IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 October 2022, accepted 30 October 2022, date of publication 7 November 2022, date of current version 22 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3220622

SURVEY

Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey

P. L. S. JAYALAXMI[1,2], RAHUL SAHA[1,3], (Member, IEEE), GULSHAN KUMAR[1,3], (Senior Member, IEEE), MAURO CONTI[3], (Fellow, IEEE), AND TAI-HOON KIM[4], (Member, IEEE)

[1]School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab 144001, India
[2]Department of Computer Science, Bhavans Vivekananda College, Hyderabad 500094, India
[3]Department of Mathematics, University of Padua, 35122 Padua, Italy
[4]Glocal Campus, Konkuk University, Chungju-si 27478, Chungcheongbuk-do, South Korea

Corresponding authors: Tai-Hoon Kim (taihoonn@daum.net) and Rahul Saha (rsahaaot@gmail.com)

This work was supported by the European Union's Horizon 2020 Research and Innovation Program for the Project COmprehensive cyber-intelligence framework for resilient coLLABorative manufacturing Systems (COLLABS) under Agreement 871518.

ABSTRACT The increasing number of connected devices in the era of Internet of Thing (IoT) has also increased the number intrusions. Intrusion Detection System (IDS) is a secondary intelligent system to monitor, detect, and alert about malicious activities; an Intrusion Prevention System (IPS) is an extension of a detection system that triggers relevant action when an attack is suspected in a futuristic aspect. Both IDS and IPS systems are significant and useful for developing a security model. Several studies exist to review the detection and prevention models; however, the coherence in the opportunistic or advancements in the models is missing. Besides, the existing models also have some limitations, which need to be surveyed to develop new security models. Our survey is the first one to present a study of risk factor analysis using mapping technique, and provide a proposal for hybrid framework for an efficient security model for intrusion detection and/or prevention. We explore the importance of various Artificial Intelligence (AI)-based techniques, tools, and methods used for the detection and/or prevention systems in IoTs. More specifically, we emphasize on Machine Learning (ML) and Deep Learning (DL) techniques for intrusion detection-prevention systems and provide a comparative analysis focusing on the feasibility, compatibility, challenges, and real-time issues. This present survey is beneficial for industry and academia to categorize the challenges and issues in the current security models and generate the new dimensions of developments of security frameworks with efficient ML or DL methods.

INDEX TERMS Intrusion detection, intrusion prevention, internet of thing, machine learning, deep learning. artificial intelligence.

I. INTRODUCTION

The past decades have seen a revolution in computing with advanced technologies and smart device communication. Internet of Thing (IoT) establishes internal communication using sensor devices. It is the most preferred technology for all day-to-day activities in this era [1]. IoT devices transfer huge data over a network with minimum human interaction using internet as a central communication medium. The impact of global connectivity and the exchange of data created major significance on education, business, health care system, military capabilities, international trade, agriculture, and home applications. Massive connectivity with heterogeneous devices, unsafe network architecture, exposure of global data, raise critical security issues in IoTs [1]. Cyber security is the major concern in this digital world to ensure protection from malicious activities, which aim to corrupt or steal data and interrupt an organization's systems with

The associate editor coordinating the review of this manuscript and approving it for publication was Sotirios Goudos.

unauthorized access. At the same time, IoT have become a major channel for the spread of dangerous malware attacks. Unpatched and less secured devices are the targets for botnet operators to capture the system and get control over the devices. Strong security services to control the access mechanism with a perfect authenticated framework is essential. An Intrusion Detection System (IDS) is a suitable solution to handle security issues and mitigate the effects of the attacks. IDS becomes an essential part of security management in the network and host systems. IDS detects intrusions or misuse of network or system by reporting to the administrators and filing a record for further investigations. It handles the suspicious events without interrupting the regular activities during the malicious outbreak [2]. Many tools and techniques are available to counter the threat of these attacks. Requirement of strong firewall protection is essential, as the existing firewall can not classify the behavior or anomaly attack. Antivirus software has less scope in recognizing the new patterns of the virus. Intrusion detection triggers an alert after an attack enters the network by doing nothing to stop the attack. Currently available IDS have several limitations such as lack of flexibility and scalability [2].

Intrusion Prevention System (IPS) is a proactive method to prevent a security attack by examining the patterns of data (network traffic) and recognizing the abnormal behavior from stored data records (signature). IPS blocks the offending data when the attack is detected [3]. We consider an IDS as the second line of the defense system; however, it faces difficulties in providing secure access control [10]. On the other hand, IPS integrated with firewall and IDS can provide preventive measures with alerts for attacks in a preserved network area. Artificial Intelligence (AI) technologies like Machine Learning (ML), Natural Language Processing (NLP), Neural Networks (NN) can provide rapid insights by identifying and mitigating the effects of the attack with daily alerts using a smart Intrusion Detection and Prevention System (IDPS) [11].

Figure 1 presents the architecture of an IDPS for IoT network. The functionality of an IDS and an IPS are almost similar; an added capability of IPS is the perimeter defense appliance, gateway monitoring, network packet inspection, and blocking the suspicious activity by comparing with known patterns. Both the systems are designed to recognize potential security violations in the network system [3]. However, basic detection system uses two principles: behavior analysis or pattern recognizing and then a prevention system uses a signature mechanism to monitor the suspicious network traffic by blocking the inbound and outbound packets before they access other resources. IPS is an integrated component that combines technical firewall protection with multi-layer support and detection functionality [4].

A. CONTRIBUTION

Our present survey focuses on Machine Learning (ML) and Deep Learning (DL) approaches for IDPS. Our main contributions are as follows.

- **Comprehensive taxonomy**: Our study provides a detailed taxonomy of intrusion detection and prevention system in IoT using machine learning and deep learning techniques with systematic review literature.
- **Performance analysis** : We provide the performance analysis of the latest IDPS models based on ML and DL techniques with accuracy and notify the limitations.
- **Prevention techniques**: Our study explores various prevention techniques, mitigation strategies, and the methods implemented for IPS in IoT.
- **Risk analysis**: We propose a risk factor analyser to identify the level of risk and take an action to implement a counter measure and mitigate effects by improving the security control in the manufacturing unit.
- **Hybrid framework**: We propose a hybrid framework to avoid the disadvantages raised by anomaly and signature based techniques and apply the risk factor based on the complication levels.

B. ORGANIZATION OF THE PAPER

We organize the rest of the paper in the following sections. Section II highlights the importance of security in IoT application with a focus on issues, attacks, vulnerabilities caused and the relevant measures. Section III discusses the detailed taxonomy of the detection systems with their pros and cons in the real time applications. Section IV reviews various detection techniques developed using machine learning techniques in the recent years highlighting their features, techniques, and performance. Section V shows some recent IPS models based on ML techniques. Section VI explores various detection models developed using deep learning techniques proposed for IoTs; it focuses on various supervised and unsupervised techniques and discusses the issues extending to future scope. In Section VII, we conduct a systematic literature review on prevention models. Further, we explore the detailed analysis on various prevention techniques developed using ML and DL methods. Section VIII provides a risk factor analyser, using mapping technique, and a hybrid IDPS framework. Section IX provides a comparative study on the available techniques, and existing surveys in the direction of IDS. Finally, we draw the logical conclusion in Section X.

II. IoT- SECURITY

With the increasing number of devices and sophistication of attack tools: hacking and security breaches have grown unlimited. Burgeoning technologies like the public cloud, IoT, artificial intelligence, paralyzed the standard security measures [5]. IoT establishes a connection of anything, anyone, at any place, and provides smart services with a secured network platform. IoT applications are extended to a wide range, which includes smart health monitoring, traffic congestion, smart cities, waste management, logistic and emergency services, smart industrial, and retail controls.

IoT establishes a heterogeneous pervasive network of smart devices. Some of the complex IoT devices relate to a hostile interface, developed on uncontrolled platforms,

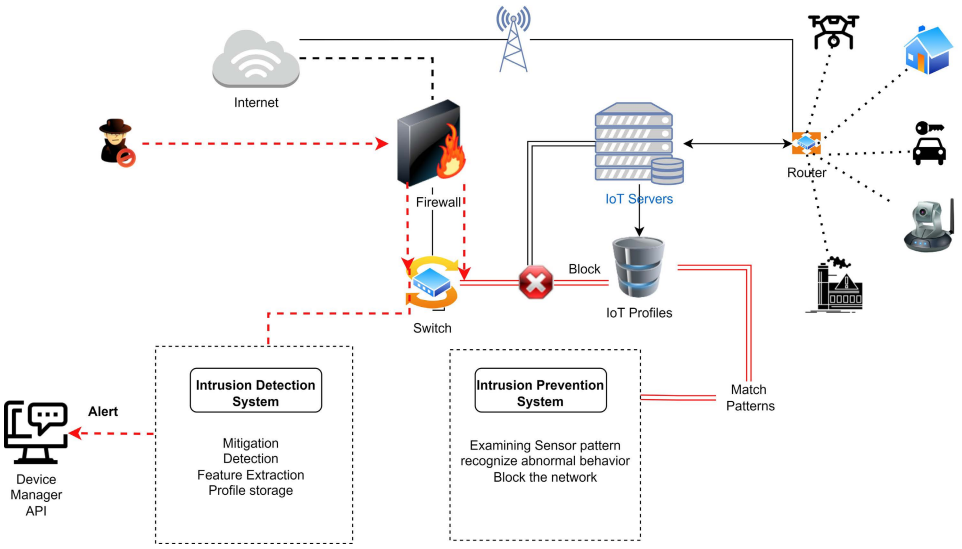

FIGURE 1. IDPS architecture.

TABLE 1. Various IoT attack and the counter measures.

Reference	IoT Device	Attack type	Device vulnerabilities	Measures
[10]	Smart Vehicle	Device software failure	Buffer overflows	Address space layout randomization (ASLR) and Stack Guard,Dynamic verification techniques.
[11]	Smart industrial devices	Node tampering attack	Hardware replacement	Tamper-resilient Cryptography techniques,Elliptic Curve Integrated Encryption Scheme (ECIES).
[12]	Smartphones and measuring devices	Eaves dropping attack	Un-encrypted communication channels	Lightweight cryptography encryption techniques,Attribute-Based Encryption,A Proxy Re-Encryption.
[13]	Smart thermostat, Smart bulb	Malicious code injection	Unsecured APIs and lack of constant integrity checks	API endpoint security,Dele-setting and configuration.
[14]	Smart car, Smart TV	Unauthorized access	Device and application vulnerabilities	Regular updates and secure key generation.
[15]	Smart health care,Smart Speakers, Garage door opener,	Social engineering attack	Weak password protection	Multi factor authentication, Collision-resistant one-way hash function.
[16]	Drone, IoT Gas pump	Device hardware exploitation	Open un-secure hardware interface	Access restrictions.
[17]	IP camera, Smart home devices	Malicious node insertion	weak encryption schemes	Symmetric key encryption, sign-cryption.

and encounter vulnerabilities to individual systems available in the integrated network [6]. Lack of interoperability and accessibility in the vast heterogeneous landscape results in poor monitoring of the security mechanism in IoT networks. We list various IoT attacks and countermeasures in Table 1; and also mention the device vulnerabilities and suggested measures for each. Scalable solutions minimize the use of resources and improve the performance to take effective decisions which mitigate anomalies in the system [7]. A strong security system is required to ensure system protection from unexpected threats, maintain confidentiality, stabilize the network connection, control network traffic, and avoid vulnerable attacks. Three major security problems of IoT as: taking control, stealing information, and disturbing services, create dangerous issues and data-threat for IoT users.

IoT connects the devices with the Internet backbone; many interactive and efficient applications use this to enhance the network services [8]. Huge private and confidential data of multiple categories are collected with these devices based on application and implementation. Ensuring high-level security for the data sent by IoT devices during transit and rest is the preliminary intention of a security control system in an IoT. Wurm et al. [8] highlights the security vulnerabilities associated with industrial and consumer IoT devices. The highest security risk is anticipated to the perception layer because of its hostile and open environment than the other network layers [9]. In the next section, we describe the security risk targeting the IoT devices and suggest some potential mitigation measures, which can help the manufacturers in strengthening the security design in future. The risk analysis also exists to mitigate the actions performed by the intruders and create a secured network framework [10]. Common steps for creating a risk analysis model are: attack and risk identification, prioritizing the categories, selection of suitable mitigation strategies, and adapting a mitigation solution based on the problem [10]. We mention some of the problem-solving solutions to avoid the intrusion activities below.

