IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 22, 2020, accepted February 21, 2020, date of publication February 27, 2020, date of current version March 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2976624

Security Analysis of Network Anomalies Mitigation Schemes in IoT Networks

MUHAMMAD AMINU LAWAL, RIAZ AHMED SHAIKH, AND SYED RAHEEL HASSAN
Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
Corresponding author: Muhammad Aminu Lawal (mlawal@stu.kau.edu.sa)

ABSTRACT The Internet of Things (IoT) is on the rise and it is giving a new shape to several fields such as smart cities, smart homes, smart health, etc. as it facilitates the connection of physical objects to the internet. However, this advancement comes along with new challenges in terms of security of the devices in the IoT networks. Some of these challenges come as network anomalies. Hence, this has prompted the use of network anomaly mitigation schemes as an integral part of the defense mechanisms of IoT networks in order to protect the devices from malicious users. Thus, several schemes have been proposed to mitigate network anomalies. This paper covers a review of different network anomaly mitigation schemes in IoT networks. The schemes' objectives, operational procedures, and strengths are discussed. A comparison table of the reviewed schemes, as well as a taxonomy based on the detection methodology, is provided. In contrast to other surveys that presented qualitative evaluations, our survey provides both qualitative and quantitative evaluations. The UNSW-NB15 dataset was used to conduct a performance evaluation of some classification algorithms used for network anomaly mitigation schemes in IoT. Finally, challenges and open issues in the development of network anomaly mitigation schemes in IoT are discussed.

INDEX TERMS Classification algorithms, Intrusion Detection System (IDS), Internet of Things (IoT), machine learning, network anomalies, security.

I. INTRODUCTION

Recently, the emergence of a new type of networking paradigm which enables physical objects to communicate with the internet, known as the Internet of Things (IoT) has caught the attention of the research communities and the Information and Communication Technology (ICT) industry. The number of the devices and data generated by the devices in IoT are on a rise, according to a forecast the IoT may have 50 billion units by 2020 [1]. Similarly, according to International Data Corporation (IDC) data generated by the things (devices in IoT) will hit 4.4 Zettabytes by 2020 [2]. The growth of IoT comes along with an increase in different challenges. Some of these challenges often happen as network anomalies i.e. deviations from a normal network traffic flow. According to the definition by Hawkins [3], anomalies can be security or performance-related.

In terms of performance, a network failure, flash crowd or changes in the link traffic can cause anomalies. While in terms of security, attacks such as flooding and probing attacks, User to Root (U2R) and Remote to Local (R2L) attacks can also cause anomalies. This challenge prompted the use of network anomaly mitigation schemes as an integral part of the defense mechanisms of IoT to further protect the devices due to their applications and benefits in our daily activities.

In terms of security, network anomalies in IoT are usually detected through the utilization of Intrusion Detection System (IDS). An IDS is a system (hardware or software) that monitors and inspects the network traffic flow for possible violations of the computer security principles of Confidentiality, Integrity, and Availability (CIA) [4]. Generally, the standard architecture of a Network Intrusion Detection System (NIDS) consists of three major units: data collection and preprocessor unit, analysis unit and response unit [5] as shown in figure 1.

i. The data collection and preprocessor unit: This unit utilizes data analysis tools such as Tcpdump [6] and Wire shark [7] to collect part of the raw data (network traffic). The data is further preprocessed, features to be utilized by the analysis unit for making its decision are selected.
ii. The analysis unit: This unit is an important part of the IDS. It constructs a model of normal network traffic

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

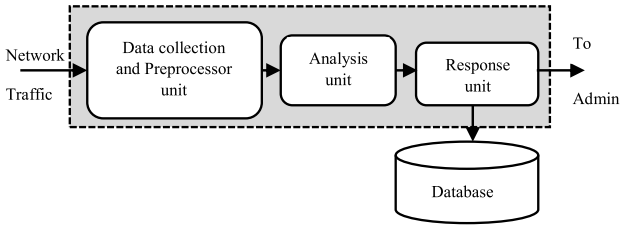

FIGURE 1. Architecture of a network IDS.

flow using the extracted features from the previous unit. It differentiates normal traffic flow from abnormal traffic flow (attack). The analysis unit then prompts the response unit to sends a warning signal when an attack is detected.

iii. The response unit performs the following actions when an attack is detected (a) activates alarms and records them in a database (b) forwards the warnings signal to a security administrator for appropriate action.

