Educational Administration: Theory and Practice
2024,30(4), 1200-1214
ISSN:2148-2403
https://kuey.net/

Research Article

Intrusion Detection Systems and its application in latest Networking Technologies – A Survey

K. Shanthi[1*], R. Maruthi[2]

[1*]Research Scholar, PRIST University, Thanjavur.
[2]Associate Professor, Hindustan Institute of Technology and Science, Chennai

Citation: K. Shanthi et al. *(2024),* Intrusion Detection Systems and its application in latest Networking Technologies – A Survey, *Educational Administration: Theory and Practice, 30(4),* 1200-1214, Doi: 10.53555/kuey.v30i4.1638

ARTICLE INFO

ABSTRACT

The attackers are using different techniques to intrude themselves into the network or system to steal our data. The intruding techniques are increasing day by day and it is very difficult to detect the attacks. Researchers find a lot of challenges and issues to design an intrusion detection system. The growth of malicious software is growing and finding the type of catastrophic failure it will create cannot be predicted and detected. This survey presents some of the methods employed in designing the Intrusion detection Systems (IDS) and it provides insights into the various IDS techniques used in different networking technologies.

Keywords: Intrusion Detection Systems, Artificial Intelligent Techniques, Internet of Things, Wireless Sensor Networks, Mobile adhoc Networks, Cloud Computing, Blockchain Healthcare

1. Introduction

An IDS is a software or hardware which detects the malicious activities in the network or systems. The aim of IDS is to identify different kinds of attacks. In general, the IDS is classified into Signature Based Intrusion Detection Systems (SIDS) [1] and Anomaly Based Intrusion Detection Systems (AIDS) and. Signature-based detection is one of the fundamental detection methods used by intrusion detection systems (IDS). It enables IDSs to quickly recognize malicious network traffic by looking for a collection of known signs. These methods use patterns or signatures to analyze the data. A signature is a distinct pattern or identifier: It could be a byte sequence in network traffic, data within a file, or a series of instructions. It is frequently compared to a fingerprint or DNA specimen in that it only belongs to that specific pattern. Others may exhibit similar traits, but each malware type's signature is unique. A well defined or known data set must be available to identify the attacks.

2. Intrusion Detection Systems(IDS) Techniques

Anomaly-based or behavior-based detection provides a more thorough analysis of network activity, establishing a baseline of patterns and activities that constitute "normal" activity. Anomaly-based findings function against this "normal" backdrop, looking for behaviour that differs from the "normal" baseline and may signal malicious activity. An anomaly or behavior-based detection system may use machine learning to establish a baseline or discover trends that could be indicative of an attack. These methods estimate the abnormal behavior of the system and it always looks into the normal behavior of the system. It means that it attempts to find out any suspicious activity. Among these two methods, the signature based methods provide better results, but at the same time the anomaly based schemes detect previously unknown activities [2].
The ability, or lack thereof, to detect new or novel attack methods distinguishes signature-based and anomaly-based systems at their core. Signature-based detections only trigger alerts when they find an exact match of a known indicator, not any variance from the known indicator, therefore they cannot detect malicious activity. When activity falls outside of an acceptable range, an anomaly-based system will send out an alert. The activity could take the shape of traffic that is not "normal" for the network or evidence of unusual attempts to connect to the network (for example, with an unauthorized device). Anomaly-based detection may also use heuristic analysis, which focuses on discovering unknown threats via pattern formation, sandbox testing, and other ways to uncover malicious activity or code that does not elicit warnings in a signature-based detection system. This

review focuses on the domains in which the IDS are employed to detect the hackers and it is shown in Figure 2.1

Figure 2.1: Intrusion Detection Systems & its Application Areas

2.1 Intrusion Detection Systems and Artificial Intelligence & Machine learning

Artificial Intelligence (AI) techniques were used in all the fields and it is gaining its importance in designing and improving IDS. The purpose of AI is to be used to improve the performance of the existing algorithms and techniques. Signature-based intrusion detection has been the most widely utilized method for detecting attacks and providing security. However, with the advent of Artificial Intelligence (AI), specifically Machine Learning, Deep Learning, and Ensemble Learning, promising findings in more efficient attack detection have been demonstrated. Leveraging IDS and AI to secure a network can ensure that the cyber infrastructure is safe from threats and unwanted behaviour. An AI/ML-based IDS seeks to learn/benchmark the common or typical types of network traffic generated by IoT devices, and discover abnormalities based on algorithms and variations from those normal or typical forms of traffic.

In paper [3] , data reduction for intrusion detection is done by AI methods in order to reduce the amount of data. In data reduction, the unnecessary or unwanted data is filtered and left with only the data necessary for the detection process. The data reduction can be carried out by methods like data filtering, feature selection and data clustering. The classification in intrusion detection is performed by AI methods to distinguish between the intruders and normal users. It is carried out using Expert Systems, Anomaly detection, rule based induction etc, The various AI and ML techniques used in the intrusion detection systems are shown in Figure 2.2

Artificial Neural Networks (ANN) is a form of machine learning algorithms and its makes use of learning rules that apply in a wide variety of classification tasks. The malicious network traffic is detected using ANN for packet inspection and it works with the accuracy of 98% and false positive rates of less than 2%.[4]. Several machine learning techniques based on computational Intelligence (CI) and the various characteristics of those techniques were considered to build efficient IDS[5]. A study in [6] provides insights into the CI techniques including ANN, fuzzy systems, evolutionary computation, artificial immune systems, swarm intelligence and soft computing. A hybrid method for intrusion detection which combines Decision trees (DT) and Support Vector Machines (SVM) has been built to design a hierarchical hybrid intelligent system model (DT-SVM) with a combination of base classifiers and other hybrid machine learning techniques [7].

An AI based IDS using a deep neural network (DNN) with KDD cup 99 dataset was investigated and verified in [8]. An artificial computational intelligence with a multi-agent support for IDPS schemes has been reviewed in [9]. A study has been conducted to develop IDS based on AI and machine learning for classification of datasets with SVM, K-nearest Neighbor(KNN), Decision Tree(DT) algorithms . The widely used dataset used to develop IDS Systems includes CSE-CIC IDS-2018, UNSW-NB15, ISCX-2012, NSL-KDD and CIDDS-001 data sets, which are widely used to develop IDS systems[10]. A machine learning based Intrusion Decision Tree(IntruDTree) is designed to build a data-driven IDS by ranking the security features[11].It is compared with the traditional machine learning models such as Naïve Bayes Classifier, logistic regression, SVM and KNN. A DNN to develop effective IDS to detect unpredictable attacks and it is applied to the datasets viz, KDDCup 99, NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, and CICIDS 2017[12]. Adversarial examples were generated using the evolutionary algorithms and deep learning approaches and it is applied in NSL-KDD and UNSW-NB15[13].

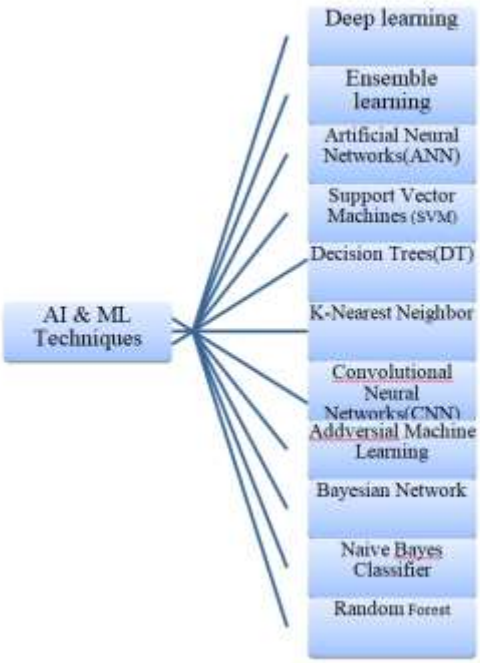

Figure 2.2 AI & ML methods for IDS

Genetic algorithms and decision trees were used to generate rules for classifying network connections with the machine learning approach [14]. A supervised machine learning model using ANN has been suggested in [15] and it is compared with the SVM technique and evaluated with NSL-KDD dataset. DNN classifier is used in [16] to identify the different types of intrusion attacks and it outperforms the SVM method. A federated learning scheme named as "DeepFed" to detect cyber threats in industrial cyber-physical systems has been developed in [17]. KNN and Random forest, the two machine learning models are used in detecting the attacks using the CIDDS-001, which is one of the most used dataset for network-based intrusion detection [18]. The network-based intrusion detection systems using fuzzy logic and ANN are reviewed using the KDD99 dataset [19]. Decision trees, random forests and SVM algorithms were used in this study for intrusion detection using CICIDS-2017 dataset[20].

