Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Comprehensive Analysis of Intrusion Prevention and Detection System and Dataset used in WSN using Machine Learning & Deep Learning

A. Sarkunavathi[1], Dr. V. Srinivasan[2], Dr. M. Ramalingam[3]
[1]Research Scholar, Department of Information Technology,
Annamalai University, India
[2]Professor, Department of Information Technology, Annamalai University, India
[3]Professor& Head, Department of Information Technology,
Mailam Engineering College, India
Corresponding Author: sarkuna.bala@gmail.com

Article Info
Page Number: 638 - 657
Publication Issue:
Vol 71 No. 3s2 (2022)

Article History
Article Received*: 28 April 2022*
Revised*: 15 May 2022*
Accepted*: 20 June 2022*
Publication*: 21 July 2022*

Abstract
The Wireless Sensor Networks (WSN), which are spatially dispersed small-sized low-power sensor devices with wireless radio transceivers that sense numerous physical events and gather data in a variety of situations. Because of their restricted capabilities, haphazard deployment, and unsupervised operations, in militant circumstances, like enemy zones, the sensor nodes were subject to a range of assaults can have their security broken. When sensor nodes are physically seized and changed during deployment in a hostile environment, WSNs are particularly vulnerable to DoS attacks. Almost every layer in WSNs is vulnerable to DoS assaults, which employ a number of attacks. In this paper, the characteristics of an effective intrusion prevention and detection system in wireless sensor networks are defined, and a detailed study of datasets used in Machine Learning (ML) and Deep Learning (DL) networks is made to see if Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can perceive and thwart DoS attacks with higher classification accuracy rates.

I. INTRODUCTION

Deep learning is widely employed in variety of applications such as cyber security, speech recognition, machine translation, among others. Using Deep Learning techniques, we can improve the efficacy and accuracy of intrusion detection and prevention in WSN. The deep learning-based system called the convolutional neural network (CNN) are the extensively used method. However, for the reason that it is difficult to state a wide range of typical use patterns, anomaly detection has a high false alarm rate. The Deep Learning system that recompenses those flaws through employing a deep neural network to learn its own properties. To reduce false warnings, machine learning and deep learning learn from a collection of intrusion on their own then identify usual use behaviours. On account of their superior functioning in processing of images, models of deep learning, particularly CNN, have reached popularity in current years. The possibility of those CNN models may have been utilised to competently identify complicated DoS attacks in addition to the DDoS attacks by turning the statistics of traffic on network as visuals.

Watchdog-based techniques are often used to identify problematic nodes in the wireless sensor networks, and path raters are used to redirect the data transmission without detrimental nodes [1].

The Self-seeking nodes are identified in the system called Reputation Rating depending on the activities of the single neighboring nodes, like energy consumption and forwarding of packets [2]. In a WSN, routes are chosen to preserve a high degree of energy, this can be done by the aspects like success full transmission of packets without draining the energy. This could be an extortionate method because performing such calculations in energy-constrained networks necessitates the establishment and maintenance of trees.

The major goal of this study is to propose new ideas for future IDS and IPS development for WSN. For a better considerate, the features, problems of several machine learning as well as deep learning algorithms which are deployed over the intrusion prevention and detection field in WSN have been examined. The various datasets that have been considered for detection and prevention are also analyzed. Finally, the idea for developing efficient IDS and IPS in future research works is also discussed.

II. Intrusion Detection System

The system which keeps on watch the traffic over the network and delivers notifications when atypical activity behavior occurs are called as Intrusion Detection System (IDS). They are software code which examines the whole network or a particular system for anomalous actions as well as any breach in the network policy. Typically, every hypothetically dangerous behaviour or violation is notified to an administrator or centralised through a security information and event management system (SIEM). With the data collected from the various network components and devices these system extricate harmful and truthless alarms with the help of special alert filtering algorithm.The first three basic components of an effective Intrusion Detection System (IDS) are represented in Figure 1.

Figure 1. Components of Intrusion Detection System

- Monitoring component: It's used to keep track of surrounding sensor nodes or local activity. Internal operations, traffic patterns, and resource use are all monitored by this component.
- Analysis component: It keeps track of all network activity, both regular and abnormal, for all nodes.
- Detection component: The main component in IDS which is established using modelling process. It works after looking at network behaviours. It is judged whether or not such acts are malicious.

The other three IDS components are actions that may be taken if anomalous behaviour is detected. These actions can be single or combination of the three.

- Logging: Maintaining and recording each packet in a log file for further analysis by security administrators.
- Alarming: This is a response-generating component that, if an intrusion is detected, may trigger an alarm to ring, warning the user about the malicious node.
- Prevention: It's a step forward that might be added to IDS to enable it to take precautionary steps when an attack is identified. For example, this can be performed by eliminating risky nodes from the network.

WSNs have greater difficulty implementing intrusion detection systems (IDS) than other types of networks since sensors are usually designed to be tiny and inexpensive, with limited hardware resources, making complex solutions impractical. WSN was motivated to create a lightweight IDS solution as a result of this issue. This IDS must be WSN-compatible and capable of identifying the greatest amount of security risks conceivable.

One of the most adaptable and helpful alternatives for protecting WSNs against known and unknown threats is intrusion detection systems. IDS marks as well as scrutinizes network traffic in order to spot irregularities and alert sensor nodes to intruders. Anderson [3] was the first to suggest this idea.

Machine learning techniques are intrinsically related to the approaches used to create intrusion detection systems (IDS) nowadays. Most machine learning system depends in offline learning where it necessitates the retention of all, or at least a portion, of earlier data in memory. However, using online learning models, there are only a few approaches to identify abnormalities. There is a need to investigate deep learning for WSN so that efficient intrusion detection and prevention systems may be developed. The multiple IDS utilized in WSN are depicted in Figure 2.

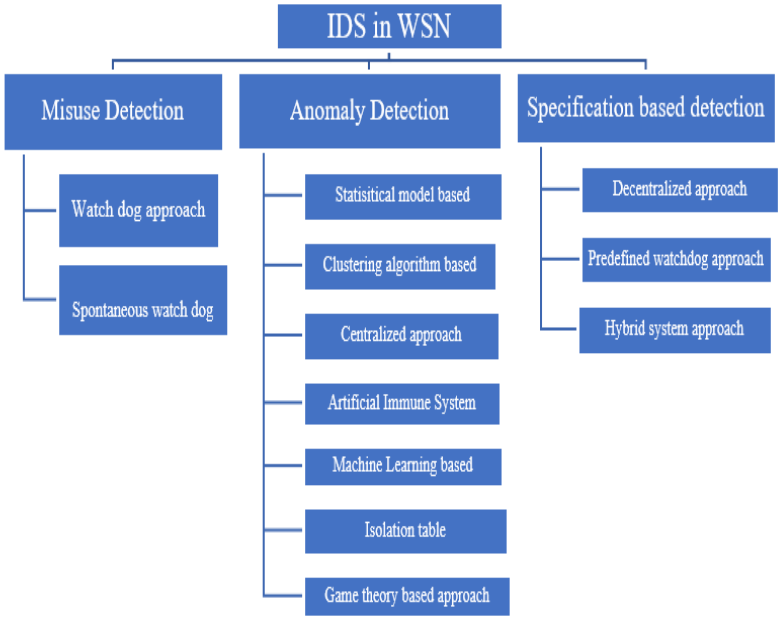

Figure 2. Categories of Intrusion Detection System used in WSN

The Table 1 shows the important features of the various IDS used in WSN.

