Hindawi
Security and Communication Networks
Volume 2022, Article ID 4016073, 13 pages
https://doi.org/10.1155/2022/4016073

WILEY | Hindawi

Review Article

Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions

Amjad Rehman Khan,[1] Muhammad Kashif,[2] Rutvij H. Jhaveri,[3] Roshani Raut,[4] Tanzila Saba,[1] and Saeed Ali Bahaj[5]

[1]*Artificial Intelligence and Data Analytics Lab (AIDA) CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia*
[2]*Department of Computer Science and Software Engineering International Islamic University Islamabad, Islamabad, Pakistan*
[3]*Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, Gandhinagar, India*
[4]*Department of Information Technology, Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India*
[5]*MIS Department College of Business Administration, Prince Sattam Bin Abdulaziz University, Alkharj 11942, Saudi Arabia*

Correspondence should be addressed to Rutvij H. Jhaveri; rutvij.jhaveri@sot.pdpu.ac.in

Received 13 February 2022; Accepted 24 June 2022; Published 9 July 2022

Academic Editor: Habib Ullah Khan

In the last decade, huge growth is recorded globally in computer networks and Internet of Things (IoT) networks due to the exponential data generation, approximately zettabyte to a petabyte. Consequently, security issues have also been arisen with the network growth. However, intrusion detection in such big data is challenging. Smart homes, cities, grids, devices, objects, e-commerce, e-banking, e-government, etc., are different advanced applications of the evolving networks. Many Intrusion Detection Systems (IDS) have been developed recently due to most computer networks' exposure to security and privacy threats. Data confidentiality, integrity, and availability damage will occur in case of IDS prevention failure. Conventional techniques are not effective enough to cope the advanced attacks. Advanced deep learning techniques have been proposed for automatic intrusion detection and abnormal behavior identification of networks. This research aims to provide an inclusive analysis of intrusion detection based on deep learning techniques followed by different intrusion detection systems. In this review, public network-based datasets of IDS are fully explored and analyzed. Deep learning techniques for IDS have been critically evaluated based on different performance metrics (accuracy, precision, recall, f-1 score, false alarm rate, and detection rate). Furthermore, existing challenges and possible solutions for networks security and privacy have been discussed.

1. Introduction

Researchers are persistent about quality of service and high security in large-scale networks. The interconnection of networks and their applications extended to more complex networks day by day for exchanging critical information. Only 50 billion IoT device networks were expected globally until the end of 2020, and an estimated $3.9–$11.1 trillion per annum economic impact rate. Many applications such as smart homes, cities, healthcare, and more enhance life excellence and the pervasive interconnection of networks with other networks and devices for communication. Figure 1 shows IoT network architecture based on network layers. Some devices use sensors to automatically collect real-time data shared across the networks for evaluation purposes [1, 2].

For most enterprises, cyber-attacks are a significant concern. Governments and enterprises are working hard to prevent the theft of sensitive information. Several technologies such as IDS, firewalls, and traffic shaping devices are available to secure a network. In addition, numerous attack modelling approaches are available to help organizations understand the nature of an assault [3–5]. One of the top

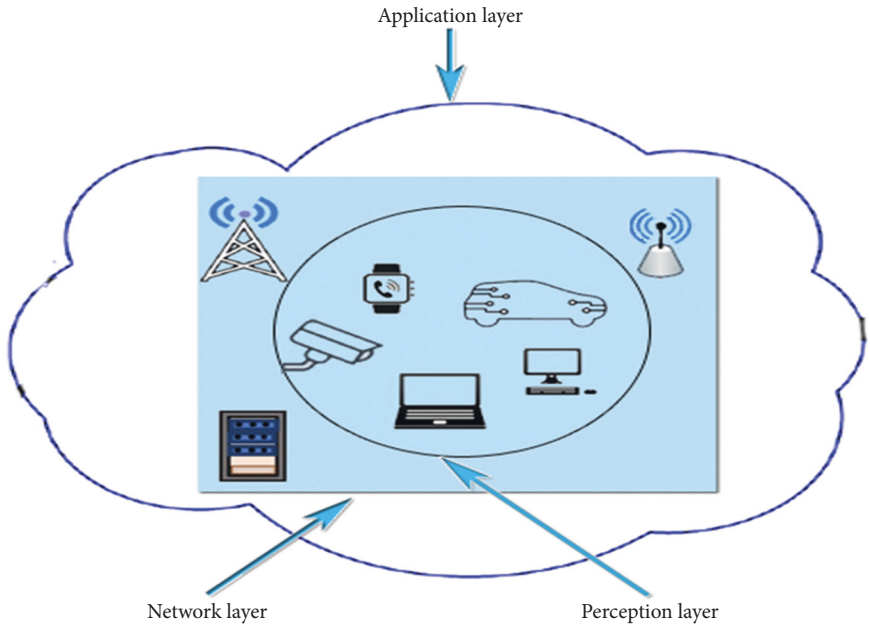

Figure 1: General IoT network architecture is based on different devices communication across network layers.

concerns for businesses is to protect their networks from the external attacks. Strong authentication, access control, and monitoring systems are often successful in detecting, mitigating, and stopping cyber-attacks. Furthermore, IDS can identify the majority of assaults at the Perception, Transport, and Network layers.

A serious security issue to the intrusion detection systems is to face the malicious software variations that lead to network security breaches and serious faults. Cyber-attacks are more complicated and challengeable in unknown malware attack identification due to the evolution of advanced evasion methods to steal critical information and evade IDS from detection [6–8]. In addition, there are cybersecurity threats during internetworks communication. Therefore, novel techniques and solutions are essential for attack prevention and timely intrusion detection techniques. Machine learning and deep learning techniques have recently been developed and applied for intrusion detection and identification of abnormal behaviors in networks and their prevention [9–11].

IDS provides the solution for different security-related issues with different types of malicious or intruders attacks in networks [12, 13]. In this research, the different intrusion detection systems are discussed. In addition, deep learning-based techniques for intrusion detection have been described comprehensively.

The following are the major contributions of this research.

(i) The main intrusion detection systems are elaborated and analyzed.

(ii) Network-based datasets for IDS evaluation are elaborated.

(iii) IDS-based deep learning methods are evaluated on benchmark datasets.

(iv) Finally, the study highlights existing network security challenges and possible solutions.

Further, in Section 2, related work is presented. Section 3 described intrusion detection systems and their types. Deep learning-based techniques developed for IDS have been demonstrated in Section 4. Section 5 discussed different publicly available datasets comprehensively. State of the art DL-based techniques for IDS have been critically reviewed based on accuracy, precision, recall, FAR, and f1 score in Section 6. Finally, the research is concluded along with future challenges and their possible solutions in Section 7.

2. Related Work

Numerous techniques and algorithms for intrusion detection are reported in the literature using machine and deep learning. Hence, this section explores existing techniques and solutions based on deep learning techniques [14, 15].