The popular classification algorithms namely, Bayesian Network, Naïve Bayes Classifier, Decision Tree, Decision Forest, Random Tree, Decision Table and ANN are employed to detect intrusions[21]. It has been proposed to use a categorization technique to group the anomalies in IDS. Prior to employing a machine learning classifier for the categorization process, the intrusions were detected using the Firefly Optimization (FFO) technique. The Knowledge Discovery Dataset (KDD-CUP 99) will be used to validate the results of the detection strategies. Several performance indicators, such as specificity, recall, F1-score, accuracy, precision, and sensitivity, will be evaluated by the implementation for different kinds of cyberattacks. The accuracy of the suggested method is a high 98.99%[22]. In order to detect attacks, a clever and effective network intrusion detection system (NIDS) based on Deep Learning (DL) has been suggested in [23]. The CICIDS2018 and Edge_IIoT real-time traffic datasets were used to train the model. The model's performance is examined by multiclass classification, and it has been found to attain 100% and 99.64% accuracy rates, respectively, during training and testing using the datasets. In [24], a neural network method for threat prediction in intrusion detection systems was proposed, utilizing Python Spyder software for simulation. It has been suggested in [25] to use a hybrid deep-learning technique to identify distributed denial-of-service assaults on the communication infrastructure of the smart grid. Recurrent gated unit algorithms and convolutional neural networks are combined in this strategy. The Intrusion Detection System dataset from the Canadian Institute for Cybersecurity and a custom dataset created with the Omnet++ simulator were the two datasets used, and both yielded a high accuracy rate of 99.86%.

The Concept of decision trees is used as predictive models to detect cyber attacks and reduces the computational complexity [26]. Adversarial machine learning (AML) strategies and defense mechanisms to reduce the attacks were discussed in [27]. A method suggested in [28] detects a group of intrusions which combines both deep learning and decomposition methods and it is evaluated using IDS 2018 and LUFlow data set. A work in [29] proposes a systematic approach that combines behavior-based deep learning and heuristic-based approaches to identify modern malware like Adware, rootkit Radware, SMS malware and ransomware and the proposed method outperforms the other deep learning methods. A Stacked Long Short Term Memory model configuration to improve the performance of AIDS has been suggested in [30] with the preprocessed CICIDS2017 data set to achieve highest accuracy. ML is used in IDS for IoT applications using VGG-16 and DenseNet, K-nearest neighbors, random forest and SVM were studied and VGG-16 stacked model shows the

highest accuracy of 98.3%. Neural network based threat prediction system has been proposed in [31] using the widely used NSL-KDD data set. Widely used supervised and unsupervised ML methods were explored and studied in [32] using CICIDS2017 dataset in real world network attacks. An unsupervised technique using temporal convolutional networks and edge computing is proposed using generative adversarial networks (GAN) is proposed in [33] for edge servers and the proposed approach is 3.8 times faster than other ML based methods and it is found to be more accurate. Controller Area Network (CAN) in vehicle communication protocol lacks message authentication and encryption schemes to protect the data and the AI-based IDS has been suggested as a countermeasure against automotive cyber attacks [34].

The implementation of appropriate detection systems is a challenging task and it depends on the network and other components in the network infrastructure like protocols, routers, firewalls etc,.[35,37]. A Hybrid model that merges ML and Deep Learning (DL) has been suggested in [36] using SMOTE for preprocessing and XGBoost for feature selection to increase the detection rates and it is tested with KDDCUP99 and CIC MAlMem-2022 datasets with an accuracy of 99.99% and 100% respectively. SCADA (Supervisory Control and Data Acquisition) Systems protection is important for national and international security. A novel European framework -7 project CockpitCI has been introduced in [38] using intelligent intrusion detection methods like rule-base approach, hidden markov model and support vector machines to protect the SCADA systems. The table 2.1 provides the summary of the methods used for the IDS and the datasets used for testing the efficiency.

Table-2.1 Methods for IDS and the dataset used

Method used	**Dataset used**
Deep Neural Network [8,12], Fuzzy Logic and Artificial Neural Networks [19,22], Bayesian Network, Naïve Bayes Classifier, Decision Tree, Decision Forest, Random Tree, Decision Table[22], ML and DL using SMOTE and XGBoost of feature selection[36], feature-weighted Naive Bayes (NB)[64], LSTM and component analysis[68]	KDD cup 99
Support Vector Machines(SVM), K-nearest Neighbor(KNN), Decision Tree(DT) algorithms [10], Deep Neural Network[12,23], DL based intrusion detection in fog computing[57]	CSE-CIC IDS-2018
Support Vector Machines(SVM), K-nearest Neighbor(KNN), Decision Tree(DT) algorithms [10], Deep Neural Network[12],], Evolutionary Algorithms and Deep learning[13], DL and CNN models[39], LSTM[42], DL based intrusion detection in fog computing[57], LSTM and component analysis[68]	UNSW-NB15
Support Vector Machines(SVM), K-nearest Neighbor(KNN), Decision Tree(DT) algorithms [10]	ISCX-2012
Support Vector Machines(SVM), K-nearest Neighbor(KNN), Decision Tree(DT) algorithms [10], Evolutionary Algorithms and Deep learning[13], Artificial Neural Networks(ANN)[15] . Neural Netwroks[31], DL and CNN models[39], LSTM[42], Deep learning algorithm and conditional generative adversarial network (CGAN)[67], LSTM and component analysis[68]	NSL-KDD
Support Vector Machines(SVM), K-nearest Neighbor(KNN), Decision Tree(DT) algorithms [10], KNN and Random forest[15]	CIDDS-001
Deep Neural Network[12], Gaussian Naive Bayes (GNB) and Stochastic Gradient Descent (SGD) algorithms[60], Stacked Convolutional Neural Network and Bidirectional Long Short Term Memory (SCNN-Bi-LSTM) model[61], Particle Swarm Optimization (PSO)-based ANN[63]	WSN-DS
Deep Neural Network[12]	Kyoto
Deep Neural Network[12], Decision trees, random forests and SVM[20], Stacked Long Short Term Memory model[30], Supervised and un-supervised ML methods[32,48], DL based intrusion detection in fog computing[57], Stacked Convolutional Neural Network and Bidirectional Long Short Term Memory (SCNN-Bi-LSTM) model[61], Deep learning algorithm and conditional generative adversarial network (CGAN)[67], LSTM and component analysis[68]	CICIDS 2017
Deep learning and decomposition methods[28]	IDS 2018
Deep learning and decomposition methods[28]	LUFlow
ML and DL using SMOTE and XGBoost of feature selection[36],	CIC MAlMem-2022
Singular Value Decomposition (SVD) method[45] Long Short-Term Memory (LSTM) network-based Secured Automatic Two-Level Intrusion Detection System (SATIDS)[46]	Ton- IoT

2.2 Intrusion detection Systems and Internet of Things

The Internet of Things (IoT) is a growing field due to the growth of new technologies and researches are emerging in this area. So it is important to protect the IoT networks from the intruders and it is finding its importance in IDS nowadays. The security concerns are particularly prominent as the number of IoT devices grows, and security vulnerabilities arise at all three layers of the IoT architecture. Conventional IoT IDS are used at the device or gateway level. These measures protect the network from attacks caused by hostile IoT or non-IoT devices in the network. However, the network edge creates new attack surfaces for malevolent actors to exploit. Intrusion detection, which has been under research for over 30 years, is thought to have the capacity to solve IoT security issues.

Deep learning(DL) and Convolutional Neural Network(CNN) models are used in the IDS and the NSL-KDD and UNSW-NB 15 were applied in the study given in [39]. AI techniques are used to improve the performance of the medical communication systems and the IDS is very much needed in IoMT(Internet of Medical Things) for smart healthcare[40]. It also discusses the IoMT architecture and security aspects of IoMT. AN IDS in IoT using the Deep Learning algorithms with CIC-IDS 2017 dataset [41]. An IDS using Long Short Term Memory(LSTM) is used to identify the attacks and it is validated using NSL-KDD, UNSW-NB15 and TON_IoT datasets. This method uses SPIP framework (S: Shapley Additive exPlanations, P: Permutation Feature Importance, I: Individual Conditional Expectation, P: Partial Dependence Plot) and it shows high detection accuracy, processing time, and high interpretability of data features and model outputs compared with other traditional techniques[42].