Table 1. Features of different IDS used in WSN

Type of IDS	Salient Features
Anomaly Detection	It employs the Game-Theoretic Framework to provide security in WSN as well as intrusion detection.
Misuse Based Detection	Signature-based intrusion detection system is another name for this system. The fundamental drawback of this method is that it lacks defined criteria, making it ineffective in detecting new threats.
Hybrid System Approach	The hybrid method combines strategies for detecting abuse and anomalies. A person creates Hybrid Detection Approaches by developing protocol specifications. It can be used as a combination approach or separately. In clustered Wireless Sensor Networks, this technique this produces an accurate IDS.
Clustering Based IDS	It is also called as Hierarchical WSN based IDS. Clustering is analogous to a single layer of uninhibited monitors. Statistical anomaly detection is used to detect misbehaviour routing. The cluster approach uses intrusion detection as a supervising agent within each cluster to protect resources.
Trust Based IDS	It's also known as reputation-based IDS, and it encourages node cooperation by supervising nodes as well as determining grades based on their performance. This reputation technique is used to evaluate a network member's contribution.
Zone-Based IDS	Gateway zones and non-overlapping zones are the two forms of zone-based IDS, where the alerts are broadcasted within the zone by the efficient IDS agents. The majority of the time, Gateway Zones are utilised to correlate and aggregate locally produced alerts. Alarms are used to identify possible attacks in the zones, while alerts are meant to warn of them.

Table 2. A comparison of WSN's anomaly detection-based IDS

IDS	Statistical models based	Clustering algorithm based	Artificial Immune System	Machine Learning	Isolation table	Game Theory based
Accuracy	Average	Maximum point	Maximum point /Average	Maximum point	Low	Maximum point /Average
Energy efficiency	Not specified	Yes	No	Yes	Not specified	No
Memory Prerequisite	Not specified	Maximum Point	No detail	Maximum	Average	Average
Network Topology	Standard	Clustered	Standard	Standard	Clustered	Standard/ Distributed

2.1. Intrusion Prevention System

Many individuals confuse intrusion detection with intrusion prevention systems, whereas in reality, IPS is one step ahead of IDS. The first stage in intrusion prevention is intrusion detection. The goal of IPS is to identify malicious activity. Keep track of any such behavior. Make an effort to prevent or stop such behaviour and report it. The Intrusion Prevention system may identify the potentially hazardous behaviour also suppress it by giving specific orders if it is needed. WIPS (Wireless Intrusion Prevention System) monitors traffic over the network and analyses its wireless networking protocol to look for unusual activity involving it. The WIPS is also like a component of the network that automatically detects unwanted access points in the radio spectrum and takes countermeasures (intrusion prevention).A good WIPS may protect from the following threats such as, Rogue access points (AP) - WIPS should be aware of the distinction between rogue and external (neighbor's) Aps, Ad hoc networks, MAC spoofing, Honeypot / evil twin attack, Denial-of-service attack, Misconfigured AP, Client mis-association, Unauthorized association, Man-in-the-middle attack

In the Wireless Intrusion Prevention System installation, users first create operational policies for the wireless network. The air traffic is subsequently evaluated by the WIPS sensors, which ultimately send the results to the WIPS server. These server compares the data, to the regulations in place, and evaluates if it is a threat. The threat is then notified to the WIPS administrator, if any policies are set for automatic defense than that will be performed by the WIPS administrator. WIPS may be set up as either a network or a hosted system.

Network implementation: In this implementation, the components such as sensor, server and the console are used. Network components connected to these private networks are inaccessible to the internetwork. Sensors communicate to server over a secure network and port. As the server are available on private network the console is accessed by user within those network. Because the server is on a private network, users can only access the console from inside that network. Firms with all locations connected to a private network should use a network implementation.

Hosted implementation: Here the sensors were placed within a private network. On the other hand, the server is housed in a secure data centre and can be reached over the Internet. The WIPS interface may be accessed from any computer with an Internet connection. As the data between the sensor and data between server and console are encrypted, a hosted WIPS system is just as secure as a network-based WIPS system. Minimal setting is required in hosted WIPS since the sensors are programmed in such a way it uses a secure TLS connection to connect to the server.

Because sensors interact with the Server via the Internet without any additional settings, a hosted WIPS system substantially simplifies implementation for a big organisation site that aren't connected to a private network. From anywhere over the Internet, Console can be safely accessed. WIPS systems that are hosted are available as a subscription-based, on-demand software as a service model. Firms aiming to please the Payment Card Industry Data Security Standard as the basic scanning requirements may find hosted solutions handy. Detecting apprehensive activity in application or upper network layer protocols (TCP or UDP) is impossible with these WIPS

III. Related Works

3.1. Intrusion prevention and detection for wireless Sensor Networks - Machine Learning and Deep Learning methods

In WSN, D Mehetre et al [4] suggested technique for detecting the intrusion and preventing them. The author of this study proposed a reliable and secure technique based on two-step procedures. Essentially, the suggested method can establish a trustworthy channel for data packet transfer. In WSN, the suggested technique can avoid selective forwarding and black holes.

For WSN, Oke et al [5] presented a two-layer trust-based IPS. This system is capable of detecting network breaches.. Developers of the suggested system evaluated several scenarios by using a different set of weights. To improve accuracy, the writers tested a variety of set combinations. The suggested method has an average accuracy of 96 percent.

Pankaj et al [6] provided an architecture for dealing with incursion that included black holes, grey holes, floods, and TDMA. The CNN algorithm is utilised to prevent the numerous incursions in this study. The suggested system has been tested several times with varying data sizes, and the system's performance is unaffected by the data variations. The suggested system's findings are compared to current mechanisms, and the comparative results demonstrate that his new method performs better with a 97 percent accuracy. The purpose of this study is to see if the same technique can be used to real-time data sets in the future.

Based on the Bagging approach and ratio of information gain Dong et al. [7] suggested an intrusion detection model for cluster-based WSN to detect DoS attacks. The ratio of information gain to the intrinsic information was employed by the authors to eliminate extraneous characteristics. An ensemble algorithm was created using the Bootstrap aggregation technique, and it was used to train and improve a series of C4.5 decision trees. To evaluate the performance of the proposed model, it was built separately using the NSL-KDD and WSN-DS datasets. In terms of performance, this method beats others.

Sindhu et al. [8] created a unique lightweight IDS based on the Decision Tree classification approach for detecting irregularities in WSNs. The authors chose Kddcup'99 as a dataset that would provide useful information for the implementation. The model is divided into three sections, the first of which employs a feature selection technique to eliminate non-essential properties in order to enhance results. The key traits were then used to determine an appropriate subset using a wrapper-based feature selection technique. The learning paradigm neurotree in IDS has to be customised towards the end. Combining the right properties with neurotree, according to the researchers, is a feasible intrusion detection approach. In reality, the model had a increased detection correctness.

