AI-Based Intrusion Detection and Prevention

Siwani Jaiswal
School of Technology
Pandit Deendayal Energy University
Gandhinagar, India
Siwani.jce20@sot.pdpu.ac.in

Suyamoon Pathak
School of Technology
Pandit Deendayal Energy University
Gandhinagar, India
suyamoon.pce20@sot.pdpu.ac.in

Viral Parmar
School of Technology
Pandit Deendayal Energy University
Gandhinagar, India
viralparmar93@outlook.in

***Abstract*—The Intrusion Detection System (IDS), used by most network systems to identify and prevent potential assaults, is currently drawing interest from both the business world and the research community. In this paper, we have studied about Intrusion detection and prevention systems that use different approaches, like signature-based, anomaly-based, stateful protocol analysis, and a hybrid system that includes some or all of the other systems, to identify and address security risks. We have studied about IDPS and its types viz. Host based and Network based. When attempting to select a technique and system to implement, the proliferation of systems that employ a variety of methodologies might be confusing. This paper aims to provide a thorough overview of each approach before presenting a means of contrasting them. We have also researched about SDN controllers and how it is used to implement NIDS (Network-based Intrusion Detection Systems).**

Keywords—intrusion detection systems, artificial intelligence, computational intelligence, hybrid intelligent systems, ensemble systems.

I. INTRODUCTION

A system that attempts to ascertain whether a system is being attacked to detect intrusions within a system is known as an intrusion detection system. IDSs, or intrusion detection systems, are often used. Attacks and anomalies are other names for intrusions. It accomplishes this by keeping an eye on the system or network activity. IDSs can be categorized in one way based on how they detect intrusion. The software is utilized to search for malicious activity or policy violations on a system or network. Any illegal activity or violation is typically logged centrally by a security information and event management (SIEM) system and notified to an administrator. A SIEM system combines the outputs from several sources and uses alarm filtering methods to distinguish between legitimate and erroneous warnings.

A network security technology known as an intrusion prevention system looks for unusual system or network behavior. The primary duties of intrusion prevention systems are to spot harmful behavior, gather data on it, report it, and make an effort to block or halt it. Because both IPS and IDS monitor network traffic and system operations for malicious behavior, intrusion prevention systems are thought of as an addition to intrusion detection systems (IDS). Typically, IPS creates reports, collects data about observed events, and alerts security administrators to significant observed occurrences. Many IPS can also react to danger by trying to stop it from happening. They employ various reaction strategies, including the IPS blocking the attack directly, altering the security context, or altering the assault's content.

II. LITERATURE REVIEW

Research on the shortcomings of intrusion detection led to the development of intrusion prevention. Research advanced a threat model that led to the development of intrusion prevention. By offering a paradigm for spotting anomalous behavior in computer systems, this research established the groundwork for intrusion.

The development of new communication technologies, including the Message Queuing Telemetry Transport (MQTT) protocol, was spurred by the development in the IoT field. Despite being the core of all MQTT-based IoT systems, MQTT servers and brokers are subject to possible cyberattacks including DoS, DDoS, and buffer overflow due to their openness. As a result, the IoT security environment currently lacks an effective intrusion detection mechanism for MQTT-based apps. Sadly, current IDSs do not enable IoT communication protocols like MQTT or CoAP to validate forged or malformed packets for securing IoT device protocol implementation vulnerabilities [1].

An Intrusion Detection System is the first option that springs to mind (Intrusion Detection System). Since the majority of intrusion detection systems rely on signatures, it is theoretically impossible to create a sophisticated intrusion detection system that can identify and stop existing attacks as well as anticipate upcoming ones. Other methods for intrusion detection are also provided, including Naive Bayes, Decision Trees, K-Nearest Neighbors, and Support Vector Machines. These methods were used to categorize both legitimate and malicious activities as well as the fundamental principles so that the appropriate responses could be taken to notify and deter incursion [2].

