Efficient Intrusion Detection System In Iot Using Hybrid Deep Learning Algorithm

[1]**Achanta V S S M L Prasad**, achantaprasad897@gmail.com
[2]**M Naresh**, nareshmtech08@gmail.com
[1&2]Newton's Institute of Engineering, Guntur, Andhra Pradesh

Abstract

The Internet of Things (IoT) has become integral to numerous applications, yet it continues to face significant security challenges despite the introduction of various protective measures. To address these vulnerabilities, this paper proposes a Hybrid Deep Intrusion Detection System (HDIDS) designed to enhance security in IoT environments. The proposed system combines Spiking Neural Networks (SNN) and the Lion Optimization Algorithm (LOA) to effectively detect intrusions. The process begins with the preprocessing of raw data, followed by feature extraction. In the classification phase, an SNN is utilized to categorize the data as either normal or indicative of an attack. The classification accuracy is further optimized through hyper parameter tuning of the SNN using LOA. The performance of the proposed HDIDS is evaluated using the KDD99 dataset. Experimental results demonstrate that the proposed SNN-based intrusion detection system outperforms existing methods in terms of key evaluation metrics, confirming its effectiveness in securing IoT environments.

Keywords*: Intrusion Detection System, Deep Learning Model, Convolution Neural Network*

1. INTRODUCTION

In recent years researches are made in the field of IoT due to its more attention of application in the fields of industrial process, health care, automation, smart environment etc. There is several security issues caused due to the variety of applications. In conventional security methods of IoT environment there is a lack of heterogeneous environment and its interoperability mechanism. Thus the security is enhanced by data authentication, confidentiality and access controls. Even there are various security measures between the IoT and user, it faces several security issues. More over these lacks of security issues leads to add separate security module in the IoT environment. An ID is such a concept which is already in use in wireless networks. Enhancing the wireless networks IDS features will help IoT to secure the network from attacks and other vulnerabilities. With the increase in the usage of the internet and computer system, securing the data (personal and professional) has become a major challenge. The computers with the help of the internet download huge amount of

data from the internet, which may also download the malwares with it .Malware has many different names such as malicious code, malicious programs or malicious executable files. The continuous growth of the malware attacks has made computer systems more vulnerable to the hacks. Malware as defined by the Kaspersky Labs in 2017 "a type of computer program designed to infect a legitimate user's computer and inflict harm on it in multiple ways." With the huge variety of malwares growing each day, anti-virus scanner does not guarantee the detection of every type of malware based on its signature, which results in millions of hosts being attacked and causing a lot of damage to the data and other related systems. According to the Kaspersky Lab (2016) 6,563,145 different machines were assailed and around 4,000,000 new types of malware were detected. Therefore, protecting the network and user machine from malwares is highly required and crucial cyber security task for single user or entire business, since even a single attack can result in significant loss and damage .The purpose of this paper is to build a malware detection system that will provide an efficient way to detect the malware based on the activities it may perform on the computer it is being installed on. A malware can be of different varieties but there are following major categories. Virus; is defined as a small is piece of code that has the ability to duplicate itself. It is attached with any legitimate file and executes its behavior once the file is downloaded or executed. Worms; are also like virus, it also has the ability to replicate itself. The only difference between a worm and virus is that worm works on the network and replicated it by sending copies of it to the machines connected to that network. Spyware; is a software that typically is attached with a free software. When the user downloads the software, spyware gets activated and start collection the personal information of the user from the system and pass it on the host system via a network.

Adware; is defined as the malicious piece of code attached with any advertisement playing on the screen or a ‘click me’ button. Once the user click on the button or advertisement the code attached to it run and downloads some virus or bot on user’s machine. Trojans; generally, confuse the user as a authenticate program, such as any login page to a website or contact information form.

Botnets: is defined as the collection of several bots over a network. A single bot is a small piece of code which is assigned with a task to provide easy entry to user’s machine to a hacker. On hacking the machine with a bot a hacker can run virus on user’s machine, collect personal information or can degrade the performance of user’s machine

Malware Detection is done in two phases.

1. Malware analysis
2. Malware detection

Malware Analysis is the first phase of the Detection. In this phase the data is collected of previously known malwares. Features are generated and extracted of those malwares and an algorithm is developed based on those features to detect the new incoming malwares

Malware Detection comes after the analysis is done and a proper algorithm is generated which provides a high accuracy in detecting the malware. The algorithm developed is then implemented on the incoming packets and then checked whether it is a malware or benign.