To discover anomalies in medical based WSN a framework was proposed by Pachauri et al. [9] by analysing various real-time medical based datasets using various classification as well as regression methods. For classification tasks, the system employs the random forests method, while for prediction tasks, it employs additive regression methodologies. According to the authors, their technique is more accurate than existing flaw detection systems, and both algorithms outperform previous research methods.

Cauteruccio et al. [10] suggested a new technique for detecting short as well as long term anomalies in heterogeneous WSN based on machine learning and a novel distance metrics called multi-parameterized edit distance. Their solution involves using edge and cloud analysis to genuine

data generated within a residential structure, which is then warped along set of fake damages. The findings suggest that this method can adjust to changes in the situation and appropriately detect issues.

To detect the anomalies both in centralized as well as decentralized WSN and in IoT application, even in circumstances where a priori knowledge is low, Bosmana et al. [11] suggested a novel simplified and light weighted architecture. With decentralized method this architecture outpaced offline centralized method in detecting anomalies making it to be used in applied application. Prediction accuracy and confusion matrix measures were utilised to test the proposed model, which was subsequently put into practise with a variety of big unreal and real-life datasets..

Bosman et al. [12] suggested a model by using an adaptive filter algorithm called Recursive Least Squares to detect the anomalies in decentralized WSN which with unsupervised online learning. In order to spot the anomalies an integrated neighborhood approach and online learning linear models are used while dipping the energy as well band spectrum utilization.

Rassam et al. [13] proposed a classifier to detect the anomalies in local sensor measurement and anomalies during energy consumption called One Class Principal Component Classifier which utilizes the Improved Principal Component Analysis(PCA) with Candid Covariance free. It has two phases namely offline phase and online Phase. In the first phase the Principal Component Analysis model was trained to develop a normal behaviour model, by the normal data obtained from each sensor. In the second online detection phase by measuring the threshold of global normal model ,each packet is detected as normal or abnormal.With new data's mean and standard deviation, the normal PCA model is restructured and retrained. The proposed model has a 96 percent detection accuracy and a 7.2 percent false detection percentage.

Martins et al. [14] proposed a sliding window-based learning mechanism for detection anomalies in online with a which is based on a Support Vector Machine with Least Squares (LSSVM) with functional analysis using Reproducing Kernel Hilbert Space with a real valued function called Radial Basis Function kernel. The performance of the proposed technique is evaluated by testing the dataset created by cloud based virtual machine. According on the simulation findings, the proposed technique outperforms others.

Samir Ifzarne et al. [15] proposed a model for intrusion detection that is reliable with WSN features using ratio of the information gain and the classifier which is online Passive aggressive. To make a decision, the information gain ratio is employed over the properties of sensor data. The classifier algorithm called online Passive Aggressive has been taught to recognise and categorise different forms of DDoS attacks. When determining if the network is working properly or is vulnerable to any type of attack, ID-GOPA model obtains a detection frequency of 96 percent. Scheduling, grey hole, flooding, and blackhole attack detection accuracy is 86 percent, 68 percent, 63 percent, and 46 percent, respectively, with ordinary traffic detection accuracy of 99 percent. These findings imply that this offline learning methodology may provide the WSN with robust anomaly detection and, in some cases, can even replace online learning.

Rajasegarar et al. [16] used the machine learning algorithm CESVM and QSSVM which are named class support vector machine such as centred hyper ellipsoidal support vector machine and the quarter-sphere support vector machine to find network errors. The flexibility of parameter selection and computational complexity are benefits of CESVM. However, because it uses a

centralised method, it has significant disadvantages with distributed WSNs. In a distributed context, QSSVM functions ideally.

Periakaruppan et al. [17] proposed an evolutionary algorithm for detecting intrusion in order to counteract the sleep deprivation assault in WSN. An asymmetric encryption technique name Modified RSA (MRSA) is used, where the key pairs are distributed over sensor nodes from the base station. Sensor nodes use ad hoc on-demand distance vector routing to find the best path before transmitting or receiving packets along with fitness calculation function is used to verify the resilience of relay nodes. The tactics employed by attackers are discovered and assessed using cross and mutation procedures. After the attacker nodes have been identified, the base station transmits forbidden signals to the network.

Shi et al. [18] studied sensor behaviour under internal and positioned attacks using a state change model over the continuous time in Markov chain (CTMC). To balance network features and security, the model merged an internal attack detection model with an epidemiological model, taking into consideration WSN's current condition, viability, energy consumption, and availability. The above-mentioned four criteria must be quantified.

Based on an enhanced V-detector technique, Sun et al. [19] proposed an intrusion detection prototype named WSN-NSA for WSN. Changes to detector generation rules and detector optimization are made to the V-detector approach, and to minimise detecting features, an analysis over principal component is performed.

An IDS based on deep neural network was proposed by Gowdhaman et al.[20].The best characteristics from the dataset are chosen using a cross-correlated technique, and the chosen best parameters became the structure blocks to identify intrusions for deep neural network associations. The suggested DNN outpaces prevailing machine learning models such as random forest , decision tree, and support vector machine in recognising assaults.

For WSN, the author [21] presented an intrusion detection architecture with multi-layer and employed a security mechanism called Défense-in-depth with two levels of detection. The first level of detection employs a Naive Bayes classifier at network edge, the area in which sensors are distributed in order to obtain the analysis of real -time decision of the packets. next level of detection, which is cloud-based, uses a Random Forest multiclass classifier to do complete analysis on the data packets under investigation. It is found that this proposed model of multi-layer detection has a increased Precision rate with values of 100 percent, 90.4 percent, 99.5 percent, 97 percent, and 99.9 percent for the Normal, Gray hole, Blackhole , Scheduling and Flooding assaults, as well as a high TPR, TNR, FPR, and FNR. The dataset WSN-DS was used, which was generated specifically aimed at intrusion detection systems in WSN.

The authors [22] developed an intrusion detection strategy with Neural network called improved Conventional Neural Network (ICNN). They first pre-processed data of traffic over network and then used the ICNN to model it. When compared to earlier models, their findings demonstrate better intrusion detection precision with a higher true positive rate, and less false positive rates.

The author [23] offered another deep learning-based intrusion detection algorithm. To train the model, they employed a network with Deep Belief in combination through a multi-restricted Boltzmann machine and a support vector machine . According to their experimental data, the recommended detection model improved detection accuracy.

Faisal et al. [24] suggested a technique for translating network traffic data into picture form and using the translated data to train a cutting-edge CNN model, deep residual network (ResNet). In the

instance of binary classification, the proposed method correctly identified DoS and DDoS 99.99 percent of the time.

