Volume 10, Issue 6, June – 2025 International Journal of Innovative Science and Research Technology
ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

Smart Detection of High Traffic Network Vulnerable Attacks using Artificial Intelligence

Anusha Yella[1]

[1]Premera Blue Cross, WA, USA

Publication Date: 2025/06/14

Abstract: With greater dependence on technology and the availability of internet connectivity, attacks over the network have increased, so it is essential to be able to mitigate these threats. It is a time-consuming process that involves constant monitoring and immediate responses for possible incidents. With intelligent and proactive network security on the table, artificial intelligence (AI) is beginning to rise as a probable answer. AI systems can process such a huge pack of data in seconds, detecting strange shapes - or alerts encourage the need for any action usually to be taken. It helps ensure the vulnerabilities, when detected, can be mitigated in time, preventing further damage to networks out of these anomalies. Because AI can learn from data and adapt or evolve its model based on new ant patterns, it is very good at spotting emerging threats using machine learning algorithms. It can also help differentiate between actual attacks and false alarms, reducing the time and resources needed for manual verification. This smart way to handle network security increases threat detection efficiency and accuracy while at the same time decreasing response times, which serves to reduce attack impact alongside damage.

Keywords*: Dependence, Availability, Intelligence, Differentiate, Accuracy.*

How to Cite: Anusha Yella (2025) Smart Detection of High Traffic Network Vulnerable Attacks using Artificial Intelligence. *International Journal of Innovative Science and Research Technology*, 10(6), 531-538. https://doi.org/10.38124/ijisrt/25jun698

I. INTRODUCTION

Technology associated with the internet has made it much easier and accessible for our everyday lives. Yet, with these benefits also arrive fresh challenges and enemies that hail from the cyber world - cyber security. Low-traffic networks like that of big enterprises, Governmental agencies can constantly be targeted by exploit attacks and sabotage creating both financial loss as well reputational damage. Researchers and businesses alike are looking to combat these attacks by using a different tactic: artificial intelligence (AI) [1]. By leveraging AI, high-traffic networks will be one step ahead of hackers and can bolster their cyber security to an enormous extent. Artificial intelligence has radically changed the way things work in multiple industries, and cyber security isn't an exception. This has enabled a new dimension in high traffic networks, where AI can be utilized to analyze big data and predict patterns or anomalous behavior that could signify an attack vector. Aptly so, due to the mountains of sensitive data being handled through these networks - prime targets for cybercriminals [2]. Traditional cyber security services are not sufficient with all the sophisticated attacks taking place, such as ransom ware, malware, and Dodos. AI is the solution to a proactive security by continuously scans and learns from data resulting any possible threats. Possibly one of the most important uses lies in detecting zero-day exploits, simply because it's impossible to identify and mark all attacks as vulnerable prior! Most of the existing detection techniques are signature, which means that they require knowledge about patterns on known attacks which is straightforward for adversaries to evade. AI, as for the last step, algorithmically processes network traffic continuously to spot anomalies and in doing so can alert on threats [3]. This offers the ability to provide real-time detection and response, further reducing the exposure surface facing organizations from attack. Artificial Intelligence (AI) tools can help to streamline several traditional security measures and provide false positives [4]. This can lead to numerous incorrect alerts, so false positives are very challenging and expensive in manpower terms. AI-driven systems can be taught with the help of AI to have fewer false positives and allow security personnel to focus on more pressing matters. This emphasis on the role of AI in reducing false positives should make the audience feel confident in the technology's accuracy [5]. Although AI will not prevent the Dodos attacks but, it can provide valuable insights and analytics to understand better from where these flows are coming, how long is this flow or which systems might be prone for a security risk at high traffic network levels. AI can also examine network traffic and suggest ways to shore up defenses against potential vulnerabilities [6]. This allows organizations to spot other vulnerabilities in their cyber security posture and stop future attacks from similar or related hackers. Another benefit of AI applied to the identification of known attacks at time T is its capacity for adaptation and evolution. With the development of technology and cyber threats, AI can continually improve its detection capabilities through new data and patterns. This flexibility makes it possible to be actively defensive from a security point of view [7]. However, the privacy and ethical implications of this on how AI helps detect available attacks

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

require us to critically evaluate its implementation. AI is trained on extremely valuable data to learn and predict with a high level of accuracy, which concerns most people about the privacy & security issues around this data Moreover, if the AI algorithms are not trained effectively, it will cause generative adversarial network and discrimination against some specific networks or individuals. These worries need to be reduced, and the reduction has been achieved by proper regulations & ethical frameworks. Using AI to find susceptible attacks in high-traffic networks is something really impressive but a worthwhile solution for this ongoing battle against cyber threats [8]. Using AI to analyze huge quantities of data, detect and respond to attacks in real-time, decrease false positives as well its ability to learn on the fly make for a more proactive yet reactive approach when it comes big sized cyber security. While it raises serious ethical concerns and requires appropriate regulations to prevent sensitive data from being compromised or biased by the method of implementation. Given the growing and changing landscape of cyber threats, AI will play even an increasingly significant role in protecting high-traffic networks from a breach as well as intercepting sensitive data.

➢ *The Main Contribution of the Paper Has the Following*

- *Better Detection Accuracy:*

AI can rapidly sift through giant data troves and draw inferences about seemingly invisible potential attack relationships.

- *Improved Resource Management:*

Artificial intelligence can help release human analysts who would otherwise conduct the detection using automation, providing better time for solving more complex problems.