Auto-IF (Autoencoder and Isolation Forest) technique was developed for anomaly detection in Fog network. Using binary classification, the method classifies the inbound traffic as normal packets or malicious attacks simultaneously. The dataset imbalance problem is avoided by taking normal traffic data using Autoencoder (AE) and removing the training attacks. Isolation forest uses the AE output as input for datapoint misfit identification to enhance the performance. The result shows that this technique achieves best performance of 95.4% accuracy, 94.81% precision, 97.25% recall, and 96.01% F-measure, respectively, by evaluating the NSL-KDD dataset [6]. WFEU-FFDNN (Feed-Forward Deep Neural Network and Wrapper Based Feature Extraction Unit) techniques were implemented. The best compact feature vector was produced using WFEU extra trees algorithms. The proposed IDS system's performance

was evaluated on two datasets, UNSW-NB15 and AWID (Aegean WiFi Intrusion Dataset). 22 and 26 attributes feature vector is formed through WFEU in the UNSW-NB15 and AWID datasets. The results demonstrate that the technique achieves accuracy of 87.10% and 77.16% for binary and multi-class classification for UNSW-NB15 and accuracy of 99.66% and 99.77% for the binary and the multi-class classification for AWID dataset. The proposed technique was compared with ML techniques such as SVM, KNN, RF, DT, and NB. The research based on AWID presents that it is appropriate for wired as well as wireless network applications. The proposed system slows down due to complex computations and time consumption throughout the experimental procedure. This research explores UNSW-NB15 and AWID dataset distinct classes detection rate and their performance influence when the proposed technique is applied. The limitations could be considered using powerful hardware [16, 17]. Automated IDS using Recurrent Neural Networks (RNN) with multi-layers was proposed for fog network security and evaluated by a stable NSL-KDD dataset. The technique consists of two main phases: traffic analysis and classification. The traffic analysis section preprocesses the data for DNN (deep neural network) processing.

In contrast, the preprocess data are classified as a normal or malicious attack in classification phase. Deep proportional recursive network and backpropagation algorithm variation were implemented to develop appropriate IDS for training. This technique analyzes traffic, yields robust and consistent real-time security in an IoT environment. When a malicious attack is detected, it warns through a security alarm. The technique's analysis reported high sensitivity to DoS attacks and detection rate of DoS 98.27% Probe 97.35% R2L 64.93% U2R 77.25% in real-time networks [18].

An IDS technique-based GBDT (Gradient Boosting Decision Tree) paralleled quadratic ensemble learning was developed to use traffic spatial part data. The GRU (Gated Recurrent Unit) variant method is used for temporal data. The GBDT and GRU techniques extracted features (spatial and temporal) are concatenated as the final IDS model. CAS2018 dataset was created in the lab for experimental analysis. This technique is evaluated on CICIDS2017 dataset that resulted in better accuracy of 99.9%, 99.9%, 99.9%, 99.9%, and 99.9%, respectively, for detecting benign, DDoS (Distributed Denial of Service), port scan, infiltration, and web attack traffic [9]. Furthermore, an FFT (Fast Fourier Transformation) algorithm was developed to enhance the CNN efficacy in network traffic intrusion detection due to CNN models' immaturity. FFT converts each network communication into images for classification [19, 20].

The data comprised of characters. The numbers are used instead of characters to make sequences for FFT to sample 4096 points. Real, imaginary parts and their summation as three channels of an image generate an image of $64 * 64$. The result shows the effectiveness in binary and multi-classification in data conversion. The experiments were performed on NSL-KDD dataset. This technique is limited in u2r and r2l detection due to low data present in the dataset. The research aimed to explore imbalanced samples of datasets and real-time network communications image conversion techniques [21, 22]. A new feature extraction technique was proposed for IDS to overcome dimensionality reduction and comprehensible risk indicators identification or extraction. This technique comprises first fuzzy class memberships created from raw data in a fuzzy allocation section followed by a feature Vec2im (vectors to images) conversion section. Siamese CNN is used to reduce dimensions 1-d feature space. NSL-KDD dataset was evaluated for experimental analysis, which resulted in the inaccuracy of 86.64%. This research aimed to exploit transform images as visual analytics systems in present IDS and could be used to evaluate complex data like healthcare [11, 23, 24].

3. Intrusion Detection System (IDS)

IDS are the systems that automatically detect and analyze the abnormal and intimidating behavior within a host or network to monitor security and protection. Simply intrusion detection detects the invasion. Sometimes, it identifies the instructions for evidence in some situations. Intrusion is the eccentricity of the network or computer from normal conduct and means a threat used to attack for stealing or damage the network data [25–27]. Currently, people use the Internet and other networks to share and store confidential data. [5] presents that IDS is an application of cybersecurity used by a firewall and antivirus software.

Moreover, the firewall limitedly analyzes the online traffic. Though IDSs can control, monitor, and maintain all networks flow even when irregular behavior or threats attacks happen within the networks, it causes an alert for network administrators. Figure 2 shows network communication flow along with intrusion detection systems across the networks [28, 29].

IDSs mainly comprise three segments. First, cyberattack evidence data is collected from input data and then processed to analyze and detect the second segment's cyberattacks. Finally, in the third segment, the attacks are reported. Machine and deep learning-based techniques were recently utilized to predict normal and abnormal behaviors and new unidentified attacks within the networks through input data analysis. The IDSs techniques could be classified into various types, for example, signature-based intrusion detection systems (SIDS), anomaly-based intrusion detection systems (AIDS), specification-Based Detection, hybrid-based detection, host-based IDS (HIDS), network-based IDS (NIDS), and distributed-based IDS (DIDS) [30, 31].

3.1. Signature-Based Intrusion Detection Systems (SIDS). SIDS is also called knowledge-based detection. It analyzes and evaluates networks based on renowned patterns or corresponding signatures for finding attack signatures in the signature databases by comparing network communication and activities. It stores the behavior and signature of each attack within a network [32, 33]. An alert is produced when the attack signature is found or matched with the stored signature database. It means that SIDS only detects the attacks whose signature is stored in a database. New attacks