The author [25] suggested an intelligent intrusion detection system that limits the attacks efficiently. A classifier based on Artificial Neural Network with Multilayer Perceptron, with holdout method and tenfold cross-validation methods was proposed by the authors. Aside from that, they've created their own dataset that's exclusive to WSN attacks. However, their technique was largely based on one detecting layer that employed a computationally intensive learning process, and their results revealed that employing one hidden layer resulted in the highest accuracy values.Although their method was mostly centred on a single detecting layer that used a computationally demanding learning process, and the findings showed that using just one hidden layer yielded the best accuracy.

The author of [26] presents a technique for detecting jamming in WSNs that relies on collaboration and input from other linked neighbours' nodes. In the model, a linked mechanism and a protracted mechanism were used. The outcome shows that when applied to a wireless Multi-Parent hierarchical protocol, this model performs better.

An advanced hybrid intrusion detection system is introduced by Singh et al. [27] which impulsively classifies threats . Furthermore, the authors of [16] suggested utilising the oversampling technique called SMOTE with synthetic minority before using the random forest technique to train the intrusion detection classifier, so that the dataset must be balanced. The random forest technique outperformed other comparable systems in simulations on a benchmark incursion dataset, with an accuracy of 92.39 percent.

In this literature, Misra et al. [28] presented an energy sensing procedure for intrusion detection that is simple and low-complexity. The principles of random automata for learning along the sampling process are combined to design the IDS.

3.2. Dataset used for IDS in Machine Learning and Deep learning-based network

The following represents are the ideal characteristics which are shown in Table 3. is necessary for the dataset to be good in the intrusion prevention as well as detection system.

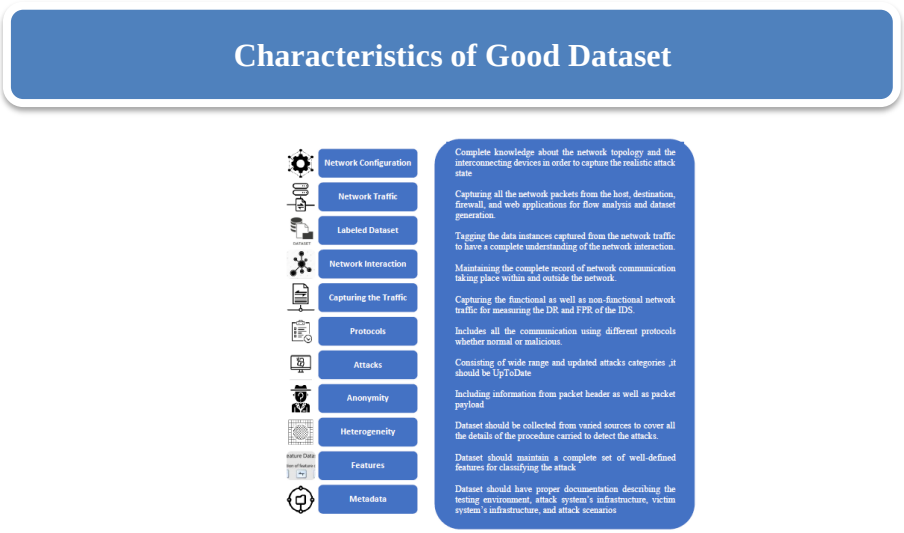

Figure 3. Characteristics of Good dataset

KDD Data set: The Knowledge Discovery and Data Mining dataset is a modified version of DARPA98 dataset, which evolved out of a DARPA-funded IDS programme at MIT's Lincoln Laboratory for evaluating IDS that discriminate between inward bound normal as well as attack connections. They were later utilized in the International Knowledge Discovery and Data Mining Tools Competition(KDD CUP 99) [29] after some filtering. About the last two decades, most academics have relied on this dataset. In the lack of alternatives, various publications have the KDD CUP 99 dataset was utilised as a commonly used benchmark for classifier precision.

The four categories of attacks in KDD are: denial-of-service (DoS), Probing, remote-to-local (R2L) and user-to-root (U2R),). Since machine learning is frequently used in IDS investigations, several IDS studies have used KDD as a dataset. The majority of these research use binary classification to categorize the full KDD as assault or benign. The multiclass classification is also used to divide the KDD into four groups.KDD-99, on the other hand, has severely skewed objectives, non-stationarity across training and test datasets, irrelevant features, and pattern repetition. The KDD CUP (Competition) dataset was created for Local Area Networks (LAN). Despite the fact that numerous researchers utilised to combat fraud and intrusion detection. Mainly KDDCup-99 was used in Anomaly, signature, and hybrid-based IDS.

KDD is by no means specialised for wireless in common or WSN in specific. As a result, there is a demanding necessity to develop a categorized, specialised dataset which accurately represents WSN to support in the study of abnormal and normal behaviour. To build the dataset and acquire the appropriate data through the broadcast and received packets in the WSN, a low-priced monitoring service is required.On the other hand, we must ensure that vital network data that aids in detecting, categorising, and then avoiding various prospective attacks is captured. Every sensor will be involved in monitoring process and they have to be capable of maintaining their neighbor group track in order to distribute the load across the sensor nodes. To keep track of all network sensors, the difficulty was calculating the ideal number of nodes for each sensor node to monitor.

The algorithm ISVMM which is support vector machine classifier with Mahalanobis distance called Incremental Learning Algorithm, was presented by Myint et al. [30]. In this work, SVM is used to make a forecast to reduce algorithm complexity by decreasing steps in calculation.It can be achieved by finding three sets namely :error set, support and remaining sets as well as making a judgement that is both hard and easy. The time hoarded may then be used to train the dataset many times. The authors utilised KDD Cup99 as a dataset for simulation to assess the system's performance. The proposed ISVMM model accurately predicts all 41 characteristics while keeping the dataset's dimensionality low.

NSL-KDD : The dataset NSL-KDD [31] was suggested to overawe the deficiencies in the KDD99 dataset. Some of the NSL-KDD recordings were wisely chosen from the KDD99. These dataset balances data from multiple classes, in order to avoid classification bias problem. These datasets deleted duplicate and redundant entries, resulting in a very small number of records. As a result, the tests may be performed over the complete dataset which provides results that appears to be similar and consistent for the other researchers. This dataset overcomes the concerns over data bias and duplication to certain level. Also on the other hand, these dataset does not use new data; therefore, minority category of class samples are yet missing and their samples are outmoded.

ISCXIDS: The New Brunswick's Information Security Centre of Excellence University generated ISCXIDS dataset. [32]. ISCXIDS 2012 incorporates both types of assaults in the network layer and application layer. This is because DoS attacks at the application layer are much impossible to detect when compared to the network layer attacks. Various layer attacks at ISCXIDS 2012, including HTTP DoS and DDoS employing an IRC Botnet. rom ISCXIDS 2012, Quadratic Discriminate, Slowloris, Hulk, Goldeneye, and LOIT were brought to CICIDS 2017 [33]. Heartleech, LOIC UDP, TCP, and HTTP from CICIDS 2017 are also included in CSE-CIC-IDS 2018.As a result the latest version of CSE-CIC-IDS 2018 is a sophisticated collection of datasets that incorporates features of previous version.

Limitation of CIC-IDS-2017 over CSE-CIC-IDS-2018:

There exist few limits in terms of data models and generated files by means of analysis of network flow which are listed below.