A hybrid approach that uses enhanced adaptive deployment algorithm (ADA-MLA), machine learning methods, and honeypot creation to assure network security against both known and unknowable assaults. The suggested approach is superior and sufficiently effective since it includes two key pieces of information, one of which is utilized to build profiles and the other to categorize those profiles after they have been built. The suggested hybrid technique develops a reliable model and

emerges as a predictive model that successfully distinguishes between threats and detects abnormal intrusions. In order to successfully identify the kind of assaults and prevent them from accessing the secure network, the suggested system is designed as an intrusion detection and prevention system [3].

Intrusion detection systems are not unaffected by the widespread usage of data mining in many fields. The network can be made more effective in the financial industry, which will mostly guarantee data security and productivity. We introduced an algorithm for intrusion detection that outperformed the signature Apriori approach in terms of outcomes. Data mining is used in security for a variety of reasons, including helping the banking and finance industries effectively address different security concerns. In order to notice the pattern or behavior of regularly targeting incursions recorded on one network and implemented on a different network, the use of machine learning and transfer learning may be extended in the future scope of this study [4].

Attacking or hacking refers to unauthorized access to a personal computer, a single system, or a network with the purpose of monitoring system access or stealing information. An effective security device known as an intrusion detection system can identify, stop, and maybe respond to hostile computer activity. Intrusion detection systems are used to safeguard computer networks and systems against misuse. The study's goal is to understand the potential for intrusion detection and extremely effective preventative measures. Using this model, it was possible to identify the effective intrusion detection algorithm, the Behavior Profiling Algorithm, as well as to carry out dynamic analysis using the Statistical Approach model using log files, which offer essential details about systems and the activities that take place on them. In the wired, wireless, and cloud networks, the suggested algorithm's model obtained results over 90%, 96%, and 98%, respectively [5].

The majority of technologies used in current IDS are unable to deal with the complex and dynamic environment of incursions, despite IDS's growing significance in the everyday digital world. To overload the resources of such incursions, modified reaction judgements should be conducted and triggered for every assault type. Then, a more advanced IDS design must be reliable, versatile, adaptive, and have a low frequency of false-positive results. Additionally, it must be able to handle increased network traffic, recognize a variety of assaults, and make wise runtime decisions. The use of artificial intelligence (AI) by many systems for intrusion detection and prevention has been growing steadily. As a result, AI's effective adaptive strategies may achieve greater detection rates, lower false alarm rates, lower transmission costs, and more efficient computational analysis. Additionally, it is capable of achieving the intelligent choice that the IDS design advocates. In addition, the AI-based IDS is taught to recognize even international threats and is quick to react to ecological variations [6].

In 5G networks, there is a lot of interest in software defined networking (SDN), network function virtualization (NFV), and cloud computing. However, this focus poses a new problem for these integrated systems' security provisioning. The intrusion detection and prevention system has lately been the focus of research in the fields of SDN, NFV, cloud computing, and 5G. (IDPS). The inadequacy of current IDPS systems might result in significant resource waste and several security risks. Timely discovery of an intruder is crucial for reducing security risks. Thus, in this study, we provide a unique method for multilayered intrusion detection and prevention (ML-IDP) in a cloud of 5G networks that is enabled by SDN and NFV. The proposed strategy uses artificial intelligence to guard against security assaults (AI) [7].

Information system security now depends heavily on intrusion detection and prevention systems (IDPS). Security technologies called IDPS are used to track, examine, and react to potential security breaches against computer and network systems. These infractions may be the consequence of system breach efforts by unauthorized external attackers or by inside privileged users abusing their power. The underlying techniques are not advancing at the same speed as the intrusion detection and prevention area and are gradually combining when new solutions are produced. When attempting to comprehend the detection procedures used by more recent systems, this leads to misunderstanding. The majority of the previous and present research in this field focuses on describing or enhancing one or two approaches. Some works compare one approach with a new one that has been offered [8].