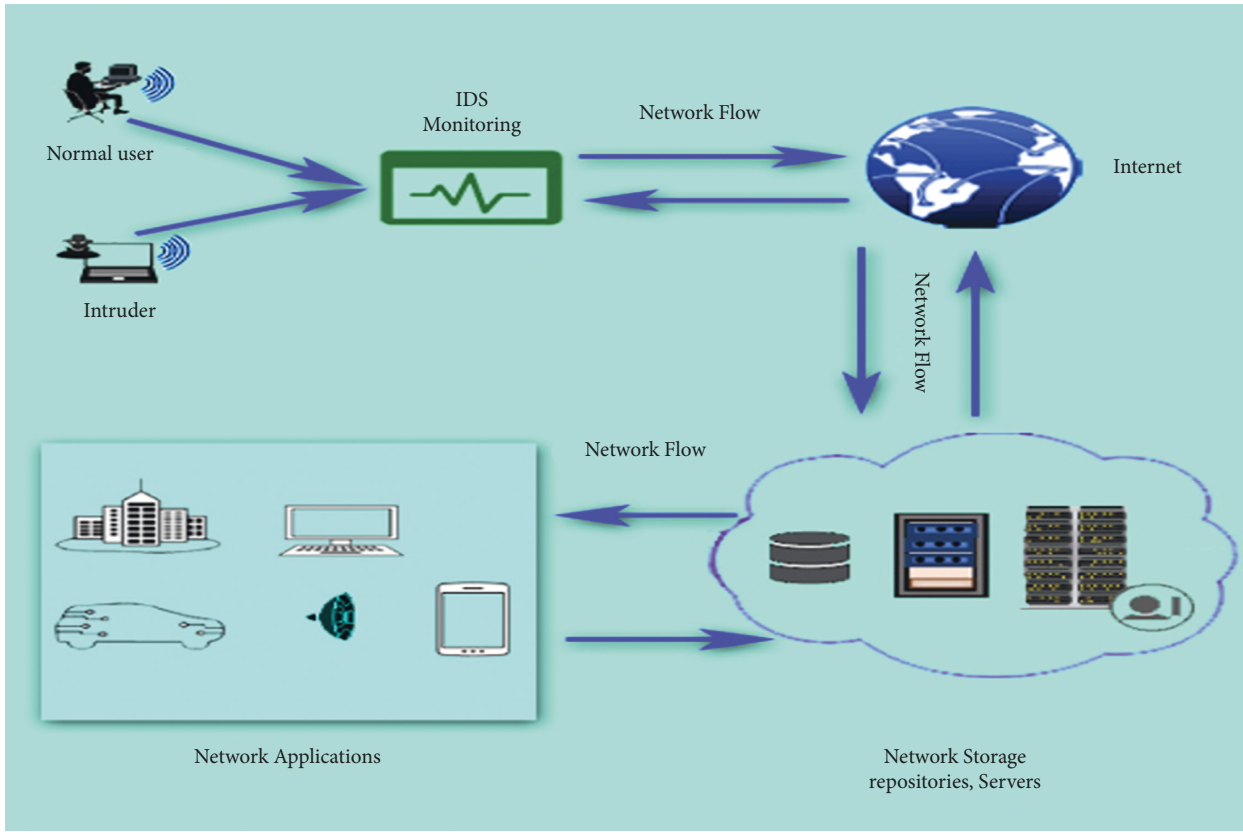

Figure 2: Network flow across the networks along with IDS.

are detected using SIDS, while it is not as accurate in the contradiction of attack variations. The alert system minimizes false alerts due to effective and accurate misbehavior identification and classification to assess network administrators' taking defensive actions. Still, activities that are not matched with the database are considered unknown irregularities, normal or attack variations. Therefore, SIDS needs persistent knowledge database update for new attack variations. SIDS conventional techniques only analyze packets by comparing with patterns in the database. It does not recognize new attack variations. AIDS (Anomaly-based intrusion detection system) techniques for this issue are possible because it works on profiling the appropriate behavior of attacks [34–36].

AIS (Artificial Immune System) method is used to tackle the SIDS limitation. This technique uses the immune cells model, which works based on attacks pattern or signatures and evaluates these by classification into normal or abnormal. It also detects new signatures by constant system monitoring. Furthermore, Suricata signature IDS based on Linux is employed to resolve the resource constraints problem.

3.2. An Anomaly-Based Intrusion Detection System (AIDS). AIDS, also known as profile-based or dynamic behavior anomaly detection, is the most extensively used model compared to SIDS due to its effectiveness against new attacks. AIDS is commonly used to overcome the limitations of SIDS. Unidentified attacks detection at different stages causes alerts to recognize the exposures and prevent them with possible techniques. AIDS monitors the system consistently to collect data for detection and recognition of normal or abnormal. Zero-day attack recognition is the core purpose of AIDS because new anomalous actions are concerned with pattern databases [37, 38]. It can learn abnormal behavior within the networks. For example, if any unauthorized activity occurs or if there is stealing from an account, the alarm is generated. Abnormality behavior is new usual actions, not unaffected intrusions, resulting in a high false-positive rate [39, 40].

Several methods are recently developed and presented in the literature for detecting and classifying abnormal behaviors. It has been studied for the last two decades, but challenges still could not be resolved [41].

3.3. Customized Intrusion Detection Methods. Customized and AIDS work similar, while this technique provides and develops specifications and rules manually to describe normal network activities. The network is monitored according to the proposed set of rules and instructions. It has a minimum false positive rate due to resistance to new attack variations. The customized IDS has limitations due to complexities and restrictions in development, time consumption, and cost [14].

3.4. Hybrid Intrusion Detection Methods. These methods, also known as compound detection, have been developed by combining anomaly, misuse, and specification detection techniques to overcome the deficiencies and enhance the detection of existing and new attack behavior. For example, SVELTE IDS technique was developed using the hybrid technique (SIDS and AIDS) for 6LoWPAN networks in IoT connected through IP. This hybrid technique was developed to accomplish the stability of these techniques' storage, processing, cost, and complexity.

DSNSF (digital signature of network segment using flow analysis) developed for new and unidentified attacks within networks communication and revealed misbehavior signatures were classified as port scan, flash crowd, Dos, or DDoS attack [12].

3.5. Host-Based IDS (HIDS). The HIDS is software installed on the network's host computer that examines, analyzes, gathers, and monitors the data actions consistently within the network and host network by inspecting firewall, server, or database logs. HIDS is limited to detecting a single host's abnormal attacks while detecting uninvolved attacks within the network [13].

3.6. Network-Based IDS (NIDS). NIDS monitors network communications by gathering packets capture and others through NetFlow. Its basic purpose is to secure the networks from the exterior attacks causing an alert/alarm when a malicious attack happens. This IDS works with multiple hosts across the networks and external firewalls by monitoring and analyzing network communications using software or hardware. Software is installed on servers for monitoring, while sensors are attached to servers to analyze the network's communications. As a result, NIDS is very effective and secured in detecting malicious attacks.

NIDS has several limitations; it cannot process and analyze the huge network data due to high bandwidth and speed traffic flow. NIDS is also incapable of encrypted network packets [14].

3.7. Distributed IDS (DIDS). DIDS comprises several different IDS on a broad network to analyze communication monitoring management, malicious attack information, and incident. Information combines using multiple sensors (NIDS and HIDS based) and a central analyzer to manage intrusion detection and prevention [42].

4. Deep Learning (DL) Techniques for IDSs

Deep learning techniques are better in the case of large datasets than Machine learning-based techniques. Deep learning techniques have grown into the most applicable and widely used intrusion detection system in networks. Deep learning, a type of machine learning, is frequently used in cybersecurity because it can discover previously undiscovered patterns in raw data. It finds higher-level characteristics via many layers of modifications [43, 44]. Deep learning addresses all pattern recognition challenges on massive databases. It automatically employs many hidden layers to select the best features for pattern recognition. Deep learning entails the simultaneous selection of features and training, whereas traditional machine learning requires feature extraction first, followed by training and testing. Deep learning has several subtypes [45, 46]. The topology of a feed-forward neural network is the basis for deep learning models. Typically, deep learning comprises an input layer, a hidden layer/layers, and an output layer. Features are inferred via layers dubbed hidden layers. The input layer is fed a property vector representing the item to be categorized as an input. The output layer generates the class vector for the input vector. Deep learning lowers the cost function and executes the learning process by altering the weight values using a backpropagation technique. First, the system gives an input vector and weights, and the error rate is calculated by comparing the output to the desired output [47, 48].

Following that, the error rate is reduced by backpropagating the weights. Moreover, deep learning techniques accomplished complicated features through automatic models' execution. DL is elevated from Artificial Intelligence that can learn unlabeled and labeled data in the supervised and unsupervised way. Numerous DL techniques have been developed for recognition and classification [49, 50]. However, this research work describes DL techniques for intrusion detection. Several deep learning techniques such as Recurrent Neural Networks (RNNs), Deep Neural Networks (DNNs), Convolutional Neural Network (CNN), Deep Autoencoders (AEs), Restricted Boltzmann Machine (RBM), Deep Belief Network (DBN), Generative Adversarial Network (GAN), Ensemble of DL Networks (EDLNs), and more [51, 52]are described. Figure 3 demonstrates the general structure of IDS based on deep learning.