- By analysis of network flow, data models created are saved to files then later on processing those files are actually time-consuming activity due to the enormous amount of data occurrences in each file.
- There exist some missing and duplicate data records in the dataset.
- All of the attack labels for processing can be found in the dataset's files, which may be concatenated. Combining samples from each assault type, on the other hand, expands the dataset, necessitating additional computer and processing time.
- In order to perform Preprocessing the dataset's files may be combined to contain overall attack labels, but combining samples of every attack category upsurges the dataset, necessitating additional computer and processing time.
- Both these datasets have a substantial class imbalance, which might lead to poor accuracy and increased FPR.

Pre-processing the data samples, employing feature engineering, or eliminating the missing information can all help alleviate these issues. Relabeling or sampling the data samples, which raises the possibility of data samples from all classes, can help to fix the high-class imbalance.

CICDDoS2019 provides data of benign and recent typical DDoS assaults that are same like real -word in the PCAP file format. These are the results of a network traffic study by the CICFlowMeter-V3, which comprised source and destination IP addresses, protocols, source and destination ports, tagged flows based on the time stamp, and attack vector in the form of CSV files. The creation of realistic background traffic was the primary goal in the creation of this dataset. This dataset was created by abstracting 25 users using the application layer protocols. In order to examine the dataset using AI algorithms, the produced data (CSV) files may be downloaded and analysed. The raw captured files (PCAP) can be utilised to extract essential features when using a new feature extractor. The produced data may subsequently be analysed using data mining techniques.

CICDDoS2019[34] is the most recent dataset, with a considerable number of models in comparison to the additional datasets on network traffic. Furthermore, it comprises both incoming and outward traffic from most recent DoS and DDoS assaults. This dataset comprises 11 groups

DDoS and DoS assault traffic and over eight network-based flow variables gathered across the real-time network.

WSN – Dataset: A dedicated dataset aimed at WSN is being developed by Almomani [25] to aid in the detection and classification of four forms of DoS attack such as grayhole, scheduling, blackhole, flooding. The most often used, hierarchical WSN routing protocols called LEACH protocol, is used by the author. On this dataset, an Artificial Neural Network (ANN) is being trained to identify and categorise various DoS attacks. By employing with one hidden layer and ten-fold cross validation yielded better results. Based on the online classifier Passive-Aggressive, he proposed an ingenious, efficient, and learnable model, while also assuring that the model is consistent with WSN features.

BoTNeTIoT-L01: BoTNeTIoT-L01[35] is a data set that includes all IoT device data files from the detection of IoT botnet attacks NBaIoT (BoTNeTIoT) data set. By limiting the features to a 10 second time window, this improved version minimised the redundancy of the original dataset. In the dataset class label, 0 represents attacks and 1 represents normal samples.The most current dataset, BoTNeTIoT-L01, comprises of 9 IoT device traffic intercepted using Wireshark on a local network employing a central switch. They have two Botnet assaults (Mirai and Gafgyt). The collection includes 23 statistically designed characteristics derived from.pcap files. Over a time, window of 10 seconds, with a decay factor of 0.1, seven statistical measures (mean, radius, magnitude, variance, covariance, count, and correlation coefficient) were computed. Four characteristics were collected from the .pcap file: jitter, outgoing packet size alone, packet count, and outbound and inbound packet size combined. At least three statistical measures were calculated, for each of these four traits, yielding a total of twenty-three features. To aid with the labelling procedure, the files were split by attack type and subcategory., DoS, DDoS, Service Scan, Data exfiltration, and Keylogging threats are all included in the dataset. DDoS and DoS assaults are further grouped based on the protocol utilised.

DEFCON dataset: In the year 2000, the first Version of dataset DEFCON-8 was created which encompasses port scanning as well as buffer overflow attacks. In the year 2002 another version DEFCON-10 was created which employs corrupt packets, port scan, FTP through Telnet, administrator privilege in addition sweeps attacks [36]., The generation of network traffic is different from the real time traffic through Capture the Flag, because it contains mostly attack traffic apart from the contextual traffic data, its application for testing IDS is restricted. Most of the data is used to test alert correlation algorithms.

CAIDA dataset : The Center of Applied Internet Data Analysis has following datasets: CAIDA OC48, which covers a wide range of data types observed on an OC48 connection; CAIDA DDOS, that includes data from an hour DDoS invasion traffic in the year August 2007, CAIDA-2016 Internet traces: The Equinix-Chicago monitor imprints the passive traffic over the speedy backbone of Internet .All of those datasets are precise to individual occurrences or assaults and anonymised in terms of protocol, destination and payload. These are ineffective standard datasets due to various flaws, as stated in [37], such as the lack of facts regarding the assault cases.

LBNL dataset: This dataset[38] comprises incognito traffic that consists solely of header data. At Lawrence Berkeley National Laboratory, these datasets are created from two edge routers by

gathering the data such as real time outgoing, incoming, and network traffic route. It didn't have a labelling method, and so no further features created.

UNSW-NB15: The researchers [39] created this dataset for the assessment of IDS at UNSW Canberra. At the Australian Centre of Cyber Security, researchers utilised the programme named IXIA Perfect Storm to produce a mix of malicious as well as benignant network traffic across two days, in 16 and 15-hour periods. The pcap files of 100 GB size with a significant amount of unique characteristics were the datasets created. NB15 was intended to be a boost from the previously described KDD99 dataset. It has ten targets, one of which is benign and remaining are anomalous, including DoS, Reconnaissance, Shell Code ,Exploits, Backdoors, Worms, Analysis, Generic, and Fuzzers. Nevertheless, the dataset was generated using a simulated milieu to generate assault actions. Among the features of these dataset are basic features, content ,flow , time and other additional features, as well as labelled features. This is a novel and most used IDS dataset in recent studies. Eventually UNSW-NB15's impact is less when compared to KDD99's, new datasets must be developed in order to develop new machine learning-based IDS.

Tezpur University IDS (TUIDS) dataset: The data set was created by Indian Professors of Tezpur University [40]. This dataset are executed from the testbed which includes DoS, DDoS, Scan Probing, U2R, attacks . The flow level data, on the other hand, contains no additional properties other than those created by the flow-capturing method.

IoTPoT Dataset : The honeypots[41] are used in obtaining the datasets which provided restricted interpretation of traffic over network as assaults conducted on the honeypots only could be detected. According to the authors, IoTPoT investigates Telnet-based attacks counter to various IoT based devices operating on various architecture of CPU like Power PC ,Million Instruction Per Second and ARM. The authors logged 76,605 malware binary download attempts from 16,934 different IP addresses in 39 days operation. The authors further contend that the current honeypots which handles the telnet password honeypot and honeypd by the telnet protocol are not capable of detecting these binaries ,because they are incapable to handle the inbound directives originated by assailants.

