BioGecko

Vol 12 Issue 03 2023
ISSN NO: 2230-5807

A REVIEW ON MACHINE LEARNING-BASED IDS FRAMEWORK FOR NETWORK BALANCING

Vineeta Shrivastava[1], Anoop Kumar Chaturvedi[2]
[1] PhD Research Scholar, School of computer science and Technology , LNCT University, Bhopal, M.P, India
[2] Professor, School of computer science and Technology , LNCT University, Bhopal, M.P, India
E-mail:-[1]Shrivastavavinita21@gmail.com, [2]anoop.chaturvedi77@gmail.com

ABSTRACT
An essential instrument for monitoring and identifying intrusion threats is the intrusion detection system (IDS). This paper tries to analyze current IDS machine-learning research. Strategy based on machine learning (ML), with a focus on datasets, ML algorithms, and metrics. To make sure the model is suitable for IDS application, dataset selection is crucial. The efficiency of the ML method can also be impacted by the dataset structure. An important aspect of intrusion detection is anomaly detection, where deviations from typical behavior point to the presence of intentional or accidentally generated attacks, malfunctions, and flaws among others. This paper provides a summary of research work and future directions for controlling the anomaly detection problem using machine learning and deep learning-based methods. Therefore, based on this review, we offer suggestions and directives to researchers.

Keywords: Anomaly detection, machine learning, security and privacy protection, Machine Learning, Soft Computing.

INTRODUCTION

Data protection is a matter of preventing and detecting unauthorized access to any computer. Computer protection thus offers a measure of the level of prevention and detection that promotes the avoidance of suspicious users. These suspicious and unauthorized users are usually referred to as “Intruders” Here, access to every section of the computer system is stopped. The detection mechanism is used to determine whether or not anyone within the target system is going to try to violet, whether it happened successfully, and whether it can be used to find logs of their activities. Intruders take over the benefits of machines from different activities in the way of banking and investing in shopping with the aid of some means of communication. Although it does not consider top secret correspondence, it does not want strangers to read emails, use computers to attack or disrupt other systems, send falsified messages or emails from a computer system, or check personal information stored on the end computer that may contain information such as financial statements, account details, etc. Attackers, crackers or hackers are often referred to as intruders. The identities of the target device owner will not care about them. They still monitor the machine so that they can use attacks against other desired computer systems to launch them. Typically, attackers gain control over target structures like government or financial firms, which allow them to mask them and their current positions and thus easily launch intrusions/attacks. If these hidden tasks are completed or only used by gamers to talk with friends, it does not matter whether a computer device that is connected to the internet is attacked. They can breach system information, reformat the hard drive, cause damage of any sort, etc. To secure the device, it is highly unfortunate that new bugs, also known as holes, are often discovered by intruders. Device or machine applications are exploited as a consequence of these vulnerabilities. The problem with software makes it impossible for computer system protection to be thoroughly tested. Alternatively, the user has to configure the

application for working in a more safe way to receive and install file patches.
In addition, such software applications have predefined common settings that allow access to other users' computer rights unless they make settings safer. For example, chat programmes that allow externals to execute commands on a computer that allows anyone to implement destructive programmes while clicking by users. It would certainly not encourage a stranger to look at sensitive documents. Similarly, you may want to keep the tasks private, whether you monitor our documents or perform other applications, on the machine. Users will need to be confident that the input information in the device is kept intact and that it is accessible if appropriate.
Security policy disqualification may be created with the potential of intentional manipulation of our device by intruders via the Internet. There are also other threats, even if users are not connected to the internet such as hard drive failures, theft, power failures, etc. The bad news is that it might not be able to plan all future threats. There is also good news here that some typical measures can be taken to decrease the risk of being hit by the most common threats. The principle of IDS is shown in figure 1.Any of these measures lead to face both the deliberate and unintended risks. Let us take a descriptive look at some of these relevant security threats before we know what we can do to safeguard our device or home network. Here are some very common methods, also briefly mentioned below, used by intruders to manipulate computers.