One powerful method for successfully detecting cyber-attack attempts in Internet of Things devices is Deep Reinforcement Learning (DRL). DRL is composed of a meta-model based on Markov Decision Processes that allows the solution of high-dimensional combinatorial optimization problems even in the absence of differentiable supervisory signals. Multiple intelligent IDS has been proposed for the IoT environment where high-level objectives are been pursued alongside the detection accuracy. These objectives include, but are not limited to, protecting sensitive data privacy, cutting down on power usage at the edge, and optimizing the computational overhead [43].A study in [44] used three methods, DL techniques with optimization algorithm, optimization algorithm for feature selection and CNN LSTM for NIDS in IoTs. IDS for identifying cyberattacks in Industrial IoT networks(IIoT) has been suggested in [45] by applying the singular value decomposition (SVD) method to enhance detection performance by reducing data features. The efficiency of the proposed model is verified using the ToN-IoT dataset and it achieves an accuracy rate of 99.99% for binary classification and 99.98% for multiclass classification.

An Improved Long Short-Term Memory (LSTM) network-based Secured Automatic Two-Level Intrusion Detection System (SATIDS) for IoT and Software Defined Networks (SDN) has been presented in [46]. For the ToN-IoT dataset, the two level IDS attains 96.35% accuracy, 96% detection rate, and 98.4% precision, while for the inSDN dataset, it obtains 99.73% accuracy, 98.6% detection rate, and 98.9% precision. ML-based IDS for IoT using stacking ensemble model as a most optimal classifier and it is evaluated using Mathew's correlation coefficient of 0.9971 and 0.9909 in the binary classification and the multi-class classification respectively [47]. Widely used supervised and unsupervised ML methods were explored in [48] using CICIDS2017 dataset in real world network attacks were studied.

2.3 Intrusion detection Systems and Cloud Computing

Cloud IDS enables a business to detect cyber threats and provide critical notifications to security staff for incident response. In actuality, the application of your security policies in the cloud will be very different from an on-premises environment. Because many cloud systems are connected to the internet, attackers can use them to enter inside networks. Network and hardware visibility are drastically different, and in many circumstances more constrained and certain resources are ephemeral, which means they may cease to exist before you even begin investigating an incident on them.

The cloud IDS consists of three levels.

1. Cloud layer
2. Network layer
3. Compute (Virtual Machines, Containers, etc.)

Figure 2.3 Cloud IDS Layers

The cloud layer is at the top, but the network layer and virtual machines rely on it. Whoever has access to the cloud management layer has influence over the network and computing layers. Some of the effective intrusion detection strategies for each level are as follows.

1. Compute Layer:

In the cloud, safe authentication is critical since anyone can attempt to enter into your AWS account from anywhere, for example. Even if you have made every effort to safeguard it, anyone may still gain access to your cloud management layer, including the APIs. Keys or accounts can be mistakenly leaked, a DevOps specialist's workstation with open sessions can be targeted, and, ultimately, while prevention is excellent, we must anticipate controls will fail at some point and be prepared to identify it. As a result, intrusion detection must take place at the cloud layer, which is one step above computation.

2. Network Layer

In an on-premises environment, such as a data centre, it is important to employ virtual private clouds (VPC). Enabling VPC flow logs and connecting the machines to the threat detection service. Instead of capturing all packets, this strategy makes use of network traffic metadata.

3. Compute Layer

Host-based intrusion detection (HIDS) is a technique for monitoring and analyzing a computer's internal data. The growth of encrypted network protocols also makes identifying network intrusions more difficult, whether in the cloud or not. Because of the usual absence of access to raw network data, the cloud is frequently the sole choice for compute-level IDS.[49]

Given the desirable qualities of IDPS and cloud computing systems, a set of pertinent needs is determined, and four ideas of autonomic computing self-management, ontology, risk management, and fuzzy theory are used to meet these requirements [50]. The IDS of the cloud environment can be proposed based on the characteristics of IDS techniques, cloud evaluation criteria, and an analysis of the various methodologies.[51]. [52] proposes an architecture for cooperative intrusion detection systems (IDS), which lessens the impact of these types of attacks. To achieve such functionality, IDSs in cloud computing regions communicate alerts with one another. In the system, each IDS has a cooperative agent that computes and decides whether to accept alarms given by other IDSs or not. Traditional IDS are generally inefficient to implement in cloud computing settings because of their openness, dynamicity, and virtualization of services. [53] proposes a unique IDS architecture for cloud computing that employs sophisticated approaches for robust, effective, and efficient cloud intrusion prevention and detection systems (CIPDS).

[54] proposes a complete and reliable solution for detecting and preventing intrusions in cloud computing systems using a hybrid method dubbed HIDCC (Hybrid Intrusion detection for Cloud Computing). A distributed Machine Learning-based intrusion detection system for Cloud environments is proposed in [55]. The system is designed to be installed in the Cloud with the Cloud provider's edge network components. This enables the physical layer's edge routers to intercept incoming network traffic. Each Cloud router's collected network data is preprocessed using a time-based sliding window approach before being passed to an anomaly detection module that employs a Naive Bayes classifier. When network congestion worsens, each anomaly detection module has access to a pool of commodity server nodes based on Hadoop and MapReduce. For each time window, abnormal network traffic data on each router side are synchronized to a central repository.[56] presents a revolutionary Distributed Intrusion Detection System (DIDS) based on a novel combination of two distinct trends in intrusion detection: behavior-based and knowledge-based intrusion detection algorithms. The behavior-based method improves detection in the dynamic cloud environment, while the knowledge-based approach strengthens the detection scheme with its definitive rule basis.

The design of a new hybrid architecture for DL intrusion detection in fog computing was given, which integrates the usage of Deep learning models. Due to the high dimensionality of network data, radial basis function-based support vector regression (RBFSVR) is first utilized to reduce dimensionality and training time. The integrated VGG19 and 2DCNN are then used on the cloud server to finish training the dataset before transferring it to the fog layer, where data traffic is monitored and dangers are identified. Experiments with the UNSW-NB15, CICIDS2017, and CICIDS2018 datasets demonstrate that the techniques presented in this paper outperform other comparable techniques in terms of detection rate, F-score, precision, recall, false alarm rate, and accuracy, thus solving the problem of intrusion detection [57].

An efficient hybrid clustering and classification technique for creating anomaly-based IDS for harmful attack type classifications is proposed in [58]. A filter-based ensemble feature selection (FEFS) and employed a deep learning model (DLM) for cloud computing intrusion detection is created in [59]. The FEFS is a combination of three feature extraction processes: filter, wrapper and embedded algorithms. Based on the above feature extraction process, the essential features were selected for enabling the training process in the DLM. Finally, the classifier received the chosen features. The DLM is a combination of a recurrent neural network (RNN) and Tasmanian devil optimization (TDO). In the RNN, the optimal weighting parameter is selected with the assistance of the TDO. The TDO helps the RNN find the best weighting parameter. The proposed technique was implemented in MATLAB, and its efficacy was evaluated using performance metrics such as sensitivity, F measure, precision, recall, and accuracy. The proposed method was compared to traditional techniques such as RNN, DNN, and RNN-genetic algorithm (RNN-GA).

2.4 Intrusion detection Systems and wireless Sensor Networks

The most important elements of a Wireless Sensor Networks (WSN) is its multihop distributed activities, which add complexity to security threat detection and prevention. In a multihop distributed system, identifying attackers or malicious nodes is extremely challenging. WSN's are made up of sensor nodes that are strategically placed to gather data about their surroundings. The distributed nature of WSNs, multihop data forwarding, and open wireless medium make them very vulnerable to security assaults at many levels. Intrusion Detection Systems (IDS) can help detect and prevent security assaults. WSNs are susceptible to a variety of security attacks due to their open wireless channel, multihop distributed communication, and installation in hostile and physically unprotected environments. The methods suggested in [60] employ machine learning techniques, notably the Gaussian Naive Bayes (GNB) and Stochastic Gradient Descent (SGD) algorithms. On the WSN-DS dataset, the proposed SG-IDS model earned a 96% accuracy rate, exceeding state-of-the-art algorithms that reached rates of 98% accuracy, 96% recall, and 97% F1. In an evaluation of an IoMT dataset, the SG-IDS performed wonderfully, with an accuracy of 0.87 and a precision of 1.00 in intrusion detection.