N-BaIoT Dataset: The authors [42] created the most recent dataset, for their online network IDS to assessment of IDS in network of IoT. Network traffic is generated and collected from the video surveillance using IP camera of IoT network which is built using nine IoT devices and three personal Computer by launching eight variant attacks which affected the integrity of video uplinks and, by infecting with Mirai botnet. Their published papers include a full explanation of the assaults and network topologies. For each of these nine assaults, the authors produced a collection of extracted feature vectors. Among the attack techniques are Active Wiretap, Video Injection , Fuzzing ,SSDP Flood, , SSL Renegotiation, OS Scan, SYN DoS, Mirai and ARP MiTM,

IV. Problem Definition

4.1. Limitation Research Gaps and Challenges

WSNs are commonly implemented in uncomfortable or even hazardous conditions because to their wide variety of possible applications. Traditional intrusion detection systems (IDSs) in WSNs have specific difficulties, such as the blockage of restricted ranges of attacks and protocols. The compute effort on nodes is increased as a result of the delayed analysis procedure. As a result,

typical IDSs may not necessarily apply to WSNs. The ML techniques like SVM, Neural Networks, others also showing promise in understanding the dynamic behavioral patterns required for cybersecurity. There appears to be huge promise for ANN, which is modelled after human brain functions. Despite fresh insights from psychology and human behavior, ANN enhancement has been strengthened now-a-days. Deep learning, which is a set of machine learning algorithms used to generate high-level abstractions, offers a variety of possibilities and prospects as a result of this. To improve the performance of the IDS and IPS, an optimization strategy is also necessary.

4.2. Proposed Architecture

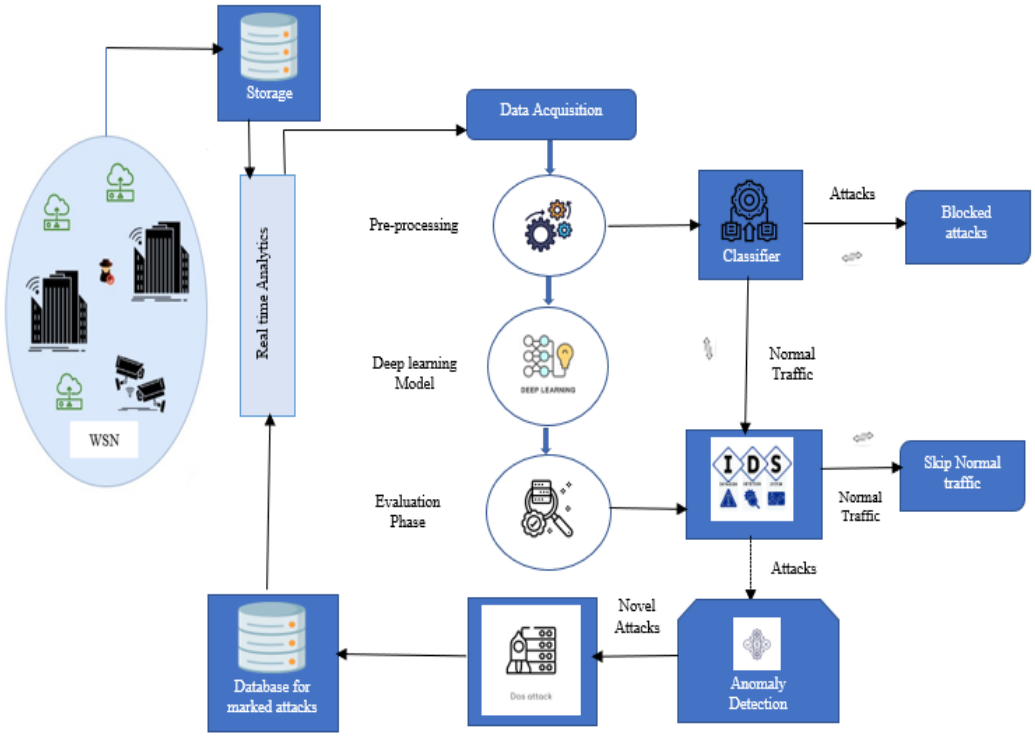

FIGURE 4. Proposed Architecture For Intrusion Prevention And Detection System In Wsn Using Deep Learning

The Proposed architecture for Intrusion detection and prevention system using deep learning is depicted in the Figure 4. In the preprocessing layer, a learning algorithm conditioned by a classified array of knowledge is utilised as a significant aspect in the detection of assaults, and a unique method for identifying security risks in particular times after the deep learning machine has been implemented.

This strategy is used to decrease false warnings over time by upgrading the learning model with information from real-time analytics performed by experts. The recommended method favours the selection of appropriate labelling of mislabeled data since the fraction of network segments seems to be the only particular information accessible. The system classifies anomalies based on

predefined discoveries, and this architecture will use a scoring technique to categorise fresh portions of data.

This intrusion prevention system also has a rapid update mechanism, which solves the problem of existing tactics' adaptability. With lower computational costs and energy, the proposed architecture is able to employ and update so called learning system by the current cognizance and, to date, developing forms of assaults.

V. Results and Discussion

5.1. Space considerations

In the contributions relating to IDS and IPS in WSN that were taken for evaluation, many sorts of attacks were explored in the Figure 4. Wormhole, Black hole, grey hole, Sybil attacks, DoS attacks, selective forwarding attacks, forging attacks, and other assaults are wreaking havoc on the WSN. The forging attack, clone attack, and cheating attack were only considered in a few works.

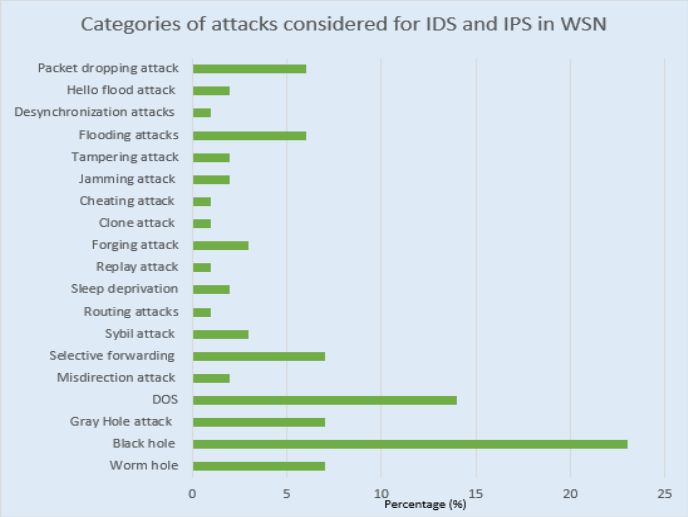

Figure 4. Percentage of attacks considered in IDS and IPS in WSN

5.2. Performance Measures

The Table 3 lists the performance criteria that were examined while assessing the IDS and IPS for WSN's efficiency and performance. Detection Rate, latency of End-to End , energy exhaustion, rate of false alarm ,ratio of delivery of packets, accuracy, are the factors.

Table 3. Features considered for IDS in WSN

Author	Parameters Considered	Attacks Handled
1. D Mehetre et al [4]	Energy consumption, Packet delivery ratio (PDR, Throughput, Latency	• Black hole, • Selective forwarding attacks,
2. Oke et al [5]	Generation of Packet Rate, Sent Packet Rate Received Packet Rate, NPR	• Malicious node intervention
3. Pankaj et al [6]	Precision, Recall, F1 Score	• DoS, Flooding, TDMA, Gray hole, Black hole.