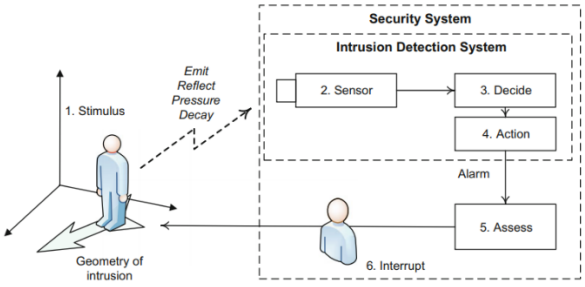

Figure 1: Principle of Intrusion Detection

BRIEF HISTORY OF IDS

The idea of detecting the intrusions or system misuses by looking at some kind malicious patterns in the network or user activity was initially conceived by James Anderson in his report titled "Computer Security Threat Monitoring and Surveillance" [2] to US Air Force in the year 1980. In the year 1984, the first prototype of Intrusion Detection System which monitors the user activities, named "Intrusion Detection Expert System" (IDES) was developed. In the year 1988, "Haystack" became the first IDS to use patterns and statistical analysis for detecting malicious activities, but it lacked the capabilities of real time analysis.
The intrusion detection market began to gain in popularity and truly generate revenues around 1997. In that year, the security market leader, ISS, developed a network intrusion detection system called "Real Secure". A year later, Cisco recognized the importance of network intrusion detection and purchased the Wheel Group, attaining a security solution they could provide to their customers. Similarly, the first visible host-based intrusion detection company, Centrax Corporation, emerged as a result of a merger of the development staff from Haystack Labs and the departure of the CMDS team from SAIC. From there, the commercial IDS world expanded its market-base and a roller coaster ride of start-up companies, mergers, and acquisitions ensued. Martin Roesch, in the year 1998 launched a light weight open source Network IDS named "SNORT" [3], which has since then gained much popularity. In year 1999 Okena Systems worked out the first Intrusion Prevention System (IPS) under the name "Storm

Watch". IPS are the systems which not only detect the intrusions but also are able to react on alarming situation. These systems can co-operate with firewall without any intermediary applications.
According to given study following problems are arise:
As network intrusion continues to evolve, the pressure on network intrusion detection is also increasing. In particular, the problems caused by imbalanced network traffic make it difficult for intrusion detection systems to predict the distribution of malicious attacks, making cyberspace security face a considerable threat.
Intrusion features selection is an issue.
Block chain systems are decentralized system with limited security so it's difficult to handle intrusions.

LITERATURE REVIEW

Within the domain of cybersecurity, particularly for detecting intrusions or cyber-attacks, several researchers used machine-getting to know the type strategies stated above.
Iqbal H.et al [8] to detect diverse cyber-assaults or anomalies in a community and construct a powerful intrusion detection system proposed a version named Intrusion Detection Tree ("IntruDTree") device-mastering-based protection version. The limitation of this work is that it does not show effectiveness on large datasets.
Li et al. [9] provided an approach to classify the predefined attack classes inclusive of DoS, Probe or scan, U2R, R2L, in addition to normal visitors making use of the maximum famous KDD'ninety nine cup dataset with the aid of the use of the hyperplane-based support vector gadget classifier with an RBF kernel.
Quanyan et al. [10], and Sangkatsanee et al. [11] used the selection tree classification approach in their research to construct intrusion detection systems. But, with the excessive dimensions of safety features, a choice tree model may additionally reason several problems including high variance with over-becoming, high computational fee and time, and occasional prediction accuracy.
Sarker et al. [12] proposed currently, a behavioral decision tree set of rules is known as BehavDT for studying behavioral styles. The exceptional acknowledged techniques for routinely building choice bushes are the ID3 and C4.5 algorithms. These days, a behavioral choice tree algorithm called BehavDT for studying behavioral patterns.
Alrowaily et al. [13] several experiments have been executed on seven device mastering algorithms by using using the CICIDS2017 intrusion detection dataset.
Zegeye et al. [14] proposed a machine gaining knowledge of Multi-Layer Hidden Markov (HMM) version-based intrusion detection. The proposed gadget is famous for its excellent overall performance amongst all assessment metrics as 98% accuracies, 93% precision, 99.9% real, and 98 % F I-score.
Papamartzivanoset al.[15] The arrival of present-day assaults drives the industrial corporation and educational network to look at for particular procedures, which control to tightly hold song of this opposition and satisfactory-song swiftly to the alterations inside the subject
Imran et al. [16] Propose an intrusion detection approach for the present-day network surroundings through thinking about the facts from satellites for computer and global networks. Incorporating machine getting to know fashions, the study proposes an ensemble version RFMLP that integrates random woodland (RF) and multilayer perceptron (MLP) for increasing intrusion detection overall performance.
Shojafaret al.[17] An unsupervised studying the approach for intrusion detection has been designed to find clusters based totally on similarity supervised getting to know fashions want labels for training and display proper consequences.