- Meticulous quality testing.
- Adaption of physical unclonable functions.
- Lightweight compatible encryption techniques.
- Regular integrity check retaining the performance.
- Critical software updates.
- Strong password protection.
- Updated standard interface.

III. IDS FOR IoTs

The open network architecture, heterogeneous device structure, and the drastic use of smart connected devices, in our daily life are leading to serious security and privacy issues [11]. The destruction of water utility pumps in industrial IoT, personal data theft [12], generating false messages as the legitimate users [13], unauthorized control over power stations, smart cars, smart restaurants, and manipulation of private information to block regular services are some of the examples of dangerous threats created in the IoT environment in the recent past [14]. Therefore, a comprehensive and distinct security mechanism is very much required to protect the digital world and secure it from serious security threats [15]. Several research proposals are available in different dimensions for securing the IoT devices, some of them include secured frameworks, privacy protection models, and authentication techniques [14], [15], [16]. However, to address these challenges and ensure effectiveness and applicability two major factors can be considered [17]. First, to identify and authenticate the devices and limit the controls for external access for sophisticated security management with real-time monitoring. Second, to coordinate the open network connectivity and ensure the security in a collaborative network [15].

A. IDS TAXONOMY

IDS is an intelligent security system for coordinating host and network activities. This analyzes the packets transferred through the network, finds suspicious events, and processes with the alert notification.

Figure 2 displays IDS classifications for two major categories: network-based and host-based detection systems. IPS also have similar classifications as network and host based prevention using Network Behaviour Analysis (NBA) and monitors the abnormal activities using Wireless Intrusion Prevention System (WIPS). The taxonomy focuses on IDS and IPS techniques used to detect the malware as an anomaly and signature-based detection methods. Figure 2 projects various machine learning and deep learning techniques suitable for each IDS category to obtain an idea of the models developed in recent times.

IDS have gained immense attention with multiple notable models proposed for creating an intense security structure [16], [17], [18] due to ever-increasing zero-day patterns of network traffic and their heterogeneity. In this context, our study investigates the novel challenges to explore potential solutions to address the issues in the detection models. In specific, we emphasize the challenges of the available detection systems concerning performance, bandwidth utilization, time taken for detection, overload of processors, etc. The study also focuses on the accuracy, false positive, and negative rates of the proposed models by highlighting the future directions.

Implementation of IDS for real-time devices is limited to the applications used, data transfer, and area of the network [19]. IDS has numerous advantages, compared to traditional firewall protection but, has a critical downfall in reducing false rates. At the same time, not all IDS procedures are similar, each category has its unique qualities in tracking and defending against policy breaching [19]. Machine learning and deep learning techniques are projected under supervised and unsupervised learning models. These techniques are mostly used for fraud detection, risk assessment, image classification, and spam filtering [38], [39], [40].

B. NETWORK BASED INTRUSION DETECTION SYSTEM (NIDS)

Generally, a NIDS is placed near a firewall with an independent sensor device specially to monitor local network traffic. This identifies the malicious events from incoming packets as denial of attacks on services and scanned ports on the network. This system resides in the network ports and works with a firewall for better protection against known attacks [20]. NIDS is defined in two forms: network-node-based NIDS and promiscuous-mode-based NIDS. Analyzing packets bounded by a single destination is the quality of node-based NIDS with distributed agents. On the other side, sniffing all the packets across the network traffic and analyzing for the suspicious attempt with a single sensor on each segment is the property of promiscuous-mode-based NIDS [20]. NIDS is set up at a selected point as a sub-net within the network to examine and match the passing traffic. Then it analyzes the pacts and raises an alert if violated [21]. These sensors activate the interfaces for managing, controlling, and receiving alerts and then forward the same to the central server. NIDS applications are attached to the network with two interfaces, one monitors the network conversation, and the other control and generate a report of the activity [21]. Table 2.

C. HOST-BASED INTRUSION DETECTION SYSTEM (HIDS)

HIDS is an intelligent detection system that acts as an agent to inspect and report suspicious activities attempted on a host device. Continuous observation of the dynamic behavior, state of the system, storage area, internal configuration, network packets targeted, program executed, and resource accessed are the primary function of HIDS [22]. Apart from this analyzing log files available on the host (kernel, system, server, and network) and monitors file access and configuration changes in run-time, and finally compares with previous attacks stored in the server the activities carried out by this system. IDS models developed for host-based detection are listed in Table 2.

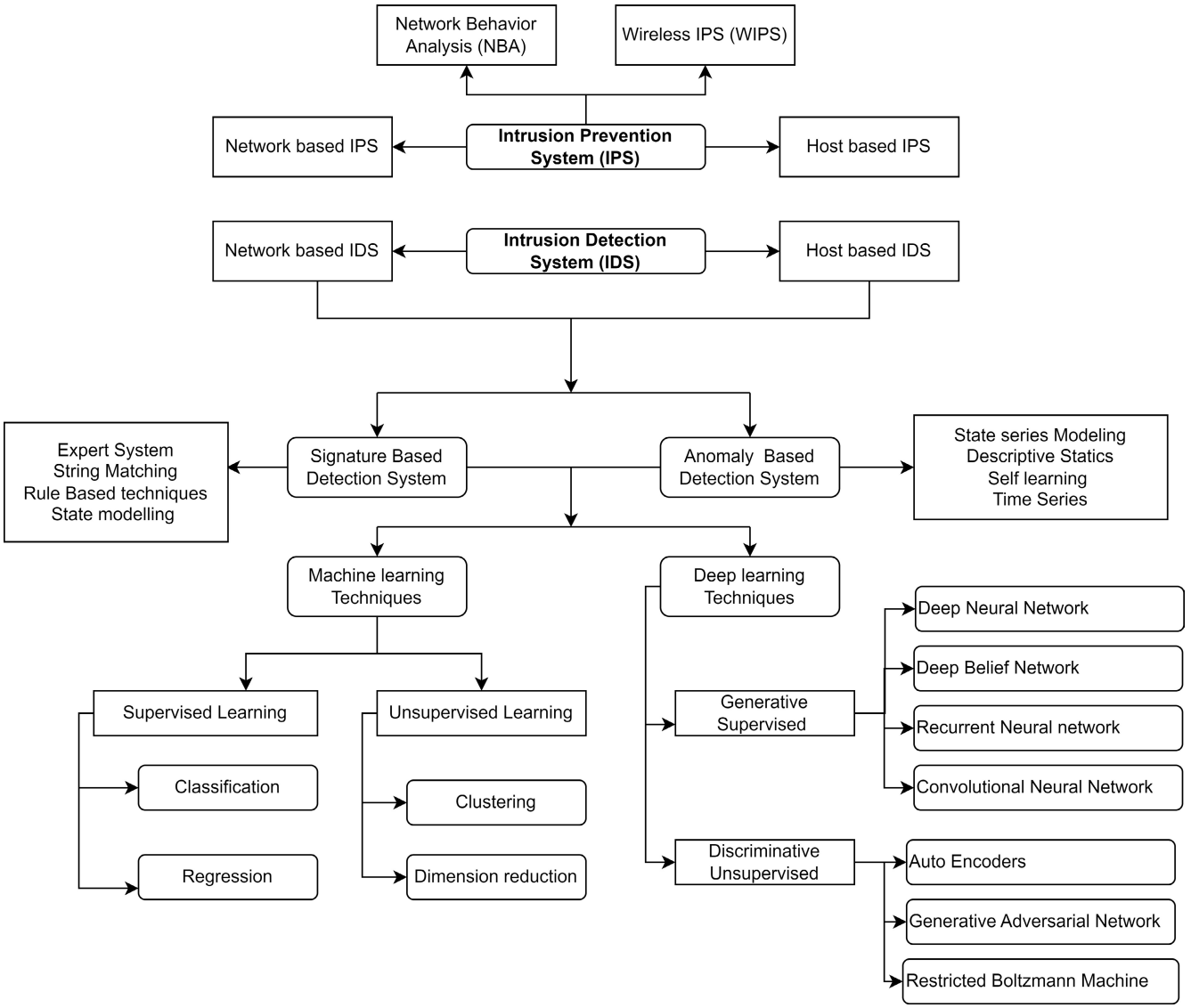

FIGURE 2. IDS classifications.

TABLE 2. NIDS and HIDS models for IoT.

References	IDS type	Features	Issues
A. Aris et al. [23].	Distributed - Hybrid IDS	Integrated with Distributed mini-firewall	DoS attacks can affect SVELTE
Kasinathan et al. [24]	Centralized- Signature based IDS	Deployed for real-world applications	Fails in Zero day attack detection.
Jun and Chi [25]	Centralized- signature based IDS	Low memory consumption	Limited to rule based detection
Cervantes et al. [26]	Distributed- Hybrid IDS	Self-repair technique	High resource complications
Surendar et al. [27]	Distributed- specification based IDS	Instant response,low drop outs, less energy consumption	Low performance in detecting unknown attacks
Fu et al. [28]	Distributed- Hybrid IDS	Suitable for heterogeneity and resource constraint environment	Causes state space explosion, less automatic.
Midi et al. [29]	Centralized and Distributed - Hybrid IDS	Lightweight, self adapting nature, multiple IoT device compatibility	Not suitable for constrained objects.
Bacem Mbarek et al. [21]	Distributed-Signature IDS	Good in testing clone attacks	Lack of real-time testing
V. Subbarayalu et al. [30]	Distributed-Hybrid IDS	Web server with integrated device access and resource restriction services	Constrained application protocols
Abhishek Verma et al. [31]	Distributed Ensemble learning based IDS	Heterogeneous ensemble with random forest of Hoeffding Trees	High time consumption.

D. SIGNATURE INTRUSION DETECTION SYSTEM (SIDS)

Signature-based detection technique looks for evidence known to be indicative based on defined patterns [32], [33]. Searching for a specific payload in a data packet, matching with the existing patterns generated by the NIDS/HIDS, and registering it as a signature of misuse is the procedure of the SIDS technique. The major limitation of this method is ignoring the newly launched attacks because of missing

TABLE 3. Opportunities and obstacles of various IDS techniques.

Detection technique	Opportunities	Obstacles
Signature based [32], [33]	• Simple to capture known intrusions. • Specifies detailed contextual analysis. • Instant protection with frequent solutions.	• Poor in detecting unknown variants • Lack of regular updates • Hard to understand the protocols and time consuming technique.
Anomaly Based [34] [35] [36]	• Good in detecting zero day and unknown attacks • Low dependency on resources	• Poor accuracy due to changes in observations. • Rate of alarm is poor and pause in service during construction of behaviour profile.
Hybrid [23] [26] [28] [30]	• More flexible based on requirement. • Adaptability of integrated mechanism.	• Overhead of power consumption. • Not suitable for memory constraints devices.

signatures. Intruders can easily deceive this method as the signatures are based on regular expressions. It uses matching string content that suits only fixed behavioral patterns.

E. ANOMALY INTRUSION DETECTION SYSTEM(AIDS)

Anomaly detection is based on the observation and deviation of behavior or activity from the normal baseline [34]. An anomaly detection system in NIDS detects the intrusion at the physical network after passing the firewall, and in HIDS it is the last layer of the protection that exists in the endpoint that allow fine-tuned protection at the application level [35]. Anomaly-based IDS has a major fall in results in false-positive rates. The detection system engine with multiple protocols must understand the process [36]. Though the protocol analysis is expensive, it has benefits of rectifying the false-positive alarms rates. The research community is working to integrate many advanced techniques such as statistical, cognition-based, machine learning, deep Learning, and data mining-based methods to develop better detection models [37]. Anomaly and signature-based detection are considered as the two primary techniques for developing detection and prevention models. We explain the opportunities and challenges faced by each category in Table 3.

IV. MACHINE LEARNING TECHNIQUES SUITABLE FOR INTRUSION DETECTION

The main aim of ML is to allow computers to learn automatically without human intervention or assistance and control actions accordingly. Machine learning is used for large-scale data processing and well suited for complex datasets with huge numbers of variables and features. The process of ML begins by accepting training data and making observations on data with direct experience, or by instruction and results with output values. Algorithm selection should be appropriate to gaze at the data patterns, improve the analytic, predictive power, and make better decisions in the future training data. Machine learning techniques are majorly categorized as supervised learning, unsupervised learning, and reinforcement learning.