4. Sindhu et al. [8]	False alarm errors, Detection rates	• Normal attacks
5. Pachauri et al. [9]	False alarm ratio	• Anomalies
6. Cauteruccio et al. [10]	False positives	• Anomalies
7. Bosmana et al. [11]	True positive (TP), False positives (FP),False negatives (FN)	• Anomalies
8. Bosman et al. [12]	F measure, prediction and recall	• Anomalies
9. Rassam et al. [13]	Detection accuracy, false alarms	• Anomalies
10. Martins et al. [14]	True Positive Rate False Positive Rate,Time Elapse	• Anomalies
11. Samir Ifzarne et al. [15]	Detection rate, accuracy	• Scheduling, Gray hole, Flooding, Blackhole attacks
12. Rajasegarar et al. [16]	Detection rate, accuracy	• Anomalies
13. Periakaruppan et al.[17]	Energy consumption,Delay, Packet delivery ratio, and Throughput	• Denial of Sleep Attack
14. Shi et al. [18]	Detection rate	• Internal attack
15. Sun et al. [19]	Memory consumption Time cost of detection.	• Normal attacks
16. Gowdhaman et al. [20].	Detection rate	• Imbalanced attacks
17. Hussein et al. [21]	TP, TN, FP, FN, Precision	• Normal, Flooding, Scheduling, Gray hole, and Blackhole attacks
18. Yang et al. [22]	Detection accuracy TP, FP	• Malicious activities
19. Qin et al. [23]	Detection Accuracy	• WEP (Wireless Equivalent Privacy) attacks
20. Faisal et al. [24]	Precision and Detection rate	• Complex DoS and DDoS attacks
21. Almomani et al. [25]	Classification Accuracy	• Blackhole, Flooding, Scheduling, and gray hole attacks
22. Del et al. [26]	Detection rate	• Jamming attack
23. Singh et al. [27]	Detection rate, TP, FP	• Sybil attack, Hello flood and wormhole attack
24. Misra et al. [28]	Packet Sampling efficiency Malicious Packet caught	• Malicious information

5.3.Conclusion

O

ne of the most important strategies for WSN security, is machine and deep learning-based intrusion detection systems (IDS). The paper depicts about analysis connected to IDS and IPS in WSN and the ML and DL-based Intrusion Detection algorithms utilized for WSN networks and devices. Based on the advocated IDS methodology for WSN the attack detection strategies implemented by researchers were analyzed. A survey of several datasets accessible for WSN security research is also provided. The research challenges that remain in the present IDS and IPS platforms were analyzed, and effective gaps that have a better scope in constructing an efficient IDS and IPS system in the future were identified. As a future work by applying the NSL-KDD dataset to the proposed architecture the different parameters such as Control Packets Overhead, Packet Delivery Rate, Energy Consumption**,** Network Lifetime**,** Throughput are taken into consideration and also to provide the suitable solution to improving the detection rate and classification accuracy by building an effective Deep Learning based Intrusion Detection and Prevention System over the mislabeled datasets.

B1, etc.

REFERENCES

[1] Sergio Marti, Thomas J. Giuli, Kevin Lai, Mary Baker (2000), *Mitigating routing misbehavior in mobile ad hoc networks*, in: 6th ACM annual international conference on Mobile computing and networking, pp. 255–265.

[2] Pietro Michiardi, RefikMolva(2002), *Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks.* Advanced Communications and Multimedia Security, Springer, US, pp. 107–121

[3] J. P. Anderson, "*Computer Security Threat Monitoring and Surveillance,"* Technical Report, James P. Anderson Company, Fort Washington, 1980 P. Anderson Company

[4] D. C., Roslin, S. E., & Wagh, S. J. (2019). *Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Cluster Computing,* 22(S1), 1313–1328.

[5] Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G., & Ajao, L. A. (2018). *Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks.* Advances in Electrical and Telecommunication Engineering, 1(1), 23–29.

[6] Pankaj R Chandre Dr Parikshit N Mahalle Dr Gitanjali R Shinde , (2021)*Intrusion Prevention Framework for WSN using Deep CNN, Turkish Journal of Computer and Mathematics*, Vol.12 No.6 , 3567-3572

[7] Abdullah, M. A., Alsolami, B. M., Alyahya, H. M., & Alotibi, M. H. (2018). *Intrusion detection of DoS attacks in WSNs using classification techniques*. Journal of fundamental and Applied Sciences, 10(4S), 298–303.

[8] S. S. S. Sindhu, S. Geetha, A. Kannan, 2012). *Decision tree based light weight intrusion detection using a wrapper approach* . Expert systems with applications, 39(1): 129–141.

[9] Pachauri, G., & Sharma, S. (2015). *Anomaly detection in medical wireless sensor networks using machine learning algorithms*. *Procedia Computer Science, 70*, 325 – 333.

[10] F. Cauteruccio, G. Fortino, A. Guerrieri, A. Liotta, D.C. Mocanu, C.Perra, G. Terracina, and M.T. Vega(2019), *Short-long term anomaly detection in wireless sensor networks based on machine learning and multiparameterized edit distance,* Information Fusion, vol. 52, pp. 13–30.

[11] H. H. Bosman, G. Iacca, A. Tejada, H. J.W¨ortche(2015), A. Liotta, *Ensembles of incremental learners to detect anomalies in ad hoc sensor networks,* Ad Hoc Networks 35 14–36.

[12] Bosman, H.H.W.J., Iacca, G., Tejada, A., Wörtche, H.J. & Liotta, A. (2017). *Spatial anomaly detection in sensor networks using neighborhood information*. Information Fusion, 33, 41-56.

[13] M. A. Rassam, M. A. Maarof, and A. Zainal(2014), "*Adaptive and online data anomaly detection for wireless sensor systems*," Knowledge-Based Systems, vol. 60, p. 44–57.

[14] Martins H, Palma L, Cardoso A and Gil P,(2015), *A support vector machine based technique for online detection of outliers in transient time series* 2015 10th Asian Control Conference (ASCC) (IEEE) pp1–6

[15] Samir Ifzarne, Hiba Tabbaa, Imad Hafidi, Nidal Lamghari(2020) ,*Anomaly Detection using Machine Learning Techniques in Wireless Sensor Networks* The International Conference on Mathematics & Data Science (ICMDS) 2020 Journal of Physics: Conference Series 1743

[16] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami,(2010) "*Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks*," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 518–533.

[17] M. Gunasekaran and S. Periakaruppan(2017), "*GA-DoSLD: genetic algorithm based denial-of-sleep attack detection in WSN*," *Security and Communication Networks*, vol. 2017, Article ID 9863032, 10 pages.

[18] Q. Shi, L. Qin, L. Song, R. Zhang, and Y. Jia(2017), "*A dynamic programming model for internal attack detection in wireless sensor networks*," *Discrete Dynamics in Nature and Society*, vol. 2017, Article ID 5743801, 9 pages.