Andresen et al. [18] Deep learning techniques to know models and deep hierarchical models Jiang et al. [19] have been proposed to research non-linear relationships of facts for malicious assault detection. ANN is applied at the KDD99 dataset for intrusion detection with the aid of lowering dimensions from correlation and statistics benefits. The version showed progressed results in terms of accuracy.

Abdulrahman et al. [20] Proposed a hybrid optimized long short-term memory (LSTM) to predict and identify network attacks in an IoT network Firefly swarm optimization is integrated with LSTM to reduce the computational overhead, which in flip increases the prediction accuracy. Nearly 19,00,503 actual-time normal and attack information had been accumulated from the experimental simulation setup primarily based on the OMNET++–Python–IoT framework.

Ruohao et al. [21] Proposed an algorithm called AMDES (unmanned aerial system multifractal analysis intrusion detection system) for spoofing attack detection based on wavelet leader multifractal analysis (WLM) and machine learning (ML) The model achieves an accuracy of 98.58%.

Zhang et al. [22] Present an exciting implementation of deep getting to know Networks along with a trainer–scholar network structure, which indicates promising perspectives for implementation in a cell environment. The proposed community is pretty lightweight, allowing it to be incorporated right into a low-electricity platform, along with a UAV, whilst being able to perform accurate traffic photo classification.

Ashraf et al. [23] present an intensive and current review of the modern-day IoT-related IDS. And also offer a complete creation to the systems of modern IoT structures. The demanding situations and corresponding IDS research are offered.

Aldweesh et al. [24] reviewed the current improvements in deep getting to know-based IDS and provide a clear evaluation of an expansion of deep gaining knowledge of-based IDS of differing taxonomies. Their article is an incredible manual for popular deep gaining knowledge of algorithms for IDS.

X. Zhou et al. [25] propose a technique to solve the economic huge statistics anomaly detection problem by way of applying a variation LSTM (VLSTM) framework, which incorporates an LSTM based encoder-decoder structure The VLSTM framework allows for the extraction of a selection of capabilities, and as a result lets in for the detection of diverse styles of anomalies.

Kushinagar et al. [26] propose a technique choice technique (EFFST) to achieve a substantial characteristic subset for internet attack detection using choosing one-fourth split of the ranked capabilities. The experimentation at the CICIDS 2017 dataset indicates that the proposed EFFST method offers a detection fee of 99.09%, with J48 the usage of 24 functions.

Wu Wang et al. [27] proposed a method to discover malicious attacks focused on SCADA systems. Specially, we look into the feasibility of a deep studying approach for intrusion detection in SCADA systems the take a look at also showed that the proposed method outperformed the standalone deep studying fashions.

Yang et al. [28] introduced a way for assessing oil and gas SCADA safety through the use of causality evaluation. This approach adopted the causality analysis evaluation method of fuzzy logic reasoning for assessing elements neurons in the added approach. It's been proven that the causality analysis-driven technique gives true ability in assessing SCADA information protection.

Pan, Z et al. [29] introduced an intrusion detector, which is based on the concept of Context Awareness and Anomaly Behavior Analysis (ABA), to identify and classify different types of attacks in Building Automation and Control network (BACnet).

Linda et al. [30] proposed an anomaly detection scheme based on neural networks, and they exploited

the SCADA network and system information to handle the problem of bad packets. However, this solution can only handle external attacks; the internal attackers can still introduce malicious command packets to infect central equipment.

Basnet et al. [31] proposed a deep studying-based intrusion detection system (IDS) to detect the denial of carrier (DoS) assaults inside the EVCS. The deep neural community (DNN) and long-quick period memory (LSTM) algorithms are carried out.

Gottumukkala et al. [32] Supervisory control, and data acquisition (SCADA) gadget, inner sensors, and electric-powered cars (EVs) through the net to make certain energy performance and availability. Permitting wireless technology might be wireless, cell, Bluetooth.

D.J Atul et al. [33] Recommend strength conscious smart home (EASH) framework to remedy the trouble in communication failures and types of network attacks are analyzed in EASH. The model achieves an accuracy of 85%.

