Similarly, when ransomware was emulated, the AI-driven system identified 96% of the threats. Ransomware, with the potential to cause huge harm to valuable data and halt business operations, is one of the most damaging types of cyberattacks, and the system's ability to detect and eliminate it successfully indicates the necessity of adding AI-based detection ability. These results reflect how adaptable the system is and capable of responding to a wide range of threat environments, making it more efficient in dynamic and complex network setups. Another feature that further increases the response capability of the system to threats is through processes with reinforcement learning (RL). RL, learning from the environment and modifying the action based on feedback given by the system, is the central mechanism of the automated response strategies engine. Through the mechanism of a dynamic process, not only is the threat discovered, but there is also an instant response with minimal intrusion of the human factor. The RL unit constantly evaluates the goodness of the action and adjusts the plan for response from moment to moment.

Therefore, the system reacts to risk quicker, reducing network downtime and making security controls run in the best possible way. For example, in the scenario of a DDoS attack, the system might initiate countermeasures such as filtering traffic, redirecting traffic, or blocking the offending IP address, whereas, in the scenario of a ransomware attack, it can quarantine affected files or slow down the propagation of the attack. Response mechanisms such as these being automated ensure that the impact of security attacks is reduced and the network continues to function even under attack. Also, the system continuously processes new data through dynamic threat intelligence feeds. The system possesses a hybrid threat detection mechanism with a blend of supervised and unsupervised learning models. Supervised models like XGBoost and Random Forest are learned using labelled data and are best suited to detect known patterns of attacks. On the other hand, unsupervised models like Isolation Forests can even identify new, unknown attacks by observing anomalies in traffic without pre-labelled data. This blend of learning processes allows the system to stay in its best state as far as possible regarding accuracy and reliability, whether the attack is known or unknown.

The threat intelligence of the current system keeps it up-to-date with new modes and media of attack so that it adapts to the changing nature of such attacks as the evolution of cybersecurity threats continues. Continuous learning and evolution are the new characteristics of the AI-based system, making it efficient in blocking newer and diversified attack strategies. Experimental results determine the major advantages of implementing AI on network security systems. Enhanced detection rates, reduced false alarms, and faster response are major characteristics of improved system performance compared to traditional processes. System responsiveness against high-impact threats such as ransomware and DDoS and reinforcement learning on auto-response make it a highly responsive and effective defence system. The merging of supervised and unsupervised models with real-time threat intelligence feeds enables the AI-based system to offer proactive and constantly updated protection for a broad range of cyber-attacks, offering strong security in adversarial network environments. The findings show that AI performs quite well in establishing security for a network, hence making AI-based models the future of pro-activity defence policies.

6. Conclusion

This research validates that defence countermeasures based on AI effectively aid prospective future cyber security attacks. This model outperformed current security systems with a greater detection ratio efficacy and quicker response time. Utilizing supervised, unsupervised, and reinforcement learning methodologies, the system becomes more active in dealing with an unexpected cyber-attack scenario. Supervised learning models such as XGBoost and Random Forest allow for high-precision identification of identified attacks, while using unsupervised models such as Isolation Forest allows for identifying novel attack patterns.

Integration of reinforcement learning allows the system to learn, adapt, and build its automated response mechanisms with time using feedback from actual attacks in real-time and become more effective in the process. This adaptability allows the system to provide proactive security against known and unknown threats. The study validates the promise of the AI future to provide improved network security through more intelligent, more perceptive, and more adaptable defences. Powered by automated sensing and response, the system abolishes the need for human intervention to zero, eliminating latency-based response to threats and allowing rapid mitigation. Overall, the proactive defence mechanism of AI is a notch higher than the evolution of cybersecurity, with an integrated, interactive solution against continuously evolving cyber threats.

6.1. Limitations

Though the demonstrated AI-based proactive defence system can perform with decent accuracy and response rates, this system has certain limitations. Of possibly most importance among them is that the system is based on data in the format that the performance strictly depends on the quality and quantity of the training data. Inaccurate, incomplete, or biased data will influence the performance of AI models in a manner that results in misclassification or lower detection rates. Complexity is one such model weakness as applying multiple machine learning approaches like supervised, unsupervised, and reinforcement learning is a computationally intensive task involving a huge amount of hardware infrastructure, especially real-time threat detection and response. This would be a limitation for low-resource organizations. Another risk to the system's functioning is attacks against the AI models. The adversarial machine learning attacks can mislead the system's detection module by offering inputs specially crafted to mislead the models into marking or bypassing malicious threats. Due to this, there always comes a necessity to make the AI models more resilient and include data protection methods, like adversarial training, to minimize the system's susceptibility to such attacks. Regardless of all these limitations, the system is far superior to the conventional method and provides a foundation for future improvement and innovation.