Traditional IDS approaches frequently fail to sufficiently secure the confidentiality of information and detect complicated unique intrusions, especially in Wireless Sensor Networks (WSNs). A new Stacked Convolutional Neural Network and Bidirectional Long Short Term Memory (SCNN-Bi-LSTM) model for intrusion detection in WSNs is proposed in [61]. This approach uses Federated Learning (FL) to improve intrusion detection performance while protecting privacy. The FL-based SCNN-Bi-LSTM model takes a novel technique, allowing several sensor nodes to collectively train a central global model without revealing private data, hence addressing privacy issues. The SCNN-Bi-LSTM model's deep learning methodology accurately detects sophisticated and previously undiscovered cyber threats by methodically studying both local and temporal links in network patterns. The model was specifically created to detect and categorize various sorts of Denial of Service (DoS) attacks using specialized WSN-DS and CIC-IDS-2017 datasets.

Underwater Wireless Sensor Networks (UWSNs) are the kind of WSNs that send the information through water medium and screen the maritime circumstances, water contents, under-ocean habitations, submerged creatures and military articles. In [62] describes a new intrusion detection system that uses Integrated Secure MAC principles and Long Short-Term Memory (LSTM) architectures to organize real-time neighbor monitoring duties. To protect data communication, the proposed system uses Generative Adversarial Network (GAN)-driven UWSN channel evaluation models as well as Secure LSTM-MAC principles. The suggested methodology uses trained distributed agents to develop an Intrusion Detection System (IDS). These agents, which run on each authorized sensor node, include a unique LSTM-MAC engine, an intrusion dataset, rule-based monitoring approaches, Secure Hashing methodology-3 (SHA-3), the Two Fish methodology, and packet filtering tools. The studies and observations show that the proposed strategies perform 5% to 10% better than existing techniques in a variety of criteria.

An innovative strategy is presented in [63] to improve the security of Wireless Sensor Networks (WSNs) by combining Particle Swarm Optimization (PSO) with an Artificial Neural Network (ANN) to create effective Network Intrusion Detection Systems (NIDS). This concept and implementation employs a Particle Swarm Optimization (PSO)-based ANN model, followed by extensive evaluations on real-world WSN datasets obtained from Kaggle, and it outperforms the KNN model. The combination of PSO and ANN contributes to a powerful and adaptable intrusion detection system designed for the resource-constrained nature of WSNs.

The technique provided in [64] is an enhanced intrusion detection system that utilizes feature-weighted Naive Bayes (NB) to improve network attack detection accuracy. First, a feature weighting technique is proposed that assigns context-based weights to various feature terms. The NB algorithm is then improved by combining Jensen-Shannon (JS) divergence, feature weighting, and inverse category frequency (ICF). Finally, the modified NB method is integrated into the intrusion detection model, and network event classification results are obtained by applying a series of data processing procedures to the associated network traffic data. The effectiveness is assessed through a comprehensive comparative study of the NSL-KDD dataset. The results show a considerable improvement in the detection accuracy of many attack types, such as normal, denial of service (DoS), probing, remote-to-local (R2L), and user-to-root (U2R). It also has a lower false alarm rate than other algorithms, which improves detection accuracy and rate while also lowering the occurrence of false detections.

[65] employs a unique framework that is trained on a dataset to detect and classify various threats. The model's output findings reveal that WSN improves the ability of the intrusion detection system by employing a higher classification, accuracy, and precision rate of 99.45% and 97%, respectively. The Weka tool is used to create an optimal model, which is then trained on a dataset including various forms of attacks using some selected classifiers. Attacks such as black hole, flooding, scheduling, and grey hole were foreseen by WSN.

The NIDS is designed using the attribute selection approach (PSO) is capable of detecting any kind of malicious activity in the network or any unusual actions in the network, enabling the detection of illegal activities and securing the enormous amounts of confidential data belonging to customers from being compromised. The datasets were created using both a network architecture and a simulation network. Wireshark collects data packets, whereas CISCO Packet Tracer simulates network configuration. Furthermore, a physical network of six node MCUs connected to a laptop and a mobile hotspot has been established, and communication packets are being recorded using the Wireshark software. PSO is an optimization approach[66]. An approach suggested in [67] is an IDS model that uses a deep learning algorithm, conditional generative adversarial network

(CGAN), enabling unsupervised learning in the model and incorporating an eXtreme gradient boosting (XGBoost) classifier for faster result comparison and display. The proposed solution eliminates the requirement to deploy additional sensors to provide bogus data to deceive the intruder. This model improves accuracy, reduces false detection rates, and achieves high precision in both the NSL-KDD and CICIDS2017 datasets, which can be utilized as a cyber intrusion detector. The suggested approach reduces false alarms by approximately 1.827%.

An enhanced empirical-based component analysis for IDS employing LSTM and component analysis for intrusion detection, verified with IDS datasets such as KDD CUP 99, NSLKDD, UNSWNB15, and CICIDS2017. When compared to existing models, the accuracy is 99.95%[68].

Many researchers, inspired by the real immune system, use artificial immunological principles to detect intrusions in wireless sensor networks, such as negative selection algorithms (NSA), hazard theory, and dendritic cell algorithms. When applying the negative selection method to wireless sensor networks, the peculiarities of wireless sensor networks, such as frequent changes in network topology and limited resources, are not taken into account sufficiently, resulting in a detection effect that requires improvement. An NSA based on spatial partition is presented and tested on hierarchical wireless sensor networks. The algorithm first evaluates the distribution of the self-set in the real-valued space, after which it divides the space into multiple subspaces. Selves are classified into many subspaces. Not all self, only those in the subspace where the detector is located must be tolerated with the randomly generated candidate detector. The time required to calculate distance is decreased by this technique. It is faster to detect antigens when the mature detectors in the subspace where the antigen is located match the antigen rather than all the detectors, as this simplifies the detector detection procedure. The approach is effective for wireless sensor network intrusion detection, saves sensor node resources and lowers energy consumption, and improves time efficiency and detector quality, according to theoretical analysis and experimental results [69].

2.5 Intrusion detection Systems and Blockchain technology

Blockchain has also been adopted in healthcare, supply chain management, and the Internet of Things. Blockchain uses robust cryptography with private and public keys, and it has numerous properties that have leveraged security's performance over peer-to-peer networks without the need for a third party[70]. A blockchain does not depend on a single, reliable central authority; instead, it uses a decentralized distributed ledger system. Because distributed ledger technology (DLT) records transactions on all network nodes, it is more difficult for hackers to access, steal, or alter data. The adoption of blockchain technology can enhance the accuracy of an intrusion detection system (IDS) by offering a decentralized, secure, and unchangeable ledger that can trace questionable activities over time and pinpoint intrusions worldwide. The authors of this research offer a brand-new approach to raise the precision of blockchain-based IDS.

A new blockchain-based hybrid intrusion detection system (BC-HyIDS), which transfers signatures between nodes in distributed IDS by utilizing the blockchain foundation has been presented in [71]. The three phases of BC-HyIDS's operation include the usage of blockchain technology in the third phase to secure data moved over the network in addition to detecting measures. Hyperledger Fabric v2.0 and Hyperledger Sawtooth on throughput, processing time, and average latency are used to assess blockchain performance. The performance of BC-HyIDS with blockchain is better.

A method to improve the accuracy of IDS in blockchain-based systems is presented in [72]. The technique is based on the fusion concept, which uses weighted votes to combine several IDS algorithms and determine the result. The suggested solution combines multiple algorithms into a single blockchain-based design, which makes it extremely secure and closely watched. Additionally, the system makes use of artificial intelligence (AI) technologies to improve scalability and accuracy using the four primary components of the proposed system are distributed blockchain-based IDS, ML-based IDS, AI-based IDS, and node-level IDS.