Rahman et al. [34] proposed a new technology-based totally on the IDS machine of the internet of things. To transmit the processing paintings, they improve comparable person models of learning that correspond to a shared set of pressure records. In mild of similar research of work whilst clarifying the mathematical outcomes and the rundown of proposed techniques, supply SDI detection exactness corresponding to senior facilities, and shows the inherent barriers among accuracy and creation time

Wenjuan Li et al. [35] studied semi-supervised studying and designed DAS-CIDS by way of making use of disagreement-based semi-supervised gaining knowledge of a set of rules to the CIDS system. The experimental results showed that their method became greater effective than conventional supervised classifiers at detecting intruders and lowering fake positives the usage of unlabelled records.

Daming Li et al. [36] proposed IoT extraction highlights and interruption popularity algorithms for the motion-primarily based intelligent city within the learning version joins the profundity version of interruption location innovation with learning.

G.Yedukondalu et al. [37] propose an application has used the SVM (Support Vector Machine) and ANN (Artificial Neural Networks) Algorithms to detect the intrusion rates. Each algorithm is used to detect whether the requested data is authorized or contains any anomalies. While IDS scans the requested data if it finds any malicious information it drops that request. These algorithms have used Correlation-Based and Chi-Squared Based feature selection algorithms to reduce the dataset by eliminating the useless data.Figure 2 shows comparasion of accuracy and precision of various techniues.

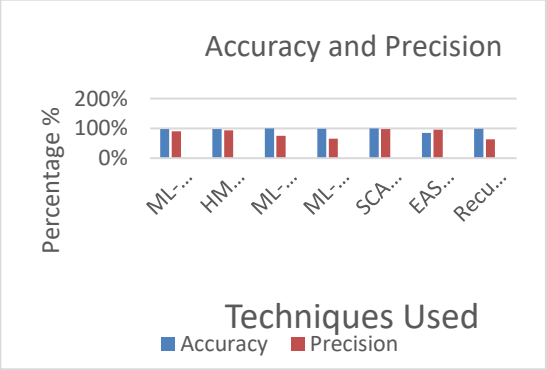

Figure 2: Comparison of accuracy and precision various techniques

INTRUSION DETECTION TECHNIQUES

Various techniques are in place for intrusion detection which can be broadly classified as follows.

- **Signature/pattern based Detection**

In this technique, the sensors which are placed in different LAN segments filter and analyse network packets in real time and compares them against a database of known attack signatures. Attack signatures are known methods that intruders have employed in the past to penetrate a network. If the packet contents match an attack signature, the IDS can take appropriate countermeasure steps as enabled by the network security administrator. These countermeasures can take the form of a wide range of responses. They can include notifications through simple network management protocol (SNMP) traps or issuance of alerts to an administrator's email or phone, shutting down the connection or shutting down the system under threat etc.

An advantage of misuse detection IDS is that it is not only useful to detect intrusions, but it will also detect intrusion attempts; a partial signature may indicate an intrusion attempt. Furthermore, the misuse detection IDS could detect port scans and other events that possibly precede an intrusion.

- **Unauthorised Access Detection**

In unauthorised access detection, the IDS detects attempts of any access violations. It maintains an access control list (ACL) where access control policies for different users based on IP addresses are stored. User requests are verified against the ACL to check any violations.

- **Behavioural Anomaly (Heuristic based) Detection**

In behavioural anomaly detection method, the IDS is trained to learn the normal behavioural pattern of traffic flow in the network over an appropriate period of time. Then it sets a baseline or normal state of the network's traffic, protocols used and typical packet sizes and other relevant parameters of network traffic. The anomaly detector monitors different network segments to compare their state to the normal baselines and look for significant deviations.

- **Protocol Anomaly Detection**

With this technique, anomaly detector alerts administrator of traffic that does not conform to known protocol standards. As the protocol anomaly detection analyzes network traffic for deviation from standards rather than searching for known exploits there is a potential for protocol anomaly to serve as an early detector for undocumented exploits.

IDS RESPONSES AGAINST ATTACK

Whenever IDS detects any intrusions or attacks, it reacts as per the preconfigured settings. The responses can range from mere alert notifications to blocking of the attacks based on the severity. The appropriate reactions on the threats are a key issue for safety and efficacy. Generally the responses can be of three types [2]

- **Active response**

IDS by itself cannot block attacks, however can take such actions which can lead to stopping of attacks. Such actions can be for example, sending TCP reset packets to the machine(s) which is being the target of attack, reconfiguring router/firewall as to block the malicious connection. In extreme cases, IDS can even block all the network traffic to avoid potential damage to the firm.