In the proposed HDIDS deep learning techniques play a major role in the cyber security of the IoT for intrusion detection and malicious identification. Various attacks and vulnerabilities identification in the IoT environment which deals with data preprocessing, feature extraction and classification stages to classify the intrusions present in the dataset . Initially the raw data are preprocessed to set a dataset and remove noise for efficient communication. After that, important features are extracted and selected to decreases the dimensionality. Moreover, the extracted features are given to classification phase which is performed by a deep learning algorithm of Spiking Neural Network (SNN) with Lichtenberg Optimization Algorithm (LOA). Classification is effectively done by optimizing the hyper parameters of SNN by using LOA. Moreover, the developed IDS approach is analyzed by using KDD99 datasets.

2. LITERATURE SURVEY

Intrusion detection in IoT networks is a critical research area due to the increasing vulnerabilities in interconnected systems. Several studies have proposed diverse methods for enhancing detection accuracy and efficiency. Roy et al. [1] introduced a two-layer fog-cloud intrusion detection model that leverages distributed detection capabilities in IoT networks. This approach efficiently handles large-scale data traffic and reduces response time. Basati and Faghih [2] proposed a novel framework called PDAE, which uses parallel deep auto encoders for efficient intrusion detection. Their model demonstrated superior performance in identifying malicious activities with reduced computational overhead. Simon et al. [3] developed a hybrid intrusion detection system for wireless IoT networks, employing deep learning algorithms to enhance detection accuracy and overcome the limitations of traditional methods. Kimani et al. [4] highlighted cyber security challenges in IoT-based smart grid networks, emphasizing the need for advanced detection mechanisms to secure critical infrastructure. In line with this, Pampapathi et al. [5] proposed a deep learning-based approach for effective intrusion detection in IoT environments, focusing on robust feature extraction. Gupta et al. [6] introduced a tree classifier-based model tailored for the Internet of Medical Things (IoMT), which achieved high accuracy in detecting anomalies. Davis and Clark [7] reviewed data preprocessing techniques for anomaly-based intrusion detection, emphasizing their significance in enhancing model performance. Tieck et al. [8] explored spiking neural networks for classifying signals, which have potential applications in intrusion detection scenarios. Choudhary and Kesswani [9] conducted a comparative analysis of KDD-Cup'99, NSL-KDD, and UNSW-NB15 datasets, demonstrating the effectiveness of deep learning models in IoT-based intrusion detection systems. Hajiheidari et al. [10] presented a comprehensive investigation into intrusion detection systems for IoT, highlighting various techniques and their limitations. Arshad et al. [11] provided a detailed review of intrusion detection systems concerning performance, energy efficiency, and privacy concerns in IoT environments. Kumar et al. [12] developed an intrusion detection and prevention system tailored for IoT environments, focusing on adaptive defense mechanisms. Simoglou et al. [13] analyzed intrusion detection systems for RPL security, offering valuable insights into protocol-specific vulnerabilities. Balla et al. [14] explored deep learning algorithms for SCADA intrusion detection, emphasizing their real-time applications. Larriva-Novo et al. [15] proposed an IoT-focused intrusion detection system with preprocessing characterization for enhanced cybersecurity. Li et al. [16] developed an IoT data feature extraction and intrusion detection system based on deep migration learning, demonstrating its effectiveness in smart city environments. Kasabov [17] explored brain-inspired spiking neural networks (SNNs) for multimodal data modeling, which have potential applications in adaptive intrusion detection. Pereira et al. [18] introduced the Lichtenberg algorithm, a hybrid physics-based meta-heuristic for global optimization, which can be leveraged for optimizing detection systems. Finally, Al-Daweri et al. [19] analyzed KDD99 and UNSW-NB15 datasets, providing critical insights into their suitability for intrusion detection.These studies collectively highlight the advancements in intrusion detection systems for IoT networks, emphasizing the need for robust, scalable, and efficient models to tackle emerging threats.

3. MATERIALS AND METHODS

Many researches are focused in the field of IoT due to its variety of applications. Even its variety of application there are many security issues such as attacks, vulnerability and traffic of data. The IDS is developed to identify the security issues which lead to confidentiality, integrity, and availability of an information system. The block diagram of proposed system is shown in figure 1.Intrusion detection system