5. Datasets

Deep learning-based IDSs require a dataset for the evaluation of intrusions. Appropriate data construction for training the model is significant and complex due to labeled normal and abnormal communication and other features like IP address [53, 54]. In addition, some network packet-based analysis datasets are not reported publicly due to security issues. However, broadly used publicly available datasets are described in this section. Table 1 shows the different types of attacks and total numbers of records for each dataset. Figure 4 describes the different IDS and attack types.

DARPA (Defence Advanced Research Project Agency) dataset was developed in 1998. It contains audit logs and network traffic of seven weeks of training and two weeks of test data of network-based attacks. However, the drawback of DARPA dataset is not to signify the real-world network traffic [55].

KDD CUP (Knowledge Discovery and Data Mining) dataset is originated from DARPA dataset that reported around 5 million suspecious activity evaluation within seven weeks of network traffic. This dataset is the updated variation

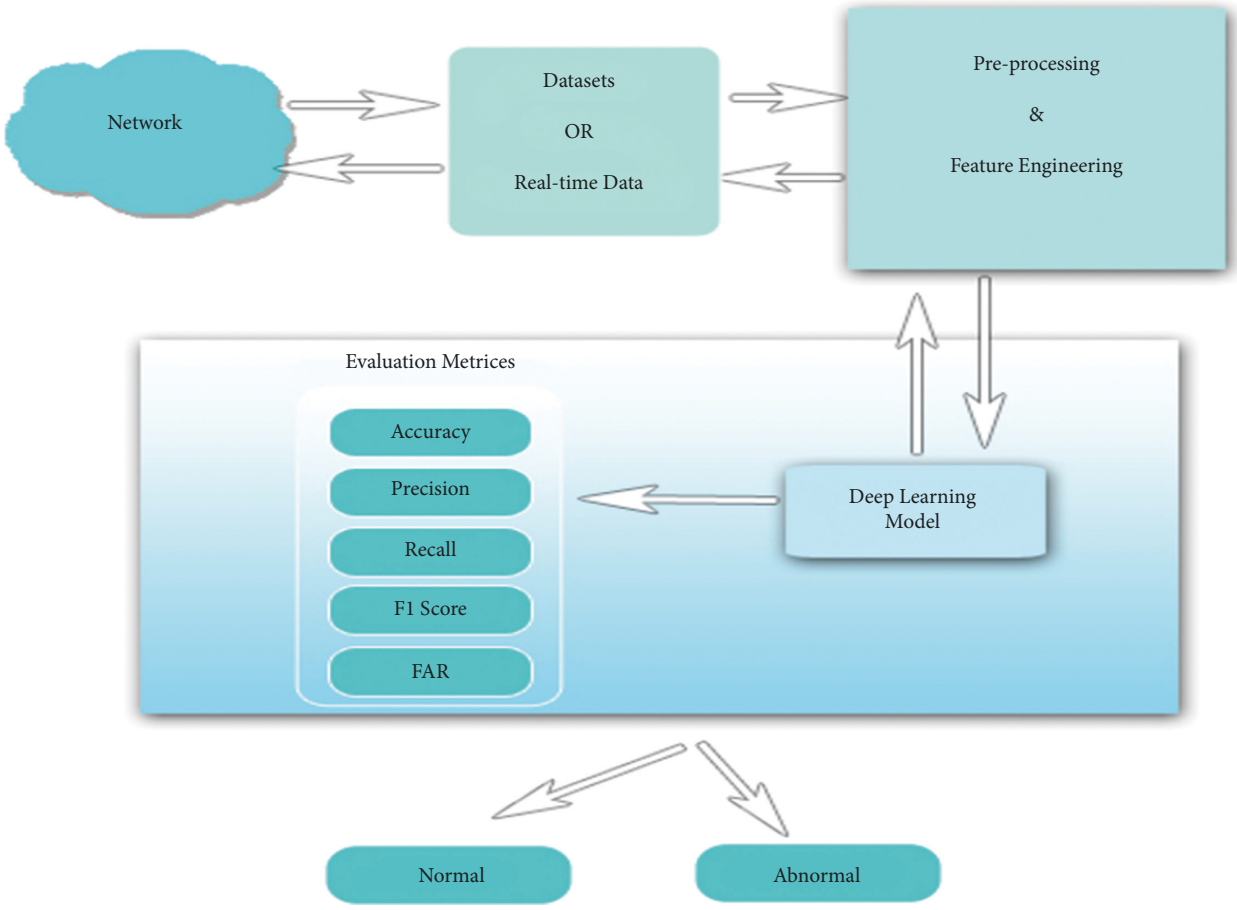

Figure 3: General architecture of deep learning-based IDS.

Table 1: Network datasets along with different attacks and numbers of total records (train and test).

Ref.	Dataset	Attacks	Total records
[26]	AWID	Deauthentication, disassociation, re association, rogue AP, krack, Kr00k, SSH brute force, botnet, malware, SQL injection, SSDP amplification, Evil_Twin, Website_spoofing	2,371,218
[27]	CICDS 2017	Brute force, DoS, heartbleed, web attack, infiltration, botnet and DDoS	2,830,108
[28]	KDD CUP 99	DoS, R2L, U2R, probe	1,152,281
[28]	NSL-KDD	DoS, R2L, U2R, probe	1,152,281
[29]	UNSW-NB15	DoS, fuzzers, analysis, backdoors, exploits, generic, reconnaissance, shellcode, worms	257,673
[30]	Bot-IoT	DDoS, DoS, OS and service scan, keylogging and data exfiltration attacks	72.000.000

of IDSs evaluation to distinguish the normal and malicious attack networks led by Lincoln Laboratory, Massachusetts Institute of Technology (MIT). It comprises 41 basic, traffic and content features classes. The attacks are also characterized based on R2L (Remote to Local attack), U2R (User to Root attack), DoS (Denial of Service attack), and Probing attack. It has been a broadly used dataset for the last two decades to evaluate IDSs techniques and most effective inaccuracy. This dataset's limitations include oldness, no stability in training and test data, maximum twisted targets, inappropriate features, and redundant patterns [56]. NSL-KDD datasets was developed to resolve the limitations of the KDD dataset. This dataset was enhanced and more stable than KDD, with no redundancy. Records are accurate, arranged in percentage form and rational. However, this dataset is still limited due to no detection of low footprint attacks [57].

DEFCON Dataset has two versions DEFCON-8, proposed in 2000 and DEFCON-10 in 2002. The DEFCON-8 version includes port scanning and buffers overflow-based attacks, while another version comprises of FTP protocol attacks, bad packet, ports scan, and sweeps attacks. This dataset is limited because real-time and normal traffic differs during CTF (Capture the Flag) competition, which causes the IDS evaluation. CAIDAs (Center of Applied Internet Data Analysis) dataset developed by Center of Applied Internet Data Analysis covers three different datasets, CAIDA Internet traces 2016, CAIDA DDOS, and RSDoS