In [73], a novel blockchain-based collaborative intrusion detection (CID) method for MMG systems in smart grids is presented. Owing to blockchain's consensus process, the method is aimed to increase intrusion detection accuracy cooperatively without requiring a central server or trusted authority. It has a mechanism for generating proposals that combines trigger and periodic patterns to produce a proposal, which is the CID detection target. From the generated proposals together with the correlation model of MMGs, a CID is achieved by using the consensus mechanism. The final detection results of CID are stored on blockchain in sequence. The use of an incentive mechanism motivates a single microgrid to participate in consensus. The effectiveness of the presented approach is demonstrated through a case study on an MMG system.

Motivated by the versatility of blockchain technology, the work in [74] attempts to develop a deep learning-based intrusion detection system (IDS) model that may potentially combine blockchain technology with intrusion detection. When it comes to the precision of identifying security breaches, the suggested model performs better than traditional ones. Some of the issues brought on by the curse of dimensionality can be resolved by using AI and metaheuristic techniques for feature selection and classification. The technique in [75] describes a blockchain-based data security strategy where blocks are created by the RSA hashing technique. To train and test our model, we first choose the blockchain-secured data and divide it into training and testing datasets using Differential Evolution (DE). The verified model may also employ a deep belief network (DBN) for attack prediction. In addition to increasing classification accuracy, the method strengthens the data's defence against attackers.

The cooperative clustering-characteristic-based data fusion solution discussed in [76] for intrusion detection in a Blockchain-based system, in which an AI model is trained and analyzed to evaluate data clusters in Blockchain networks, and a mathematical model of data fusion is constructed. After several rounds of mutual competition across clustering nodes, the aberrant traits in a Blockchain data set are detected, a weighted combination is performed, and the weighted coefficients among multiple nodes are obtained. Together, the weighted coefficient and the similarity matching relationship can detect anomalous intrusive behaviour with high accuracy when they exhibit a standard pattern. According to experimental findings, the suggested method performs well in real-time attack detection on a blockchain and has a high recognition accuracy.

AI is used as an analytical tool to deliver consistent findings in decision-making because the devices and sensors in an IoT network enabled by blockchain generate a lot of data. Data analysis and security-related issues are managed at the network's edge thanks to the fog computing paradigm, which decentralizes cloud-based centralized security mechanisms. Using fog computing, a distributed IDS is created to identify DDoS assaults on the memory pool in an Internet of things network enabled by blockchain. Two well-known machine learning algorithms—random forest and XGBoost—are utilized in distributed architecture to assess the suggested detection system. The model's performance is examined using an actual IoT-based BoT-IoT dataset, becausee it contains a variety of current botnet-related attacks, including stealing, DDoS, and DoS. Various assessment criteria, including precision, false alarm rate, accuracy, and detection rate, are employed to fully examine the performance of the suggested [77].

A Software Defined Networking platform for collaborative IDS (CIDS) based on blockchain. Rapid advancements in SDN, which divides the controller plane from the forwarding plane, can reduce network complexity. Without being aware of the devices' underlying configuration, the controller is able to oversee the entire network. CIDSs are still a crucial component of a secure SDN solution for identifying underlying bad nodes or devices, however they may be susceptible to insider threats, in which a hostile attacker acts within the network [78].

A cryptographically safe and secure method for obtaining verified and unchangeable entries in a chain that is arranged chronologically by discrete timestamps is also provided by blockchain. With practically everything being digital these days, organizations are becoming increasingly concerned about the rising rates of cyber threats, mishaps, and policy violations. It makes sense to leverage the wide range of capabilities provided by blockchain to support intrusion detection systems (IDSs) [79].

2.4 Intrusion detection Systems in Mobile Ad-hoc Networks

A mobile ad-hoc network, or MANET, is a dispersed, decentralized network of wireless portable nodes that connects directly to one another without the need for a centralized administrative system or fixed communication base station. Ad hoc network intrusion detection is a sort of defense mechanism that keeps an eye on, gathers, and examines mobile ad hoc node activity data in order to spot invasive activities. The nodes in the MANET may randomly link to one another because there is no infrastructure. The Intrusion Detection System (IDS) is an observation parameter that alerts the security operation centre when it detects unusual activity within the network.

Key considerations in the design of intrusion detection systems (IDS) and mobile ad hoc networks (MANET) prevention techniques include memory usage with the least amount of overhead and an analysis of detection rate. The two optimization issues in MANETs where nodes move randomly in any direction and undergo constant topology changes are node mobility and node energy. The Centrality Coati Optimization Algorithm (COA)based Cluster Gradient for multi attack intrusion identification was developed in [80] to overcome those two issues.

The Multi-Gated Self Attention Gated Graph Convolutional Network (MSA-GCNN) with a hybrid form of IDS and is implemented in the NS-2 network simulator. It is capable of recognizing many types of attacks, such as DoS and Zero-Day attacks. Attack detection rate, memory usage, and computation time are examples of performance metrics that are employed. The method preserves a higher attack identification rate with less processing time while reducing IDS traffic and memory use overall. The following results are obtained with the suggested technique: 4.299%, 10.375%, and 6.935 % Accuracy; 5.262%, 8.375%, and 7.945 % Precision; 7.282%, 10.365%, and 5.935 % Recall; and 9.272%, 5.355 %, and 8.965 %.

In order to reduce correlation and model pertinent characteristics with high-level representation, a stacked autoencoder-based method for MANET (Stacked AE-IDS) is developed in [81]. By using this technique, the input is replicated with a lower correlation, and the Deep Neural Network (DNN) classifier (DNN-IDS) uses the autoencoder's output as its input. The suggested Deep Learning-based intrusion detection system (IDS) uses the majority of possible assaults that affect mobile network routing services, with a particular emphasis on Denial of Service (DoS) attacks within labeled datasets that are accessible for intrusion detection. By increasing the efficiency of IDSs, the suggested Stacked AE-IDS technique may be used to improve MANET security. This method can be used to identify various attack types, especially denial-of-service (DoS) attacks, and their effects on routing services in Mobile Networks.

The study in [82] examines the leading components and performance of mobile nodes while providing a thorough examination of MANET security measures. Fuzzy Logic Systems (FLS) are used in performance reliability evaluation models and detection methods.

An approach in [83] uses Dual Interactive Wasserstein Generative Adversarial Networks (DIWGAN) optimized with Namib Beetle Optimization Algorithm. Mobile users for the intrusion detection and attack prevention in MANETs first register with the Trusted Authority by using the One Way Hash Chain Function. For the purpose of authenticating themselves, each mobile user submits a finger vein biometric along with their user ID, latitude, and longitude. The four components of intrusion detection are the packet analyzer, feature extraction, preprocessing, and classification. Using the suggested method, the classification unit divides the packets into five categories: DoS, Probe, U2R, R2L, and Anomaly. Ultimately, compared to the current models, the suggested approach offers 26.26%, 15.57%, 32.9% more accuracy, 33.06%, 23.82%, and 38.84% less delay analysis.

In [84], an entirely novel fuzzy extreme learning machine (PCA-FELM) based on Principal Component Analysis was presented. Principal Component Analysis is used for feature extraction, while PCA-FELM is used for classification, yielding a 99.08% accuracy rate compared to the previous approaches. In [85], an improved intrusion detection system (IDS) for mobile ad hoc networks that tackles routing attacks is proposed. This technique primarily creates 11 sub-datasets, uses a probabilistic methodology for feature ranking, and assesses the quality of each one using a fuzzy logic system. Ineffective features are eliminated from training and test sets in the following procedure. Next, the ambiguous and unknown samples are subjected to the Bayesian rough set classifier, which uses incoming packets to classify the behaviour of mobile nodes. This approach outperforms the previous IDS approaches, achieving an average detection accuracy of 94.37% for blackhole attacks and 99% for wormhole attacks.

Infrastructure-less networks are more vulnerable to various security attacks like black hole attack, network partition, node selfishness, and Denial of Service (DoS) attacks because of their overall decentralized architecture and hardware resource limitations. Deep learning artificial neural networks (ANNs) are used in the construction of an intrusion detection predicting strategy for Mobile Ad hoc networks in order to address the aforementioned problems. To raise the general security level of mobile ad hoc networks, a deep ANNs modelling and a simulation-based evaluation are proposed for identifying and isolating a Denial of Service (DoS) attack[86].