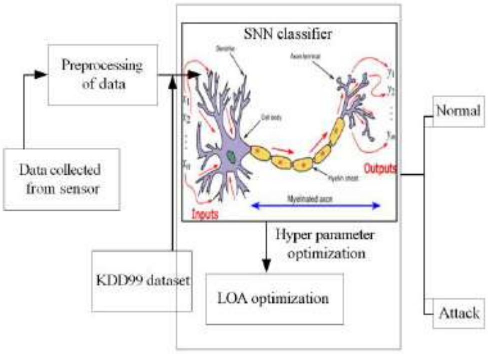

Fig.1: Block Diagram of Proposed System

The operations of IDS can be divided into three stages. The first stage is the monitoring stage, which relies on network-based or host-based sensors. The second stage is the analysis stage, which relies on analyzing the preprocessed data. The final stage is the detection stage, which relies on detecting the attacks present in the proposed system. The detection phase is done by the SNN classifier which classifies the data as normal and attack. In SNN the hyper parameters are optimized by LOA optimization technique. The proposed approach is deeply explained in below sections.

i) Intrusion detection system

History of Intrusion Detection System Generally, IDS includes both software and hardware mechanisms and IDS is responsible for identifying malicious activities by monitoring network environments and systems. In other words, IDS is used for detecting cyber-attacks and providing immediate alerts. Overall, IDS acts like a safeguard to the networks and systems. IDS are normally deployed after the firewall and are used with an intrusion prevention system. IDS are not a new term in the fields of IoT research regarding security and privacy. A significant number of publications have appeared in recent years. Cyber security experts have been concerned about the security and privacy of IoT environments for some time. This has led to the introduction of the concept of IDS embedding into IoT architectures and devices to deal with cyber-attacks. Researchers are mostly interested in inventing new mechanisms and models to counter intruders in conventional network protocols. However, traditional IDS mechanisms are incompatible with IoT devices connected through IPv6 and other complex network structures More comprehensive research on the use of machine learning methods is essential for IDS to secure and protect privacy in IoT.

ii) Classes of IDS

IDS are classified in two main categories as follows:

1. Host-based IDS
2. Network-based IDS

Host-based IDS detects intrusion behavior by scanning log and audit records. This kind of IDS is usually used on important hosts to protect the host security from all directions. The advantage of the host-based IDS is that it provides more detailed information, lower false alarm rates, and has less complexity than network-based IDS. However, it reduces the efficiency of the application system and relies excessively on the log data and monitoring capability of the host . Because of the characteristics of the IoT and because many IoT devices can be connected to the network, network-based IDSs need attention. Network-based IDS can detect the abnormal behavior and data flow in the network, to find potential intrusions. It does not change the host configuration and does not affect the performance of the business system. Even if the network IDS fail, it will not affect normal business operation. A problem is that network-based IDS only check its direct connection to the network segment without looking at other network segments. It is also difficult to process encrypted sessions with network-based IDS.

iii) Detection methods

Detection Methods Based on the nature of various intrusion attacks , intrusion detection methods are classified into four major categories: signature-based methods, specification-based methods, anomaly-based methods and hybrid methods .

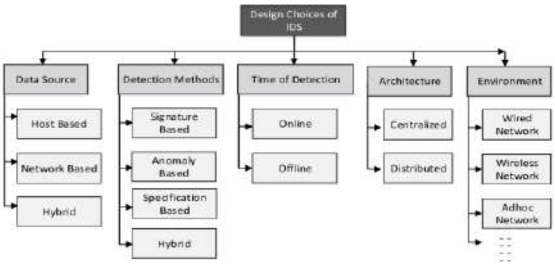

Fig 2: Detection methods

Signature-based methods first scan the data in the network and compare it with a feature database. If the scanned data is found to match the features in the signature database, the data will be treated as an intrusion. The advantage is that it can accurately determine the type of attack. It is relatively convenient to use, and the demand for resources is comparatively small. Specification-based methods require the system administrators to set rules and thresholds in advance. IDS detect the status of the current system and network according to the rules and thresholds set by administrators. If the threshold is exceeded or the rules are violated, the IDS will detect an abnormal situation and act accordingly. Anomaly-based methods depend on identifying abnormal patterns and by comparing traffic patterns. The advantage of using this method is that it enables the detection of new and unknown intrusions. However, the primary limitation is that the method tends to result in high false positive rates. Research is now focusing on applying machine learning algorithms in anomaly-based intrusion detection methods to improve the robustness of this kind of method. By employing machine learning algorithms, anomaly-based intrusion detection methods can monitor the ongoing intrusion footprints and compare them with existing datasets to be alert to potential future attacks. Hybrid methods refer to the use of any combination of the above-mentioned detection methods in the same IDS. This approach can help to overcome the shortcomings of a single method thereby enhancing the reliability of the entire IoT system. However, the obvious drawback is that the entire IDS will become very large and complex. This will make the whole system more difficult to operate and will require more resources. Especially when there are many protocols involved in the IoT system, the intrusion detection process will have large resources and time demands.