The study of intrusion detection systems has been carried out for over three decades [8]. Consequently, it has been an important part of the security mechanism employed in protecting networks with many commercialized implementations available. However, the IDS used in the traditional IP networks is inappropriate for resource-constrained IoT networks due to its operational requirements. Hence, many IDS schemes [27]–[48] have been proposed for IoT networks by several researchers.

In an effort to consolidate the proposed solutions, there are few surveys that have been conducted aimed at reviewing the IDS schemes proposed for IoT networks. Zarpelão *et al.* [9] provided a review of IDS schemes for IoT networks proposed between 2009 and 2016. The authors guided their discussion using a taxonomy that consists of the deployment strategies, detection methodologies, security threats and validation techniques employed in IDS for IoT networks. A summary of the reviewed schemes was also presented in a table. Another survey by Benkhelifa *et al.* [10] gives a review and comparison of IDSs for IoT based on architectural deployments, detection techniques, and technology coverage (Bluetooth, WSN, 6Lowpan, etc.) employed. The authors further proposed an intrusion detection system architecture for IDS in IoT which encompasses the entire IoT model (three-layer). Chaabouni *et al.* [11] presented a survey of IDS solutions for IoT based on traditional and machine learning techniques. The survey elaborates on the IDS implementation tools and datasets used for evaluation. Furthermore, a review and comparison of IDS schemes for IoT systems based on learning techniques with a focus on deployments, detection techniques as well as attacks treated by each scheme is presented. Elrawy *et al.* [12] provide a review of IDS solutions for IoT based systems in a smart environment. The surveys focus on detection methods, features and the mechanism of the proposed schemes. The authors also presented a comparison and descriptive statistical analysis of the reviewed schemes.

In summary, the aforementioned surveys discussed the general IoT network landscape, architecture, standards, and protocols as well as a review of the proposed IDS schemes for IoT. All the surveys focus on common points which are: deployment architecture, detection methodology, security threats and validation techniques employed in the schemes. Additionally, qualitative evaluations on the proposed IDS schemes were presented. Open and future research issues were also highlighted. However, none of the surveys provided a quantitative evaluation.

In this paper, similar to the abovementioned surveys we focus on IDS schemes for IoT networks. An overview of the IoT concept, security threats, and IDS will be discussed. A review of some proposed state of the art IDS schemes in IoT network will be provided with emphasis on the objectives, operations, and strengths of each scheme. In addition, a hierarchal taxonomy based on the detection methodology will be presented along with a comparison table of the reviewed schemes. Largely, intrusion detection or anomaly detection issues are classification problems i.e. distinguishing between normal and abnormal network traffic. Hence, unlike the other surveys, our survey will include both qualitative and quantitative evaluations. Performance evaluation of some machine learning algorithms (classification algorithms) used in network anomaly mitigation schemes in IoT will be presented.

Table 1 provides a comparison of the surveys on IDS in IoT networks. The comparison is in terms of the outcome of the review and evaluation of the IDS schemes for IoT networks in each survey.

The organization of the remaining paper is described in figure 2. Section 2 provides a background on the three related domains, which are the Internet of Things (IoT), security threats (general and examples of real incidents) in IoT networks and defines Intrusion Detection Systems (IDS) and its types. Section 3 provides a taxonomy of IDS schemes in IoT networks, which will guide a reader through a review of the proposed IDS schemes as well as comparison tables. Section 4 provides the performance analysis of some common and effective approaches that were identified in Section 3, it discusses the dataset utilized, algorithms employed for evaluation, performance metrics evaluated as well as the results and discussions. Based on the findings of section 3 and section 4, future research issues and problems are discussed in Section 5. Finally, section 6 concludes the paper.