Training with fully class labeled data, and establishing the relation between the input and target units are the properties of supervised algorithms. Classification and regression are the two major categories of supervised learning. Some of the popular classification algorithms are Support Vector Machine (SVM) [38], Naïve Bayes [39], Nearest Neighbour [49], Neural Network [44], Discriminant Analysis, and Logistic Regression [40]. Algorithms under the regression category most prominently usable for intrusion detection analysis includes Linear Regression, Support Vector Regression (SVR), Ensemble methods, Decision Tree (DT) [50], and Random Forest [51]. Unsupervised learning techniques find the hidden structure in the unlabelled data without training. Reduction and clustering are the two major techniques used to make relevant groups for comparison and compression with unique identification. Some of the popular clustering algorithms are K-Means, C-Means. Singular Value Decomposition (SVD) and Principle Component Analysis (PCA) are the popular feature reduction techniques.

We list the properties, advantages, and issues of machine learning approaches in IDS with in Table 4. This emphasizes the need and importance of each technique in detection process. The table provides a view of the trend for machine learning approaches to help future IDS developers to choose the appropriate technique.

V. REVIEW ON ML-BASED IDS MODELS FOR IoT

The most popular machine learning algorithms which achieve good results in detecting the specious activities of IDS are decision trees, random forest, SVM, and neural networks. The accuracy of the models and the efficiency of the algorithms depend on the application and the type of attack detected. Some of the proposed models have high performance only for the binary class detection and some are good in identifying multi-class attacks [37]. Many researchers focus only on the overall detection accuracy but, the detection effect for small-scale data is often very low. Considering the imbalance between the research done and the real-time applications, we have presented some of the popular machine learning models for IDS. Many of the traditional techniques are experimented on some popular intrusion datasets as KDD99, NSLKDD, UNSWNB-15 CSIDS. The single view model results in incomplete pattern identification, especially for large datasets. As the multiview learning models are having high popularity for detection techniques, Dinesh chowdary et al. [43] proposes Multi-View Federated-based Learning for Intrusion Detection (MV-FLID). This can learn from different data views and delivers the most distinguished prediction. Federated learning benefits peer learning and protection for profile aggregation. The authors in [45] propose seven

TABLE 4. Machine learning techniques used for IDS.

Approaches	Properties of the Method	Advantage	Issues
Signature (knowledge-based Detection) [24] [21]	• Processing with defined signatures. • Pattern matching technique.	• Low False positive rate with fast and accurate detection. • Effective in detecting known patterns, Flexible, and Robust. • Suitable for all network levels Source.	• Difficulty in analysing information/state. • New attacks are ignored. • Complex in updation.
Anomaly-based Detection [23] [36]	• Create a default profile for identifying the normal state. • Deviation from baseline detected as an anomaly. • Profile updates based on new behavior and critical events.	• Identification based on labels and behavior (normal/abnormal). • Specialized in identifying Zero-day attacks. • Multiple profile management difficult for the hacker hide identification.	• More time consuming for training phase. • Alteration of the threshold is difficult for managing false rates. • Low efficiency and high computational cost.
Hybrid Detection [26], [28]	• Combined detection process. • Both Predefined pattern behavior Detection.	• Suitable for both Supervised and unsupervised methods. • Integration of methods for best performance.	• Integrated product of Anomaly and signature detection system with added advantages. • The implementation cost is very high comparatively.
Probabilistic packs marking-based attack source detection [38]	• Encodes information into a packet header. • Identification field are used to mark and reconstruct attack path.	• Manage with the regular traffic for communication. • Reconstruction of attack path without ISP influence.	• High false-positive rates. • Requirement of large number of packets.
Deterministic Packet Marking based attack Source detection [39]	• Marks packets which are near to the source of the attack. • 16-bit identification field are used.	• Reduces storage and computational overhead. • flexible for small packet.	• High false-positive rates. • Trace only nearby source, identification of origin is delayed.
Support Vector Machine [38]	• Hyper plane setup for traffic area, suitable for classification and regression. • Effective in parameter identification, implemented for discreet valued kernels.	• High accurate. • Handle complex nonlinear decision boundaries. • Less over fitting problems.	• Complex in implementation and extensive memory requirement . • Choice of Kernel is difficult. • Slow in training and testing.
K-Nearest Neighbour [39]	• Classification and decision based on behavior patterns /classes. • Multiple parameters and transformation with K nearest value.	• Analytically tractable, Simple in implementation. • Use local information and yield highly adaptive behavior. • Suitable for parallel processing.	• Huge storage space requirement . • Highly susceptible to the curse of dimensions. • Slow in the classification of test tuples.
Bayesian Method [47], [49]	• Follow Joint probabilities rules. • Eliminate condition with relative frequencies form training sets.	• Simplifies the computations. • High speed and accurate for large database.	• Decision based on assumptions. • Lack of available probability data(less updated).
Decision Tree [48], [51]	• Based on binary classification nodes corresponds to Variable/attributes. • Branches for positive and negative instance.	• Construction does not require any domain knowledge. • Capable of handling high dimensional data. • Suitable for numerical and categorical data.	• Output attribute must be categorical. • Unstable result patterns. • Complex as created with numerical datasets.
Artificial Neural Network models [49]	• An adaptive system with changing structure based on information flow in the network. • Depended on training element find the distance of comparison.	• Require less formal statistical training. • Detect complex nonlinear relationships between variables. • High tolerance to noisy data, with multiple training algorithms.	• Black box nature (based on specifications). • Greater computational burden. • Requires long training time.

pre-processing techniques based on traffic for ML algorithm, evaluated based on scalar and normalization functions. They apply the models on four features under the category of content, statistical properties, basic and traffic connectivity.

The results of the study proves that application of categorical study enhances the performance to 45% comparatively. This help in proper classification based on the parameters related to possible attacks. Dhanke JyotiAtul et al. [47] proposes Energy Aware Smart Home (EASH) framework tested on real-time sensor data for selected IoT devices. The study is experimented with J48, Naive Bayes, Multi-Layer Perceptron (MLP), multi-nominal logistic regression for classification and detection on anomalies. Amongst all the techniques MLP has high accuracy with the capability of self learning and recognizing minute factors. We discuss some of the popular models developed in the recent years for mitigating the issues of intrusion for IoT environment in Table 5.

All the above-mentioned techniques are evaluated under two scenarios; first, under the assumption that both the training and testing data are of the same source and second, the testing samples are new and unknown patterns. This type of process helps us to understand the patterns of IDS in handling new malicious patterns. Testing on unknown patterns is very essential for new IDS models and helps in tracing the intruders who escape from the security control. The results in Table 5 show that the supervised ML techniques have better accuracy than the unsupervised models in some cases. Among these algorithms, decision tree and random forest have achieved the best results with 99% accuracy and low false rates. If there are unseen attacks in the test data, then the detection rate of supervised models decreases, as the patterns are not registered while training the data. This is where the unsupervised models have a better hold in performance as they do not show a significant difference in accuracy for known and unknown patterns.

According to the results mentioned in Table 5 random forest and K-Nearest Neighbour models (KNN) show high accuracy compared to the other classification techniques [42], [49]. Many of the integrated models with federated learning and/or self-learning methods show competitive performance than the traditional methods [43], [47]. Multi-layer framework [52], [55] with different levels of testing has more impact, where the data is filtered for multiple times and the identification becomes much stronger with clustering techniques [52], [54]. Experimenting on multiple models for better performance, and trace the most suitable model is the recent research trend. Following this concept, Verma et al. [38] experiments with six machine learning techniques as AdaBoost, random forests, gradient boosted machine, extremely randomized trees, classification, regression trees, and multi-layer perceptron for intrusion detection. All these models are tested on CIDDS-001, UNSW-NB15, and NSL-KDD datasets and the results prove that supervised techniques achieve better performance. Jinxin Liu [39] have examined eleven machine learning techniques includes Decision Tree, Matthews correlation coefficient (MCC), XGBoost, Bagging Tree, Random Forest, Bayes Net, Support Vector Machine, Naïve Bayes, AdaBoost, Expectation-Maximization, DBSCAN, K-Means. They focus on seven attack categories as SynFlood, Land, UDP Flood, Ping of Death, Smurf, IP sweeping, and Port Scan. The XGBoost model results in high performance with 0.970 accuracy and 0.968 recall. Secondly Bagging and SVM methods perform better as compared to RF and DT. The NB classification has the least results with 0.452 accuracy among all the proposed eleven techniques.

VI. DEEP LEARNING BASED INTRUSION DETECTION SYSTEM

Focusing on security applications, deep learning techniques with remarkable quality of self learning are beneficial to develop the intrusion detection models. This models result in low false rates and high accuracy as compared to traditional machine learning techniques. The standard Neural Network (NN) architecture is created with multi-layer perceptron developed using a liner stack classifier. We show a simple NN designed with input, hidden and output layers in Figure 3

Raw data in the form of numbers/images/audio are fed into the neurons as input represented with $x_1, x_2, x_3, \ldots, x_n$. Each input is multiplied by weights $(w_1, w_2, w_3, \ldots, w_n)$ and passed to an activation function. An activation function is a step function that maps the input signals into an output signal which is needed for the function of the neural network. A fully connected network model with more than three hidden layers is considered a Deep Neural Network (DNN). The feed-forward algorithm begins with the input layer move forward by updating the state of each unit by multiplying the weights and add the bias, finally terminates at the output layer when all units are updated.

$$z = f(b + \sum_{i=1}^{N} x_i w_i). \tag{1}$$

In Equation 1, x represents the inputs, w represents weights to be added for each input, z is used for output, b represents bias, and f represents the activation function. The model adjusts the weights and repeats the task to improve the accuracy using back propagation.

Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) are the most popular methods used for detecting malware activities with self-learning techniques. Natural Language Processing (NLP) is strong in identifying spam and social engineering attacks with new forms of communication and language patterns. Artificial Neural Networks (ANN) are emphatic in monitoring network traffic and detect Imminent attacks. ANN, DNN, and CNN are some of the supervised instance learning with a feed-forward neural network. RNN and Long Short-Term Memory (LSTM) are under the category of supervised sequence learning method. Restricted Boltzmann Machine (RBM) and Deep Belief Network (DBN) follow semi-supervised instance learning. DL also supports transfer learning methods used to generate generic problem statements and reuse them with other models. CNN and RNN are the most popular techniques used for conditional /discriminate models whereas AE, DBN, RBM,

TABLE 5. Review on latest IDS models using machine learning in IoT from 2020.

Author and Reference	Technique	Data-set	Results
Verma et al. [38]	Six ML techniques	CIDDS-001, UNSW-NB15, and NSL-KDD	Random Forest(RF) with 94.4% accuracy
Jinxin Liu et al. [39]	Eleven ML techniques	NSL-KDD	XGBoost with 99.6% accuracy
Amouri A et al. [40]	Data collection using dedicated sniffers and linear regression process for classification	Real-time dataset	98% power node velocity
Smys et al. [41]	Hybrid convolutional neural network	UNSW NB15	Hybrid CNN with 98% accuracy
Pascal Maniriho et al. [42]	Anomaly detection using Random Forest algorithm	IoT-ID20	99.95% overall accuracy
Dinesh Chowdary Attota et al. [43]	Multi-View Federated Learning-based ID (MV-FLID)	MQTT protocol dataset	94.17% accuracy
Md Arafatur Rahman et al. [44]	Centralized IDS with deep feature abstraction and Artificial Neural Network(ANN)	Aegean Wi-Fi Intrusion Dataset	99.95% accuracy
Larriva-Novo et al. [45]	Preprocessing with content characterization multi-layer perceptron for detection	UGR16, UNSW-NB15, KDD99	KDD99 with 95.5% accuracy
Sikha Bagui et al. [46]	Logistic Regression, Support-Vector Machine and Random Forest for BoT attack detection.	UCI's machine learning repository	Random forest with 99.0% accuracy
Dhanke JyotiAtul et al. [47]	NB, MLP, Multi nominal logistic regression	Real-time sensor data	MLP with 92.66% accuracy
Muhammad Ahmad et al. [48]	Random Forest (RF), Support Vector Machine and Artificial Neural Networks	UNSW-NB15	RF with 98.67% accuracy
Andrew Churcher et al. [49]	K-Nearest Neighbour (KNN), Support Vector Machine, Decision Tree , Naive Bayes, Random Forest (RF), Artificial Neural Network (ANN), and logistic regression	Bot-IoT dataset	RF and KNN with 99.0% accuracy
Iqbal H. et al. [50]	Intrusion Detection Tree ("IntruDTree")	Cyber-security datasets	98.0% accuracy
Hamed Alqahtani et al. [51]	Random Forest (RF)	KDD99	94.00% accuracy
Mohammad Noor Injadat et al. [52]	Multi-stage optimized ML-based NIDS framework	CICIDS 2017 and the UNSW-NB 2015	99.00% accuracy
Md ArafaturRahman et al. [53]	Decentralized(semi-distributed) and distributed paradigms	AWID dataset	99.97% accuracy
Martin Sarnovsky et al. [54]	Multi stage a hierarchical, Ensemble model IDS	KDD99	97.6% accuracy
Maonan Wang et al. [55]	SHapley Additive exPlanations (SHAP)	NSL-KDD	83.0% accuracy