By checking the network and server functionalities and alerting the analyst if any suspicious behavior is found in the network traffic, secure automated threat detection and prevention is the more efficient method to decrease the burden of analysts. It continually monitors the system and reacts in accordance with the threat environment. From phase to phase, this reaction action changes. In this case, suspicious activity is discovered with the use of artificial intelligence, which serves as a virtual analyst while working with network intrusion detection systems to protect against the threat environment and take necessary action with the analyst's approval. In the process's last stage, packet analysis is used to search for attack vectors and classify supervised and unsupervised data. With the assistance of analyst feedback, the unsupervised data will be decoded or transformed to supervised data, and the algorithm (Virtual Analyst Algorithm) will then automatically update. In order for the algorithm to improve over time and grow stronger and more efficient, it uses an active learning mechanism. As a result, it can fight against similar or identical assaults [9].

Network traffic is tracked by Intrusion Detection and Prevention Systems (IDPS), which analyzes and offers corrective measures when malicious activity is found. IDPS systems based on physical, virtual, and cloud infrastructure search for patterns in behavior or features that signal malicious traffic, notify the appropriate administrators and stop assaults in real time.

Malware, social engineering assaults, and other web-based threats, such as DDoS attacks, can all be found using IDPS technologies [10]. Additionally, they can offer proactive intrusion protection against internal threats and potentially vulnerable systems.

A. Types of IDPS:

1) Host-Based IDPS: Host-Based IDPS is software only used to track connections to and from the host. Usually, it just shields one particular endpoint. In some circumstances, it might also check the host's system files for unapproved modifications and active processes. Over network interfaces and the computer system, it detects and examines network packets. Systems on business networks that contain private data are the focus of attacks. The HIDS identifies the programs that can access assets and takes note of them. Assailants can still change the verification information because HIDS also monitors the data in the system.

2) Network-based IDPS: Network-based IDPS, also known as network intrusion detection systems (NIDS), are set up so they can watch over all of the activity on a network segment or subnet. Their functioning is similar to firewalls, which are limited to blocking incursions from the outside and enforcing Access Control Lists (ACLs) between networks. If no potentially harmful packets are transferred during the traffic monitoring, data is transmitted to the property owner. The network segment is monitored for illegal access and unusual activity [11]. In NIDS, packets accumulate from the network, and a NIDS detector or sensor is typically deployed at the organization's demilitarized zone.

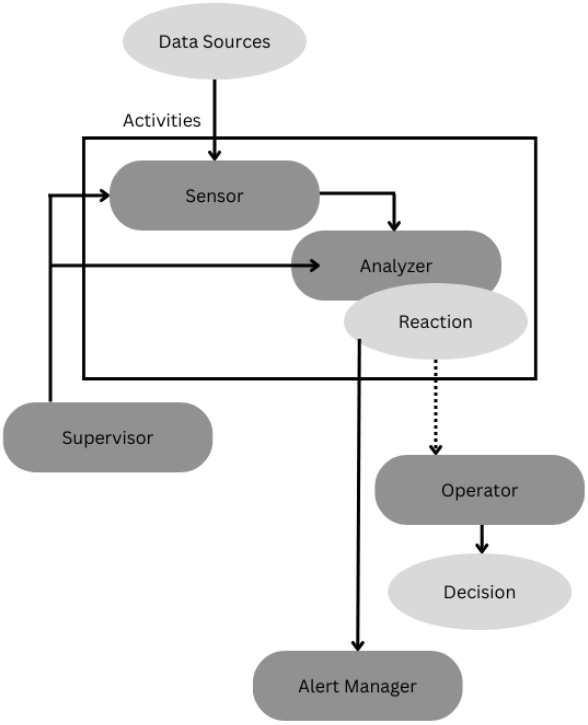

Fig1: General View of IDPS System

An IDPS system takes required data from its sources and passes through its sensors. Then, the sensor sends the results to analyzer where a reaction is generated. This analyzer decides if it is malicious, or not. If it is harmful to the system, it sends the reaction to Alert Manager and the user is alerted. Else, the reaction is sent to Operator and output is generated as per user's needs. Sensing and analyzing phase is also being continuously monitored by a Supervisor.