- **Passive response**

Passive solutions deliver information to IDS administrator on the current situation and leave the decision to take appropriate steps to his discretion. Many commercial systems rely on this kind of reactions. Examples for this kind of actions can be simple alarm messages and notifications. Notifications can be sent on email, cellular phone or via SNMP messages.

- **Mixed response:**

Mixed responses combine both active as well as the passive responses appropriately as per the needs of situation.

DEEP LEARNING METHODS FOR IDS

Deep learning is one of the most up-to-date ways to improve the accuracy of facial recognition software. Deep learning extracts unique facial embedding from images of faces and uses a trained model to recognize photos from a database in other photos and videos.

- **Deep Learning Techniques used in IDS**

Intrusion detection systems primarily use two key intrusion detection methods: signature-based intrusion detection and anomaly-based intrusion detection. Signature-based intrusion detection is designed to detect possible threats by comparing given network traffic and log data to existing attack patterns.

Convolutional Neural Networks: Convolutional neural networks (CNNs) or shift invariant artificial neural networks (SIANNs) are particular types of neural networks that, in their hidden layer they have different filters or regions that respond to a specific feature of the input signal. The visual neural cortex as a spatially specialized structure, in which every region responds to a specific characteristic of the input signal. One positive perspective of CNNs is the ability to learn features from high-dimensional input data; however, it also learns features from small variations and distortion appearance that leads to the large storage requirement at the time of development. Hence, in CNNs, there usually exists a layer of convolution followed by a down sampling mechanism.

- **Deep Convolutional Neural Networks**

Deep convolutional networks usually consist of multiple layers of convolution nodes, followed by one or more fully connected layers to finish the classification task. In SER, there are many efforts on deep convolutional neural networks, which we will review some of the most recent ones in the following part.A method based on a deep neural network containing convolutional pulling and fully connected layers. They have implemented their system on the Berlin Database of Emotional Speech. To compare to previous research, they have limited their classes to angry, neutral, and sad. [9]

- **Recurrent neural networks**

Recurrent neural networks can learn and react to the temporal event without changing the slowly shaped weights thanks to their feedback connection, forming short-term activations for recent events. This feature can be beneficial in case of applications that time is an essential feature, like Speech Processing, music composition, and video description. However, as they are trained using Back Propagation through Time, error signals flowing backward in time can either become bigger and bigger or vanish depending on the size of the weights. This will create either oscillating weights or makes the network to be slow to train and converge.

PROPOSED METHODOLOGY

Methodology

The proposed deep intrusion detection model composed of two major engines: learning and detection. The learning unit pre-processes traffic link records, resulting in traffic data in a format suitable for processing by the deep convolution neural network of the classification engine, with these connections categorized as regular or assault by the deeper intrusion prevention engine. For improved normal/attack classification prediction, the model uses a neural network trained by an adaptive version of the detection CNN algorithm. Fast response and reliable real-time security safety for the IoT system are enabled by a recursive structure from nonlinear parts' outputs of neurons to the liner parts. The CNN network reflects the designation analysis for traffic, namely analyzing the network traffic attempting to

access the IoT requirements and ensuring warning message when the attack is detected. The flowchart of proposed model is shown below in figure 3 and figure 4 which shows learning model and detection model respectively.

In this research, a deep learning-based approach was used to detect attacks based on the similarity of sliding windows that can detect type of attacks. The proposed model consists of two stages.

Proposed Algorithm

Algorithm: Stage 1 (Learning)

1: Extract the features of incoming traffic
2: Evaluate the similarities among them.
3: Set the sliding window on incoming data packets.
4: Learn the CNN model.
5: Evaluate error
6: Increment the window.

Algorithm: Stage 1 (Detection)

7: Extract the features of distributed IoT network from incoming traffic
8: Set the sliding window on incoming data packets.
9: Evaluate the deviation from normal behavior.
10: Increment the window.