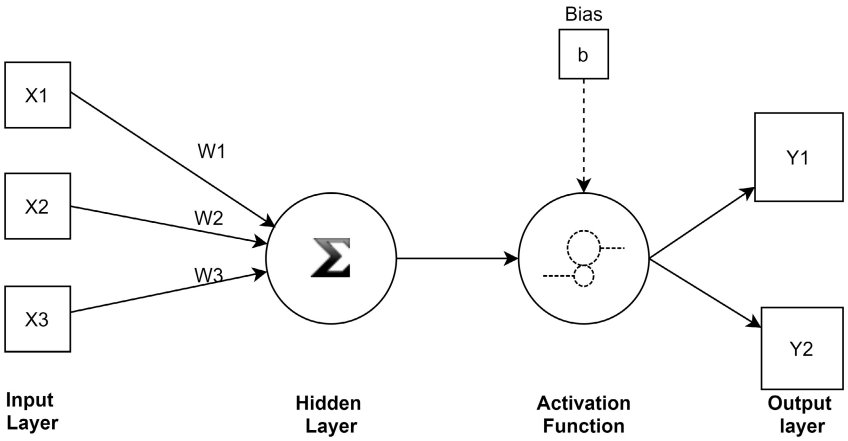

FIGURE 3. Structure of perceptron.

GAN are generative DL techniques, and the combination of both is considered as an ensemble technique. We discuss some of the DL techniques, their importance for IDS, and the issues in Table 6.

Yazan et al. [56] propose a Spider Monkey Optimization (SMO) algorithm for dimensionality reduction and the Stacked-Deep Polynomial Network (SDPN) for attack classification. The work considers four attack categories and uses various training phases as: Global Leader Learning phase (GLL), Local Leader Learning phase (LLL), Local Leader Decision (LLD), Global Leader Decision (GLD). The Deep Feature Embedding Learning (DFEL) model has been compared with KNNs, DT, and SVM and results with 99.14% F1 score. Transient Search Optimization (TSO) algorithm by Fatani et al. [73] maintain the balancing between exploitation and exploration phases. The model is tested on the most

TABLE 6. Deep learning techniques used for IDS.

Approaches	Properties of the Method	Advantage and Applications	Issues
Convolutional Neural Network [41] [69] [70]	• Convolutional layer with kernel function and pooling layer with max pooling. • Popular for Image processing applications.	• Automatic feature learning methods. • High accuracy in performance. • Face recognition, Image classification, Action recognition, Human pose estimation, etc..	• High computational cost . • Complex in updation. • limited to some applications
Recurrent Neural Network [60] [57]	• Store previous input state and preserves the relationship • Self loop structure. • Good for time series prediction	• Feed forward method with backward connection points. • Long Short-Term Memory for lengthy-time period dependencies. • Anomaly Detection, Stock Price Forecasting,Sentiment Analysis etc.	• Existence of vanishing gradient problem. • Fixed Model Size • Compatibility issues with Tanh or Relu activation feature.
Auto-Encoder (AE) [59]	• Preferred for dimensionality reduction. • Equal Input and output layers. • compress and decompress the data	• low-dimensional abstraction and training with back propagation. • Sparse AE,Denoising AE ,Contractive . • Data Compression, Image Denoising,Dimensionality Reduction,Image Generation etc.	• Additional computation time.. • Deterministic bias resulting with over fitting problem
Restricted Boltzmann machine [74], [75]	• Bidirectional data flow . • Transform high dimensional data.	• Restrictions connections faster performance. • Motion-capturing, video sequencing, image procession etc.	• Unsupervised training lack of general application • Procession on unstructured input,but explicit structure is not considered.
Deep belief network [59], [61] , [63], [64], [66]	• Integrated component with RBM and sigmoid . • Generates deep hierarchical representation.	• Sequential learning strategies. • Unsupervised learning and avoid over-fitting and under-fitting problems.	• Increased run time complexity • Low processing rate for clamped inputs.
Generative adversarial network [76]	• Combination of generative and distributive model . • High potential rate self training to mimic distribution of data.	• Easy training compared to RBM and DBN. • Domains used are: music, image, speech, prose.	• Unstable training. • Complex for Text representation.

popular IoT datasets including KDD99, NSL-KDD, BoT-IoT, and CICIDS-2017. It achieves higher accuracy compared to several existing approaches. Thamilarasu G. et al. [64] propose a three layer framework with network connection phase, anomaly detection phase, and the mitigation phase to identify, analyse, and reduce the risk factor using CNN techniques.

VII. LITERATURE REVIEW ON INTRUSION PREVENTION SYSTEM

Intrusion Prevention System (IPS) monitors the network and identifies the abnormal activity with the traditional techniques. IPS prevents the similar attack occurrence in future by closing the access points, terminating the TCP session, reprogram the firewalls, removing the traces of attack from payloads, headers, and infected files. IPS follows signature, anomaly, and stateful protocol based analysis for network-based and host based intrusion identification. Generally, from implementation perspectives, IDS and IPS are configured together and complementary to each other; thus, it makes Intrusion Detection and Prevention System (IDPS). Available IDPS techniques lack in dynamic attack detection for complex network structure. Probabilistic learning [77], fuzzy logic for high density attacks [78], analysing risk factors with C4.5 Decision Tree algorithms [79], genetic techniques [80], clustering [81], analyzing features and their impact with regression [82] are some of the approaches used for intrusion prevention models. All these techniques are used to frame a data-driven prediction model or the robust detection model for a feasible network to prevent intrusion and security breaches.

A. ML-BASED PREVENTION MODELS FOR IoT

A recent work experiments with interception, injection, and denial of service attacks; IPS is found to be immune to these attacks [83]. It uses K-Means techniques after removing the outliers and integrates Local Outlier Factor (LOF) algorithm to evaluate a score reflecting the abnormality of the observations. Tree Automata based on Automatic Approximations for the Analysis of Security Protocols, abbreviated

TABLE 7. Review deep learning based IDS models for IoT.

Author and Reference	Technique	Data set	Results
Yazan Otoum et al. [56]	Spider Monkey Optimization algorithm (SMO) for feature selection and the Stacked-Deep Polynomial Network (SDPN) for classification	NSL-KDD dataset	99.2% accuracy
Manoj Kumar et al. [57]	Gated Recurrent Neural Networks(GRU)	DARPA/KDD99	98.91% accuracy
Olakunle Ibitoye et al. [58]	Self-normalizing Neural Network (SNN)	BoT-IoT dataset	avobr 90% accuracy
Meidan et al. [59]	Auto Encoders (AE), Deep Belief Network (DBN) for malicious code	KDD99	92.10% accuracy
Atiga et al. [60]	Recurrent Neural Network (RNN) for botnet attack	UNCYO and CVUT	97.0% accuracy
Zhang et al. [61]	DBN for anomaly detection in IoT mobile network	Simulated dataset	94.0% accuracy
Roopak et al. [62]	DBN for network attacks	UNSW-NB15, CIDIDS-01	99.9% accuracy
Tama et al. [63]	DBN for IoT SCADA network for Reconnaissance attack, Injection attack, DoS	SCADA N/W dataset	95.06% accuracy
Thamilarasu G. et al. [64]	Three phase model with DBN and DNN	Real-time	97.0% accuracy
S. Smys et al. [41]	Hybrid Convolutional Neural Network	UNSW NB15	98.6% accuracy
Balakrishnan N. et al. [66]	Deep Belief neural network	Real-time	99.76% Precision.
Chao Liang et al. [67]	Multi-agent system with blockchain and deep learning (DNN) algorithms	NSL-KDD dataset	91.50% accuracy
Mohamed Amine Ferrag et al. [68]	RDTIDS: Rules and Decision Tree-Based Intrusion Detection System	CICIDS2017 and BoT-IoT	96.95% accuracy
Abdelouahid Derhab et al. [69]	Temporal Convolution Neural Network (TCNN) with Synthetic Minority Oversampling Technique-Nominal Continuous (SMOTE-NC)	Bot-IoT dataset	99.98% accuracy
Alkahtani.H et al. [70]	Hybrid convolution neural network with the long short-term memory (CNN-LSTM)	IoTID20	98.80% accuracy
Mengmeng.Ge et al. [71]	Multiclass Feed-Forward Neural Networks (FNN)	BoT–IoT	99.79% accuracy
Qureshi et al. [72]	Random neural network -IDS (RNNIDS)	NSL-KDD	95.25% accuracy
Fatani A et al. [73]	Deep learning and metaheuristics (MH) algorithms	DDCup-99, NSL-KDD, BoT-IoT, and CICIDS-2017	99.62% accuracy

as TA4SP, processes the intruder knowledge using regular tree language [84]. Nikhil et al. [85] propose an integrated technique for prediction and prevention in agriculture sector with smart connected devices. The experiment conducted on the real-time agriculture data using sensor devices and processed using machine learning and deep learning techniques. It uses Support Vector Clustering (SVC) for analysis and predicting the crop suitability based on soil condition, weather, rain estimation, ultrasonic, and infrared rays. CNN technique trains the model with three sample animal images and prevent the physical intrusion damage caused for the crops. USB camera inputs are compared with existing image using signature based detection and raise an email notification with an alarm for avoiding the harm caused for ecosystem [85]. Seo et al. propose a two level hybrid detection and prevention technique [86]. It uses random forest method and evaluate the decision tree for statistical analysis. If the ratio is less than zero the packet are forwarded, else the packets are dropped. The best features analysed from level one pass to the next level, the anomaly detection is implemented and traced for the suspicious event and dropped the packet in level two. The experiment is conducted on UNSW-NB15 and CICIDS2017 dataset. The model results with 99.80% accuracy in the second level of detection. Werth et al. [87] propose a layer-based prevention technique that stimulates a physical system based on payloads of the packets. An additional contribution of the study explores various threat model that creates consequences. It uses three layers: layer zero for physical devices, layer one for ladder logic program, and layer two to activate the internal states of the ladder logic program. Change of pattern in the layer indicates a malicious activity [87]. Serial connectivity of the network is the character of a prevention system; this may lead to potential and communication issues. Hui li et al. [88] introduce a ML technique using SVM in snort IDS to minimize the error rate and improve the performance. The combination of this model with a firewall gains high defensive ability. This proposed IPS is implemented with two-floor classification; first, to identify the possibility of intrusive event and pass to the second floor if any suspicious activity is registered and classify the category of the attack else pass on to the next packet. Inbuilt resources as Netfilter/iptables are used to build the prevention system for inline snort.

Generic IDPS with M2M standard using edge ML technique with three level detection and prevention module is proposed by Chaabouni et al. [89]. The first level acquires the data and selects the best features; the second level classifies the packets based on know patterns to identify the normal and attack class. In the final step, the attack packets are classified into flooding or amplification class to take relevant actions and update the patterns in the database. Constantinides et al. discusses prevention framework with incremental phases based on the input levels named Self-Organizing and Incremental Neural Network Winner-Takes-All Support Vector Machine (n-SOINN-WTA-SVM) [91]. After initializing the weights and bias the model finds the nearby input value and finds the first and second winner. The signature patterns are matched and inserted between the class and check the second winner's availability. If no traces are found, the process is restarted else, the old edges are deleted

and proceed for multi-class classification. Chandre Pankah et al. [92] propose a classification-based prevention technique using five machine learning and one deep learning technique. It uses Support vector machine, random forest, k-nearest neighbors, Naïve Bayes, and Decision Tree from machine learning category and for comparison the model was tested with Convolutional Neural Network (CNN). CNN gives a better performance than SVM as NN models are much capable for larger datasets comparatively. However apart from the techniques mentioned above, there are numerous security solutions available to prevent network intrusion or illegal access in IoT environment. [93] proposed a bio-metric-based smart locking system that allows only authorized people in to the house. It can also be used to gain access if keys are lost or for disable people. Circuit-based Secure Vehicle Operating System by [94], which monitors and controls with mobile tilting and sends messages via google assistant for network authentication.