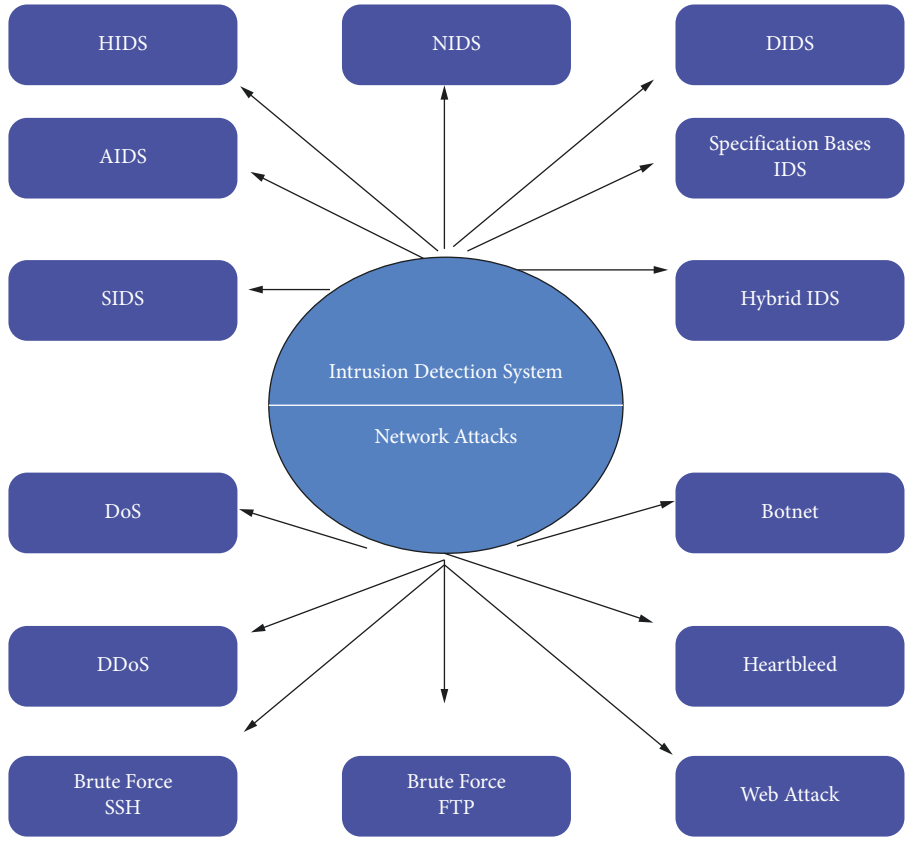

Figure 4: Different network IDS and attacks types.

Attack Metadata (2018-09). Explicitly it is monitored on the fast Internet network CAIDA's Equinix-Chicago traced passive traffic. 5-minute pcap files division was obtained from traffic of a one-hour DDoS attack. UCSD Network Telescope gathered backscatter packets of incidental spoofed DoS attacks. This dataset is inaccurate due to several disadvantages, attack variations, ground truth inaccessibility, and the lack of features collection from network cause normal and malicious communication classification difficult [3]. CIDS 2017 dataset was developed in 2017, including normal and malicious attacks like Brute Force SSH, Brute Force FTP, DoS, DDoS, Web Attack, Heartbleed, and more. Eighty features are collected from network traffic through the CIC Flow Meter tool and 25 users' intangible actions were extracted based on FTP, HTTP protocols. The features are labeled on the source and destination IPs, timestamp, source and destination ports, and attacks and protocols [58].

ISCX IDS dataset was proposed by the Information Security Center of Excellence in 2012 to implement and analyze network intrusion and attacks detection strategies implementation and analysis. It contains one-week network analysis for normal and abnormal behavior (Inside attacks, DoS, DDoS, and Brute Force SSH) of HTTP, FTP, SMTP, IMAP, SSH, and POP3 protocols. Datasets include 17 properties and labeled as approximately 1512000 packets with 19 features. LBNL (Lawrence Berkley National Laboratory) developed a dataset through uPMU by collecting two routers' traffic flow inside, outside the network. 120 Hz, 12 streams were generated using micro-phasor measurement units. This dataset comprised 79,000 flows without having abnormal behavior. Traffic flow is not categorized as normal or abnormal, and the labels only present communication through application protocols [13]. Novel Bot-IoT dataset is proposed for IoT networks in Cyber Range Lab, center of UNSW Canberra Cyber. It consists of DoS, DDoS, OS, Service Scan, Data exfiltration, and Keylogging attacks in more than 72.0 0 0.0 0 0 records. It also includes combined normal and botnet traffic. A lightweight MQTT network protocol is used for M2M communication and Node-red tool used for network activities simulation [3]. Table 2 provides open access links of benchmark datasets.

6. Discussion

With the rise of applications and users on networks, security is a major concern for the network systems. Physical layer problems include physical damage, device failure, and power constraints. Network layer issues include denial of service assaults, sniffer, gateway attacks, and illegal access. Numerous IoT devices rely on self-security systems and so are vulnerable to different attacks. The authentication issue and physical threats are the initial obstacles that an IoT system must overcome. Confidentiality concerns exist between IoT devices and the network layer gateways. Next category of security problems is concerned with the integrity of data sent between services and applications. Data integrity issues arise

Table 2: Datasets and their access links.

Dataset	Access links
AWID	https://icsdweb.aegean.gr/awid/awid3
CICIDS2017	https://www.unb.ca/cic/datasets/ids-2017.html
LBNL	https://icir.org/enterprise-tracing
KDD CUP 99	https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
NSL-KDD	https://www.unb.ca/cic/datasets/nsl.html
CAIDA	https://www.caida.org/data/overview/
UNSW-NB15	https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/
Bot-IoT	https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php

when a network system is compromised by spoofing attacks or noise. DoS, DDoS, and probing assaults are examples of arbitrary attacks that may compromise IoT systems and services. The fourth category of issues is concerned with privacy. Privacy of data is a critical component of security in IoT systems. Different IoT components employ various item identification methods; as a result, each thing has its unique identification tag that contains personal, location, and movement data [59, 60].

This section critically evaluates deep learning techniques for intrusion detection and prevention in existing systems and networks based on performance measures such as accuracy, precision, recall, *f* measure, FAR, classification, and misclassification rate.

A novel IDS based on DNN (deep neural network) was implemented to overcome the challenges of modern complicated security-related networks and advancement in attacks. The proposed technique is designed to resolve the issue of overfitting. IDS manages the communication of normal and abnormal behavior within the networks. The KDD99 dataset had been preprocessed and normalized through mean and standard deviation. ReLU (Rectified Linear Unit) and softmax are applied as the activation function for hidden layers and the last layer due to the complex classification process. Stochastic technique Adam optimizer is applied as backpropagation and loss function was calculated. Softmax was evaluated as a classifier to distinguish normal and abnormal attacks amongst multiple classes. The experimental analysis reported accuracy and loss function of 99.91% and 0.005%, respectively, in numerical data type. While accuracy and loss function of 99.78% and 0.015%, respectively, were reported for mix data type. This research explored the proposed technique using feature extraction methods for efficiency and consistency enhancement [19]. Deep image learning based on DCNN was proposed for anomaly detection, classification, and characterization. This research work is categorized in feature selection and model layers. 80 Features are extracted through CICFlowMeter by computing CICIDS2017 and CSECIC-IDS2018 datasets. Best features are selected for generating 2D gray images after forest tree computation, followed by ranking features used as CNN input. A vector of 9×9 was produced in the model layers section.

A novel technique TSDL (two-stage deep learning) was developed due to new attack variations prevention. The method used for NIDS is through stacked autoencoder and a softmax classifier. There are two mechanisms. First, the probability score value is used for classifying the records as normal or abnormal, followed by using it in the second step for normal and other attack classes detection as an additional feature. This technique effectively learns efficient representation of features from large-scale unlabeled records. The experimental analysis reported a better efficacy and recognition rate by evaluating two open-source datasets, UNSW-NB15 and KDD99. The accuracy in KDD99 and UNSW-NB15 datasets was shown 99.996% and 89.134%. The critical analysis based on the KDD99 dataset in terms of normal and abnormal classes presents 87785 records classified as normal while 53 records were misclassified. 57701 records were classified as abnormal, while 47 records were misclassified. Overall, 145,486 out of 145,586 records were classified. Other performance matrices, e.g., precision, recall, F-measure, and FAR (False Alarm Rate) for two classes, 99.93%, 99.93%, 99.93%, and 0.0007% were reported. In the case of multi-class attacks (normal, DoS, U2R, Probe, and R2L) analysis of the KDD99 dataset, 145,580 records out of 145,586 were accurately classified. Other performance matrices include precision, recall, F-measure, and FAR (False Alarm Rate) for multi-classes, 99.99%, 99.99%, 99.99%, and 0.0000001% were reported.