[19] Z. Sun, Y. Xu, G. Liang, and Z. Zhou(2018), "*An Intrusion Detection Model for Wireless Sensor Networks with an Improved V-Detector Algorithm*," IEEE Sens. J., vol. 18, pp. 1971-–1984, 2018.

[20] Gowdhaman, V., Dhanapal, R.(2021) *An intrusion detection system for wireless sensor networks using deep neural network. Soft Computing* https://doi.org/10.1007/s00500-021-06473-y

[21] Hussein, Dina & Ibrahim, Dina & Alruhaily, Nada. (2021). *A Multi-layer Machine Learning-based Intrusion Detection System for Wireless Sensor Networks.* International Journal of Advanced Computer Science and Applications.

[22] H. Yang and F. Wang(2019), "*Wireless network intrusion detection based on improved convolutional neural network*," IEEE Access, vol. 7, pp. 64366– 64374.

[23] H. Yang, G. Qin, and L. Ye(2019), "*Combined Wireless Network Intrusion Detection Model Based on Deep Learning*," IEEE Access, vol. 7, pp. 82624–82632.

[24] Faisal Hussain,Syed Ghazanfar Abbas, Muhammad Husnain,Ubaid U. Fayyaz, Farrukh Shahzad,Ghalib A. Shah(2020), *IoT DoS and DDoS Attack Detection using ResNet* ,2020 IEEE 23rd International Multitopic Conference (INMIC).

[25] Almomani, B. Al-Kasasbeh, and M. Al-Akhras(2016), "*WSN-DS: A dataset for intrusion detection systems in wireless sensor networks,*" Journal of Sensors; Hindawi, vol. 2016, pp. 1–16.

[26] C. Del-Valle-Soto, L.J.; Valdivia, and J.C. Rosas-Caro(2019), "*Novel detection methods for securing wireless sensor network performance under intrusion jamming*," In the International Conference on Electronics, Communications and Computers (CONIELECOMP), IEEE, pp. 1–8.

[27] R. Singh, J. Singh, and R. Singh(2017), "*Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks*," Wireless. Communication. Mobile. Computing., vol. 2017, pp. 1-–14.

[28] S. Misra, P. V. Krishna, and K. I. Abraham(2011), "*A simple learning automata-based solution for intrusion detection in wireless sensor networks," Wireless Communications and Mobile Computing*, vol. 11, no. 3, 441 pages.

[29] KDD. KDD CUP. Available online: https://kdd.ics.uci.edu/databases/kddcup99/task.html
[30] Myint H O and Meesad P (2009) *Incremental Learning Algorithm Based n Support Vector Machine With Mahalanobis Distance for intrusion prevention* ,6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology vol 2 (IEEE) pp 630–633
[31] NSL-KDD dataset,https://www.unb.ca/cic/datasets/nsl.html
[32] Mohammadpour, L., Ling, T. C., Liew, C. S., & Chong, C. Y. (2018). *A Convolutional Neural Network for Network Intrusion Detection System.* Proceedings of the Asia-Pacific Advanced Network, 46(0), 50–55.
[33] Osken, S., Yildirim, E. N., Karatas, G., & Cuhaci, L. (2019). *Intrusion detection systems with deep learning: A systematic mapping study*. 2019 Scientific Meeting on Electrical-Electronics and Biomedical Engineering and Computer Science, EBBT 2019, 1–4.
[34] Panigrahi R, Borah S(2018). *A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems.* International Journal of Engineering & Technology. ; 7 (3.24): 479–482.
[35] Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani(2019), "*Developing realistic distributed denial of service (ddos) attack dataset and taxonomy,*" in 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 1–8.
[36] Sharafaldin, I.; Gharib, A.; Lashkari, A.H.; Ghorbani, A(2018) *Towards a reliable intrusion detection benchmark datase*t. Softw. Netw. , 2018, 177–200.
[37] Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A(2018). *Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization.* In Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP, Funchal, Portugal,; pp. 108–116.
[38] Bhuyan, M.H.; Bhattacharyya, D.K.; Kalita, J.K(2015). *Towards Generating Real-life Datasets for Network Intrusion Detection*. IJ Netw. Secur., 17, 683–701.
[39] Moustafa, N.; Slay, J(2015). UNSW-NB15: *A comprehensive data set for network intrusion detection systems(UNSW-NB15 network data set).* In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6.
[40] Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B(2019). *Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset*. Future Gener. Comput. Syst.,100, 779–796.
[41] Ajitha, P.Sivasangari, A.Gomathi, R.M.Indira, K."Prediction of customer plan using churn analysis for telecom industry",Recent Advances in Computer Science and Communications,Volume 13, Issue 5, 2020, Pages 926-929.
[42] "Sivasangari A, Ajitha P, Rajkumar and Poonguzhali," Emotion recognition system for autism disordered people", Journal of Ambient Intelligence and Humanized Computing (2019)."
[43] Ajitha, P., Lavanya Chowdary, J., Joshika, K., Sivasangari, A., Gomathi, R.M., "Third Vision for Women Using Deep Learning Techniques", 4th International Conference on Computer, Communication and Signal Processing, ICCCSP 2020, 2020, 9315196
[44] Sivasangari, A., Gomathi, R.M., Ajitha, P., Anandhi (2020), Data fusion in smart transport using convolutional neural network", Journal of Green Engineering, 2020, 10(10), pp. 8512–8523.
[45] A Sivasangari, P Ajitha, RM Gomathi, "Light weight security scheme in wireless body area sensor network using logistic chaotic scheme", International Journal of Networking and Virtual Organisations, 22(4), PP.433-444, 2020
[46] Sivasangari A, Bhowal S, Subhashini R "Secure encryption in wireless body sensor networks",Advances in Intelligent Systems and Computing, 2019, 814, pp. 679–686

[47] Sindhu K, Subhashini R, Gowri S, Vimali JS, "A Women Safety Portable Hidden camera detector and jammer", Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018, 2018, pp. 1187–1189, 8724066.

[48] Gowri, S., and J. Jabez. "Novel Methodology of Data Management in Ad Hoc Network Formulated Using Nanosensors for Detection of Industrial Pollutants." In International Conference on Computational Intelligence, Communications, and Business Analytics, pp. 206-216. Springer, Singapore, 2017.

[49] Gowri, S. and Divya, G., 2015, February. Automation of garden tools monitored using mobile application. In International Confernce on Innovation Information in Computing Technologies (pp. 1-6). IEEE.

[50] Pa, Y.M.P.; Suzuki, S.; Yoshioka, K.; Matsumoto, T.; Kasama, T.; Rossow, C(2015). *IoTPOT: Analysing the rise of IoT compromises. In Proceedings of the 9th USENIX Workshop on Offensive Technologies (WOOT 15)*, Washington, DC, USA, 10–11 .

[51] Mirsky, Y.; Doitshman, T.; Elovici, Y.; Shabtai, A. Kitsune(2018): *An ensemble of autoencoders for online network intrusion detection*. arXiv , arXiv:1802.09089.