III. PROBLEM STATEMENT

The objective is to understand a network intrusion detector or prediction model and distinguish between intrusions and attacks, which are in poor, and good connections.

IV. PROPOSED STATEMENT

Network monitoring-based machine learning techniques have been used in several industries. The evaluation and identification of traffic accidents using bi-directional long-short-term memory neural networks are given in a social media network monitoring system. The recommended remedy gathers data on social media traffic via query-based crawling (Facebook and Twitter). This process collects sentences describing traffic-related incidents, including backups, road closures, etc. Many researches proposed machine learning algorithm for intrusion detection to reduce false positive rates and produce accurate IDS. However, to deal with Big Data, the machine learning traditional techniques take a long time in learning and classifying data. Using Big Data techniques and machine learning for IDS can solve many challenges such as speed and computational time and develop accurate IDS. The objective of this paper is to introduce techniques that deal with Big Data in IDS in order to reduce computation time and achieve effective classification. For this purpose, we propose an IDS classification based on decision trees.

V. RESEARCH GAP

Machine learning models are commonly used to identify threats, although AI-based IDS systems are preferable. Chuck Everette, director of cybersecurity advocacy at Deep Instinct, claims their accuracy rate may vary from the low 90 percentile to the 80 percentile. Most research on network intrusion detection systems (NIDS) that involve machine learning (ML) uses well-known datasets like KDD-CUP99, NSL-KDD, UNSW-NB15, and CICIDS-2017. In this context, it is necessary to investigate the potential of machine learning approaches to achieve metrics improvements over the reported baselines (model-centric approach).

VI. RESEARCH METHODOLOGY

An attacker creates and disseminates attacks online. The SDN c ontroller is used to implement NIDS. The NIDS component architecture consists of the following three main parts: The infrastructure layer's two main components are hardware and software. The physical components include things like switches and routers. Software components are those that communicate with hardware, such as OpenFlow switches.

The control layer consists of an intelligent network controller, such as an SDN controller. The control layer manages activities and traffic data by authorizing or denying each network flow. The application layer is the one that manages all network management tasks. An SDN controller and a NIDS can perform these tasks.

Because it actively listens to the network and examines every traffic for specified attack signatures, the NIDS may identify the attacker's scanning attempts. Through its administration, administrators are informed, and the connections are forbidden due to specific firewall or router regulations.

The IDPS employs a variety of approaches to identify alterations in the systems they watch—these alterations are assaults from the outside or inappropriate use by employees within. Four techniques stand out among the numerous others and are extensively applied. These are anomaly-based and signature-based, Based on stateful protocol analysis and a hybrid approach.

A. Anomaly-Based Methodology

Instead of producing fingerprints, anomaly-based intrusion detection constructs an initial "normal" behavior model for a particular system. The system will then compare every real-time behavior with the generated standard model to detect behavioral anomalies [12]. These unusual activity instances are considered for identifying prospective threats and setting off alarms.

B. Signature-Based Methodology

Intrusion detection using signatures searches for instances of recognized attacks. When malicious content is found, it is examined for distinctive characteristics to produce a fingerprint or attack signature. This signature could take the form of a recognized identity or behavioral pattern. Signature-based systems then determine the specific type of attack by comparing this fingerprint to a database of pre-existing signatures. The drawback of these systems is that they require constant updating to detect new and evolving attack types.

A signature-based technique is computer software that scans user activity for harmful behavior by comparing it to known signatures. Where the formula that describes the threat is the signature, the systems are aware of how risks appear by employing this technique [13]. Although this method is entirely accurate at detecting planned assaults and has a low rate of false positives, it cannot detect unknown threats.