II. BACKGROUND

This section provides a brief overview of the IoT concept, security threats and examples of real-life incidents as well as the intrusion detection systems and its categories.

A. OVERVIEW OF IoT CONCEPT

The IoT can simply be referred to as a network where physical objects (things) can communicate with the internet. The root of this concept can be traced back to 1999 when the Auto-ID center was developed at Massachusetts Institute of Technology (MIT). In 2003, the centre utilized the Radio Frequency

TABLE 1. Comparison of surveys.

S/No	Authors	Strengths	Shortcoming
1.	Zarpelao et al. [9]	-Reviewed and performed qualitative evaluations of 18 schemes published during the period 2009 to 2016. -Highlights open issues and future directions.	-No performance evaluations. -Comparison based on 4 attributes
2.	Benkhelifa et al. [10]	- Reviewed and performed qualitative evaluations of 31 schemes published during the period 2008 to 2017.	-No performance evaluations. -Comparison based on 4 attributes
3.	Nadia et al. [11]	- Reviewed and performed qualitative evaluations of 18 schemes published during the period 2013 to 2018. - Highlights open issues and future directions.	No performance evaluations.
4.	Elrawy et al. [12]	- Reviewed and performed qualitative evaluations of 22 schemes published during the period 2011 to 2018. - Highlights open issues and future directions	-No performance evaluations. -Comparison based on 4 attributes
5.	Our paper	- Reviewed and performed qualitative evaluations of 37 schemes published during the period 2012 to 2019. - Highlights open issues and future directions.	

Identification (RFID) as a pillar to create an electronic product code number [12], it serves as a critical point in the IoT journey. The IoT has been described and defined in different ways by several organizations as highlighted in [13], [14].

In regards to the architectural framework of the IoT, the generic three-tier architecture which includes: perception (sensing) or physical layer, network or transport & communication layer and application layer is widely adopted as there is no standard architecture available yet [15].

The perception or physical layer deals with data collection from the physical environment. Generally, short-range communication such as Bluetooth and IEEE 802.15.4 with limited data rates and sensing devices such as RFID, GPS are utilized at this layer. The network or transport and communication layer deal with the transmission of the data collected at the perception layer to the application layer. Technologies for longer distance communication such as IEEE 802.3, IEEE 802.11 4G, etc. are used in this layer. The application layer deals with the processing and management of the data collected to acquire meaningful information about the sensed data. This information is often used by applications and physical objects to make decisions. At this layer, middleware is

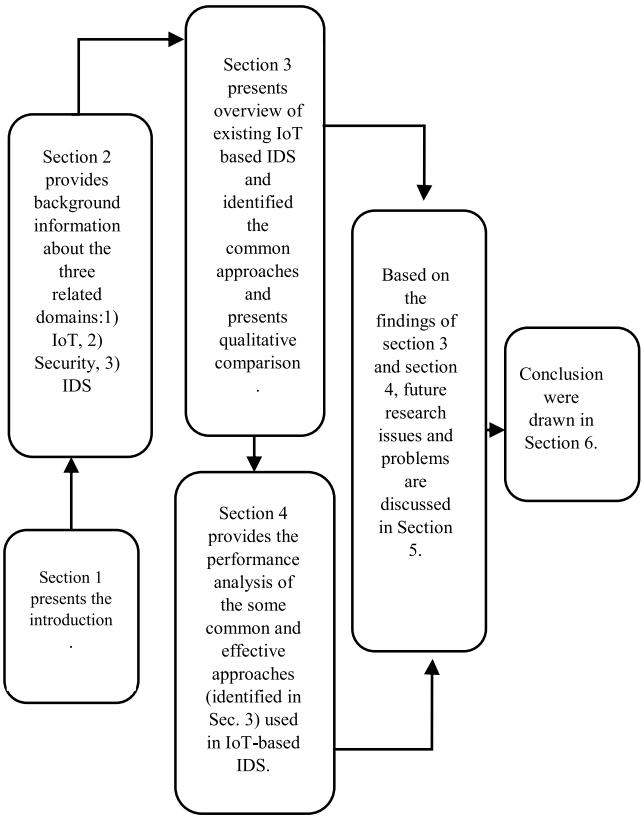

FIGURE 2. Organization of the paper.

utilized to facilitate integration and communication between the devices and applications [12], [16].