Flowchart of Proposed Model

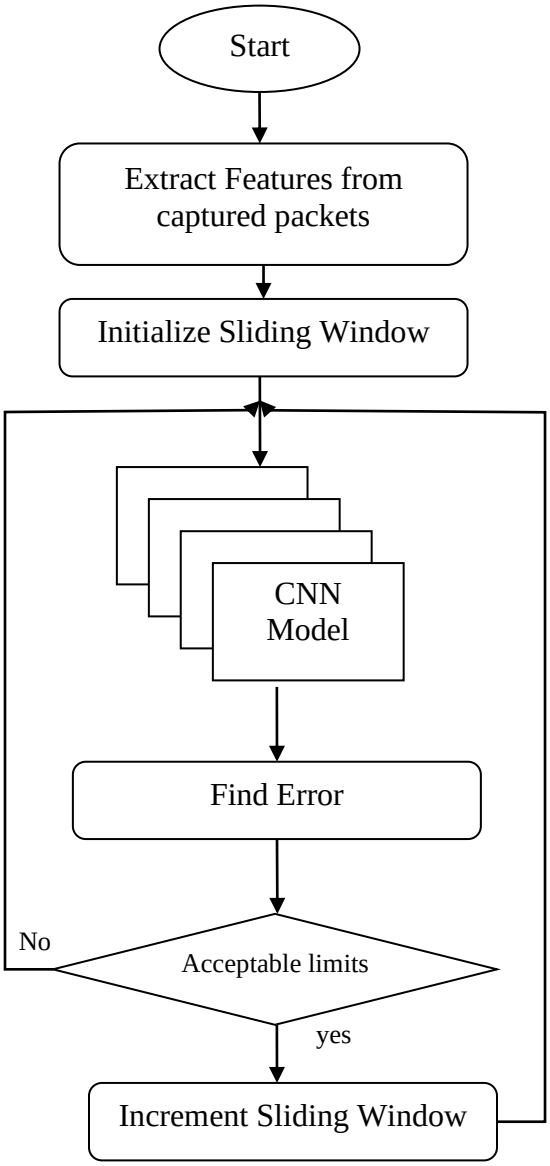

Figure 3: Learning Flow Chart

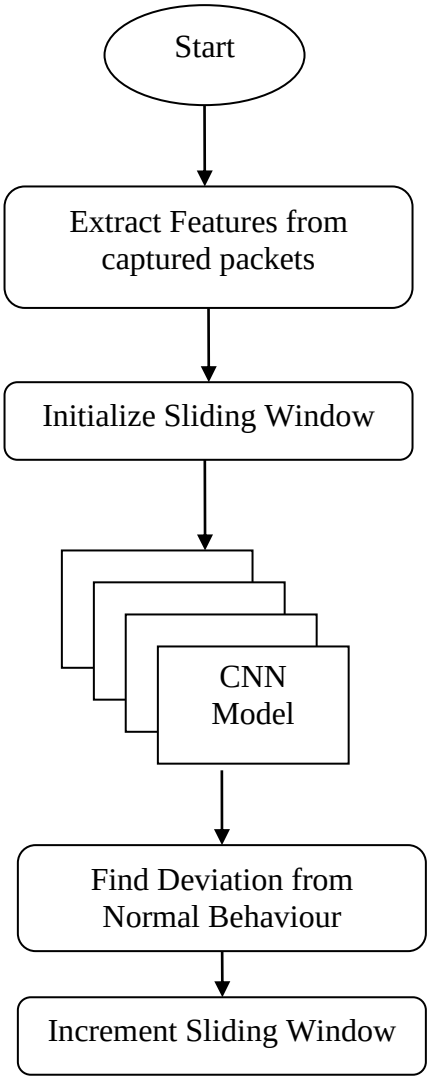

Figure 4: Detection Flow Chart

Key features of designed models are:

- Can handle class imbalance issue while learning.
- Can also handle missing data issues while learning.
- Can handle distributed network traffics.
- Can handle heterogeneous nature of network.
- Can be scalable.

CONCLUSION AND FUTURE DIRECTION

The rising amount of network traffic poses a security risk for security breaches such as DoS attacks, etc. It calls for a safety solution to avoid such attacks. First, we need to consider a method for detecting attacks to prevent all kinds of attack. Machine learning techniques have proven to be effective for intrusion detection. Intruder detection of intruders can be achieved with machine learning techniques, although the accuracy of detection also depends on several other factors. Some of them choose the right set of functions, choose the appropriate training and test data, etc. In future work we will implement our

proposed workflow to get better accuracy. Following features will enhance the performance of the system.