C. Stateful Protocol Analysis

The Stateful protocol analysis approach compares actual behavior to predefined profiles of how protocols should behave. Stateful protocol analysis includes a thorough grasp of how the protocols and applications should interact and function, in contrast to signature-based technique, which just checks observed behavior against a list. The systems have a relatively high overhead as a result of this thorough understanding and analysis. Hybrid approaches have become more popular as a result of stateful protocol analysis's ability to complement and integrate well with existing IDPS methodologies [14]. As a foundation for creating IDPS that comprehend web traffic behavior and are successful at securing websites, stateful protocol analysis's in-depth understanding of how protocol should operate serves as a key foundation. Attacks that adhere to and remain within the permissible behavior of protocols can readily avoid Stateful protocol analysis, despite its thorough comprehension of the monitored protocols. Over the last ten years, stateful protocol analysis approaches and techniques have been gradually adopted and integrated into other methodologies. Due to this, IDPS that only use Stateful protocol analysis approach are on the decrease. Stateful protocol analysis is less viable as a solo IDPS approach since the majority of research on IDPS methodologies focuses primarily on anomaly, signature, and hybrid methodologies.

D. Hybrid Approach

Combining two or more of the other approaches is how the hybrid-based methodology functions. The outcome is an improved approach that benefits from the advantages of the merged methodologies. One of the earliest hybrid intrusion detection systems (IDS), Prelude, provided a framework based on the Intrusion Detection Message Exchange Format (IDMEF), an IETF standard that enables the communication of various sensors. In order to improve detection, Snort is updated by adding an anomaly-based engine to its signature-based engine. The new hybrid system is then evaluated against the original Snort using the same test data. Compared to the standard system, the hybrid one found more incursions. An anomaly-based model was used to filter the data in the hybrid intrusion detection system of cluster-based wireless sensor networks before it was followed by a signature-based model to detect intrusion attempts [15]. On the basis of how the human immune system functions, a different hybrid methodological model was put up. The suggested system "uses a hybrid architecture that applies both anomaly and abuse detection methodologies, and is built on the framework of the human immune system. The first approach analyzes the monitored environment before passing it on to the second and third methodologies. An improved system results from this.

	Anomaly	**Signature**	**SPA**	**Hybrid**
Resistance to evasion	Medium	Low	Low	High
High Accuracy rate	Medium	Medium	Medium	High
Market Share	Medium	High	Medium	Medium
Scalability	Medium	High	High	Medium
Maturity Level	High	High	High	Medium
Overhead on Monitored System	Medium	Low	Low	Medium
Maintenance	Low	Medium	Medium	Medium
Performance	Medium	High	High	Medium
Easy to configure	No	Yes	Yes	No
Easy to use	Medium	Low	Low	Low

Protection against new attacks	High	Low	Medium	High
False Positives	High	Low	Low	Low
False Negatives	High	Medium	Medium	Low

TABLE 1. Parameters for evaluating IDPS methodologies.

VIII. FUTURE WORK

In the upcoming studies, other assessment indicators will be applied. The method will be implemented using various deep neural network techniques, such as Auto-Encoder, Generative Adversarial Networks, and Recurrent Neural Networks, including GRU and LSTM. These techniques have been shown to offer workable solutions for anomaly detection in NIDS applications in the literature. We also plan to evaluate these approaches and add one or more neural network designs to learn more about how we may develop an efficient anomaly detection system in NIDS with reduced time and resource usage.

IX. SCOPE LIMITATION

There is a good chance that the promising capabilities of the advancements in hybrids and ensembles of existing techniques for more proactive detection of network intrusions will find even more successful applications, given the reports in the literature about the successful applications of AI techniques and the few ones reported on hybrid techniques.