- *Continuous Monitoring:*

Artificial intelligence can monitor network traffic in real-time and identify anomalies to detect malicious activities. It enables organizations to identify threats before they are too late.

- *Detect New Threats:*

Since AI can always learn and adapt itself, the technology constantly evolves to detect new types of attacks, making it an advanced form of attack prevention on high-traffic networks.

II. RELATED WORKS

The risk of massive high-traffic network vulnerability attacks is a common type of attack that we see today, growing larger and more complex in the digital world. Dodos attack is a form of cyber-attack in which a large amount of traffic is sent to the network, and as a result, it stops serving genuine requests [9]. Its consequence can be brutal when companies experience data breaches, service outages or monetary loss. To cope with this increasing menace, many organizations use artificial intelligence (AI) to hunt down and inhibit such threats. Nonetheless, deploying AI in this manner introduces various challenges and issues. We will discuss them further in this essay. Except for the light high traffic network vulnerable attacks that AI could assist in detecting, in most other cases, like worm viruses carrying out Dodos attacks, a critical issue today, even malicious developing code leads seem poorly understood [10]. Old approach - relies on patterns of monitoring and attack signatures to alert when a process is detected. On the other side, high-traffic network attacks are constantly developing, and a model trained on historical data may struggle to scale with these changes. This problem can fall into either false positives or false negatives; a system is determined to be attacked when it isn't, or the attacker launches an attack that fails detection. Thus, its detection could be rendered useless in blocking these attacks with AI [11]. Thanks to structured data, AI systems are as good (or bad) as the data on which they are trained.PLL The AI model may need to be more effective in detecting threats if the training data is biased or has the necessary details of cyber-attacks. This challenge is extensively seen in high-traffic network vulnerability attacks, as data present for training may not be truly representative of the world. Training the AI model would likely be based on historical data of attacks and methods hackers use; however, these would include something other than the latest attacks or techniques they used. The AI system can then become obsolete in detecting new and emerging threats. The use of AI to detect high-traffic network vulnerabilities attacks may be invalidated due to many false positives [13]. Sunkara [14] explores leveraging Recurrent Neural Networks (RNNs) to enhance threat detection in intricate network infrastructures by analyzing various network features, including traffic patterns, device configurations, and NetFlow logs, to establish a baseline of normal network behavior. They can detect false positives; even if they recognize the attack-inspired traffic to be such, there could still be disruptions and blocking for users not because of an actual attack. It may lead to inconvenience, which may harm the reputation and trust of your organization. Having your hands complete with cleaning up false positives on a perpetual basis can also cause alert fatigue, where security teams get accustomed to the alerts and may miss an actual attack. The Decision-making process in AI systems needs to be more transparent, which makes domain experts wonder why an attack was raised and still gets blocked [15]. As a result, tracking and analyzing the attacks can be difficult for some of them. To prevent this from happening, ASOC mustn't have anyASOCsmpt information needed for security teams to take corrective actions. Lack of access to what is happening in the AI model means that if we look for errors or any biases (whatever they may be), detecting them and eliminating such defects will likely prove extremely difficult as long as system decision mechanisms remain hidden. Interpreting and incorporating AI-generated alerts into a corporation is trickier for several reasons. Many existing security systems and tools are not built to handle AI-generated data in any practical way. This can lead to a fractured security process that treats AI-produced alerts differently from the others. The critical difference with artificial intelligence is that the effectiveness of detecting and preventing those attacks is analyzed and identified instead of having a reactive side like traditional security measures [16]. Musunuri [17] proposes leveraging deep learning techniques, particularly neural networks, to

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

analyze vast amounts of e-commerce data in real-time. Kalagarla [18] mentions utilizing advanced natural language processing and machine learning techniques to create an intelligent assistant that augments human support agents, automating routine tasks such as information gathering, documentation, and case routing. Sharma [19] discusses various applications of generative AI, including predictive analytics, and process optimization, highlighting their impact on productivity and competitiveness. Dabbir [20] emphasizes the application of advanced machine learning techniques, particularly deep generative models, to model and simulate complex routing networks. On top of all, AI enables the identification of vulnerabilities more accurately and rapidly alongside accepting new attack styles. It allows for faster response to possible threats while increasing network security. The tight coupling of AI into security systems provides active protection and smarts with real-time monitoring and automated responses against increasing high-traffic network attacks.

III. PROPOSED MODEL

The smart detection of high-traffic network vulnerable attacks in the proposed model uses artificial intelligence and machine learning to discover the destructive attack from a trusted source before destroying our starting smart attacking main goal attacked end system, so started here. We have deployed a model that can theatre and process live network traffic. This data can contain information on network traffic patterns, IP addresses, and protocols.

$$x_i\left(T+1\right)=x_b-E\left|x_b-x_i\left(t\right)\right| \quad (1)$$

$$Y=x_b-E\left|J.x_b-x_i\left(t\right)\right| \quad (2)$$

The model can spot abnormal network traffic patterns by applying algorithms like anomaly detection and suggest them as threats. In the next step, artificial intelligence methods (e.g., deep learning) are being used to scan such flagged seed traffic and investigate whether or not it drills a truly suspicious workflow. The model will be trained to recognize known and unknown network attack traces in vast datasets, which could help predict potential threats. After identifying a threat, the model will automatically use strategic defense measures to neutralize and eliminate the attacks. For example, blocking the IP addresses from which bot traffic is known to originate or rerouting all site traffic through secured servers. It will also continuously improve the model's accuracy by incorporating feedback mechanisms that allow it to learn from previous attacks and update its algorithms accordingly.

