Advanced Network Security System: Honeypot-Based Intrusion Detection with Machine Learning and Visualization

Ashwini Lakshmipathy[1], Muthupandi Gurusamy[1], Siti Fatmawati Lalo[2], Nonia Sakka Lebang[3], Karthikeyan Selvaraj[4] and Aws A. Abdulsahib[5]

[1]*Department of Computer Science and Engineering, Chennai Institute of Technology, 600069 Chennai, Tamil Nadu, India*

[2] *Department of Master of Laws Study Program, Universitas Sulawesi Tenggara, 93121 Kendari, Indonesia*

[3] *Department of Government Science Study Program, Universitas Sulawesi Tenggara, 93121 Kendari, Indonesia*

[4]*Center for Advanced Multidisciplinary Research and Innovation, Chennai Institute of Technology, 600069 Chennai, Tamil Nadu, India.*

[5]*Department of Computer Science, Dijlah University College, 10021 Baghdad, Iraq*

ashwinil.cse2022@citchennai.net, pg.muthupandi@gmail.com, stfatmawati@un-sultra.ac.id, noniasakkalebang@un-sultra.ac.id, karthikeyans.mech@citchennai.net, aws.abdulkareem@duc.edu.iq

Keywords: Honeypots, Intrusion Detection Systems (IDS), Machine Learning in Cybersecurity, Network Security Visualization, Anomaly Detection.

Abstract: This paper focuses on developing a proactive approach to network intrusion detection through integration of honeypots with machine learning for improved security in complex network system. The system utilizes honeypots to capture attackers whereby the honeypots capture real-time traffic details which the system maps and analyzes packet content related to protocols. Blending with machine learning, the detection model analyzes the accurate data to detect known as well as unknown forms of cyber threats. There is a new feature called Visualization Dashboard that gives analytics and reports to network administrators. It provides information about honeypot engagements, traffic, and intrusion detected empowering the monitoring and management process. Incorporating the proactive defense measures into the proposed system eliminates the weakness of the conventional intrusion detection approach in managing new forms of cyber threats. The honeypots are designed to contain the attackers and simultaneously acquiring useful information about the intrusive activities. The effectiveness is enhanced by the ability of the Machine Learning model in enhancing the detection rates besides the flexibility in accommodating new techniques of detection of attacks. The Visualization Dashboard improves usability since it contains an easily navigable interface for current security monitoring and past performance examination. This approach guarantees the entirety of network protection by integrating the effectiveness of the deception-based honeypot systems and the machine learning approach based on big data. The paper reveals that the system is capable of enhancing detection rates, reducing false positives and providing valuable information regarding the network status to administrators. Thus, the provided system is considered ideal for contemporary cybersecurity issues. Advanced technologies combined in this system offer a flexible and expandable system to protect networks from the steadily growing number of threats.