The critical analysis based on the UNSW-NB15 dataset regarding normal and abnormal classes presented those 108540 records were classified as normal while 15874 records were misclassified. 103467 records were classified as abnormal while 8442 records were misclassified. Overall, 212,007 out of 236,323 records were classified. Other performance matrices include precision, recall, F-measure, and FAR (False Alarm Rate) for two classes, 89.74%, 89.59%, 89.79%, and 0.1015 d. In case of multi-class attacks, (Anal., Back., DoS, Exp., Fuzz., Gene., Norm., Reco., Shell, and Worm.), analysis of UNSW-NB15 dataset 210,643 records out of 236,323 records were classified. Performance matrices such as precision, recall, F-measure, and FAR (False Alarm Rate) for multi-classes, 89.130%, 63.270%, 90.85%, and 0.00750% were reported. The research aimed to design and explore DL multitasking and reinforcement learning techniques to enhance the developed NIDS [21]. An autonomous and smart IDS was implemented for dynamic security of networks to be capable of zero-day attack detection. The proposed technique was designed to decrease the manual work. It is comprised of different techniques: GRU (gated recurrent unit), CNN (convolutional neural network), and RF (random forest). Snort and Bro IDS tools store and analyze solo connection network packets followed by extracting features. The features were classified as

Table 3: Deep learning techniques-based IDS evaluation on different performance metrics.

Ref.	Technique	Database	Loss	Accuracy	Precision	Recall	F1 score	FAR	Classified records	Misclassified records	Total records
[19]	DNN, ReLU and softmax	KDD99 (numerical data type)	0.005%	99.91%	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported
		KDD99 (mix data type)	0.015%	99.78%	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported
[20]	Image-based DCNN	CICIDS2017	Not reported	99%	Not reported	Not reported	Not reported	Not reported	98.7%	1.3%	100%
		CSE-CIC-IDS2018	Not reported	97.5%	Not reported	Not reported	Not reported	Not reported	3,164,103	81,954	3,246,057
[21]	TSDL	KDD99	Not reported	99.996%	99.99%	99.99%	99.99%	0.0000001%	145,580	6	145,586
		UNSW-NB15	Not reported	89.134%,	89.130%	63.270%	90.85%	0.00750%	210,643	25680	236,323
[22]	Autonomous IDS based on RNN, GRU, CNN and RF	KDDTest+	Not reported	87.28%	Not reported	Not reported	Not reported	Not reported	19,676	2867	22,543
		KDDTest-2	Not reported	76.61%	Not reported	Not reported	Not reported	Not reported	90,79	2771	11,850
[23]	CNN	NSL-KDD	Not reported	Not reported	99.68%	92.48%	95.94%	Not reported	Not reported	Not reported	Not reported
[24]	DNN	CICIDS2017	0.0289	99.29%	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported
[6]	Auto-IF	NSL-KDD	Not reported	95.4%	94.81%	97.25%	96.01%	Not reported	Not reported	Not reported	Not reported
[32]	NN	NSW-NB 15	Not reported	92%	92%	92%	Not reported	Not reported	Not reported	Not reported	82,332
[32]	PCA + DNN [rFGSM]	NSW-NB 15	Not reported	93.9%	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported	82,332
[33]	Autoencoder	NSL-KDD	Not reported	92.96%	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported
[34]	MLP DNN	Drebin	Not reported	77.2%	Not reported	Not reported	Not reported	Not reported	Not reported	Not reported	5,560

normal or malicious by applying multiple classifiers including RNN, GRU, CNN, and RF and concatenating their votes and logic. The results display their method could detect new malicious attacks through automatic learning. However, in case of attack misclassification, automatic learning will manage it in the future. The experiments are conducted on the NSL-KDD dataset, 87.28% and 76.61% accuracy claimed for KDDTest+ and KDDTest-. This research achieved better performance and enhanced to overcome training time and accuracy, but it is still limited to real-time networks and attack types detection [22, 33].

A new technique based on deep learning was proposed for error rate reduction during the training procedure. The proposed technique was designed in two major stages: first in preprocessing step, the unwanted data or redundant data were reduced through the Threshold-based ranking technique to achieve better efficacy. CNN model was evaluated along with different gradient optimization approaches such as Adaptive Moment Estimation (Adam), Adaptive Gradient Moment (Adagrad), Root Mean Squared Propagation (RMSProp), and Adaptive Delta Moment (Adadelta), for error minimization. NSL-KDD dataset evaluated for experimental purpose. The comprehensive analysis reported 99.68%, 98.56%, 93.81%, and 91.93%, for Adam, RMSProp, Adadelta, and Adagrad. While overall recall of 92.48%, 90.08%, 89.17% and 83.20% was reported, respectively, for Adam, RMSProp, Adadelta, and Adagrad. Overall f1-score of 95.94%, 93.87%, 89.27%, and 87.27 was reported, respectively, for same algorithms. The results show that the Adam approach is better in performance than other optimization approaches. This research investigates intrusion identification using AI techniques to learn advanced attacks and their prevention [34, 35].

DNN model-based IDS was implemented for big data in large-scale networks security. The big network datasets evaluation is still challenging. The proposed technique uses two stages: first, the imbalance data of the CICIDS2017 dataset was analyzed by extracting and selecting the best features, then eliminating redundant records, normalizing, stabilizing, and label encoding of data. Because the dataset comprised of 79 labeled and imbalanced attributes and classes of real-world data, DNN model was employed for classification in the second stage. The dataset was categorized into different attacks, for example, DoS, DDoS, Web, Infiltration, Botnet, Heartbleed, and Brute force. The dataset was modified for experiments to evaluate the model as flow and packet-based. The experiments exhibited that the model achieved a better recognition rate and loss of 99.13%, 0.0232 and 99.29%, 0.0289, respectively, for binary and multi-classification. ROC (Receiver operating characteristics) score reported as 100%. This research is limited due to minimum data for several attacks such as Web, Infiltration, and Heartbleed. That is why the technique could not classify it. The study aimed for low records issue detection [24]. SRU-DCGAN (simple recurrent unit and deep convolutional generative adversarial networks) model was implemented to resolve big complicated data in large- and high-scale networks for accurate processing and to reduce irregularities of high false positive and negative rates NIDS. This technique uses the raw data for feature extraction to produce new training data. LSTM (long short-term memory) is applied for automatic feature learning of network intrusion activities. Due to the LSTM limitation, the SRU is implemented for dependency elimination and real-time intrusion permitting. The Mahalanobis distance approach was applied to map the data into the 2D vector in the preprocessing stage. The output is used as input for the DL network. KDD99 and NSL-KDD datasets were used for experimental analysis, resulting in 99.73% and 99.62% accuracy. CICIDS2017 was also evaluated for intrusion detection of each attack type. The comparison reported that in the KDD99 and NSL-KDD datasets, the ML techniques achieve up to 94% and 83% of accuracy [25].