B. DL-BASED PREVENTION MODELS FOR IoT

SVC and CNN based integrated prevention system by Nikhil et al. experimented on real time agriculture dataset. The entry of animals were captured as image input ant trained by the model. The model resulted accurate by preventing the entry of three animals in agriculture field.

Raghavendra et al. propose a Least square Bolster-based support vector machine-based prevention technique with two segments [95]. A half and half component is used to remove the redundant information in the upper level. It uses the wrapper method to select the relevant features for the classification in the lower level. After the classification of attack, the features having a high impact on the classification are observed to block the related entries for preventing intrusions. Akhil et al. propose a multi-layer perception with SVM for detection of DOS, Probe, R2L, and U2R attacks [96]. An internal script uses features like the IP address and the port number are considered for preventing the attacks. Discriminate Deep Belief Network (DDBN) based detection and prevention technique for local and non-local regularization is proposed by the work in [97]. The model is tested for two popular datasets with Hopfield, SVM, generative adversarial network (GAN), and Deep Belief Network-Random Forest (DBN-RFS) classifiers. Various parameters are changed in the process of developing prevention techniques to reduce the time span for detection of the attack category. It is been observed that the running time decreases as the hidden layers in the model are increased. Balamurugan et al. propose a two phase detection and prevention technique for real-time cloud dataset using three elements: Cloud Controller (CC), Trust Authority (TA), and Virtual Machine Management (VMM) [98]. CC monitors and migrates the packets to idle cloudlets if the traffic is heavy and scrutinize the packet based on arrival time confidence levels and the packet count using header information. Normalized K-means (NK) Recurring Neural Network model (NK-RNN) is used to classify the intruder packets available in VMM. A Queue modelling technique is used to discard the intruder packet. Finally, these packets are blocked for the network to avoid the intrusions in future [98].

A Software Defined Network (SDN) based IDPS for IoT network proposed by Amir Ali et al. [99] uses a three-tier framework. It process the user validation for IoT layer as the first tier, packet validation for data plane layer using fuzzy filtering methods to classify the attack records. Finally, the third tier flows validation with control plane layer for detection and prevention. The control layer is integrated with CNN and Deep Packet Inspection (DPI) for detecting and predicting the attack values. The model is compared with SVM, ANN, Fuzzy, and other ML techniques and results in 1% false rates. A hybrid model with the combination of Bootstrapped Optimistic Algorithm for Tree Construction (BOAT) and Artificial Neural Network for classification and One Way Hash Chain (SHA-256) for preventing in MANET is proposed by [100]. The major components of the model are packet analyzer using fuzzy controller, data pre-processing using logarithmic, and linear normalization, feature extraction using Mutual information function to select optimum feature set, and classification using Association Rule Tree (ART) [100]. The input data is considered based on the breaches caused by three test cases framed on confidentiality, authentication, and access control [101]. A risk analysis model is proposed by James et al. to prevent the attack in various levels: The initial level is to identify risk based on the event and the relations defined [101]. Then, it prioritize the event, evaluate, and rank the risk factor. It choose a mitigation strategy based on the risk connection and the common cause of the threat. Finally, it checks the feasibility and implements the suitable solution by tracking the performance with regular monitoring.

We summarize various machine learning and deep learning techniques for IPS in Table 8. The table also enlists the dataset on which the techniques are evaluated. Various mitigation strategies and the dataset used for experiment with the results based on time taken for prevention and detection accuracy are presented.

VIII. OPPORTUNISTIC SOLUTIONS

Continuous network monitoring and defending are the essential factors of network security to predict and avoid the malicious activity. Traditional detection system monitor and alert when suspicious event occurs, whereas the prevention system take a relevant action when the malware is detected. Based on the models and theories developed for detection, anticipating the importance of the risk and take significant actions,

we have proposed a mapping technique. This evaluate the event type analyze the risk factor and suggested a mitigation strategy. Identifying and providing early warning for intrusion and violating the next action is very much necessary for IoT network structure. The system must be active in classifying and analyzing the risk factor to distinguish the suspicious packets and trigger the prevention technique. IPS is an inline product that focuses on identifying and blocking

TABLE 8. Review on IPS models using machine learning and deep learning.

Author and Reference	Technique	Data set	Results (Time / Accuracy)
Alves at al. [83]	Embedded IPS	UAH SCADA Lab data	Time:0.149 minutes
Pankaj Ramchandra Chandre et al. [84]	Decision Tree and AVISPA tools	Real-time	Time:0.07 seconds
Seo et al. [86]	RFDT hybrid two level IDPS model	UNSW-NB15, CICID2017	Accuracy: 99.80%
Chaabouni N et al. [89]	ML J48 and DL	Real-time	Time: 0.928 Milliseconds.
Nakagawa et al. [90]	Non-Deterministic Finite automation (NFA) and set theory	Real-time	Time 20seconds
Constantinides et al. [91]	n-SOINN-WTA-SVM"	NSL-KDD dataset	Time :2857 seconds Accuracy:82.59%
Chandre Pankah et al. [92]	5 ML and CNN	WSN-DS	Accuracy:98.0%.
Akhil Krishna et al. [96]	Multi-Layer perceptron	KDD99	Accuracy:91.4%
Xian G et al. [97]	DDBN, SVM, GAN, and DBN-RF	NSL KDD99	Time: 1613 seconds, Accuracy: 97.76%
V. Balamurugan et al. [98]	KNRNN	Real-time Cloud DS	Time: 5 microseconds, Accuracy:98.0%
Amir Ali et al. [99]	CNN and DPI	OMNeT++ Simulation Setup.	Time: 2 Seconds delay, Accuracy 99.0%
Islabudeen.M et al. [100]	One Way Hash Chain (SHA-256)	NSL-KDD	Accuracy: 97.86%
James.F et al. [101]	Mitigation strategies	NS3 (Network Simulator 3) with three sets of IoT devices	Time: 1.5 seconds

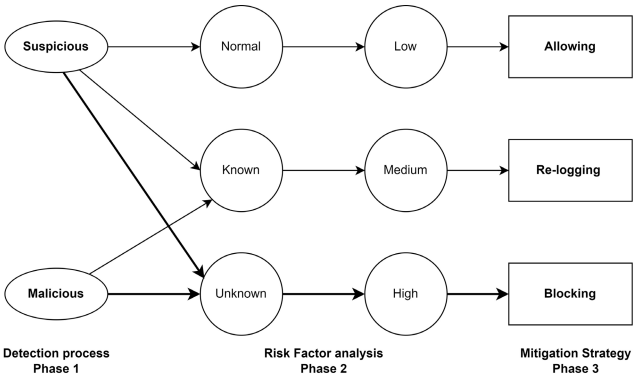

FIGURE 4. Risk factors mapping.

the attack in real-time. Considering this we have proposed a risk factor analysis using a mapping technique, to identify and classify the suspicious and malicious events and rate the level of risk in the next section VIII.

A. RISK FACTOR ANALYSIS

The proposed approach is assumed to increase the accuracy of the model, with three strategic layers for detection, prediction, and mitigation. Furthermore, we combine our mapping technique with a hybrid IDPS framework for accurate identification and reorganization of the threat. The mapping factor is divided into three phases defined in Figure4.The data flow for normal packet is indicated with plain arrow, and the suspicious event flow with dashed arrow mark, and unknown patterns are indicated with dark arrow lines in Figure 4.

In phase one the detection phase behavior pattern change is captured and classified into suspicious and malicious packet. In phase two risk factors are analysed by matching the packets with the known attack patterns, then classified as normal, known, or unknown attack types. Mitigation strategy the phase three analyzes the risk factor rating as high, medium, and low. Thus, the active response from the event is used to analyze the network traffic in real-time. This will trigger the action as a block, allow or logging to mitigate the network complication, or block the process associated with the event. Overall the risk factor identification help in summarizing the following solutions for three cases:

1) Case one: When the event is found suspicious but does not have any further attack variations is considered as a normal activity with a low-risk rate and allowed for further processes.
2) Case two: Suspicious event traced with known signature patterns, analyzed with medium risk rate, and logging is implemented to recheck the authentication of the user. case
3) Case three: When a suspicious or malicious event is undermined in the detection process and categorized as unknown events result in False Positive(FP) or False Negative values. These type of cases causes high-risk factor and lead to process blocking and mitigating the effects of the attack.

B. FRAMEWORK FOR FOUR LEVEL SECURITY STRUCTURE

Features required to develop an effective IDPS model are: high application-level analysis, active threat identification, and integrated prevention model with sophisticated response capability. The research community is keen on providing multiple detection models and frameworks to mitigate the external threat, many of the models focus on signature-based detection and prevention methods.

Many of the methods discussed above lack in the identification of unknown patterns and are poor in handling zero-day attacks; they also fail in avoiding inside intrusion threats. Recent research explores that the deployment of a hybrid model for detection and prevention results in better performance. Figure 5 projects a four-level security framework model with the combination of anomaly and misuse-based detection. This approach is the extension of the subsequent research proposed by Stiwan et al. [2]. The study enhances the mapping procedure and is brief about the hybrid

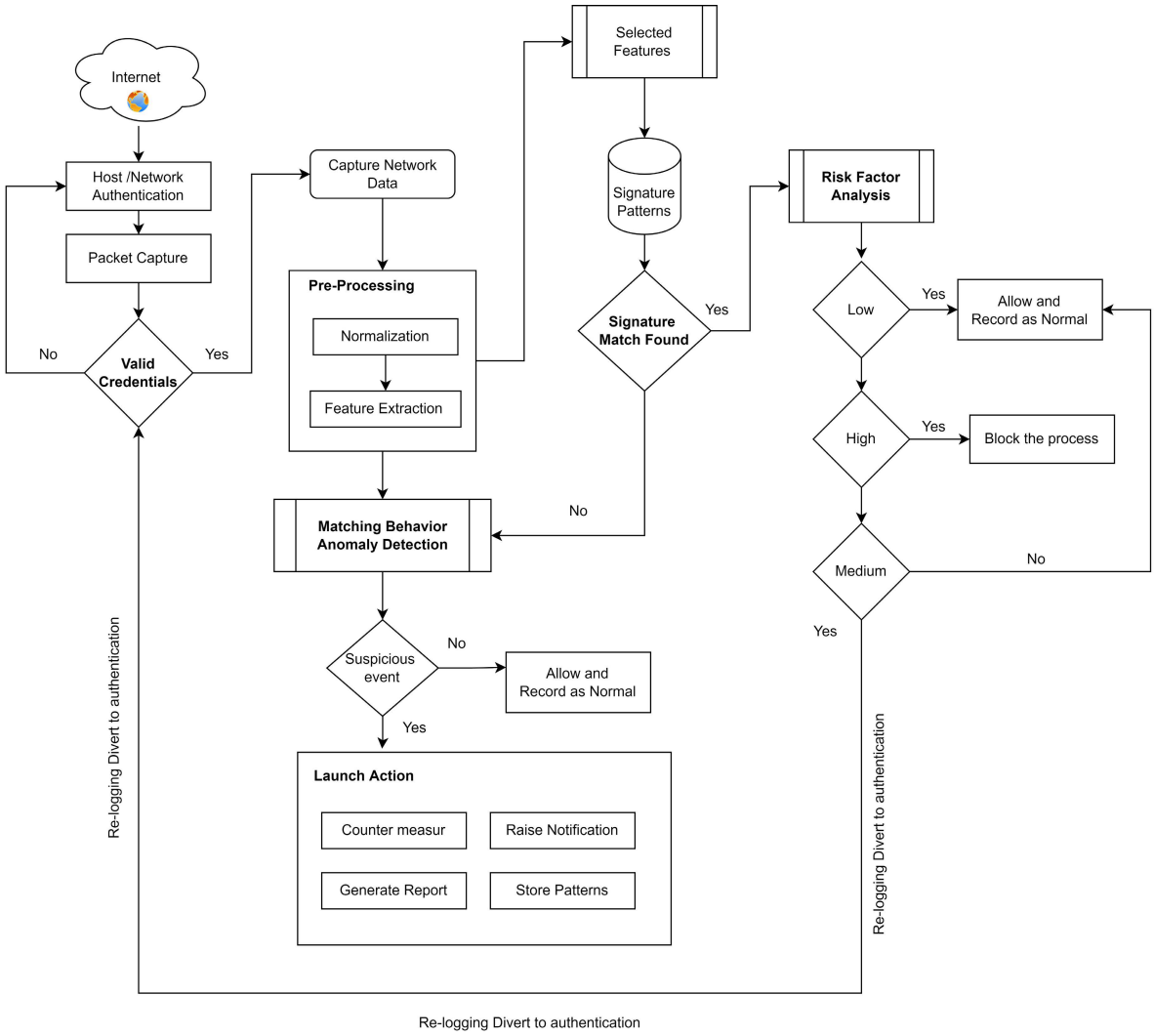

FIGURE 5. Mapping factors.