1 INTRODUCTION

Network security is one of the central pillars of the present and future society as the global interconnectedness of business, governmental and private life is based on networks. High-intensity threats like ransomware, phishing or DDoS attacks show that the fundamental strategies insufficient Security must evolve. As more information including financial records, health record and intellectual property is transmitted through networks, the impact of a breach is catastrophic. Additionally, the increased pace at which new waves of IT technologies such as cloud, Internet of Things and Artificial Intelligence is implemented in the organization increases the exposure to threats [1]. These interrelated systems that are driving innovation and enhancing company efficiency are the same systems that makes them susceptible to hackers. Network security has become mandatory since most businesses have gone online to protect their valuable information and assets from cyber-attacks. Network security is a decoy system that is deployed with the intention of enticing attackers to engage, thus expose their tool, prey and procedures (TTPs) [2]. These interactions offer desired input to security analysts on emergent threats as well as enhance the general security framework. Low-interaction honeypots mainly encompasses known vulnerability honeypots and research honeypots while high-interaction honeypots encompass HoneyD as well as high interaction hoax honeypots. Different type of honey pots are Low interaction honeypots mimic simple service or protocol and thus consume minimum resources, it easily capture key level attacks like scanning or brute force attempt without putting the system in real danger [3]. High-interaction honeypots, on the other hand, emulate normal systems and therefore provide substantial detail about complex intrusions. They are costlier and exposed to higher risk compared to the first type, but offer a much higher level of insight into the attackers tactics and goals. In addition to honeypots, Intrusion Detection Systems (IDS) in the network looking for suspicious events or policy infringements that warrant an alarm to be issued. IDS are divided into two types: The first type is the signature-based IDS, which identifies threats based on a prior known signatures for comparison with network performance, the second is the anomaly-based IDS which identifies abnormal performance or activity that suggests threats. Whereas, honeypot attracts attackers to let them learn more about them, IDS run all the time and are different layers to network. Machine learning has also improved IDS because it has been able to overcome some common issues including high number of false alarms, inability to identify new threats and dependence on static signatures [4]. Machine learning uses linear methods, clustering, classification, and artificial neural networks, which help detect as yet unknown or new-age threats. They also help in the elimination of false positives wherein only real anomalous signals are picked up, and thus provides less noise for the security groups to filter [5]. Essential applications of the current machine learning models of big data include the capacity to analyse the real-time traffic data and offer proactive solutions to detected threats. Furthermore, ML systems can update relevant knowledge bases via real-time learning for new learning cases of attacks and new environments dynamically. Immersive the honeypots with IDS, and machine learning is a full proof and comprehensive solution to confront the threats on the network security [6], [7].

2 LITERATURE SURVEY

A lot of literature today has explored the use of honeypot, Intrusion Detection System, and machine learning to bolster network security in the recent developments in threats. Honeypots have been known to be valuable measures that enable the gathering of intel on the attacker performing various kinds of analysis [8], [9]. Spitzner (2003) defined honeypots as a preventive security that can bend attackers and mimic their strategies, processes and procedures (SPP). Further works developed more kinds of honeypots; low interaction honeypots that provide simple services of network and high interaction honeypots that provide full systems to get better understanding of complex attacks [10] - [12]. Low-interaction honeypots are inexpensive and safe while providing relatively limited data, on the other hand, as described by Seung Woo et al. (2015), high-interaction honeypots generate more data but require more resources and can lead to system compromise. Similar to firewalls, IDS are another crucial paradigms of network security research. Other conventional approaches to IDS, for example the signature-based approach have been developed and applied widely since they work well against the known threats [13] - [15],. Nevertheless, a major drawback of such schemes is their ability to do not identify new or unknown attacks. This has been accomplished by the introduction of Anomaly based IDS which are IDS that observe anomalies within the framework of the normality. Similarly, Liao et al. (2013) mentioned that anomaly-based detection can accurately identify zero-day attacks, but at the same time it has a major disadvantage, being high false positive rates [16] - [18]. This shortcoming has led to development of work that seeks to integrate IDS with machine learning algorithm for better results and to eliminate false alarms. The IDS systems’ capability in applying machine learning in IDS has greatly enhanced systems due to the dynamism of the network and the emerging threats in the market. Another research by Bou-Harb et al. (2017), emphasizes that supervised learning algorithm including SVM and Random Forest are capable to categorize known threatening types including DDoS and phishing. Other methods of learning based on the independence of the model from initial data includes clustering for the identification of new threats in form of outliers [19], [20]. Neural networks especially the deep learning architectures have been widely embraced because of their capability in analyzing high dimensional data to produce symphonies of detecting complicated patterns in traffic flow in the network. For example, Tang et al. (2018) provide a proof of concept of how to use convolutional neural networks (CNNs) for accurate identification of malware traffic. The integration of honeypots and machine learning has been a topic of considerable interest in the recent past. The basis of this method is the application of honeypots in live network environments to collect attack data in real conditions. As pointed out by Choi et al. (2020) on the same, this approach allows IDS to be useful in situations where new threats are not recognized thus possessing no signature. More so, honeypot systems are reinforced by machine learning to analyze the captured data without requiring human input. This integration gives a dynamic and flexible system that can embrace modern cybersecurity challenges that are unique hence making the system scalable. Visualization has been found as an auxiliary solution to honeypots and IDS providing the analyst with an environment to analyze measures and make decisions based on them. According to Yip et al. (2019), visualization proved to be effective in representing attack patterns, distribution patterns, and threat intelligence in a form of interactive dashboards. There are libraries such as D3.js and Matplotlib, used to represent the activity in form of graphics on the network while the monitoring tools such as Power BI offer data visualization as part of a single interface. Combining visualization with honeypots and machine learning guarantees that she is delivering the right information in a manner that can improve the overall tactical awareness, as well as response times. The significance of evaluation metrics can be well understood with the help of the given figure. The basic measures including accuracy, precision, recall rate and the F1 numeric figure rating are commonly used to compare IDS and machine learning models. In their study, Sharma et. al (2021) highlighted that one must always employ balanced metrics and especially when there are certain types of attacks that have for instance fewer samples in a dataset. Researches also describe pre-testing of models in real life conditions to determine their effectiveness and stability in practice.