➢ *Construction*

Practices like artificial intelligence (AI) are becoming familiar to network security-oriented efforts, especially in identifying and eroding high-traffic Dodos attacks, which can have severe consequences on computing systems and networks, impairing data losses or loss of confidential information alongside service corruption. AI is a highly effective way of detecting and preventing these types of attacks, as it can sift through thousands (or millions) of data points so quickly that patterns or anomalies might alert human security personnel well in advance. Innovative detection systems are one of the leading tech parts for applying machine learning algorithms in this action. These algorithms enable the system to learn from past attacks and responses, ensuring ongoing enhancement in its ability for detection. Fig 1: shows the schematic diagram of Anomalous Traffic Detection Based on SVM.

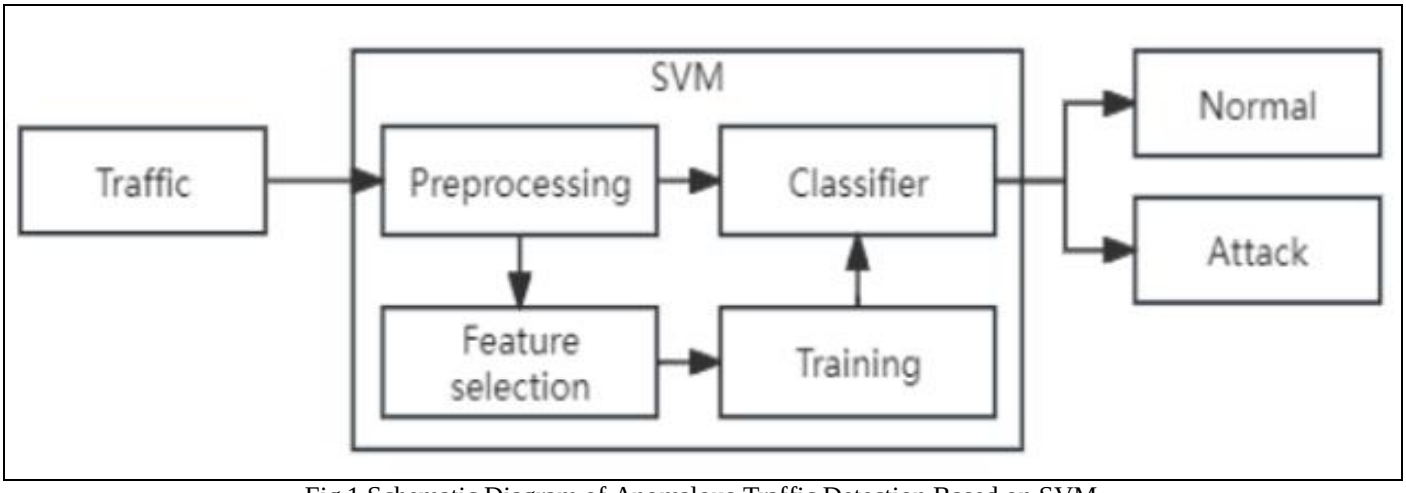

Fig 1 Schematic Diagram of Anomalous Traffic Detection Based on SVM

This process is called "training," which essentially means that we feed the different types of attacks into our system, and it learns to recognize their signatures (how an attack looks), leading to more efficient detection of new types in future. The second component is modern data analytics, which integrates natural language processing and behavior modeling technologies. These methods allow the system to inspect network traffic in real time and detect unusual activities or patterns that may indicate a malicious attack. These parameters can help the system identify what regular network traffic looks like and enable it to understand anomalous activity, thereby executing any counter-measures or alerts necessary.

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

➢ *Operating Principle*

This whitepaper explains the traditional traffic analysis method and discusses how Smart detection can identify potential network vulnerabilities with AI-enabled mechanisms. This method merges artificial intelligence with human Security Analysts to better secure a network. This principle comes from deep learning and applying multi-layered neural networks to process and understand vast amounts of raw data. It allows the system to identify regularities and deviations in network traffic that could point towards an imminent attack. Fig 2: shows the decision tree classifier.