- Scalable Intrusion Detection Techniques: The Internet of Things (IoT) is a large-scale heterogeneous network with different networking paradigms and applications, each with its own set of capabilities and specifications. Intrusion detection will thus be a challenging task for such a communication environment.
- Capable of Handling generic attacks: The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. IDS and IPS technologies offer many of the same capabilities, and administrators can usually disable prevention features in IPS products, causing them to function as IDS.

REFERENCES

M. Zeeshan et al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," in IEEE Access, vol. 10, pp. 2269-2283, 2022, doi: 10.1109/ACCESS.2021.3137201.

O. Alkadi, N. Moustafa, B. Turnbull and K. -K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9463-9472, 15 June15, 2021, doi: 10.1109/JIOT.2020.2996590.

M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March1, 2021, doi: 10.1109/JIOT.2020.3002255.

N. Ravi and S. M. Shalinie, "Semi-supervised-Learning-Based Security to Detect and Mitigate Intrusions in IoT Network," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 11041-11052, Nov. 2020, doi: 10.1109/JIOT.2020.2993410.

Li, J., Zhao, Z., Li, R., Zhang, H.: AI-based two-stage intrusion detection for software defined IoT networks. IEEE Internet Things J. 6, 2093–2102 (2019).

S. SibiChakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi and B. Raman. Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks. IEEE Access, 2020;8: 169944-169956.

S. U. Jan, S. Ahmed, V. Shakhov and I. Koo. Toward a Lightweight Intrusion Detection System for the Internet of Things. IEEE Access, 2019;7: 42450-42471

I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, “IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model,” *Symmetry (Basel).*, vol. 12, no. 5, 2020, doi: 10.3390/sym12050754.

Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, “An efficient intrusion detection system based on support vector machines and gradually feature removal method,” *Expert Syst. Appl.*, vol. 39, no. 1, pp. 424–430, 2012, doi: https://doi.org/10.1016/j.eswa.2011.07.032.

Q. Zhu, C. Fung, R. Boutaba, and T. Basar, “GUIDEX: A Game-Theoretic Incentive-Based Mechanism for Intrusion Detection Networks,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 11, pp. 2220–2230, 2012, doi: 10.1109/JSAC.2012.121214.

P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, “Practical real-time intrusion detection using machine learning approaches,” *Comput. Commun.*, vol. 34, no. 18, pp. 2227–2235, 2011, doi: https://doi.org/10.1016/j.comcom.2011.07.001.

I. H. Sarker, A. Colman, J. Han, A. I. Khan, Y. B. Abushark, and K. Salah, “BehavDT: A Behavioral Decision Tree Learning to Build User-Centric Context-Aware Predictive Model,” *Mob. Networks Appl.*, vol. 25, no. 3, pp. 1151–1161, 2020, doi: 10.1007/s11036-019-01443-z.