3 MATERIALS AND METHODOLOGY

3.1 System and its Implementation

The identified solution is the use of honeypots and IDS with machine learning and is a proactive and dynamic security model. Honeypots on the other hand are fake systems that imitates real ones by providing an interface to the network services, attackers are drawn to thus gathering vast information on their techniques and actions. Known attacks are identifiable as they are present in the IDS component and developed from the data collected from users that help the system detect various types of attacks, including known and unknown. The data collected are later used to train a machine learning model improving detection potential of the system and allowing it to escalate protection against new cyber threats. The data captured is also parsed to obtain protocol details to packet level; pay load size and other features. These insights provide the inputs to update the machine learning algorithms to provide a more dynamical and efficient detection system. Figure 1 shows the integration of main components of network security [11], [12].

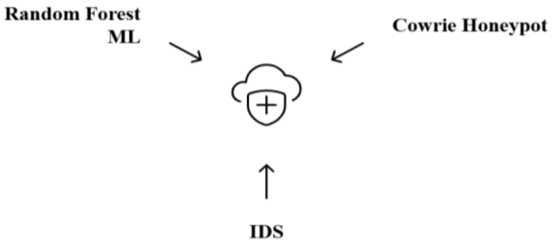

Figure 1: Integration of components of network security.

3.2 Honeypot Deployment

It includes non intrusive honeypot like cowrie which logs brute force and protocol level attacks and the more complex honeypots ready for entertaining smart attackers in a monitored and constrained environment. One type of honeypots, and which are also low-interaction honeypots, are focused specifically on emulating popular services such as SSH and Telnet and logging all activities, including commands typed in by the attacker and the replies they get. From this data information on the behavior of attackers can be gathered as well as information that will assist in the identification of regular target points. In contrast high-interaction honeypots are set up to emulate genuine OS environments using virtualization tools such as VMware this makes the attackers to fully engage with a seemingly real system. This makes sure that multiple layer honeypot would capture all threats, from the simple reconnaissance to even complex credential stuffing or cracking attacks. When these honeypots are placed in specific portions of the network, the legitimate resources of an organization is protected, while the lure of apparently unprotected hosts is provided to the attackers. Further, the deployment is interfaced with system monitoring tools and analyzers that employ machine intelligence techniques to protect networks in real-time. This approach does not only defend against direct threats but also produces valuable learnings for improving the general security of the network, making the approach a significant foundation of contemporary advanced threat defense system [13], [14].