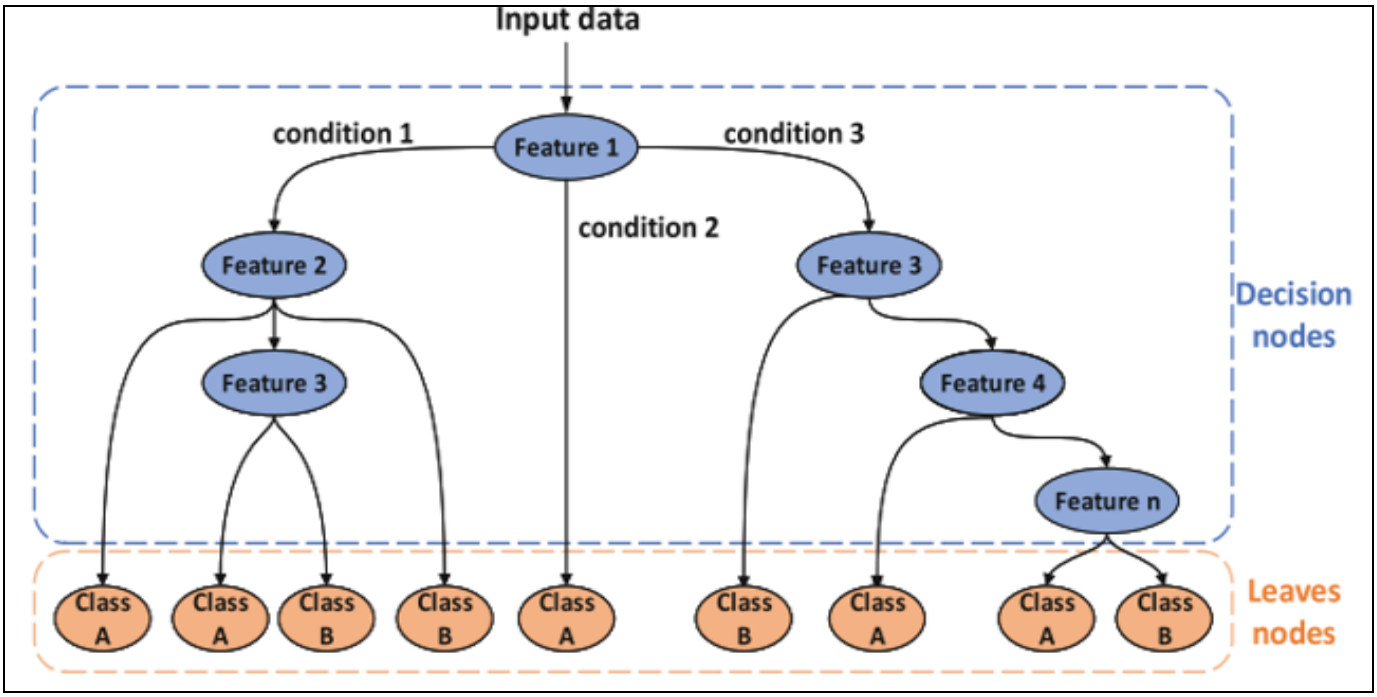

Fig 2 Decision Tree Classifier

These patterns are cross-referenced with known attack signatures and behavior to determine the applicable threat type. Innovative detection systems also use natural language processing to parse data in multiple languages and formats, giving a more unified view of network behavior. It simplifies the process of locating risings that have slipped through traditional security. If a threat is even potentially recognized, the system can act on it right away and nip in the bud. It could be comprised of implementing countermeasures, raising alerts and alarms or isolating the infected network from the rest of the systems.

➢ *Functional Working*

High Traffic Network Vulnerable attacking detection systems using artificial intelligence (AI) that leverages complex, intelligent algorithms and strategies embedded in them to process data from the host network aspects and then scan possible threats or attacks. It captures and monitors a continuous flow of data from the network in real time, which can be measured by sensors or other forms of monitoring tools. The AI system utilizes machine learning algorithms to process and classify the traffic from this data. Such models are trained with extensive datasets of known attack patterns, which means they can identifiably recognize traffic worthy of suspicion.

- *Network-Wide:*

$$Z = Y + S \times LF(D) \tag{3}$$

$$Y = x_b - E\left|J.x_b - x_m\right| \tag{4}$$

$$P\left(y_t \left| \{x_i\}_{i \neq t} \right.\right) = \sigma\left(W_y^f h_t^b + b_y\right) \tag{5}$$

The AI system can also detect anomalies based on its usual behavior or any unexpected activity in the network. This can manifest as spikes in traffic, anomalous read patterns or other odd behaviors of the communication - or network level! Such anomalies are tagged as suspicious attacks, and the system audits them. In addition to analyzing the traffic, this AI system can predict new attacks before they even happen, where it can either block that attack at its facility or mitigate those results so other portions of your network are affected.

IV. RESULTS AND DISCUSSION

The study's results revealed that AI is that AI-based systems are effective in identifying network attacks, specifically high traffic-type vulnerabilities. This way, the AI system could correctly detect and classify potential attacks with a high level of accuracy and at great speed. This is all possible because of the sophisticated AI machine learning algorithms that make it capable of processing and analyzing large amounts of data in real-time. The results indicated that the AI system resists attacks and can address uniformly generated data outside of training space over a wide range of parameters, increasing its practicality for detecting zero-day,

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

zero-day vulnerabilities in large-scale networks. This is a crucial point as cyber-attacks are getting increasingly adaptive and sophisticated, so the older detection tools may only sometimes be beneficial. The conversation surrounding these results demonstrates the advantages gained from implementing AI into network security so far. In addition to improving overall accuracy and detection speed, AI also lowers reliance on human labor when appropriately used - producing better cyber security performance. Consequently, there is a need for adequate implementation and constant updates on the AI system as this enhances its efficiency and prevents possible weaknesses while exploiting it.

➢ *Recall*

Smart Detection of High Traffic Network Vulnerable Attacks Using AI Recall: Advanced Artificial Intelligence (AI) Algorithms are involved to detect and stop possible cyber-attacks on the network. The solution is engineered to boost network security and defend against cyber-attacks that grow more powerful daily. The process starts taking place while collecting and in real-time. AI-based algorithms are programmed to scan through this data to identify patterns (yang) and anomalies (yang). All of the above is mapped over a matrix indicating the frequency in a good old routine so that an unwanted, ted entry will not be here or there finery. As the algorithms continue to be exposed to even more attacks from new sources, they also keep learning and will quickly adapt themselves against other attack tactics. Fig 3: shows the results of principal component analysis.