In [87], an innovative approach for an intrusion detection and prevention system (SA-IDPS) using machine learning techniques is provided to lessen attacks in MANETs. The mobile users register with the Trusted Authority via the One Way Hash Chain Function, and each user provides their user ID, latitude and longitude, and finger vein biometric as verification of authentication. The Packet Analyzer, Preprocessing Unit, Feature Extraction Unit, and Classification Unit are the four entities that are used to carry out intrusion detection. Any attack pattern is examined by the packet analyzer, which uses a Type 2 Fuzzy Controller to accomplish it. Logarithmic normalization and encoding techniques, which are time series and appropriate for any application, are taken into consideration in the preprocessing unit. Mutual Information is used in the feature extraction unit to obtain the best set of characteristics for packet classification. The packets in the classification unit are categorized into five classes using the Bootstrapped Optimistic Algorithm for Tree Construction with Artificial Neural Network: DoS, Probe, U2R, R2L, and Anomaly. The association rule tree is then used to determine whether the attack is frequent or rare. In this instance, the packets are classified using a history table. In order to assess the effectiveness of the suggested SA-IDPS scheme in terms of detection rate (%), false positive rate (%), detection delay (s), and energy consumption(j), tests are finally carried out and tested.

A new system called "Accurate and Cognitive Intrusion Detection System" (ACIDS) has been created to identify the black hole attack, which is the most dangerous packet dropping assault[88]. In order to detect intruders, this system analyzes characteristics such the Destination Sequence Number (DSN) and Route Reply (RREP) and looks for deviations from the expected behaviour. NS2 was used to simulate the suggested system, and the results of the investigation confirm that ACIDS is more effective than AODV routing protocol at identifying packet dropping circumstances related to black hole attacks. Several machine learning techniques, including -nearest neighbour (KNN), support vector machine (SVM), decision tree (DT), linear discrimination analysis (LDA), naïve Bayes (NB), and convolutional neural network (CNN), are used to classify wormhole attacks[98]. The classification outcomes demonstrate that the DT performs better than the other classifiers, with the accuracy of the KNN, SVM, DT, LDA, NB, and CNN techniques being 97.1%, 98.2%, 98.9%, 95.2%, 94.7%, and 96.4%, respectively.

2.5 Intrusion detection Systems and Health care Systems

The system may monitor patient data in real-time and identify intrusions as soon as they happen by integrating with IoT. Healthcare providers may reduce the harm caused by invasions and respond promptly to security breaches with the use of real-time detection. Create a unique feature set to prevent data interpretation errors. Networking servers offer an enhanced intermediate platform for data storage, communication, and many other features in smart e-healthcare systems. Physicians, clinical specialists, patients, and labs are the end users who can use the PHR and cloud servers. Any authorized person may do so. Malicious activity and network traffic must be identified and categorized. The system is made more secure and can identify network intrusion with the aid of attack type detection and network traffic classification [90].

In [91], a study was conducted on privacy and authentication in the context of smart healthcare, wireless communications, and privacy control. The study also established an intelligent and efficient online system that was required. An intrusion detection system with a high detection rate and a more accurate false alarm rate

was created using a machine learning support system that paired a Random Forest (RF) and a genetic algorithm.

It has been proposed in [92] to create a real-time testbed for the Enhanced Healthcare Monitoring System (EHMS) that gathers network traffic metrics and keeps track of patients' biometrics. A distant server receives the tracked data in order to make additional diagnosis and treatment decisions. Cyberattacks using man-in-the-middle techniques have been employed, and a dataset containing over 16,000 records of both attack and normal healthcare data has been generated. The performance has improved by 7% to 25% in certain circumstances, according to the results, demonstrating the reliability of the suggested approach in delivering accurate intrusion detection.

Wirelessly communicating medical equipment provides for features like remote monitoring and are rapidly being linked to the Internet and one another. Attacks on medical devices with Internet connections have the ability to seriously injure patients' bodies and endanger their lives. a cutting-edge intrusion detection system based on mobile agents to safeguard the network of linked medical equipment with excellent precision and low overhead[93].

The hybrid technique described in [94] called "ImmuneNet" uses deep learning to identify the most recent intrusion attempts and protect medical data. In order to achieve high accuracy and performance, the framework makes use of several feature engineering processes, oversampling approaches to enhance class balance, and hyper-parameter optimization techniques.

An Intrusion Detection System (IDS) known as "HEKA" was suggested as a method to track and identify assaults on personal medical device traffic. Through the use of several machine learning algorithms and an n-gram-based methodology, HEKA passively connects to the personal medical traffic produced by medical equipment in order to learn the contiguous sequence of packet information from the collected traffic and identify abnormal traffic-flow patterns[95]. HEKA has an accuracy of 98.4% and Fl-score of 98% in detecting various threats on personal medical equipment.

Conclusion

This paper presents the various techniques and methods used for detecting the cyber-attacks by intruders. Most of the methods used in the IDS strive to find the malicious pattern and inform or provide an alert to the authenticated users. It is evident from the study that IDS can be used in any networking applications with the thorough understanding of the strengths and weaknesses. In this paper, a survey of IDS and the networking technologies has been presented. Most of the IDS are designed using AI and ML based techniques to improve the accuracy with low false alarms. The datasets used for detecting the various attacks are also discussed to provide insights into the available datasets for IDS.

References

1. Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7.
2. Garcia-Teodoro, Pedro, et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security 28.1-2 (2009): 18-28.
3. Frank, Jeremy. "Artificial intelligence and intrusion detection: Current and future directions." Proceedings of the 17th national computer security conference. Vol. 10. 1994.
4. Shenfield, Alex, David Day, and Aladdin Ayesh. "Intelligent intrusion detection systems using artificial neural networks." Ict Express 4.2 (2018): 95-99.
5. Zamani, Mahdi, and Mahnush Movahedi. "Machine learning techniques for intrusion detection." arXiv preprint arXiv:1312.2177 (2013).
6. Wu, Shelly Xiaonan, and Wolfgang Banzhaf. "The use of computational intelligence in intrusion detection systems: A review." Applied soft computing 10.1 (2010): 1-35.
7. Peddabachigari, Sandhya, et al. "Modeling intrusion detection system using hybrid intelligent systems." Journal of network and computer applications 30.1 (2007): 114-132.
8. Kim, Jin, et al. "Method of intrusion detection using deep neural network." 2017 IEEE international conference on big data and smart computing (BigComp). IEEE, 2017.
9. Shamshirband, Shahaboddin, et al. "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique." Engineering Applications of Artificial Intelligence 26.9 (2013): 2105-2127.
10. Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. "Machine learning methods for cyber security intrusion detection: Datasets and comparative study." Computer Networks 188 (2021): 107840.
11. Sarker, Iqbal H., et al. "Intrudtree: a machine learning based cyber security intrusion detection model." Symmetry 12.5 (2020): 754.
12. Vinayakumar, Ravi, et al. "Deep learning approach for intelligent intrusion detection system." Ieee Access 7 (2019): 41525-41550.
13. Alhajjar, Elie, Paul Maxwell, and Nathaniel Bastian. "Adversarial machine learning in network intrusion detection systems." Expert Systems with Applications 186 (2021): 115782.