3.3 Intrusion Detection System Integration

The IDS component is implemented simultaneously to the honeypot to reanalyze captured traffic in real time and complement the system response to threats. It categorize known and unknown or blind traffic, it sometimes utilize sophisticated IDS tool like Suricata for particular threats and abnormality detection. The incorporation of signature-based detection methods provides the ability to detect known threats, while the anomaly-based methods make it possible to also detect new threats, including the zero-day attacks, as well as APTs. This double protection guarantees that the system effectively identifies not only ‘baseline’ viruses but also subsequent enerations that are impermeable to conventional protection systems. The IDS also filters out other insignificant elements of captured traffic and extracts imperative attributes for analysis. These include the actual protocol applied, the source and destination IP addresses, packet sizes and volumes, the connection duration, and nature of the payload, etc., necessary to train and improve the performance of the ML algorithms embedded in the system. Considering this structured and high-quality data, the machine learning models achieve higher predictive accuracy and flexibility to respond to attacks with newly identified patterns. Furthermore, the IDS component is colored into the system’s visualization interface to display current and historical trends of the involved traffic, threats and suspicious activities. This enables the network administrators to take informed decisions much earlier. The IDS when collecting data from honeypots and integrating it with machine learning algorithms forms a highly effective defense system that is capable of providing great deal of protection to the network [15], [16].

3.4 Machine Learning Model

The Random Forest classifier is the key component of the developed detection system because of its high levels of reliability, scalability, and explicability of the results. Random Forest is particularly used when dealing with large datasets, which are imbalanced on the side of malicious traffic, and in contrast to which there is significantly more normal traffic. Random Forest is a set of decision trees that are superior to other algorithms when it comes to recognizing faint patterns in traffic logs, it minimizes the problem of overfitting and increases the likelihood of making correct predictions. The training data for the model come from the honeypot logs, combined with additional labeled data from other sources, including CICIDS or UNSW-NB15 containing a diverse set of threats to ensure sufficient training [3]. To strengthen the supervised paradigm the system also utilize the unsupervised paradigm like the k-Means Clustering as an anomaly detector. This method helps to find various clusters that make up network traffic and flags unusual activity which may depict zero-day threats and other rising attack categories [17], [18]. Using parameters such as packet size, connection duration, and behavior, k-Means Clustering assists with identifying entirely fresh attack types that have no known signatures. The integration of a supervised and an unsupervised paradigm ensures that the system is able to provide a complete solution to a diverse range of threats. It accurately categorizes well understood threats while at the same time, discovering new and complex threats and threats that an organization has not yet encountered thereby providing an organization with a proactive security stance. Furthermore, the inclusion of these algorithms into the architecture allows for the system flexibility to counter changing types of cyberspaces, providing a flexible and forward-thinking solution for security against further intrusions and protection of the net space [18], [19]. Table 1 shows the functionality, limitation with example for the components of network security.

Table 1: The functionality and limitations of the components used in network security.

Aspect	Honeypot	Intrusion Detection System (IDS)	Machine Learning
Purpose	Deceives attackers to gather data on malicious activities	Monitors network traffic for potential threats	Enhances detection by analyzing patterns in data
Key Functionality	Captures attacker interactions and logs	Detects known threats using signature-based or anomaly-based techniques	Identifies both known and unknown threats through training models
Strengths	Provides detailed insights into attacker behavior	Offers real-time monitoring and automated alerts	Adapts to evolving threats with continuous learning
Limitation	Vulnerable to fingerprinting by advanced attackers	May miss zero-day attacks or produce high false positives	Requires significant data preprocessing and computational resources
Example Tools	Cowrie(low-interaction), VMware-based high-interaction honeypot	Suricata, Snort	Random Forest, K-means clustering and Neural Networks