M. Alrowaily, “Digital Commons @ University of South Florida Investigation of Machine Learning Algorithms for Intrusion Detection System in Cybersecurity,” no. March, 2020.
W. K. Zegeye, R. A. Dean, and F. Moazzami, “Multi-Layer Hidden Markov Model Based Intrusion Detection System,” *Mach. Learn. Knowl. Extr.*, vol. 1, no. 1, pp. 265–286, 2019, doi: 10.3390/make1010017.
D. Papamartzivanos, F. Gómez Mármol, and G. Kambourakis, “Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems,” *IEEE Access*, vol. 7, pp. 13546–13560, 2019, doi: 10.1109/ACCESS.2019.2893871.
I. Ashraf *et al.*, “A Deep Learning-Based Smart Framework for Cyber-Physical and Satellite System Security Threats Detection,” *Electronics*, vol. 11, no. 4, 2022, doi: 10.3390/electronics11040667.
M. Shojafar, R. Taheri, Z. Pooranian, R. Javidan, A. Miri, and Y. Jararweh, “Automatic Clustering of Attacks in Intrusion Detection Systems,” in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, 2019, pp. 1–8. doi: 10.1109/AICCSA47632.2019.9035238.
G. Andresini, A. Appice, N. Di Mauro, C. Loglisci, and D. Malerba, “Multi-Channel Deep Feature Learning for Intrusion Detection,” *IEEE Access*, vol. 8, pp. 53346–53359, 2020, doi: 10.1109/ACCESS.2020.2980937.
K. Jiang, W. Wang, A. Wang, and H. Wu, “Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network,” *IEEE Access*, vol. 8, pp. 32464–32476, 2020, doi: 10.1109/ACCESS.2020.2973730.
A. S. Alqahtani, “FSO-LSTM IDS: hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks,” *J. Supercomput.*, 2022, doi: 10.1007/s11227-021-04285-3.
R. Zhang, J.-P. Condomines, and E. Lochin, “A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System,” *Drones*, vol. 6, no. 1, 2022, doi: 10.3390/drones6010021.
J. Zhang, W. Wang, C. Lu, J. Wang, and A. K. Sangaiah, “Lightweight deep network for traffic sign classification,” *Ann. Telecommun.*, vol. 75, no. 7, pp. 369–379, 2020, doi: 10.1007/s12243-019-00731-9.
J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, “A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions,” *Electronics*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071177.
A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues,” *Knowledge-Based Syst.*, vol. 189, p. 105124, 2020, doi: https://doi.org/10.1016/j.knosys.2019.105124.
X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, “Variational LSTM Enhanced Anomaly Detection for Industrial Big Data,” *IEEE Trans. Ind. Informatics*, vol. 17, no. 5, pp. 3469–3477, 2021, doi: 10.1109/TII.2020.3022432.
D. Kshirsagar and S. Kumar, “Towards an intrusion detection system for detecting web attacks based on an ensemble of filter feature selection techniques,” *Cyber-Physical Syst.*, vol. 0, no. 0, pp. 1–16, 2022, doi: 10.1080/23335777.2021.2023651.
W. Wang, F. Harrou, B. Bouyeddou, S.-M. Senouci, and Y. Sun, “A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems,” *Cluster Comput.*, vol. 25, no. 1, pp. 561–578, 2022, doi: 10.1007/s10586-021-03426-w.
L. Yang, X. Cao, and X. Geng, “A novel intelligent assessment method for SCADA information security risk based on causality analysis,” *Cluster Comput.*, vol. 22, no. 3, pp. 5491–5503, 2019, doi: 10.1007/s10586-017-1315-4.
Z. Pan, J. Pacheco, S. Hariri, Y. Chen, and B. Liu, “Context Aware Anomaly Behavior Analysis for Smart Home Systems,” vol. 13, no. 5, pp. 261–274, 2019, [Online]. Available: http://waset.org/publications/10010351/pdf
O. Linda, T. Vollmer, and M. Manic, “Neural Network based Intrusion Detection System for critical infrastructures,” in *2009 International Joint Conference on Neural Networks*, 2009, pp. 1827–1834. doi: 10.1109/IJCNN.2009.5178592.
M. Basnet and M. Hasan Ali, “Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station,” in *2020 2nd International Conference on Smart Power Internet Energy Systems (SPIES)*, 2020, pp. 408–413. doi: 10.1109/SPIES48661.2020.9243152.

R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical System Security of Vehicle Charging Stations," in *2019 IEEE Green Technologies Conference(GreenTech)*, 2019, pp. 1–5. doi: 10.1109/GreenTech.2019.8767141.

D. J. Atul, R. Kamalraj, G. Ramesh, K. Sakthidasan Sankaran, S. Sharma, and S. Khasim, "A machine learning based IoT for providing an intrusion detection system for security," *Microprocess. Microsyst.*, vol. 82, p. 103741, 2021, doi: https://doi.org/10.1016/j.micpro.2020.103741.

M. A. Rahman, T. Asyhari, L. S. Leong, G. Satrya, M. Tao, and M. Zolkipli, "Scalable Machine Learning-Based Intrusion Detection System for IoT-Enabled Smart Cities," *Sustain. Cities Soc.*, vol. 61, p. 102324, 2020, doi: 10.1016/j.scs.2020.102324.

W. Li, W. Meng, and M. H. Au, "Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments," *J. Netw. Comput. Appl.*, vol. 161, p. 102631, 2020, doi: https://doi.org/10.1016/j.jnca.2020.102631.

D. Li, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *Int. J. Inf. Manage.*, vol. 49, pp. 533–545, 2019, doi: https://doi.org/10.1016/j.ijinfomgt.2019.04.006.

G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh, and A. SaiTeja, "Intrusion Detection System Framework Using Machine Learning," in *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2021, pp. 1224–1230. doi: 10.1109/ICIRCA51532.2021.9544717.