7. Conclusion, Challenges, and Possible Solutions

Intrusion detection systems are improved along with the emergence of large-scale, high-dimension IoT and computer networks. The network applications are grown and easily accessible. Therefore, it faces many data security, privacy, confidentiality, and reliability challenges. Numerous intrusion detection systems are discussed and analyzed in this research. Additionally, deep learning-based IDS for network challenges have been comprehensively analyzed. The detailed study on IDS methodologies, types (SIDS, AIDS, NID, HIDS, DIDS, and more) and technologies with their advantages, limitations, and network-based public datasets are analyzed in depth. Deep learning techniques for intrusion detection and prevention evaluation in state of the art and networks environments are also evaluated on different performance measures such as accuracy, precision, recall, *f* measure, FAR, classification, and misclassification rate.

Future challenges and possible solutions are described as follows:

(i) Parallel processing of amalgamed distributed data gathering was supposed for intrusion detection contributes better performance for the challenges in research studies of real-time detection, big data processing frameworks, and high-data throughput rates.

(ii) The challenges in the technical model are features, labels, and instances based. Noisy data, redundant and weakly correlated data are feature-based challenges. Too few labeled data and imbalanced data are labels' challenges, while big data, dynamic and small data are the challenges of instances. Solutions are also provided. Some are implemented for these challenges: feature normalization and density-based clustering, redundancy elimination methods, feature selection, autoencoder, and dimensionality for noisy, redundant, and weakly correlated data. Adversarial sample generation, transfer learning, oversampling and under-sampling, genetic programming, optimal feature extraction, Siamese neural network, and feature fusion are solutions to too few labeled data and imbalanced data challenges. Incremental, meta, transfer and

reinforcement learning, parallelism and multithreading cloud computing, data reduction, stream data techniques are solutions to big, dynamic, and small data challenges.

(iii) In anomaly detection, normality, adaptability, dynamic profile update, noisy data, false alarm rates, and complexity are the main challenges of creating a precise idea of normality. Intrusions are consistently changing or updating with time; therefore, IDS needs to update continuously. In addition, false alarm rate needs to be eliminated or minimized, but it is still a challenge to avoid it.

Data security, infrastructure, and real-time update issue, computational restriction, and algorithms exploitation and privacy leakage challenge IoT-based networks. Data augmentation techniques were supposed to create more accurate and reliable datasets for training the ML and DL models. Robust software infrastructure must be developed for IoT network security. Security measures must be included at every level of the IoT system, from hardware to software, to provide a secure environment. IoT devices must be able to deal with massive data volumes with few resources.

Additionally, when machine learning algorithms are integrated into an IoT system, they increase the system's computational complexity. As a result, systems are slowed down. Therefore, it is necessary to reduce complexity via artificial intelligence algorithms. Actually, common users have no idea what, how, or where their personal information has been shared. All IoT devices adhere to fundamental security procedures, including authentication, encryption, and security upgrades. As a result, IoT devices must encrypt messages before sending them via the cloud to ensure their confidentiality. However, privacy protection must be a primary issue when designing IoT devices. As further work, this study will be extended to provide comprehensive security, privacy, and cyber-attacks frameworks in IoT-based innovative environments since much enhancements are still required.

Data Availability

The dataset employed in this review article will be provided from the author on reasonable request.

Conflicts of Interest

The authors declared no conflicts of interest for this research.

Acknowledgments

This research was technically supported by Artificial Intelligence and Data Analytics Lab (AIDA) CCIS Prince Sultan University, Riyadh, Saudi Arabia.

References

[1] A. Y. Khan, R Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, "Malicious insider attack detection in IoTs using data analytics," in *Proceedings of the IEEE Access*, vol. 8, pp. 11743–11753, December2019.

[2] Y. He, H. U. Khan, K. Zhang et al., "D2D-V2X-SDN: Taxonomy and Architecture towards 5G mobile Communication System," in *Proceedings of the IEEE Access*, November 2021.

[3] S. Naeem, N. Jamil, H. U. Khan, and S. Nazir, "Complexity of deep convolutional neural networks in mobile computing," *Complexity*, vol. 2020, Article ID 3853780, 2020.

[4] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, "Enterprise credential spear-phishing attack detection," *Computers & Electrical Engineering*, vol. 94, Article ID 107363, 2021.

[5] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[6] Y. Ali and H. Ullah Khan, "GTM approach towards engineering a features-oriented evaluation framework for secure authentication in IIoT environment," *Computers & Industrial Engineering*, vol. 168, Article ID 108119, 2022.

[7] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper-based feature extraction for wireless intrusion detection system," *Computers & Security*, vol. 92, Article ID 101752, 2020.

[8] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, Article ID 102031, 2020.

[9] J. Yang, Y. Sheng, and J. Wang, "A GBDT-paralleled quadratic ensemble learning for intrusion detection system," *IEEE Access*, vol. 8, pp. 175467–175482, 2020.

[10] W. Liu, L. Xu, D. Xiaoqiang, and H. Qi, "A novel network intrusion detection algorithm based on Fast Fourier Transformation," in *Proceedings of the 2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, pp. 1–6, IEEE, Shenyang, China, July 2019.

[11] I. Abunadi, A. A. Albraikan, J. S. Alzahrani et al., "An automated glowworm swarm optimization with an inception-based deep convolutional neural network for COVID-19 diagnosis and classification," *Healthcare*, vol. 10, no. 4, p. 697, 2022.

[12] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020.

[13] G. Fernandes, J. J. P. C. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, "A comprehensive survey on network anomaly detection," *Telecommunication Systems*, vol. 70, no. 3, pp. 447–489, 2019.

[14] A. R. Khan, "Facial emotion recognition using conventional machine learning and deep learning methods: current achievements, analysis and remaining challenges," *Information*, vol. 13, no. 6, p. 268, 2022.

[15] S. Sengan, R. H. Jhaveri, V. Varadarajan, R. Setiawan, and L. Ravi, "A secure recommendation system for providing context-aware physical activity classification for users," *Security and Communication Networks*, vol. 2021, 2021.

[16] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT," in *Proceedings of the IEEE Access*, vol. 6, pp. 20085–20103, IEEE, April 2018.

[17] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," *Journal of Infection and Public Health*, vol. 13, no. 10, pp. 1567–1575, 2020.

[18] S. K. Sahu, S. Sarangi, and S. K. Jena, "A detail analysis on intrusion detection datasets," in *Proceedings of the 2014 IEEE International advance Computing Conference (IACC)*, pp. 1348–1353, IEEE, Gurgaon, India, 2014 February.

[19] S. Ahmad, F. Arif, Z. Zabeehullah, and N. Altaf, "Novel approach using deep learning for intrusion detection and classification of the network traffic," in *Proceedings of the 2020 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CMSA)*, pp. 1–6, IEEE, Tunis, Tunisia, June 2020.

[20] G. Kaur, A. H. Lashkari, and A. Rahali, "Intrusion traffic detection and characterization using deep image learning," in *Proceedings of the 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pp. 55–62, IEEE, Calgary, AB, Canada, 2020 August.

[21] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: a two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[22] A. Andalib and V. T. Vakili, "An autonomous intrusion detection system using an ensemble of advanced learners," in *Proceedings of the 2020 28th Iranian Conference on Electrical Engineering (ICEE)*, pp. 1–5, IEEE, Tabriz, Iran, August 2020.