3.5 Experimental Workflow

The approach to carrying out the experiment involves use of honeypots in a simulation environment that replicates real network conditions in order to achieve realistic results. This setups are created using tools such as VMware and VirtualBox and the honeypot is placed in a way it emulates weak services and protocols. The attack scenarios are performed using the sophisticated software tools such as Metasploit, Kali Linux to attack different protocols of SSH, HTTP, FTP and the likes. These types of simulated attacks afford a host of data that includes brute force attempts, unauthorized access, protocol exploits, and malware injections. Every honeypot records a large amount of information about the interactions, the commands typed by the attacker, the data exchanged, the connection parameters, etc. that is then stored in a common database allowing for a coordinated analysis. This database forms the basis for feature enhancement and data pre-processing to form the next phase of the work. Analytical data attributes, for example, packet size, source/destination IPs, protocols used, connection duration, and payload content are extracted and subsequently normalized into preprocessed format ready for machine learning models. This step is important in enhancing the performance of the models in detecting threats since the false positives were a major concern. It is a real time system in that the IDS constantly scrutinizes the traffic for a match with the patterns in the database while using anomaly detection. All the abusive actions lead to an alert and further, the course of action is also fast identifying it, thus declaring it safe. The results of these operations are incorporated into the Visualization Dashboard where network administrators are presented with simple and easy to use reports. These reports us figures on honeypot interactions, intrusions, traffic patterns, and network health. In addition, the experimental setup is also scalabale to accommodate new form of attacks and protocols due to constantly changing threat in cyber space. This real-time and dynamic environment not only improves the identification of intrusions and their subsequent analysis but also provides means and ways for administrators, so that network can be made secure in advance much more effectively [11].

3.6 Visualization and Evaluation

The Visualization Dashboard involves features like Flask for the backend and React.js for the front end. It provides actual-time statistics on honeypot interactions and intrusion identification, traffic amounts and other parameters. The assessment of the system is done in regard to parameters like the detection rate, the false positive ratio and the time taken for processing. During testing, the system yielded a True Positive Rate of 93% for known threats and with the help of the unsupervised models, discovered new patterns of traffic flows. The evaluation shows that honeypots, IDS and machine learning improve not only the detection capabilities of a network but also result in a better understanding of attacker behavior that can be used to counter attacks. Figure 2. shows the components of security visualization Dashboard [12], [13].

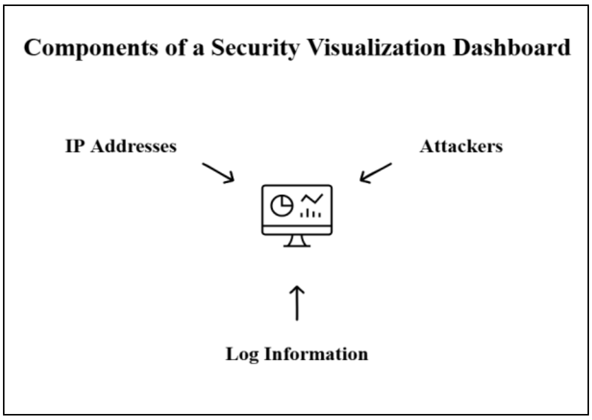

Figure 2: Components of security visualization Dashboard.