iv) Classification of Intrusion Detection System:

IDS are classified into 5 types:

a) **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

b) **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

c) **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

d) d)**Application Protocol-based Intrusion Detection System (APIDS):** Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

e) **e)Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

4. RESULTS AND DISCUSSION

The proposed system HDIDS gets the data from sensors which are then preprocessed and features are extracted. The extracted features are then given to classification phase which is performed by a deep learning algorithm of Spiking Neural Network (SNN) with Lichtenberg Optimization Algorithm (LOA). Classification is effectively done by optimizing the hyper parameters of SNN by using LOA. Moreover, the developed IDS approach is analyzed by using KDD99 datasets. Finally the proposed approach is compared with other existing algorithm in terms of performance matrices.

4.1. KDD99 dataset description

The first dataset is KDDCup-99, collected from the DARPA intrusion detection challenge (1998), incorporating 100's users after monitoring the network traffic on 1000's machines using UNIX operating system . The challenge period lasts for ten weeks by the MIT Lincon laboratory to store the collected traffic data in TCP dump format. Our experiments used 10% of the collected traffic data to build the KDDCup-99 dataset, which contains five attack types and 41 features. The KDDCup-99 dataset features are classified into three categories, including basic, content, and time-based traffic features.

4.2 Comparison of proposed and existing approaches in terms of evaluation matrices

The proposed approach of HDIDS is the combination of SNN and LOA which is deeply explained in above section. The performance of proposed approach should be evaluated so that KDD99 dataset is used. The proposed approach is evaluated in terms of accuracy, precision, recall, F-Measure, sensitivity and specificity. After that it is compared with existing approaches which is explained below,

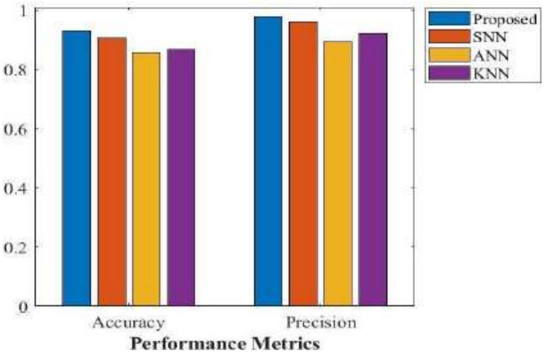

Fig.3: comparison in terms of accuracy and precision

In figure 3 the accuracy of proposed approach and existing approaches are 95%, 93%, 85% and 87%. Then the precision of proposed approach and existing approaches are 97%, 95%, 85% and 80%. Thus the result shows that the proposed approach has high accuracy and precision.

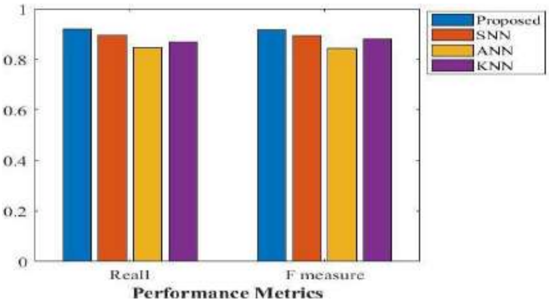

Fig 4: comparison in terms of recall and F-Measure

In figure 4 the recall of proposed approach and existing approaches are 93%, 90%, 82% and 87%. Then the F-measure of proposed approach and existing approaches are 93%, 90%, 82% and 87%. Thus the result shows that the proposed approach has high recall and F-Measure.

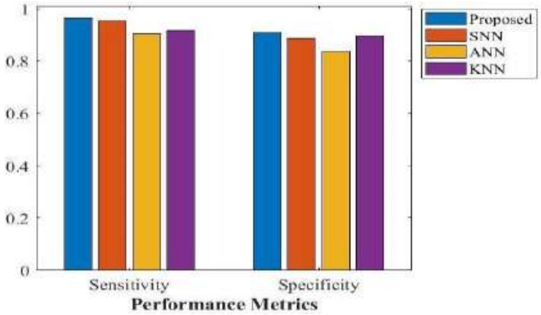

Fig 5: comparison in terms of sensitivity and specificity

In figure 5 the sensitivity of proposed approach and existing approaches are 95%, 93%, 85% and 88%. Then the specificity of proposed approach and existing approaches are 86%, 84%, 82% and 85%. The result shows that the proposed approach has high sensitivity and specificity. Thus the evaluations based on performance matrices showed that the proposed approach has high performance than other existing approaches.