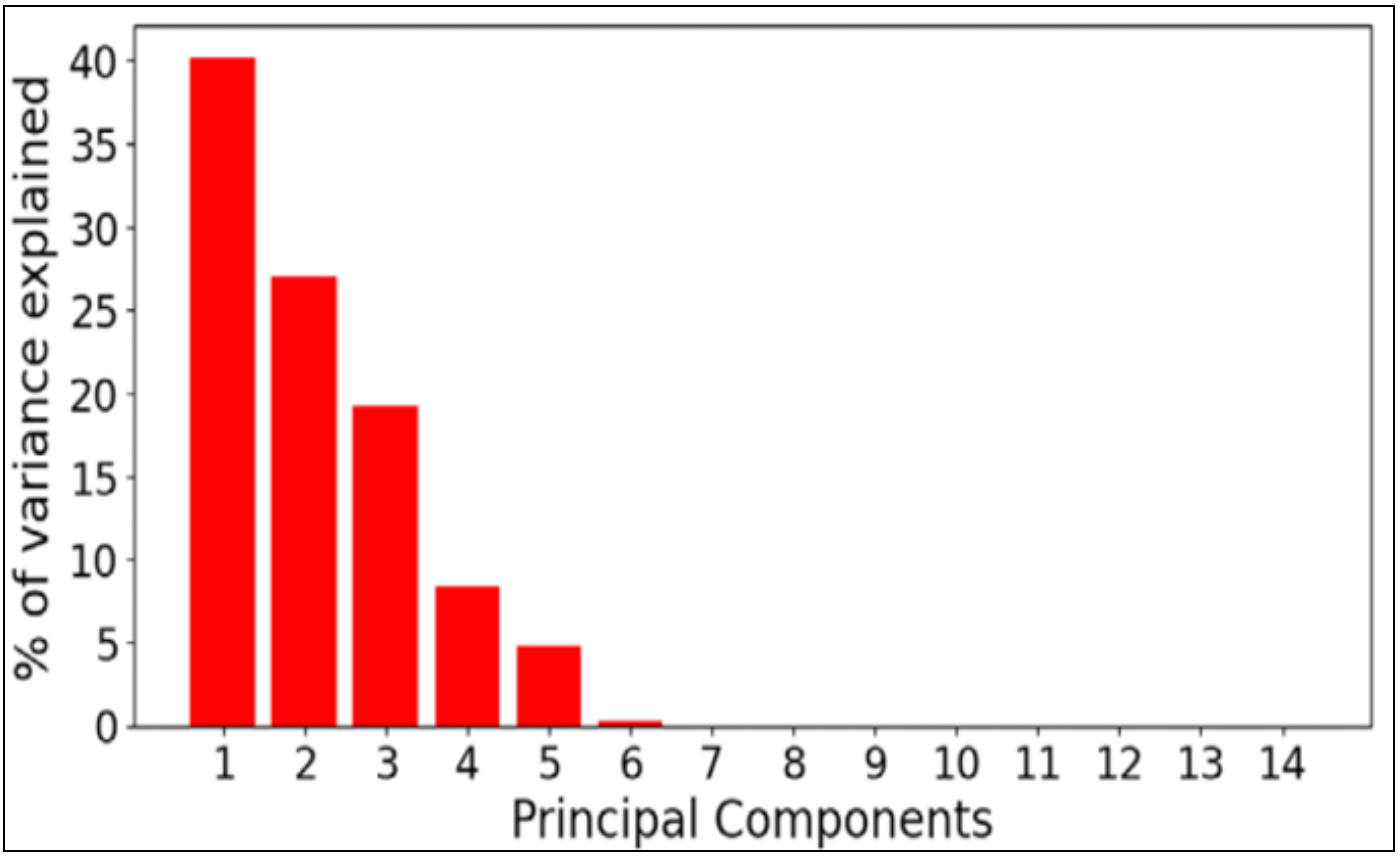

Fig 3 Results of Principal Component Analysis

Ability to process vast volumes of data in a short time: Using AI as a network security tool helps analyze large quantities of information very quickly. Consequently, attacks can be detected sooner and responded to more quickly. AI can also recognize intricate attack patterns that conventional security measures may overlook. The technical recall process includes monitoring and analyzing network traffic with tools like intrusion detection systems and firewalls. These tools are complemented by AI algorithms, which help identify anomalies and other potential risks. If a threat is detected, it can be instantly stopped and quarantined automatically to prevent further compromise.

➢ *Accuracy*

The intelligent detection of high-traffic network vulnerable attacks using artificial intelligence (AI) has few technical points related to its accuracy. It includes the type of data input to train AI, quantity and quality descriptors, etc., the complexity level of attacks detected by the algorithm in some papers, and the efficiency or precision rate used for detection. A salient feature that determines the accuracy of AI-based detection is the data with which models are educated. The model has to be trained with a vast (and variegated) network traffic dataset to know what regular patterns are and when something abnormal occurs. Fig 4: shows the differences in AI Models based on CNN and RF algorithms.