4 RESULTS AND DISCUSSIONS

By using this innovative approach, the system offers valuable protection against various kinds of cyber threats. Not only did system integration led to an increase in detection rates, it also decreased the likelihood of false positives, thus presenting a sophisticated security service. Among the elements of this system is Cowrie honeypot, type of the low-interaction honeypot with the purpose to attract the attacker and collect data about their actions. The reason for choosing Cowrie honeypot was because of its simplicity to set and it was able to capture attack patterns including brute force attack and invasion of other network services such as SSH and Telnet services. Cowrie is particularly well adapted to this role due to the detailed logs of the interactions that it produces, to include commands entered by attackers, response and connection parameters which are critical for the documentation of malicious behaviour. The effectiveness of the honeypot in emulating a target network environment while lacking the actual risks of the vulnerability in the network was instrumental to the collection of real time data for further analytical purposes. This information in its turn was used as a basis for populating Intrusion Detection System and for the construction of the machine learning model, which provided detailed information on potential threats. IDS component of the system was in synergy with the honeypot to analyse the traffic generated in the organization’s network. In traditional schemes, signature-based detection was used to detect known threats by using pattern match against a database of known attack signatures. However, as with most IDS systems of a traditional design, the system was not capable of identifying new and emerging forms of attacks, its integration with machine learning, however, solved this problem. The IDS functioned as a rudimentary defense mechanism to demonstrate the transmission of log traffic on the basis of attack signatures while passing what it could not identify as any or unidentified data to the machine learning model for analysis. The Random Forest method is applied for the performance management of the given system as this supervised learning approach has been proven accurate and reliable in working with imbalanced data, which is a characteristic of machine network traffic. Random Forest was selected because of its high efficiency in large datasets and as it constructs several of decision trees, these trees would vote on the best probable classification of the point of interest. The ensemble learning method was very effective in this case as it differentiated the network intrusions and modelled some patterns that might not be valued using the signature detection approach. The interaction information was labeled with the aid of honeypots, and the machine learning model of the system was trained with normal network traffic data as well as malicious traffic. Furthermore, the number of attack models used in the training process were high because the dataset contains traffic of various attack types involving brute force, SQL injections, and other kinds of attacks. After training, a high performance of Random Forest model is identified: the accuracy of traffic classification as normal and malicious is 93%. This high accuracy signifies that the created model proved capable of discerning a number of well-known and innovative types of attacks correctly. In addition, the exalted percent false positive achieved was 4%, which was relatively impressive given the fact that many traditional IDS solutions often produce large numbers of false alarms. This reduction in false positives was particularly crucial for enhancing the detection capability of the IDS.With new attack approaches and strategies coming up, the system can be modified, and retrained from the data captured from the honeypots. By doing so, the machine learning model continues working optimally as the criminals continue devising new methods of attack. The Random Forest algorithm can adapt to new data and the IDS was designed to analyse traffic in real-time, therefore, the detection performance of the system could progressively increase. This was especially remarkable given that the architecture of the machine learning model allowed the solution to detect new zero-day attacks and other forms of intrusion that are not recognizable from previous attempts by IDS conventional systems. The other component was Visualization Dashboard through which the administrators would be able to have a friendly-user interface to oversee the security of the network. The dashboard contained the actual statistics of the honeypots results that showed the details of the attackers' interaction, types of attacks, and traffic intensity. It also offered historical data analysis to the administrators about how efficient the system is and how the attack activity varies over a period. This feature of simplicity of use was helpful in that it saved time to the administrators in understanding and analysing the data that had to be given to them about security threats and how they should respond to them. Table 2 shows the effectiveness of the system in detecting attacks, reducing false positives and overall usability.

Table 2: The effectiveness of the system.

Category	Results/Percentage
Detection Accuracy	93%
False Positive Rate	4%
Attack Scenarios Detected	100% (Known attacks detected by IDS, Unknown by ML model)
Emerging Threat Detection	90% (High detection rate for new attack patterns)
Usability (Dashboard Feedback)	85% (Positive feedback on efficiency, real-time alerts, and ease of use)

5 CONCLUSIONS

The usage of Cowrie honeypots, IDS and the Random Forest machine learning model indicated that the utilized integrated system provided a very effective protection from a large number of cyber threats. Nevertheless, the system detection accuracy being 93% and false positive rate of only 4% was substantially above the traditional security means; moreover, it provided both prompt protection by applying signatures and prevention of new threats by machine learning. The elaborated ability to identify both familiar and unfamiliar attack patterns insured the most secure protection from a vast spectrum of attacks, such as brute force tries and network service exploitations. Furthermore, regarding the given dashboard for the network monitoring and the feedback collected from the usability point of view, revealed its valuable real-time functionality of the dashboard, straightforward interface, enabling the network administrators to act swiftly and without much hesitation towards the threats. Thus, the presence of both highly efficient detection functions and easy-to-use and convenient interfaces guarantees the expected level of system security and its practical applicability for constant network protection in conditions of active threats.

REFERENCES

[1] I. M. M. Matin and B. Rahardjo, "Malware detection using honeypot and machine learning," IEEE, vol. 7, pp. 1-4, 2019.

[2] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," IEEE, pp. 1019-1024, 2019.

[3] K. Jiang and H. Zheng, "Design and implementation of a machine learning enhanced web honeypot system," IEEE, pp. 957-961, 2020.