5. CONCLUSION

Many of the applications developed in IoT environment but it has some security issues even introducing several methods. Thus the proposed approach is developed to enhance the security issued in the IoT environment. In this paper HDIDS was proposed to identify intrusion which is the combination of SNN and LOA. Initially the raw data were preprocessed and features were extracted. Then classification phase was performed by a SNN to classify the data as normal and attacks.. Classification was effectively done by optimizing the hyper parameters of SNN by using LOA. Moreover, the developed IDS approach was analyzed by using KDD99 datasets. Finally the proposed SNN algorithm was compared with other existing algorithm in terms of evaluation indicators. Thus the results showed that the proposed method has high performance than other existing methods.

REFERENCES

[1] Souradip Roy, Juan Li and Yan Bai, "A Two-layer Fog-Cloud Intrusion Detection Model for IoT Networks", Internet of Things, Vol. 19, No. 100557, 2022.

[2] Amir Basati and Mohammad Mehdi Faghih, "PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders", Information Sciences, Vol. 598, pp. 57-74, 2022.

[3] Judy Simon, N.Kapileswar, Phani Kumar Polasi and M. Aarthi Elaveini, "Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm", Computers and Electrical Engineering, Vol. 102, No. 108190, 2022.

[4] Kenneth Kimani, Vitalice Oduol and Kibet Langat, "Cyber security challenges for IoT- based smart grid networks", International Journal of Critical Infrastructure Protection, Vol. 25, pp. 36-49, 2019.

[5] PampapathiB M, Nageswara Guptha M and M S Hema, "Towards an effective deep learning-based intrusion detection system in the internet of things", Telematics and Informatics Reports, Vol. 7, No. 100009, 2022.

[6] Karan Gupta, Deepak Kumar Sharma, Koyel Datta Gupta and Anil Kumar, "A tree classifier based network intrusion detection model for Internet of Medical Things", Computers and Electrical Engineering, Vol. 102, No. 108158, 2022.

[7] Jonathan J.Davis and Andrew J.Clark, "Data preprocessing for anomaly based network intrusion detection: A review", Computers & Security, Vol. 30, No.6-7, pp. 353-375, 2011.

[8] J. Camilo Vasquez Tieck, Sandro Weber, Terrence C.Stewart, Jacques Kaiser, Arne Roennau and Rudiger Dillmann, "A spiking network classifies human sEMG signals and triggers finger reflexes on a robotic hand", Robotics and Autonomous Systems, Vol. 131, No.103566, 2020.

[9] Sarika Choudhary and Nishtha Kesswani, "Analysis of KDD-Cup’99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT", Procedia Computer Science, Vol. 167, pp. 1561-1573, 2020.

[10] Somayye Hajiheidari, Karzan Wakil, Maryam Badri and Nima Jafari Navimipour, "Intrusion detection systems in the Internet of things: A comprehensive investigation", Computer Networks, Vol. 160, pp. 165-191, 2019.

[11] Junaid Arshad, Muhammad Ajmal Azad, Roohi Amad, Khaled Salah, Mamoun Alazab, and Razi Iqbal, "A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT", Electronics, Vol. 9, No.4, 2020.

[12] Ajay Kumar, K. Abhishek, M. R. Ghalib, A. Shankar and X. Cheng, "Intrusion detection and prevention system for an IoT environment Intrusion detection and prevention system for an IoT environment", Digital Communications and Networks, 2022.

[13] George Simoglou, George Violettas, Sophia Petridou and Lefteris Mamatas, "Intrusion detection systems for RPL security: A comparative analysis", Computers & Security, Vol. 104, No. 102219, 2021.

[14] Asaad Balla, Mohamed Hadi Habaebi, MD. Rafiqul Islam and Sinil Mubarak, "Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system", Cleaner Engineering and Technology, Vol. 9, No. 100532, 2022.

[15] Xavier Larriva-Novo, Victor A. Villagra, Mario Vega-Barbas,Diego Rivera and Mario Sanz Rodrigo, "An IoT-Focused Intrusion Detection System Approach Based on Preprocessing Characterization for Cybersecurity Datasets", Cybersecurity and Privacy in Smart Cities, Vol. 21, No. 2, 2021.

[16] DamingLi, Lianbing Deng, Minchang Lee and Haoxiang Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning", International Journal of Information Management, Vol. 49, pp. 533-545, 2019.

[17] Nikola K. Kasabov, "Deep Learning and Modelling of Audio, Visual, and Multimodal Audio-Visual Data in Brain-Inspired SNN", Springer Series on Bio- and Neurosystems, Vol. 7, pp. 457–477, 2018.