14. Sinclair, Chris, Lyn Pierce, and Sara Matzner. "An application of machine learning to network intrusion detection." Proceedings 15th annual computer security applications conference (ACSAC'99). IEEE, 1999.'
15. Taher, Kazi Abu, Billal Mohammed Yasin Jisan, and Md Mahbubur Rahman. "Network intrusion detection using supervised machine learning technique with feature selection." 2019 International conference on robotics, electrical and signal processing techniques (ICREST). IEEE, 2019.
16. Roy, Sanjiban Sekhar, et al. "A deep learning based artificial neural network approach for intrusion detection." Mathematics and Computing: Third International Conference, ICMC 2017, Haldia, India, January 17-21, 2017, Proceedings 3. Springer Singapore, 2017.
17. Li, Beibei, et al. "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems." IEEE Transactions on Industrial Informatics 17.8 (2020): 5615-5624.
18. Carneiro, José, et al. "Machine learning for network-based intrusion detection systems: an analysis of the CIDDS-001 dataset." International Symposium on Distributed Computing and Artificial Intelligence. Cham: Springer International Publishing, 2021.
19. Li, Jie, et al. "Machine learning algorithms for network intrusion detection." AI in Cybersecurity (2019): 151-179.
20. Patil, Shruti, et al. "Explainable artificial intelligence for intrusion detection system." Electronics 11.19 (2022): 3079.
21. Alqahtani, Hamed, et al. "Cyber intrusion detection using machine learning classification techniques." Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1. Springer Singapore, 2020.
22. Omer, Nadir, et al. "A novel optimized probabilistic neural network approach for intrusion detection and categorization." Alexandria Engineering Journal 72 (2023): 351-361.
23. Hnamte, Vanlalruata, and Jamal Hussain. "DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system." *Telematics and Informatics Reports* 10 (2023): 100053.
24. Jain, Jay Kumar, and Akhilesh A. Waoo. "An Artificial Neural Network Technique for Prediction of Cyber-Attack using Intrusion Detection System." *Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172* 3.02 (2023): 33-42.
25. AlHaddad, Ulaa, et al. "Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks." *Sensors* 23.17 (2023): 7464.
26. Al-Omari, M., Rawashdeh, M., Qutaishat, F., Alshira'H, M., & Ababneh, N. (2021). An intelligent tree-based intrusion detection model for cyber security. Journal of Network and Systems Management, 29, 1-18.
27. Alotaibi, A.; Rassam, M.A. Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defense. *Future Internet* 2023, *15*, 62. https://doi.org/10.3390/fi15020062
28. Belhadi, A., Djenouri, Y., Djenouri, D. et al. Group intrusion detection in the Internet of Things using a hybrid recurrent neural network. Cluster Comput 26, 1147–1158 (2023). https://doi.org/10.1007/s10586-022-03779
29. Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation. Symmetry, 15(3), 677.
30. Figueiredo, J.; Serrão, C.; de Almeida, A.M. Deep Learning Model Transposition for Network Intrusion Detection Systems. Electronics 2023, 12, 293. https://doi.org/10.3390/ electronics12020293
31. Jay Kumar Jain, & Waoo, A. A. . (2023). An Artificial Neural Network Technique for Prediction of Cyber-Attack using Intrusion Detection System. Journal of Artificial Intelligence,Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 3(02), 33–42. https://doi.org/10.55529/jaimlnn.32.33.4.
32. Maseer, Ziadoon Kamil, et al. "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset." IEEE access 9 (2021): 22351-22370.
33. P. F. de Araujo-Filho, M. Naili, G. Kaddoum, E. T. Fapi and Z. Zhu, "Unsupervised GAN-Based Intrusion Detection System Using Temporal Convolutional Networks and Self-Attention," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2023.3260039.
34. Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). Ai-based intrusion detection systems for in-vehicle networks: A survey. ACM Computing Surveys, 55(11), 1-40.
35. Talaei Khoei, T.; Kaabouch, N. A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems. Information 2023, 14, 103. https://doi.org/10.3390/info14020103.
36. Talukder, M. A., Hasan, K. F., Islam, M. M., Uddin, M. A., Akhter, A., Yousuf, M. A & Moni, M. A. (2023). A dependable hybrid machine learning model for network intrusion detection. Journal of Information Security and Applications, 72, 103405.
37. Vanlalruata Hnamte, Jamal Hussain,DCNNBiLSTM - An Efficient Hybrid Deep Learning-Based Intrusion Detection System, Telematics and Informatics Reports, Volume 10,2023,100053,ISSN 2772-5030,https://doi.org/10.1016/j.teler.2023.100053.
38. Yasakethu, S. L. P., and J. Jiang. "Intrusion detection via machine learning for SCADA system protection." 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1. 2013.
39. Sharma, Bhawana, et al. "Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach." Expert Systems with Applications 238 (2024): 121751.

40. Hernandez-Jaimes, Mireya Lucia, et al. "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures." Internet of Things (2023): 100887.
41. Jose, Jinsi, and Deepa V. Jose. "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset." International Journal of Electrical and Computer Engineering (IJECE) 13.1 (2023): 1134-1141.
42. Keshk, Marwa, et al. "An explainable deep learning-enabled intrusion detection framework in IoT networks." Information Sciences 639 (2023): 119000.
43. Rizzardi, Alessandra, Sabrina Sicari, and Alberto Coen Porisini. "Deep Reinforcement Learning for intrusion detection in Internet of Things: Best practices, lessons learnt, and open challenges." Computer Networks 236 (2023): 110016.
44. Jasim, Alaa Firas Jasim, and Sefer Kurnaz. "New automatic (IDS) in IoTs with artificial intelligence technique." Optik 273 (2023): 170417.
45. Soliman, Sahar, Wed Oudah, and Ahamed Aljuhani. "Deep learning-based intrusion detection approach for securing industrial Internet of Things." *Alexandria Engineering Journal* 81 (2023): 371-383.
46. Elsayed, Rania A., et al. "Securing IoT and SDN systems using deep-learning based automatic intrusion detection." Ain Shams Engineering Journal (2023)102211.
47. Guo, G., Pan, X., Liu, H., Li, F., Pei, L., & Hu, K. (2023, March). An IoT Intrusion Detection System Based on TON IoT Network Dataset. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0333-0338). IEEE.
48. Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. J. Sens. Actuator Netw. 2023, 12, 29. *https://doi.org/10.3390/jsan12020029* 48
49. https://www.uptycs.com/blog/intrusion-detection-in-cloud-computing
50. Patel, Ahmed, et al. "An intrusion detection and prevention system in cloud computing: A systematic review." *Journal of network and computer applications* 36.1 (2013): 25-41.
51. 51.Riaz, Amna, et al. "Intrusion detection systems in cloud computing: A contemporary review of techniques and solutions." *Journal of Information Science and Engineering* 33 (2017): 611-634.
52. Lo, Chi-Chun, Chun-Chieh Huang, and Joy Ku. "A cooperative intrusion detection system framework for cloud computing networks." *2010 39th International Conference on Parallel Processing Workshops*. IEEE, 2010.
53. Patel, Ahmed, et al. "Taxonomy and proposed architecture of intrusion detection and prevention systems for cloud computing." *Cyberspace Safety and Security: 4th International Symposium, CSS 2012, Melbourne, Australia, December 12-13, 2012. Proceedings 4*. Springer Berlin Heidelberg, 2012.
54. Hatef, Mohammad Amin, et al. "HIDCC: A hybrid intrusion detection approach in cloud computing." *Concurrency and Computation: Practice and Experience* 30.3 (2018): e4171.
55. Idhammad, Mohamed, Karim Afdel, and Mustapha Belouch. "Distributed intrusion detection system for cloud environments based on data mining techniques." *Procedia Computer Science* 127 (2018): 35-41.
56. Krishnan, Deepa, and Madhumita Chatterjee. "An adaptive distributed intrusion detection system for cloud computing framework." *Recent Trends in Computer Networks and Distributed Systems Security: International Conference, SNDS 2012, Trivandrum, India, October 11-12, 2012. Proceedings 1*. Springer Berlin Heidelberg, 2012.
57. Binbusayyis, Adel. "Hybrid VGG19 and 2D-CNN for intrusion detection in the FOG-cloud environment." *Expert Systems with Applications* 238 (2024): 121758.
58. Samunnisa, K., G. Sunil Vijaya Kumar, and K. Madhavi. "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods." *Measurement: Sensors* 25 (2023): 100612.
59. Kavitha, C., et al. "Filter-Based Ensemble Feature Selection and Deep Learning Model for Intrusion Detection in Cloud Computing." *Electronics* 12.3 (2023): 556.
60. Saleh, Hadeel M., Hend Marouane, and Ahmed Fakhfakh. "Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning." *IEEE Access* (2024).
61. Bukhari, Syed Muhammad Salman, et al. "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability." *Ad Hoc Networks* (2024): 103407.
62. Rajasoundaran, S., et al. "Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks." *Wireless Networks* 30.1 (2024): 209-231.
63. Srivastava, Atul, et al. "Network Intrusion Detection System (NIDS) for WSN using Particle Swarm Optimization based Artificial Neural Network." *International Journal of Intelligent Systems and Applications in Engineering* 12.15s (2024): 143-150.
64. Wu, Hongjiao. "Feature-Weighted Naive Bayesian Classifier for Wireless Network Intrusion Detection." *Security and Communication Networks* 2024 (2024).
65. Jeevaraj, Deepa, et al. "Intrusion detection in WSN using Supervised Machine Learning Techniques." *International Journal of Intelligent Systems and Applications in Engineering* 12.9s (2024): 483-490.