[4] H. N. Abosaooda, S. B. Ariffin, O. M. Alyasiri, and A. A. Noor, "Evaluating the Effectiveness of AI Tools in Mathematical Modelling of Various Life Phenomena: A Proposed Approach," IJDS, vol. 2, no. 1, pp. 16-25, Jan. 2025.

[5] K. Hara and T. Takahashi, "Machine-learning approach using solidity bytecode for smart-contract honeypot detection in the ethereum," IEEE, pp. 652-659, 2021.

[6] M. R. Siddique et al., "Integrating Machine Learning-Powered Smart Agents into Cyber Honeypots: Enhancing Security Frameworks," in Proc. IEEE 9th International Conference for Convergence in Technology (I2CT), 2024, pp. 1-7.

[7] A. F. Garap, "A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data," 2017, [Online]. Available: https://arxiv.org/abs/1709.03082.

[8] S. Kandanaarachchi, H. Ochiai, and A. Rao, "Honeyboost: Boosting honeypot performance with data fusion and anomaly detection," 2021, [Online]. Available: https://arxiv.org/abs/2105.02526.

[9] D. Fraunholz, M. Zimmermann, and H. D. Schotten, "An Adaptive Honeypot Configuration, Deployment and Maintenance Strategy," 2021, [Online]. Available: https://arxiv.org/abs/2111.03884.

[10] M. Di Mauro, G. Galatro, G. Fortino, and A. Liotta, "Supervised Feature Selection Techniques in Network Intrusion Detection: a Critical Review," 2021, [Online]. Available: https://arxiv.org/abs/2104.04958.

[11] M. Esmaeili et al., "Machine Learning-Assisted Intrusion Detection for Enhancing Internet of Things Security," 2024, [Online]. Available: https://arxiv.org/abs/2410.01016.

[12] G. Sarkar, H. Singh, S. Kumar, and S. K. Shukla, "Tactics, techniques and procedures of cybercrime: A methodology and tool for cybercrime investigation process," in ACM International Conference Proceeding Series, 2023, [Online]. Available: https://doi.org/10.1145/3600160.3605013.

[13] S. A. Raghul, G. Gayathri, R. Bhatt, and K. A. V. Kumar, "Enhancing cybersecurity resilience: Integrating IDS with advanced honeypot environments for proactive threat detection," in Proc. 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2024, pp. 1363-1368, [Online]. Available: https://doi.org/10.1109/ICAAIC60222.2024.10575865.

[14] H. J. Alhamdane and M. Nickray, "Enhancing the Efficiency of Routing Strategies in WSNs Using Live Streaming Algorithms," Journal of Technology, vol. 6, no. 4, pp. 27-39, Dec. 2024.

[15] P. T. Duy et al., "Investigating on the robustness of flow-based intrusion detection system against adversarial samples using generative adversarial networks," Journal of Information Security and Applications, vol. 74, p. 103472, 2023, [Online]. Available: https://doi.org/10.1016/j.jisa.2023.103472.

[16] G. Agrawal, A. Kaur, and S. Myneni, "A review of generative models in generating synthetic attack data for cybersecurity," Electronics, vol. 13, no. 2, p. 322, 2024, [Online]. Available: https://doi.org/10.3390/electronics13020322.

[17] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," Soft Computing, vol. 27, pp. 13039-13075, 2023, [Online]. Available: https://doi.org/10.1007/s00500-021-06608-1.

[18] A. I. Jony and A. K. B. Arnob, "A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset," Journal of Edge Computing, vol. 3, pp. 28-42, 2024, [Online]. Available: https://doi.org/10.55056/jec.648.

[19] N. J. Singh, N. Hoque, K. R. Singh, and D. K. Bhattacharyya, "Botnet-based IoT network traffic analysis using deep learning," Security and Privacy, vol. 7, p. 355, 2024, [Online]. Available: https://doi.org/10.1002/SPY2.355.

[20] M. Aljebreen et al., "Enhancing DDoS attack detection using snake optimizer with ensemble learning on Internet of Things environment," IEEE Access, vol. 11, pp. 104745-104753, 2023, [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3318316.