6.2. Future Scope

All further development of AI-driven proactive defence systems must solve the technology limitation of what is available to employ and push the system to new levels. An emerging research area could be incorporating federated learning models to facilitate privacy-sensitive data analysis. Federated learning enables models to be trained from data scattered at numerous places without ever sharing sensitive information, offering more privacy while leveraging the benefit of massive data analysis. This would prove particularly beneficial where data privacy legislation is tight or companies must protect confidential information. Model interpretability is another prime area of future research. Although AI systems are highly performant, they are "black boxes"; therefore, security analysts cannot know why some decisions were made.

Deployment of XAI techniques would assist in facilitating transparency of security decisions made from AI and establishing trust in the system to allow security analysts to authenticate and refine automated controls. Finally, the most promising research direction in the future is to use blockchain technology for decentralized threat sharing. Blockchain could be used as a tamper-proof, secure ledger to share threat information among organizations and to develop a more cooperative defence community as a whole that is safer. This network would facilitate and significantly improve the detection and response to threats by organizations and form a more secure, cohesive defence network. Pursuing those fronts would be placing AI-deployment defence systems in conjunction with new-wave cyber-attacks to provide stronger security.

Acknowledgment: I am deeply grateful to Charter Communications, Hutto, Texas, United States of America.

Data Availability Statement: The data for this study can be made available upon request to the corresponding author.

Funding Statement: This manuscript and research paper were prepared without any financial support or funding.

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Ethics and Consent Statement: This research adheres to ethical guidelines, obtaining informed consent from all participants.

References

1. R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, "Intelligent manufacturing in the context of industry 4.0: A review," Engineering (Beijing), vol. 3, no. 5, pp. 616–630, 2017.
2. A. Schumacher, W. Sihn, and S. Erol, "Automation, digitization, and digitalization and their implications for manufacturing processes," in Innovation and Sustainability Conference Bukarest, Amsterdam, The Netherlands, 2016.
3. D. T. Matt, V. Modrák, and H. Zsifkovits, Industry 4.0 for SMEs: Challenges, Opportunities and Requirements. Cham, Springer, Switzerland, 2020.
4. D. Wu, A. Ren, W. Zhang, F. Fan, P. Liu, X. Fu, and J. Terpenny, "Cybersecurity for digital manufacturing," J. Manuf. Syst., vol. 48, no. 7, pp. 3–12, 2018.
5. A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," Comput. Ind., vol. 114, no. 1, p. 103165, 2020.
6. N. Kaloudi and J. Li, "The AI-based cyber threat landscape: A survey," ACM Comput. Surv., vol. 53, no. 1, pp. 1–34, 2020.

7. W. Matsuda, M. Fujimoto, T. Aoyama, and T. Mitsunaga, “Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud,” in 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 2019.
8. A. Angelopoulos, E. T. Michailidis, N. Nomikos, P. Trakadas, A. Hatziefremidis, S. Voliotis, and T. Zahariadis, “Tackling faults in the Industry 4.0 era—A survey of machine-learning solutions and key aspects,” Sensors (Basel), vol. 20, no. 1, p. 109, 2019.
9. H. Ji, O. Alfarraj, and A. Tolba, “Artificial intelligence-empowered edge of vehicles: Architecture, enabling technologies, and applications,” IEEE Access, vol. 8, no. 8, pp. 61020–61034, 2020.
10. M. Brundage et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv, Ithaca, New York, 2018. [Preprint-Accessed by 11/02/2024]
11. L. Monostori, B Kadar, T Bauernhansl, S Kondoh, S Kumara, G Reinhart, O Sauer, G Schuh, W Sihn and K Ueda, “Cyber-physical systems in manufacturing,” Cirp Annals., vol. 65, no. 2, pp. 621–641, 2016.
12. M. Wu, Z. Song, and Y. B. Moon, “Detecting cyber-physical attacks in Cyber Manufacturing systems with machine learning methods,” J. Intell. Manuf., vol. 30, no. 3, pp. 1111–1123, 2019.
13. H. Alkahtani and T. H. H. Aldhyani, “Artificial intelligence algorithms for malware detection in Android-operated mobile devices,” Sensors (Basel), vol. 22, no. 6, p. 2268, 2022.
14. S. Mishra, “An optimized gradient boost decision tree using enhanced African buffalo optimization method for cyber security intrusion detection,” Appl. Sci. (Basel), vol. 12, no. 24, p. 12591, 2022.
15. M. Dekker and L. Alevizos, “A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making,” Secur. Priv, vol 7, no. 1, pp. 1-18, 2024.
16. J. Malik, A. Akhunzada, I. Bibi, M. Imran, A. Musaddiq, and S. W. Kim, “Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN,” IEEE Access, vol. 8, no. 7, pp. 134695–134706, 2020.