66. Sivagaminathan, V., Sharma, M. & Henge, S.K. Intrusion detection systems for wireless sensor networks using computational intelligence techniques. *Cybersecurity* 6, 27 (2023). https://doi.org/10.1186/s42400-023-00161-0
67. Sood, T., Prakash, S., Sharma, S. *et al.* Intrusion Detection System in Wireless Sensor Network Using Conditional Generative Adversarial Network. *Wireless Pers Commun* 126, 911–931 (2022). https://doi.org/10.1007/s11277-022-09776-x
68. Liu Zhiqiang, Ghulam Mohiuddin, Zheng Jiangbin, Muhammad Asim, Wang Sifei, Intrusion detection in wireless sensor network using enhanced empirical based component analysis, Future Generation Computer Systems,Volume 135,2022,Pages 181-193,ISSN 0167-739X, https://doi.org/10.1016/j.future.2022.04.024.
69. Ruirui Zhang, Xin Xiao, "Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division", *Journal of Sensors*, vol. 2019, Article ID 5451263, 20 pages, 2019. https://doi.org/10.1155/2019/5451263
70. Al-E'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S., & Hasbullah, I. (2022). Intrusion detection systems using blockchain technology: A review, issues and challenges. *Computer Systems Science and Engineering*, *40*(1), 87-112. https://doi.org/10.32604/CSSE.2022.017941
71. Khonde, S.R., Ulagamuthalvi, V. Hybrid intrusion detection system using blockchain framework. J Wireless Com Network 2022, 58 (2022). https://doi.org/10.1186/s13638-022-02089-4
72. Abubakar, Aliyu Ahmed, Jinshuo Liu, and Ezekia Gilliard. "An efficient blockchain-based approach to improve the accuracy of intrusion detection systems." Electronics Letters 59.18 (2023): e12888.
73. Hu, Bowen, et al. "A collaborative intrusion detection approach using blockchain for multimicrogrid systems." IEEE Transactions on Systems, Man, and Cybernetics: Systems 49.8 (2019): 1720-1730.
74. Saveetha, D., and G. Maragatham. "Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning." Pattern Recognition Letters 153 (2022): 24-28.
75. Aljabri, Ahmed, Farah Jemili, and Ouajdi Korbaa. "Intrusion detection in cyber-physical system using rsa blockchain technology." Multimedia Tools and Applications (2023): 1-22.
76. Liang, Wei, et al. "Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems." IEEE Internet of Things Journal 9.16 (2021): 14741-14751.
77. Kumar, Randhir, et al. "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network." *Journal of Parallel and Distributed Computing* 164 (2022): 55-68.
78. Li, Wenjuan, Jiao Tan, and Yu Wang. "A framework of blockchain-based collaborative intrusion detection in software defined networking." *Network and System Security: 14th International Conference, NSS 2020, Melbourne, VIC, Australia, November 25–27, 2020, Proceedings 14*. Springer International Publishing, 2020.
79. Tanmay Shetty, Saloni Negi, Anushka Kulshrestha, Shaifali Choudhary, Ramani S, Marimuthu Karuppiah, Chapter 5 - Blockchain for intrusion detection systems, In Hybrid Computational Intelligence for Pattern Analysis, Blockchain Technology for Emerging Applications, Academic Press, 2022, Pages 107-136, ISBN 9780323901932, https://doi.org/10.1016/B978-0-323-90193-2.00003-X.
80. Reka, R., et al. "Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET." *Computers & Security* 136 (2024): 103526.
81. Meddeb, Rahma, et al. "A deep learning-based intrusion detection approach for mobile Ad-hoc network." *Soft Computing* (2023): 1-15.
82. Prasad, Mahendra, Sachin Tripathi, and Keshav Dahal. "An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks." *Engineering Applications of Artificial Intelligence* 119 (2023): 105760.
83. Krishnasamy, Bala, et al. "DIWGAN optimized with Namib Beetle Optimization Algorithm for intrusion detection in mobile ad hoc networks." *IETE Journal of Research* (2023): 1-20.
84. Singh, C. Edwin, and S. Maria Celestin Vigila. "Fuzzy based intrusion detection system in MANET." *Measurement: Sensors* 26 (2023): 100578.
85. Prasad, Mahendra, Sachin Tripathi, and Keshav Dahal. "A probability estimation-based feature reduction and Bayesian rough set approach for intrusion detection in mobile ad-hoc network." *Applied Intelligence* 53.6 (2023): 7169-7185.
86. Sultan, Mohamad T., Hesham El Sayed, and Manzoor Ahmed Khan. "An Intrusion Detection Mechanism for MANETs Based on Deep Learning Artificial Neural Networks (ANNs)." *arXiv preprint arXiv:2303.08248* (2023).
87. Islabudeen, M., and M. K. Kavitha Devi. "A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks." *Wireless Personal Communications* 112 (2020): 193-224.
88. Sivanesh, S., and VR Sarma Dhulipala. "Accurate and cognitive intrusion detection system (ACIDS): a novel black hole detection mechanism in mobile ad hoc networks." *Mobile Networks and Applications* 26 (2021): 1696-1704.
89. Abdan, Masoud, and Seyed Amin Hosseini Seno. "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)." Wireless Communications and Mobile Computing 2022 (2022): 1-12.

90. Akram F, Liu D, Zhao P, Kryvinska N, Abbas S, Rizwan M. Trustworthy Intrusion Detection in E-Healthcare Systems. Front Public Health. 2021 Dec 3;9:788347. doi: 10.3389/fpubh.2021.788347. PMID: 34926397; PMCID: PMC8678532.
91. Iwendi, Celestine, et al. "Security of things intrusion detection system for smart healthcare." Electronics 10.12 (2021): 1375.
92. Hady, Anar A., et al. "Intrusion detection system for healthcare systems using medical and network data: A comparison study." IEEE Access 8 (2020): 106576-106584.
93. Thamilarasu, Geethapriya, Adedayo Odesile, and Andrew Hoang. "An intrusion detection system for internet of medical things." IEEE Access 8 (2020): 181560-181576.
94. Akshay Kumaar, M., et al. "A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning." Frontiers in Public Health 9 (2022): 824898.
95. Newaz, AKM Iqtidar, et al. "Heka: A novel intrusion detection system for attacks to personal medical devices." 2020 IEEE Conference on Communications and Network Security (CNS). IEEE, 2020.
96. Triawang, G., Kurniawan, E. The Effect of Digital Literacy Towards The Selection of Social Science Teacher Learning Media(2021) Pegem Egitim ve Ogretim Dergisi, 11 (4), pp. 316-319. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85117965727&doi=10.47750%2fpegegog.11.04.30&partnerID=40&md5=0b7bd042b8eeea05af42984f0a424423 DOI: 10.47750/pegegog.11.04.30
97. Uvarajan, K. P., and K. Usha. "Implement A System For Crop Selection And Yield Prediction Using Random Forest Algorithm." *International Journal of communication and computer Technologies* 12.1 (2024): 21-26.
98. Srinivasareddy, S., Y. V. Narayana, and D. Krishna. "Sector beam synthesis in linear antenna arrays using social group optimization algorithm." National Journal of Antennas and Propagation 3.2 (2021): 6-9.
99. Pakkiraiah, C., and R. V. S. Satyanarayana. "Design and FPGA Realization of Energy Efficient Reversible Full Adder for Digital Computing Applications." Journal of VLSI circuits and systems 6.1 (2024): 7-18.

Authors

R.Maruthi completed her MCA, M.Phil anPh.D from Mother Teresa Women's University, currently working as an associate Professor & HoD , in the Department of Computer Applications , Hindustan Institute of Technology and Science, Chennai, having 21 years of experience in teaching and research in various reputed institutes like Velammal Engineering College, SSN college of Engineering etc., published 40+ papers in International conferences and Journal

K.Shanthi received Master in Computer Application with first Class in 2010, Masters in Philosophy in 2017 and is currently pursuing PhD in PRIST University. She is working as Assistant Professor in the Department of Computer Science in Shri Krishnaswamy College, Chennai. She has published many papers at national /international Journals and Conferences in the areas of Cloud Security.She published three books and own a patent in IOT based cybersecutity