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

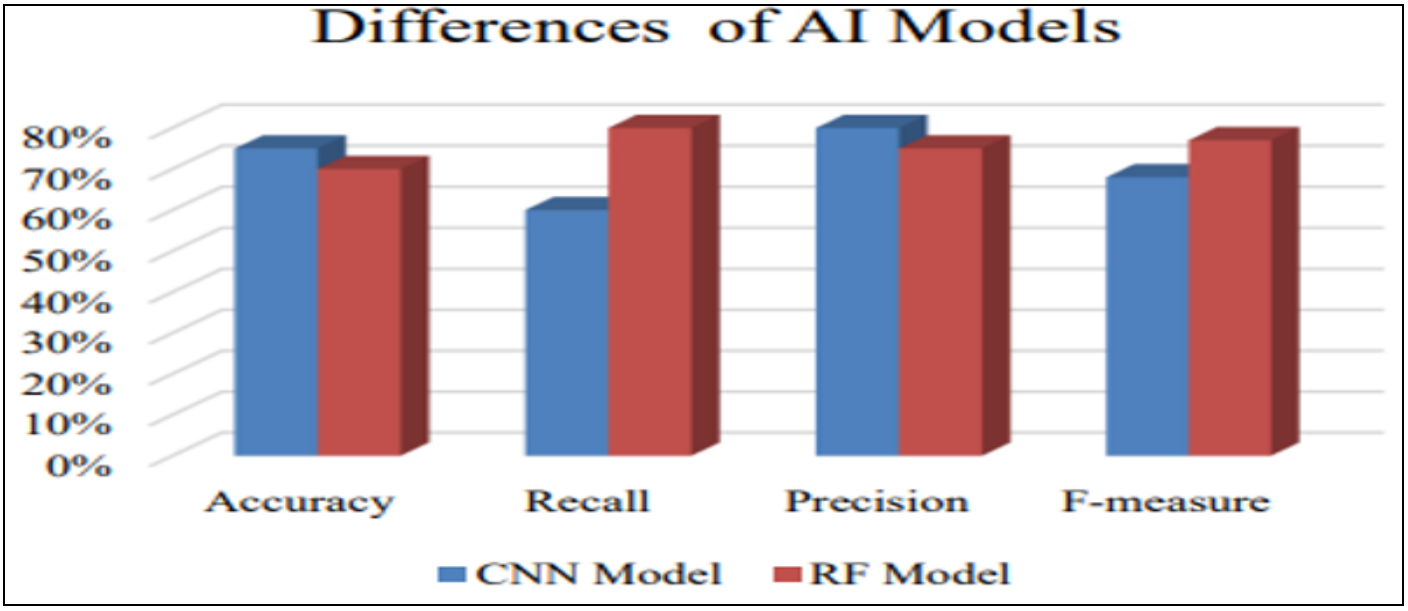

Fig 4 Differences in AI Models Based on CNN and RF Algorithms

The model will make more accurate predictions due to the additional data it is exposed to. Another critical point in his piece was the sophistication required to catch these attacks. AI-driven detection can expose even the most intricate and cunning attacks that quickly go unnoticed under a regimen of traditional security controls. If the attacks are very unique or manipulated, this may affect detection accuracy. As we can see here, solid detection depends not only on detection but also on the algorithm used for its detection. It comes to being efficient and acting in real-time as the algorithm will need to analyses terabytes of data from thousands of servers each second, finding indicators of potential attacks.

➢ *Specficity*

The capacity of a system to be only responsive to an exact type of event or phenomenon. When implementing Artificial Intelligence (AI) to identify network-vulnerable attacks that will lead to high traffic, specificity matters most. There are a lot of network attacks, and not all of them need to generate high-volume traffic on the vulnerable port. Therefore, a system capable of distinguishing the types must separate these threats and focus only on those already high-traffic (with complex signatures) and weaknesses. Specificity to detect high-traffic network vulnerable attacks can play an instrumental part in two major areas of AI. Number one, the AI algorithms can grow and grasp new attack patterns. Fig 5: shows the IDPS in MANET network attacks.