[23] A. R. Gupta and J. Agrawal, "A comprehensive survey on various machine learning methods used for intrusion detection system," in *Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 282–289, IEEE, Gwalior, India, April 2020.

[24] K. Farhana, M. Rahman, and M. T. Ahmed, "An intrusion detection system for packet and flow-based networks using deep neural network approach," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, p. 5514, 2020.

[25] J. Yang, T. Li, G. Liang, W. He, and Y. Zhao, "A simple recurrent unit model-based intrusion detection system with dcgan," *IEEE Access*, vol. 7, pp. 83286–83296, 2019.

[26] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset," in *Proceedings of the IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, February 2016.

[27] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, and A. Abuzneid, "Features dimensionality reduction approaches for machine learning-based network intrusion detection," *Electronics*, vol. 8, no. 3, p. 322, 2019.

[28] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1–6, Ottawa, ON, Canada, July 2009.

[29] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, IEEE, Canberra, ACT, Australia, 2015 November.

[30] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[31] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, p. 21, 2018.

[32] R. Abou Khamis, M. O. Shafiq, and A. Matrawy, "Investigating resistance of deep learning-based IDS against adversaries using min-max optimization," in *Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland*, June 2020.

[33] H. Hindy, R. Atkinson, C. Tachtatzis, J. N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," *Electronics*, vol. 9, no. 10, p. 1684, 2020.

[34] M. Sewak, S. K. Sahay, and H. R. Deepintent, "Implicitintent based android ids with e2e deep learning architecture," in *Proceedings of the 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications London, UK*, August 2020.

[35] M. Li, S. Nazir, H. U. Khan, S. Shahzad, and R. Amin, *Modelling Features-Based Birthmarks for Security of End-To-End Communication System*, Security and Communication Networks, 2020.

[36] A. Rehman, M. Harouni, M. Omidiravesh, S. Mohamed Fati, and S. Ali Bahaj, "Finger vein authentication based on wavelet scattering networks," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 3369–3383, 2022.

[37] O. A. Arqub and Z. Abo-Hammour, "Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm," *Information Sciences*, vol. 279, pp. 396–415, 2014.

[38] Z. Abo-Hammour, O. Abu Arqub, O. Alsmadi, S. Momani, and A. Alsaedi, "An optimization algorithm for solving systems of singular boundary value problems," *Applied Mathematics & Information Sciences*, vol. 8, no. 6, pp. 2809–2821, 2014.

[39] K. Meethongjan, M. Dzulkifli, A. Rehman, A. Altameem, and T. Saba, "An intelligent fused approach for face recognition," *Journal of Intelligent Systems*, vol. 22, no. 2, pp. 197–212, 2013.

[40] S. Roy, T. D. Whitehead, J. D. Quirk et al., "Optimal co-clinical radiomics: sensitivity of radiomic features to tumour volume, image noise and resolution in co-clinical T1-weighted and T2-weighted magnetic resonance imaging," *EBioMedicine*, vol. 59, Article ID 102963, 2020.

[41] M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, "Digital watermarking for images security using discrete slantlet transform," *Applied Mathematics & Information Sciences*, vol. 8, no. 6, pp. 2823–2830, 2014.

[42] R. Sagar, R. Jhaveri, and C. Borrego, "Applications in security and evasions in machine learning: a survey," *Electronics*, vol. 9, no. 1, p. 97, 2020.

[43] H. Yar, T. Hussain, Z. A. Khan, D. Koundal, M. Y. Lee, and S. W. Baik, "Vision sensor-based real-time fire detection in resource-constrained IoT environments," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 5195508, 15 pages, 2021.

[44] I. M. Nasir, M. Raza, J. H. Shah, M. A. Khan, and A. Rehman, "Human action recognition using machine learning in uncontrolled environment," in *Proceedings of the 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA)*, pp. 182–187, IEEE, Riyadh, Saudi Arabia, May 2021.

[45] I. Abunadi and R. L. Kumar, *Blockchain and Business Process Management in Health Care, Especially for COVID-19 Cases*, Security and Communication Networks, vol. 2, 2021.
[46] H. Ullah, N. Gopalakrishnan Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5G communication: an overview of vehicle-to-everything, drones, and healthcare use-cases," *IEEE Access*, vol. 7, Article ID 37251, 2019.
[47] N. Islam, M. Altamimi, K. Haseeb, and M. Siraj, "Secure and sustainable predictive framework for IoT-based multimedia services using machine learning," *Sustainability*, vol. 13, no. 23, Article ID 13128, 2021.
[48] M. Elhoseny, K. Haseeb, A. A. Shah, I. Ahmad, Z. Jan, and M. I. Alghamdi, "IoT solution for AI-enabled PRIVACY-PREServing with big data transferring: an application for healthcare using blockchain," *Energies*, vol. 14, no. 17, p. 5364, 2021.
[49] S. Roy, T. D. Whitehead, S. Li et al., "Co-clinical FDG-PET radiomic signature in predicting response to neoadjuvant chemotherapy in triple-negative breast cancer," *European Journal of Nuclear Medicine and Molecular Imaging*, vol. 49, no. 2, pp. 550–562, 2022.
[50] S. Roy, A. Mitra, S. Roy, and S. K. Setua, "Blood vessel segmentation of retinal image using Clifford matched filter and Clifford convolution," *Multimedia Tools and Applications*, vol. 78, no. 24, Article ID 34839, 2019.
[51] Y. Dagli, S. Choksi, and S. Roy, "Prediction of two year survival among patients of non-small cell lung cancer," in *Computer Aided Intervention and Diagnostics in Clinical and Medical Images*, vol. 31, pp. 169–177, Springer, Cham, 2019.
[52] A. Rehman, S. Alqahtani, A. Altameem, and T. Saba, "Virtual machine security challenges: case studies," *International Journal of Machine Learning and Cybernetics*, vol. 5, no. 5, pp. 729–742, 2014.
[53] S. Roy, D. Bhattacharyya, S. K. Bandyopadhyay, and T. H. Kim, "An iterative implementation of level set for precise segmentation of brain tissues and abnormality detection from MR images," *IETE Journal of Research*, pp. 1–15, 2017.
[54] R. Abbasi, J. Chen, Y. Al-Otaibi, A. Rehman, A. Abbas, and W. Cui, "RDH-based dynamic weighted histogram equalization using for secure transmission and cancer prediction," *Multimedia Systems*, vol. 27, no. 2, pp. 177–189, 2021.
[55] M. H. Ali, M. M. Jaber, S. K. Abd et al., "Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT)," *Electronics*, vol. 11, no. 3, p. 494, 2022.
[56] H. U. Khan, F. Ali, Y. Alshehri, and S. Nazir, "Towards enhancing the capability of IoT applications by utilizing cloud computing concept," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 233531, 14 pages, 2022.
[57] M. H. Ali, M. M. Jaber, S. K. Abd et al., "Harris hawks sparse auto-encoder networks for automatic speech recognition system," *Applied Sciences*, vol. 12, no. 3, p. 1091, 2022.
[58] M. Sharif, F. Naz, M. Yasmin, M. A. Shahid, and A. Rehman, "Face recognition: a survey," *Journal of Engineering Science and Technology Review*, vol. 10, no. 2, pp. 166–177, 2017.
[59] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers & Electrical Engineering*, vol. 99, Article ID 107810, 2022.
[60] M. Yasin, A. R. Cheema, and F. Kausar, "Analysis of Internet Download Manager for collection of digital forensic artefacts," *Digital Investigation*, vol. 7, no. 1-2, pp. 90–94, 2010.