techniques. Another hybrid detection model with the combination of the immune system proposed by Yu et al. [102] with neural network techniques. The study emphasizes more on accurate detection with self-learning techniques. All the above-discussed models are good in improving the performance and accuracy level, but lack in reducing the false rate. Considering this our framework is integrated with detection, prevention, and risk factor analysis. The main aim of the framework is to integrate both anomaly and signature-based detection, to handle zero-day attacks and avoid inside intrusions with behavioral matching strategies. The framework has four key elements to avoid security violations. The first level of security is to authenticate the network packets with credentials and proceed to pre-processing techniques. This level normalizes the data packets and extracts required features based on the dimensionality reduction techniques. A two-level detection is implemented in this process using anomaly and signature-based detection methods. The complete dataset will all collected features are observed for variation in the behavior using anomaly detection techniques. And at the same time selected features are matched with predefined signature patterns to find the malicious activity under level two. Finally, if any suspicious event is observed, the risk factor analysis is activated and performs required action based on the level of risk identified. If no thereat is detection the packet is sent back to the network for the regular procedure.

IX. SYNOPSIS OF ML-BASED AND DL-BASED IDS/IPS METHODS

ML and DL techniques reduce the human intervention and automate the detection in a short time. DL models are not compatible with large datasets and complex structures as compared to the ML techniques. ML techniques are mostly used for signature intrusion detection that acts according to the stored patterns. On the other hand, DL has a capability for self-learning; hence, it is more compatible for anomaly detection. Analyzing and detecting the attacks based on behavior helps in handling zero-day vulnerabilities. Though the ML techniques require less computational power, the DL techniques are faster than the ML techniques.

The multidimensional Compatibility of a DL technique to train and test on image, audio, video, and sequential data give a unique priority for developing new innovations.

Figure 6 provide an over all summary of the current study. This study only looked at the most recent methods developed using ML and DL techniques between 2018 and 2021. In Figure 6, we first discussed various malware attacks and mitigation techniques based on the article's literature review. Because IDPS is the primary goal of the study, we will summarise the various IDS and IPS techniques proposed in the study. Finally, a list of ML and DL techniques is discussed in the paper's review section VI. In Figure 6, we provide a brief overview of the vulnerabilities caused by attack variants, as well as a list of available solutions, which is required to develop a unique model for a future feature. Our present study emphasizes various ML and DL techniques and the mitigation strategies evaluated from the models as a road map for future research. In the following, we compare the existing surveys in the direction of IDS/IPS notifying the highlights of our study and also provide some research questions to address by the researchers.

A. COMPARISON WITH EXISTING SURVEYS

Table 9 and Table 10 provide comparative summarization of various parameters included in the research articles in the direction of IDS/IPS in the recent years. We use *Y* in the table to represent the description about the specific category in the given study. Any attribute having *N* signifies that a particular study does not have a particular property of discussion.

From the comparison, we see that the maximum of the available studies provide a detailed IDS taxonomy that describes the types of IDS; they also provide sub-classification based on area and the application. Our study evolves around various categories of IDS with ML-based and DL-based techniques suitable for developing the detection or prevention model.

B. HIGHLIGHTS OF CURRENT STUDY

Our work differs from the above-mentioned surveys in the following points.

- The present survey provides the detailed taxonomy of IDS and compares the IDS with security services, whereas the above mentioned surveys present the taxonomy and describe only selected modules with comparative analysis.
- Our survey explores various techniques, methods, models, the framework proposed for IDS with performance and accuracy. On the other hand, the existing surveys either provide a comparative analysis on attacks and methods or the glitches faced by available methods for limited period.
- Our study emphasizes various ML and DL proposals and models of IDS and IPS for IoT with ML and DL techniques. The existing surveys are specific to data storage issues, physical (vehicle security) issues, network-based IoT and IDS implementation issue, and etc.
- The study examines various intrusion prevention techniques and the mitigation strategies,in respect to machine learning and deep learning techniques. It is been observed that there are very limited review articles on prevention techniques, all the above mentioned articles are limited to techniques and models. Our study emphasis the mitigation techniques.
- We propose a mapping technique for analysis of the level of risk and develop a effective prediction model framework to be used as a blueprint for future developments.
- We propose an integrated multilevel hybrid framework that combines signature and anomaly detection with risk factor mapping and identify all types security threats. This framework is beneficial for future development of IDS/IPS.

C. RESEARCH QUESTIONS

Development of accurate detection model and enhancing the security in of IoTs and its allied domains are very prominent research directions in the present time. Our present survey explores more than 100 research papers related to IoT security. These papers propose different classifiers for intrusion detection. Our survey also presents a reasonable perspective of each model and provides a comparison of works in this field. We notify some research questions to provide an insight towards the futuristic development of IDS/IPS.

- **RQ-1: Available dataset are compatible for research? Solution:** Available datasets for intrusion detection do not follow standard features. Each dataset results with different attributes based on the network and application. Consideration of common features selection technique for all models before classification obtains better results.
- **RQ-2: What is the importance of feature reduction? Solution:** Strong feature extraction technique to be implemented to remove irrelevant and redundant features in training; it improves the model performance. To generate a prevention model, it is very important to know the relation between the feature and analyse the behaviour to control the zero day attack.
- **RQ-3:Which is the most suitable technique for feature extraction?**
  Solution: Machine learning models are effective in feature selection and deep learning models are effective in feature reduction. According to the study, it is stated that deep learning auto-encoder is the popular feature reduction technique. Apart form this, integrating multiple feature selection algorithms, and working with the best possible features is helpful for accurate classification.
- **RQ-4:Which is best classifier - single or multiple ?**
  Solution: Use of single classifiers or baseline classifiers in performance measurement can be replaced by hybrid or ensemble classifiers.
- **RQ-5: What is the risk factor after applying the available models? Solution:** Existing models are

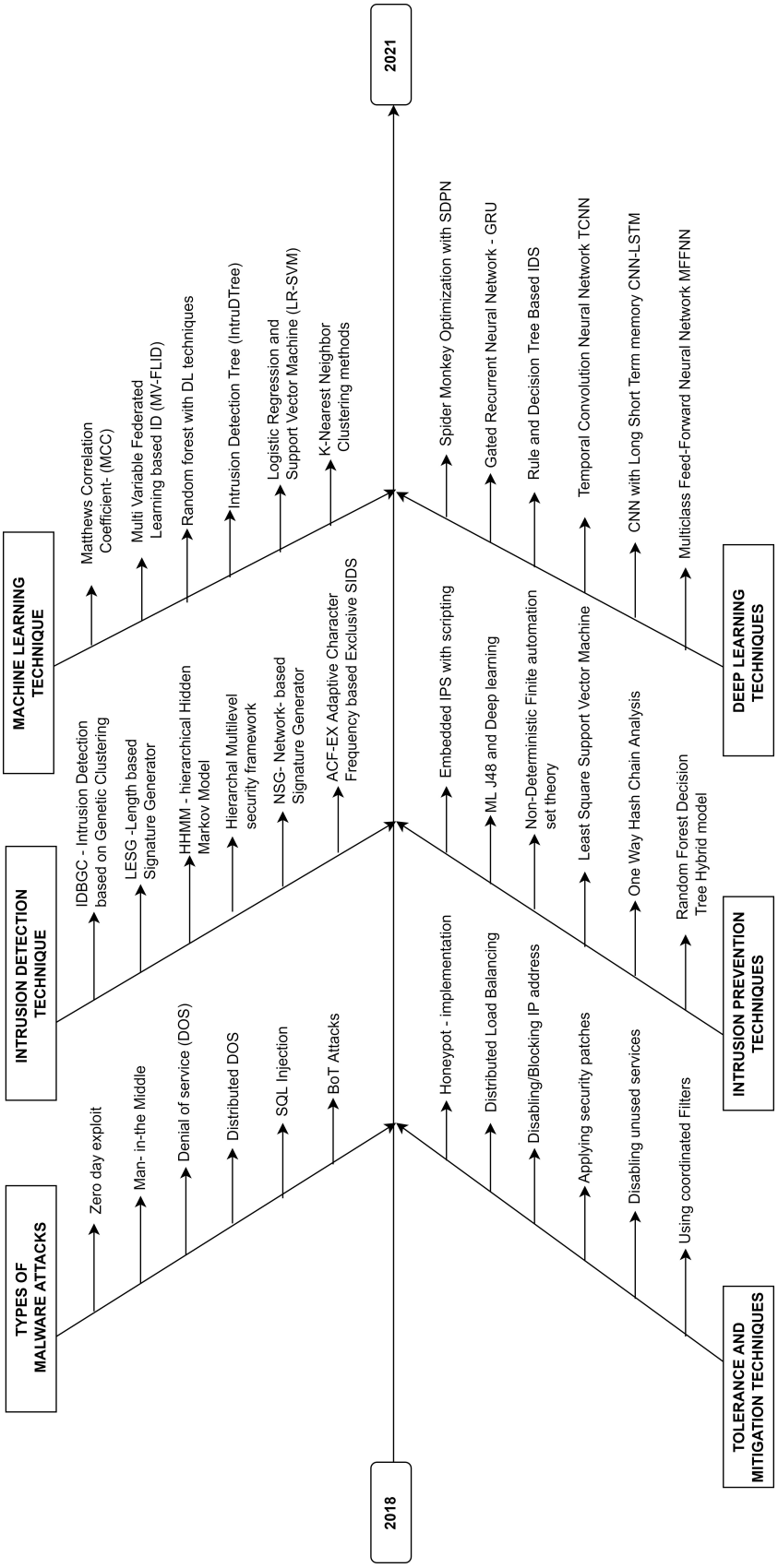

FIGURE 6. Synopsis of intrusion detection and prevention models.

TABLE 9. Comparative analysis of research papers on IDS for IoT.

Author and reference	Year	Taxonomy of IDS	ML & DL techniques	IoT based threats	Dataset issues	Network issues
George Loukas et al. [103]	2018	N	N	Y	N	Y
Elhadj Benkhelifa et al. [104]	2018	N	Y	Y	N	Y
Preeti Mishra et al. [105]	2018	Y	Y	N	N	N
Aldweesh et al. [106]	2018	Y	N	Y	Y	N
Markus Ring et al. [107]	2018	Y	N	N	Y	Y
Khalid Khan et al. [108]	2018	Y	N	Y	N	Y
Ankit Thakkar et al. [109]	2018	Y	Y	N	N	Y
Kelton A.P.et al. [110]	2018	N	Y	Y	N	Y
Zolanvari [111]	2018	Y	Y	Y	N	Y
Butun.I et al. [112]	2018	N	N	Y	N	Y
Adnan et al. [113]	2021	Y	Y	N	Y	N
Hanan Hindy et al. [114]	2020	N	Y	N	Y	Y
Al-Garadi et al. [115]	2020	N	Y	Y	N	N
Hassan Heba A et al. [116]	2021	Y	Y	Y	Y	Y
Current Study	2022	Y	Y	Y	N	Y

TABLE 10. Comparative analysis of research papers on IPS for IoT.

Author and reference	Year	Taxonomy of IDS	ML Techniques	DL Techniques	Dataset issues	Network issues
Chakraborty et al [117]	2013	Y	Y	N	N	Y
Soubhik Das et al. [118]	2017	Y	Y	Y	N	N
Ravipati R.D et al [119]	2019	Y	Y	N	Y	Y
Azeez.N et al [120]	2020	Y	Y	N	N	N
Ahmed Patel et al [122]	2013	Y	Y	N	N	N
Priteshkumar Prajapati et al [121]	2021	N	Y	Y	N	N
Current Study	2022	Y	Y	Y	N	Y

limited to binary or limited attack classification; majority of the models use pattern recognition and signature based techniques. Extending the detection for a wide range of attacks will be feasible to identify zero day vulnerability which has to be duly considered.