By fine-tuning the parameters of existing techniques, further effort can be put into improving them. Some specific search techniques, including genetic algorithms, particle swarm optimization, ant colony optimization, etc., can be used to adjust parameters automatically.

X. CONCLUSION

Given the brief overview of the use of artificial intelligence techniques and their developments, and their outstanding performance in literature, we conclude that more research in this field is required, given the promising outcomes that may be obtained from such techniques. The combination and hybridization of multiple AI algorithms also point to a promising future for IDS analysis and prediction of its numerous properties for efficient real-time network security.

XI. ACKNOWLEDGEMENTS

We would like to acknowledge the Department of Computer Science And Engineering, School Of Technology, Pandit Deendayal Energy University, Gandhinagar, Gujarat, India for their support during this study.

REFERENCES

[1] Abdulhammed, R., Faezipour, M., & Elleithy, K. M. (2016). Network intrusion detection using hardware techniques: A review. *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. https://doi.org/10.1109/lisat.2016.7494100

[2] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2020). Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. *Computer Networks*, *179*, 107364. https://doi.org/10.1016/j.comnet.2020.107364

[3] Adat, V., & Gupta, B. B. (2017). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423–441. https://doi.org/10.1007/s11235-017-0345-9

[4] Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

[5] Ahmed, M. R. A. G., & Ali, F. M. A. (2019). Enhancing Hybrid Intrusion Detection and Prevention System for Flooding Attacks Using Decision Tree. *2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*. https://doi.org/10.1109/iccceee46830.2019.9071191

[6] An Efficient Intrusion Detection System by Using Behaviour Profiling and Statistical Approach Model. (2020). *The International Arab Journal of Information Technology*, *18*(1), 114–124. https://doi.org/10.34028/iajit/18/1/13

[7] Azad, M. A., Morla, R., & Salah, K. (2018). Systems and methods for SPIT detection in VoIP: Survey and future directions. *Computers &Amp; Security*, *77*, 1–20. https://doi.org/10.1016/j.cose.2018.03.005

[8] Et. al., K. N. (2021). A Hybrid Adaptive Development Algorithm and Machine Learning Based Method for Intrusion Detection and Prevention System. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), 1226–1236. https://doi.org/10.17762/turcomat.v12i5.1789

[9] Husnain, M., Hayat, K., Cambiaso, E., Fayyaz, U. U., Mongelli, M., Akram, H., Ghazanfar Abbas, S., & Shah, G. A. (2022). Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System. *Sensors*, *22*(2), 567. https://doi.org/10.3390/s22020567

[10] Karan Napanda, Harsh Shah, & Lakhsmi Kurup. (2015). Artificial Intelligence Techniques for Network Intrusion Detection. *International Journal of Engineering Research And*, *V4*(11). https://doi.org/10.17577/ijertv4is110283

[11] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems:

techniques, datasets and challenges. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-019-0038-7

[12] Mudzingwa, D., & Agrawal, R. (2012). A study of methodologies used in intrusion detection and prevention systems (IDPS). *2012 Proceedings of IEEE Southeastcon*. https://doi.org/10.1109/secon.2012.6197080

[13] Nazih, W., Hifny, Y., Elkilani, W., Abdelkader, T., & Faheem, H. (2019). Efficient Detection of Attacks in SIP Based VoIP Networks Using Linear l1-SVM Classifier. *International Journal of Computers Communications &Amp; Control*, *14*(4), 518–529. https://doi.org/10.15837/ijccc.2019.4.3563

[14] Cremers, C. J. F., Lafourcade, P., & Nadeau, P. (2009). Comparing State Spaces in Automatic Security Protocol Analysis. *Formal to Practical Security*, 70–94. https://doi.org/10.1007/978-3-642-02002-5_5

[15] Singh, P., & Venkatesan, M. (2018). Hybrid Approach for Intrusion Detection System. *2018 International Conference on Current Trends Towards Converging Technologies (ICCTCT)*. https://doi.org/10.1109/icctct.2018.8551181