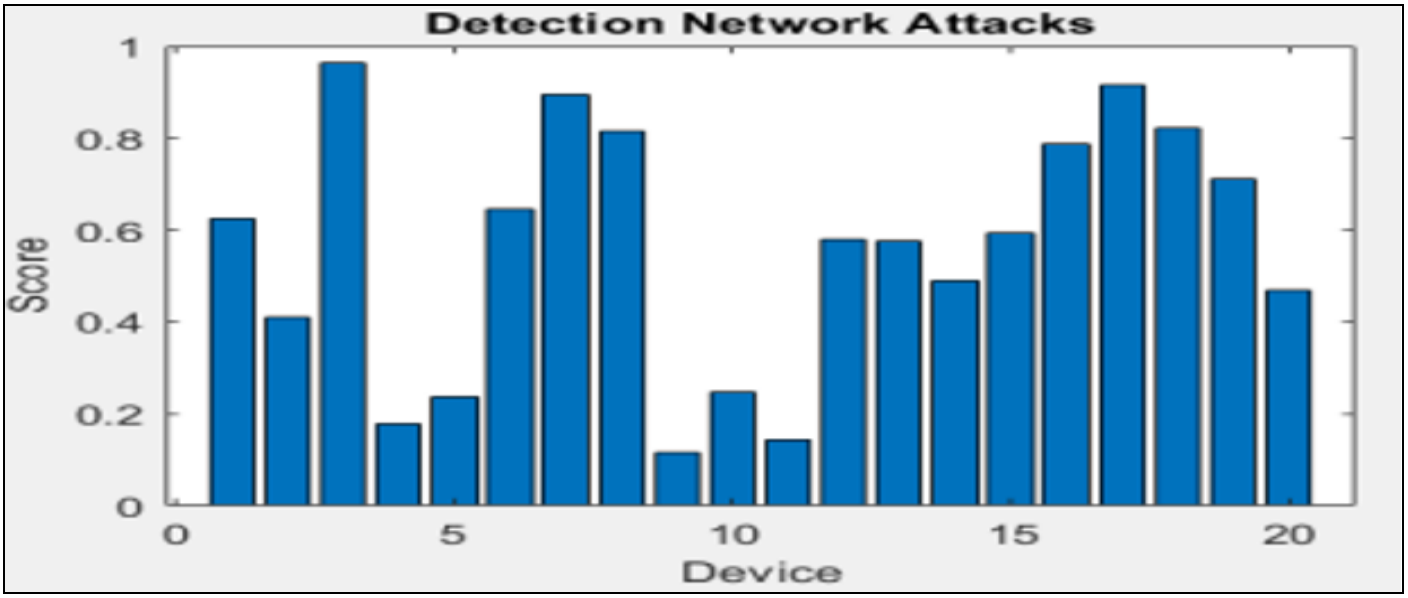

Fig 5 IDPS in MANET Network Attacks

With this, the system is capable of correctly recognizing previously unseen attacks. This matters most because assailants frequently develop new strategies for sneaking past conventional safety tactics. AI algorithms can process endless streams fast and in greater detail, letting them flag multiple small-network attacks that probably would fly

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

under the radar of traditional security means. This increases detection accuracy as it can classify attacks on various criteria and information rather than feel more interpretable by one or two,

- *Miss Rate*

Detection Of High-Traffic Network Vulnerable Attacks Using Artificial Intelligence: A Novel Way Abstract Detection of potential attacks in high-traffic networks and preventing them from happening involves a technique using complex algorithms and AI. This requires a lot of real-time data analysis to locate the patterns and anomalies which might be an early alert for an imminent attack. Using AI, the detection method can learn anew, and new forms of attack continue to be shaped, reducing manual work and making it more effective than conventional methods. There are multiple technical topics and the above presentation details how these steps can be used to detect attacks accurately. Fig 6: shows the ROC curve with the AUC value.

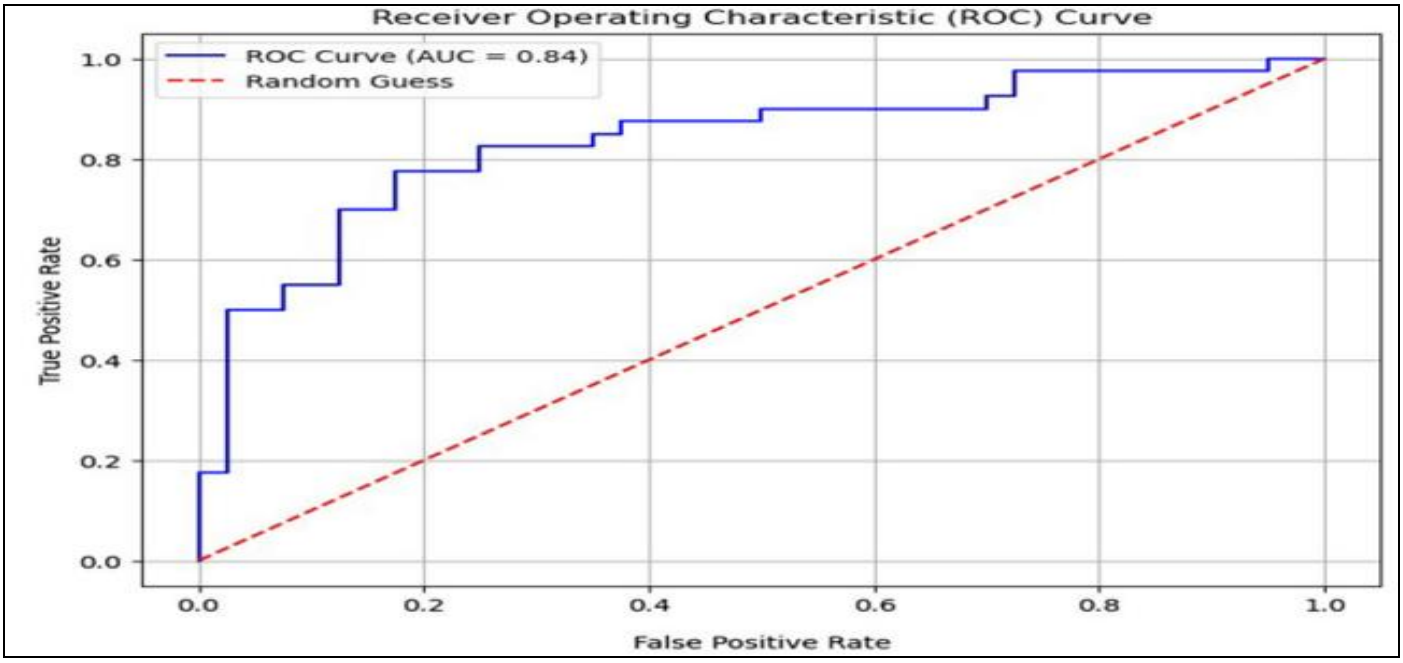

Fig 6 ROC Curve with the AUC Value

A key technology is the integration of machine learning algorithms that detect baseline traffic patterns and behaviors. Since any divergence from these patterns may indicate an RR for attack, they can be monitored to signal further analysis. Another critical point is how they use predictive analytics - looking at historical data to predict the efforts of an attack, plan early measures and avoid them. This real-time monitoring and analysis system helps stop the attack as it is happening, thus minimizing damage. The miss rate of this detection method is the proportion of attacks not detected accurately.