- **RQ-6: Which method is the most suitable for IoT?**
  Solution: Light weight and resource compatible ad-hoc network IDS are required without degrading the security requirements.
- **RQ-7:How to solve the problem of false rates of the model?**
  Solution: Detection delays decrease the performance of the underlying networks and generate false rates. To achieve desirable detection accuracy with effective performance time, researchers should focus on model compression techniques.
- **RQ-8:What is the impact of the models on real time data?**
  Solution: Real-Time detection models activate early warning by alert messages and protect the system from threats and suspected activities. The existing detection models lack in identifying zero-day attacks and result in high false alarms, and create impact on the response time of the model.

X. CONCLUSION

Our survey focuses on various research works evolving around IDS and IPS. We elaborate the categories of intrusion detection and prevention based on methodologies, techniques, and provide a detailed analysis of each of the models. The use of machine learning and deep learning methods in IDS has also enhanced its performance. The presented survey analyses the pros and cons of the methods to provide a pathway to the researchers in this domain. We discuss a base of IDS in various categories depending on architecture, positions, and functions. The various solutions for IDS are also classified based on latest research works. We have proposed a risk factor analysis using mapping techniques with mitigation methods. Such a survey with framework and prevention model is not yet available and therefore, our survey is helpful for the IDS and IPS designers to conceptualize the progress path of IDS/IPS methods and technologies. The state-of-the-art comparison of IDS models is also given in the paper. Each ML and DL model is compared and explained through detailed tables. Finally, we have pointed some of the research issues and propose some solutions for research direction.

REFERENCES

[1] R. D. McLeod, K. Ferens, and M. R. Friesen, "The IoT: Examples and trends," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2015, pp. 336–339.

[2] D. Stiawan, A. H. Abdullah, and M. Y. Idris, "Characterizing network intrusion prevention system," *Int. J. Comput. Appl.*, vol. 14, no. 1, pp. 11–18, Jan. 2011.

[3] T. Ghorbani, *Network Intrusion Detection and Prevention : Concepts and Technique*. Springer, 2009.

[4] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," *Inf. Secur. Tech. Rep.*, vol. 10, no. 3, pp. 134–139, 2005.

[5] J. Wang, *Computer Network Security: Theory and Practice*. New York, NY, USA: Springer, 2009.

[6] R. M. Gomathi, G. H. S. Krishna, E. Brumancia, and Y. M. Dhas, "A survey on IoT technologies, evolution and architecture," in *Proc. Int. Conf. Comput., Commun., Signal Process. (ICCCSP)*, Feb. 2018, pp. 1–5.

[7] L. Santos, C. Rabadão, and R. Gonçalves, "Flow monitoring system for IoT networks," in *Proc. World Conf. Inf. Syst. Technol.*, in Lecture Notes in Control and Information Sciences, 2019, pp. 420–430.

[8] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *Proc. 21st Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2016, pp. 519–524.

[9] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.
[10] G. Mullen and L. Meany, "Assessment of buffer overflow based attacks on an IoT operating system," in *Proc. Global IoT Summit (GIoTS)*, 2019, pp. 1–6, doi: 10.1109/GIOTS.2019.8766434.
[11] K. Carvalho and J. Granjal, "Security and privacy for mobile IoT applications using blockchain," *Sensors*, vol. 21, no. 17, p. 5931, Sep. 2021.
[12] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions," *J. Ambient Intell. Humanized Comput.*, pp. 1–18, May 2017.
[13] B. Yuan, Y. Jia, L. Xing, D. Zhao, X. Wang, and Y. Zhang, "Shattered chain of trust: Understanding security risks in cross-cloud IoT access delegation," in *Proc. 29th USENIX Secur. Symp. (USENIX Security)*, 2020, pp. 1183–1200.
[14] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.
[15] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Comput. Netw.*, vol. 177, Aug. 2020, Art. no. 107333.
[16] T. Varshney, N. Sharma, I. Kaushik, and B. Bhushan, "Architectural model of security threats and theircountermeasures in IoT," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Oct. 2019, pp. 424–429.
[17] A. Fongen, "Identity management and integrity protection in the Internet of Things," in *Proc. 3rd Int. Conf. Emerg. Secur. Technol.*, Sep. 2012, pp. 111–114.
[18] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017.
[19] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Comput. Netw.*, vol. 31, no. 8, pp. 805–822, 1999.
[20] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.
[21] B. Mbarek, M. Ge, and T. Pitner, "Enhanced network intrusion detection system protocol for Internet of Things," in *Proc. 35th Annu. ACM Symp. Appl. Comput.*, Mar. 2020, pp. 1156–1163.
[22] J. Liu and L. Li, "A distributed intrusion detection system based on agents," in *Proc. IEEE Pacific-Asia Workshop Comput. Intell. Ind. Appl.*, Dec. 2008, pp. 553–557.
[23] A. Aris and S. F. Oktug, "Poster: State of the art IDS Design for IoT," in *Proc. Int. Conf. Embedded Wireless Syst. Netw.*, Junction, Feb. 2017, pp. 196–197. [Online]. Available: http://dl.acm.org/citation.cfm?id=3108009.310803
[24] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "DEMO: An IDS framework for Internet of Things empowered by 6LoWPAN," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2013, pp. 1337–1340, doi: 10.1145/2508859.2512494.
[25] C. Jun and C. Chi, "Design of complex event-processing IDS in Internet of Things," in *Proc. 6th Int. Conf. Measuring Technol. Mechatronics Autom.*, Jan. 2014, pp. 226–229.
[26] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 606–611.
[27] M. Surendar and A. Umamakeswari, "InDReS: An intrusion detection and response system for Internet of Things with 6LoWPAN," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2016, pp. 1903–1908.
[28] Y. Fu, Z. Yan, J. Cao, O. Kon, and X. Cao. (May 2017). *An Automata Based Intrusion Detection Method for Internet of Things*. [Online]. Available: https://www.hindawi.com/journals/misy/2017/1750637/abs/
[29] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalis—A system for knowledge driven adaptable intrusion detection for the Internet of Things," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 656–666.
[30] V. Subbarayalu, B. Surendiran, and P. A. R. Kumar, "Hybrid network intrusion detection system for smart environments based on Internet of Things," *Comput. J.*, vol. 62, no. 12, pp. 1822–1839, Nov. 2019.
[31] A. Verma and V. Ranga, "ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things," in *Proc. 4th Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Apr. 2019, pp. 1–6.
[32] H. Kozushko, "Intrusion detection: Host-based and network-based intrusion detection systems independent study," Tech. Rep., 2003.
[33] H. Wu, S. Schwab, and R. L. Peckham, "Signature based network intrusion detection system and method," U.S. Patent 7 424 744, Sep. 9, 2008.
[34] D. M. Teal, "Intrusion detection system and method having dynamically loaded signatures," U.S. Patent 6 477 651, Nov. 5, 2002.
[35] S. Jose, D. Malathi, B. Reddy, and D. Jayaseeli, "A survey on anomaly based host intrusion detection system," *J. Phys., Conf.*, vol. 1000, Apr. 2018, Art. no. 012049.
[36] V. Jyothsna, V. V. R. Prasad, and K. M. Prasad, "A review of anomaly based intrusion detection systems," *Int. J. Comput. Appl.*, vol. 28, no. 7, pp. 26–35, Aug. 2011.
[37] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, nos. 1–2, pp. 18–28, Feb. 2009.
[38] A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," *Wireless Pers. Commun.*, vol. 111, no. 4, pp. 2287–2310, Apr. 2020.
[39] J. Liu, B. Kantarci, and C. Adams, "Machine learning-driven intrusion detection for contiki-NG-based IoT networks exposed to NSL-KDD dataset," in *Proc. 2nd ACM Workshop Wireless Secur. Mach. Learn.*, Jul. 2020, pp. 25–30.
[40] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "A machine learning based intrusion detection system for mobile Internet of Things," *Sensors*, vol. 20, no. 2, p. 461, Jan. 2020.
[41] D. S. Smys, D. A. Basar, and D. H. Wang, "Hybrid intrusion detection system for Internet of Things (IoT)," *J. ISMAC*, vol. 2, no. 4, pp. 190–199, Sep. 2020.
[42] P. Maniriho, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L. J. Mahoro, and T. Ahmad, "Anomaly-based intrusion detection approach for IoT networks using machine learning," in *Proc. Int. Conf. Comput. Eng., Netw., Intell. Multimedia (CENIM)*, Nov. 2020, pp. 303–308.
[43] D. C. Attota, V. Mothukuri, R. M. Parizi, and S. Pouriyeh, "An ensemble multi-view federated learning intrusion detection for IoT," *IEEE Access*, vol. 9, pp. 117734–117745, 2021.
[44] M. A. Rahman, A. T. Asyhari, O. W. Wen, H. Ajra, Y. Ahmed, and F. Anwar, "Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection," *Multimedia Tools Appl.*, vol. 80, pp. 1–19, Mar. 2021.
[45] X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera, and M. S. Rodrigo, "An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets," *Sensors*, vol. 21, no. 2, p. 656, Jan. 2021.
[46] S. Bagui, X. Wang, and S. Bagui, "Machine learning based intrusion detection for IoT botnet," *Int. J. Mach. Learn. Comput.*, vol. 11, no. 6, pp. 399–406, Nov. 2021.
[47] D. J. Atul, R. Kamalraj, G. Ramesh, K. S. Sankaran, S. Sharma, and S. Khasim, "A machine learning based IoT for providing an intrusion detection system for security," *Microprocessors Microsystems*, vol. 82, Apr. 2021, Art. no. 103741.
[48] M. Ahmad, Q. Riaz, M. Zeeshan, H. Tahir, S. A. Haider, and M. S. Khan, "Intrusion detection in Internet of Things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–23, Dec. 2021.
[49] A. Churcher, R. Ullah, J. Ahmad, F. Masood, M. Gogate, F. Alqahtani, B. Nour, and W. J. Buchanan, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, 2021.
[50] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, no. 5, p. 754, 2020.
[51] H. Alqahtani, I. H. Sarker, A. Kalim, S. M. M. Hossain, S. Ikhlaq, and S. Hossain, "Cyber intrusion detection using machine learning classification techniques," in *Proc. Int. Conf. Comput. Sci. Commun. Secur.* Singapore: Springer, 2020, pp. 121-131.
[52] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Multi-stage optimized machine learning framework for network intrusion detection," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1803–1816, Jun. 2021.

[53] M. A. Rahman, A. T. Asyhari, L. S. Leong, G. B. Satrya, M. H. Tao, and M. F. Zolkipli, "Scalable machine learning-based intrusion detection system for IoT-enabled smart cities," *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102324.

[54] M. Sarnovsky and J. Paralic, "Hierarchical intrusion detection using machine learning and knowledge model," *Symmetry*, vol. 12, no. 2, p. 203, Feb. 2020.

[55] M. Wang, K. Zheng, Y. Yang, and X. Wang, "An explainable machine learning framework for intrusion detection systems," *IEEE Access*, vol. 8, pp. 73127–73141, 2020.

[56] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: A deep learning–based intrusion detection framework for securing IoT," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3803, Mar. 2019.

[57] M. K. Putchala, "Deep learning approach for intrusion detection system (IDS) in the Internet of Things (IoT) network using gated recurrent neural networks (GRU)," Tech. Rep., 2017.

[58] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[59] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018.

[60] J. Atiga, N. E. Mbarki, R. Ejbali, and M. Zaied, "Faulty node detection in wireless sensor networks using a recurrent neural network," *Proc. SPIE*, vol. 10696, Apr. 2018, Art. no. 106962P.

[61] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019.

[62] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0452–0457.

[63] B. A. Tama and K.-H. Rhee, "Attack classification analysis of IoT network via deep learning approach," in *Proc. Res. Briefs Inf. Commun. Technol. Evol. (ReBICTE)*, vol. 3, 2017, pp. 1–9.

[64] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the Internet of Things," *Sensors*, vol. 19, no. 9, p. 1977, 2019.

[65] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in *Proc. 2nd Int. Conf. Adv. Cloud Big Data*, Nov. 2014, pp. 247–252.

[66] N. Balakrishnan, A. Rajendran, D. Pelusi, and V. Ponnusamy, "Deep belief network enhanced intrusion detection system to prevent security breach in the Internet of Things," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100112.

[67] C. Liang, B. Shanmugam, S. Azam, A. Karim, A. Islam, M. Zamani, S. Kavianpour, and N. B. Idris, "Intrusion detection system for the Internet of Things based on blockchain and multi-agent systems," *Electronics*, vol. 9, no. 7, p. 1120, Jul. 2020.

[68] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks," *Future Internet*, vol. 12, no. 3, p. 44, Mar. 2020.

[69] A. Derhab, A. Aldweesh, A. Z. Emam, and F. A. Khan, "Intrusion detection system for Internet of Things based on temporal convolution neural network and efficient feature engineering," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–16, Dec. 2020.

[70] H. Alkahtani and T. H. H. Aldhyani, "Intrusion detection system to advance Internet of Things infrastructure-based deep learning algorithms," *Complexity*, vol. 2021, pp. 1–18, Jul. 2021.

[71] M. Ge, N. F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly, "Towards a deep learning-driven intrusion detection approach for Internet of Things," *Comput. Netw.*, vol. 186, Feb. 2021, Art. no. 107784.

[72] A. U. H. Qureshi, H. Larijani, J. Ahmad, and N. Mtetwa, "A heuristic intrusion detection system for Internet-of-Things (IoT)," in *Proc. Intell. Comput. Conf.* Cham, Switzerland: Springer, Jul. 2019, pp. 86-98.

[73] A. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness, and S. Lu, "IoT intrusion detection system using deep learning and enhanced transient search optimization," *IEEE Access*, vol. 9, pp. 123448–123464, 2021.

[74] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment," *J. Ambient Intell. Hum. Comput.*, vol. 12, no. 3, pp. 3609–3619, 2019.

[75] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in *Proc. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2016, pp. 195–200.

[76] S. Huang and K. Lei, "IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in Ad-hoc networks," *Ad Hoc Netw.*, vol. 105, Aug. 2020, Art. no. 102177.

[77] M. C. J. Sekhar, K. Tulasi, V. V. Amulya, D. R. Teja, and M. S. Kumar, "Implementation of IDS using snort on Bayesian network," *Int. J. Comput. Sci. Mobile Comput.*, vol. 4, no. 4, pp. 790–795, Apr. 2015.

[78] R. Shanmugavadivu and N. Nagarajan, "Network intrusion detection system using fuzzy logic," *Indian J. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 101–111, 2011.

[79] K. Rai, M. S. Devi, and A. Guleria, "Decision tree based algorithm for intrusion detection," *Int. J. Adv. Netw. Appl.*, vol. 7, no. 4, pp. 2828–2834, 2016.

[80] M. S. Hoque, "An implementation of intrusion detection system using genetic algorithm," *Int. J. Netw. Secur. Appl.*, vol. 4, no. 2, pp. 109–120, Mar. 2012.

[81] M. V. Rao, A. Damodaram, and N. C. B. Charyulu, "Algorithm for clustering with intrusion detection using modified and hashed K—Means algorithm," in *Advances in Computer Science, Engineering & Applications* (Advances in Intelligent Systems and Computing), vol. 167. Springer, 2012, pp. 737–744.

[82] L. Hui, G. Xiao-Hong, Z. Xin, and H. Chong-Zhao, "Network intrusion detection based on support vector machine," *J. Comput. Res. Develop.*, to be published.

[83] T. Alves, R. Das, and T. Morris, "Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers," *IEEE Embedded Syst. Lett.*, vol. 10, no. 3, pp. 99–102, Sep. 2018.

[84] P. R. Chandre, P. N. Mahalle, and G. R. Shinde, "Machine learning based novel approach for intrusion detection and prevention system: A tool based verification," in *Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*, Nov. 2018, pp. 135–140.

[85] R. Nikhil, B. S. Anisha, and R. Kumar P., "Real-time monitoring of agricultural land with crop prediction and animal intrusion prevention using Internet of Things and machine learning at edge," in *Proc. IEEE Int. Conf. Electron., Comput. Commun. Technol. (CONECCT)*, Jul. 2020, pp. 1–6.

[86] W. Seo and W. Pak, "Real-time network intrusion prevention system based on hybrid machine learning," *IEEE Access*, vol. 9, pp. 46386–46397, 2021.

[87] A. Werth and T. H. Morris, "A specification-based intrusion prevention system for malicious payloads," in *National Cyber Summit*. Cham, Switzerland: Springer, Jun. 2019, pp. 153–168.

[88] H. Li and D. Liu, "Research on intelligent intrusion prevention system based on snort," in *Proc. Int. Conf. Comput., Mechatronics, Control Electron. Eng.*, Aug. 2010, pp. 251–253.

[89] N. Chaabouni, M. Mosbah, A. Zemmari, and C. Sauvignac, "A oneM2M intrusion detection and prevention system based on edge machine learning," in *Proc. NOMS IEEE/IFIP Netw. Operations Manage. Symp.*, Apr. 2020, pp. 1–7.

[90] Y. Nakagawa, Y. Kazato, and Y. Nakatani, "Inspecting intrusion prevention system signatures for false blocking using set theory," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[91] C. Constantinides, S. Shiaeles, B. Ghita, and N. Kolokotronis, "A novel online incremental learning intrusion prevention system," in *Proc. 10th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Jun. 2019, pp. 1–6.

[92] P. R. Chandre, P. N. Mahalle, and G. R. Shinde, "Deep learning and machine learning techniques for intrusion detection and prevention in wireless sensor networks: Comparative study and performance analysis," in *Design Frameworks for Wireless Networks*. Singapore: Springer, 2020, pp. 95–120.

[93] N. Y. L. Venkata, C. Rupa, B. Dharmika, T. G. Nithin, and N. Vineela, "Intelligent secure smart locking system using face biometrics," in *Proc. Int. Conf. Recent Trends Electron., Inf., Commun. Technol. (RTEICT)*, Aug. 2021, pp. 268–273.

[94] S. Irfan, C. Rupa, K. Vinay, M. K. Veni, and R. Rachana, "Smart virtual circuit based secure vehicle operating system," in *Proc. 2nd Int. Conf. Innov. Mech. for Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 386–390.

[95] N. R. Sai, A. G. Raghavendra, N. C. M. Deepak, and M. Poojitha, "A machine learning intrusion prevention and detection system using securing smart grid," *Int. J. Recent Technol. Eng.*, vol. 8, no. 5, pp. 2278–3878, 2020.

[96] A. Krishna, A. J. Mathewkutty, D. S. Jacob, and M. Hari, "Intrusion detection and prevention system using deep learning," in *Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Jul. 2020, pp. 273–278.
[97] G. Xian, "Cyber intrusion prevention for large-scale semi-supervised deep learning based on local and non-local regularization," *IEEE Access*, vol. 8, pp. 55526–55539, 2020.
[98] V. Balamurugan and R. Saravanan, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," *Cluster Comput.*, vol. 22, no. S6, pp. 13027–13039, Nov. 2019.
[99] A. Ali and M. M. Yousaf, "Novel three-tier intrusion detection and prevention system in software defined network," *IEEE Access*, vol. 8, pp. 109662–109676, 2020.
[100] M. Islabudeen and M. K. K. Devi, "A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks," *Wireless Pers. Commun.*, vol. 112, no. 1, pp. 193–224, May 2020.
[101] F. James, "IoT cybersecurity based smart home intrusion prevention system," in *Proc. 3rd Cyber Secur. Netw. Conf. (CSNet)*, 2019, pp. 107–113, doi: 10.1109/CSNet47905.2019.9108938.
[102] X. Yu, "A new model of intelligent hybrid network intrusion detection system," in *Proc. Int. Conf. Bioinf. Biomed. Technol.*, 2010, pp. 386–389.
[103] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Netw.*, vol. 84, pp. 124–147, Mar. 2019, doi: 10.1016/j.adhoc.2018.10.002.
[104] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: Towards universal and resilient systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3496–3509, 4th Quart., 2018, doi: 10.1109/comst.2018.2844742.
[105] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 686–728, 1st Quart., 2019, doi: 10.1109/comst.2018.2847722.
[106] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowl.-Based Syst.*, vol. 189, Feb. 2020, Art. no. 105124, doi: 10.1016/j.knosys.2019.105124.
[107] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Comput. Secur.*, vol. 86, pp. 147–167, Sep. 2019, doi: 10.1016/j.cose.2019.06.005.
[108] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless Ad-hoc networks," *J. Syst. Archit.*, vol. 105, May 2020, Art. no. 101701, doi: 10.1016/j.sysarc.2019.101701.
[109] A. Thakkar and R. Lohiya, "Role of swarm and evolutionary algorithms for intrusion detection system: A survey," *Swarm Evol. Comput.*, vol. 53, Mar. 2020, Art. no. 100631, doi: 10.1016/j.swevo.2019.100631.
[110] A. P. K. da Costa, P. J. Papa, O. C. Lisboa, R. Munoz, and C. V. H. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, Mar. 2019, pp. 147–157, doi: 10.1016/j.comnet.2019.01.023.
[111] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019.
[112] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2019.
[113] A. Adnan, A. Muhammed, A. A. A. Ghani, A. Abdullah, and F. Hakim, "An intrusion detection system for the Internet of Things based on machine learning: Review and challenges," *Symmetry*, vol. 13, no. 6, p. 1011, Feb. 2021.
[114] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," *IEEE Access*, vol. 8, pp. 104650–104675, 2020, doi: 10.1109/ACCESS.2020.3000179.
[115] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, and X. Du, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1646–1685, 3rd Quart., 2020.
[116] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair, and F. E. A. El-Samie, "A survey on SDN-based intrusion detection systems on the Internet of Thing: Concepts, issues, and blockchain applications," Tech. Rep., 2021.
[117] N. Chakraborty, "Intrusion detection system and intrusion prevention system: A comparative study," *Int. J. Comput. Bus. Res.*, vol. 4, no. 2, pp. 1–8, 2013.
[118] S. Das and M. J. Nene, "A survey on types of machine learning techniques in intrusion prevention systems," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2017, pp. 2296–2299, doi: 10.1109/wispnet.2017.8300169.
[119] R. D. Ravipati and M. Abualkibash, "Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets—A review paper," *Int. J. Comput. Sci. Inf. Technol.* vol. 11, no. 3, p. 16, 2019.
[120] N. A. Azeez, T. M. Bada, S. Misra, A. Adewumi, C. Van der Vyver, and R. Ahuja, "Intrusion detection and prevention systems: An updated review," in *Proc. Data Manag., Anal. Innov.*, 2020, pp. 685–696.
[121] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Jú or, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013.
[122] P. Prajapati, B. Bhatt, G. Zalavadiya, M. Ajwalia, and P. Shah, "A review on recent intrusion detection systems and intrusion prevention systems in IoT," in *Proc. 11th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2021, pp. 588–593, doi: 10.1109/confluence51648.2021.9377202.

P. L. S. JAYALAXMI has received the master's degree from IGNOU, in 2018. She is currently pursuing the Ph.D. degree with Lovely Professional University, India. She is working as an Assistant Professor with the Bhavans Vivekananda College, India. Her research interests include cyber-security, financial fraud analysis, intrusion detection, and authentication in the IoT networks.

RAHUL SAHA (Member, IEEE) has received the Ph.D. degree in cryptography from Lovely Professional University, Punjab, India. He is currently working as an Associate Professor with Lovely Professional University and also as a Postdoctoral Researcher with the University of Padua, Italy. His research interests include network security, cryptography, blockchain, DLTs, and the IoT security.

GULSHAN KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Lovely Professional University, Punjab, India, in 2017. He is currently working as a Postdoctoral Researcher with the University of Padua, Italy and an Associate Professor with Lovely Professional University. His current research interests include cyber physical systems, blockchain, edge, and cloud computing, wireless sensor networks, and optimization techniques.

MAURO CONTI (Fellow, IEEE) is a Full Professor with the University of Padua, Italy. His main research interests include security and privacy. He is a Senior Member, ACM. He is a member of the Blockchain Expert Panel of the Italian Government. He is afellow of the Young Academy of Europe.

TAI-HOON KIM (Member, IEEE) received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degrees from the University of Bristol, U.K., and the University of Tasmania, Australia. He is currently with Glocal Campus, Konkuk University, South Korea. His main research interests include security engineering for IT products, IT systems, development processes, and operational environments.