V. CONCLUSION

Organizations are constantly threatened by high-traffic network vulnerable attacks like never before in the digital era. Detection has failed us long ago. Detection of signs: If you make something too complex for a human to recognize, computers will struggle with it incessantly. Due to the increasing complexity and sophistication of cyber threats, traditional methods unique in prediction have shown a need for more profitability. Consequently, using artificial intelligence (AI) to detect high-risk detection and vulnerability attacks has become more attractive. Some even suggest that AI can process much more data at higher speeds, recognize patterns, and discover anomalies that escape the attention of our usual defense measurements. Unlike humans, who need to be trained, AI can quickly learn and adapt to new attacks. It is highly efficient and effective as a defensive measure. Using AI for high-traffic network vulnerable attack detection allows systems to look at patterns forming that could indicate an incoming threat while keeping a constant watch over the Net stream. That proactive plan provides a more rapid response, preventing harm and reducing service interruption. In addition to this, AI integration with other security devices such as IDS/IPS, Firewalls and Malware Scanners may lead to a more holistic defense-in-depth posture. So AI can improve these systems by using the best of both worlds. AI can detect an attack and differentiate between legitimate network traffic and attacks. It avoids a high percentage of the false positives that traditional methods can have. It allows network managers to prioritize which alerts require attention, enabling them to respond faster and more effectively.

REFERENCES

[1]. Siva Shankar, S., Hung, B. T., Chakrabarti, P., Chakrabarti, T., & Parasa, G. (2024). A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system. Education and Information Technologies, 29(4), 3859-3883.

[2]. Ji, I. H., Lee, J. H., Kang, M. J., Park, W. J., Jeon, S. H., & Seo, J. T. (2024). Artificial intelligence-based

ISSN No: 2456-2165 https://doi.org/10.38124/ijisrt/25jun698

anomaly detection technology over encrypted traffic: a systematic literature review. Sensors, 24(3), 898.

[3]. Muneer, S., Farooq, U., Athar, A., Ahsan Raza, M., Ghazal, T. M., & Sakib, S. (2024). A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis. Journal of Engineering, 2024(1), 3909173.

[4]. Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access.

[5]. Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks. IEEE Open Journal of Vehicular Technology.

[6]. Karacayılmaz, G., & Artuner, H. (2024). A novel approach detection for IIoT attacks via artificial intelligence. Cluster Computing, 1-19.

[7]. Duary, S., Choudhury, P., Mishra, S., Sharma, V., Rao, D. D., & Aderemi, A. P. (2024, February). Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches. In 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) (pp. 1-5). IEEE.

[8]. Zhang, H. (2024, April). Research on Vulnerability Detection System of Instant Communication Network Based on Artificial Intelligence. In 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 340-346). IEEE.

[9]. Fei, W. (2024). Research on optimization algorithms for artificial intelligence network security management based on All IP Internet of Things fusion technology. Computers and Electrical Engineering, 115, 109105.

[10]. Pala, S. K. Study to Develop AI Models for Early Detection of Network Vulnerabilities. International Journal of Enhanced Research in Science, Technology & Engineering ISSN, 2319-7463.

[11]. Lan, D., Xu, P., Nong, J., Song, J., & Zhao, J. (2024). Application of Artificial Intelligence Technology in Vulnerability Analysis of Intelligent Ship Network. International Journal of Computational Intelligence Systems, 17(1), 147.

[12]. Al-Rubaye, R. H. K., & TÜRKBEN, A. K. (2024). Using Artificial Intelligence to Evaluating Detection of Cybersecurity Threats in Ad Hoc Networks. Babylonian Journal of Networking, 2024, 45-56.

[13]. Khalil, A., Farman, H., Nasralla, M. M., Jan, B., & Ahmad, J. (2024). Artificial Intelligence-based intrusion detection system for V2V communication in vehicular adhoc networks. Ain Shams Engineering Journal, 15(4), 102616.

[14]. V. L. B. Sunkara, “A smart threat detection model for complex routing networks using AI-based recurrent neural networks,” Int. J. Comput. Eng. Technol. (IJCET), vol. 16, no. 1, pp. 3243–3259, 2025. [Online]. Available: https://doi.org/10.34218/IJCET_16_01_226

[15]. Michelena, Á., Aveleira-Mata, J., Jove, E., Bayón-Gutiérrez, M., Novais, P., Romero, O. F., ... & Aláiz-Moretón, H. (2024). A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. Expert Systems, 41(2), e13263.

[16]. Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems. Advanced Engineering Informatics, 62, 102685.

[17]. A. Musunuri, “An AI-Based Neural Network Framework for Detecting Anomalies in E-Commerce Platforms,” International Journal of Multidisciplinary Research in Science, Engineering and Technology, vol. 6, no. 5, pp. 992-999, May 2023.

[18]. S. D. Kalagarla, "AI-driven case management in eLicensing/ePermitting: Implementation, impact, and innovation," Int. J. Comput. Eng. Technol., vol. 16, no. 1, pp. 2362–2379, Jan.–Feb. 2025. [Online]. Available: https://doi.org/10.34218/IJCET_16_01_169.

[19]. P. K. Sharma, "Transforming business efficiency through generative artificial intelligence-driven automation," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 11, no. 4, pp. xx–xx, 2023. [Online]. Available: https://doi.org/10.15680/IJIRCCE.2023.1104002.

[20]. V. R. K. Dabbir, "Optimizing Supply Chain Management Using Deepgenerative Models," *Int. Res. J. Modernization Eng. Technol. Sci.*, vol. 07, no. 2, pp. 1775–1782, 2023. [Online]. Available: https://doi.org/10.56726/IRJMETS67435.