In terms of standards and protocols, numerous organizations have proposed several protocols for the IoT, this heterogeneity of protocols is one of the contributing factors of security challenges in IoT. An extensive survey on standards and enabling technologies of IoT can be found in [17].

B. SECURITY THREATS IN IoT

Like other networks, security in IoT is important as it seeks to preserve the cardinal principles of security, which are Confidentiality, Integrity, and Availability (CIA). However, ensuring security in IoT is a multi-layered problem [18] due to the huge number and heterogeneity of devices, technologies & protocols as well as the amount of data exchange involved [10]. Some of the generic security threats and their applications (real-life attack incidents) in IoT are explained below.

- Sybil and Spoofing attacks: In the Sybil attack, a malicious user uses several fake identities to operate at the same time in order to degrade the network. While spoofing attack refers to an attack where a malicious user impersonates a legal user in order to get unauthorized access to resources 19]. Examples of spoofing attacks are ARP spoofing, IP spoofing, Domain Name Service (DNS) server spoofing [11].
- Man-In-The-Middle attack: In the Man-In-The-Middle attack, the malicious user intercepts the communication

between two parties by eavesdropping [20]. Examples of this attack are session hijacking, port stealing, poisoning, etc., [11].

- Routing attacks: In routing attacks, malicious users target the routing protocol by spoofing, altering or modifying the routing information content in order to create deceptive behaviors. Examples of routing attacks are selective forwarding, sinkhole attack, black hole attack, wormhole attack, etc., [11].
- Denial of Service (DoS)/ Distributed Denial of Service (DDoS): In DoS attacks, the malicious user makes resources such as bandwidth unavailable to legitimate users by overwhelming the network with unwanted traffic or requests. In DDoS several compromised nodes are used for the purpose of the attack. Botnets are usually used for performing DDoS attacks effectively. Examples of DoS/DDoS attacks are flooding attacks, amplification attacks, logical software attacks, etc., [21].
- Elevation of privilege (EoP) attacks: In EoP attacks, malicious users elevate their privileges or right in order to access resources without permission. Examples of EoP are User-To-Root (U2R) and Remote-to-Local (R2L) [11], [22].
- Botnet attacks: A botnet is a group of compromised computer systems or IoT devices controlled by malicious users remotely. These nodes are utilized to perform several types of attacks [21]. Prior to the botnet attacks, some botnet activities or preliminary attacks [23] such as fuzzers, analysis, backdoors, exploits, generic, reconnaissance, shellcode, and worms attacks are executed to check or scan for vulnerabilities of network nodes. These activities enable malicious users to hijack more network nodes and increase the size of the botnet. An example of an attack carried out with botnets is DDoS.

Malicious users or Hackers utilize one or more of these generic attack types to perform malicious activities. Although several reports highlight the vulnerability and possibility of attacks on the IoT devices without real incidents, an example of such possibilities is the jeep hack[1]. Reports from security researchers confirmed that an attack on jeep Cherokee is possible. The attack can exploit the vulnerability in a firmware update. The hackers were able to alter the temperature inside the car and take full control of the vehicle's steering and brakes systems. Similarly, an example of vulnerable devices is pacemakers and defibrillators[1] used in hospitals as well as the cameras used for surveillance.[2]

The popular real-life security incidents on IoT devices is a DDoS attack. A notable example is the Dyn attack (Mirai botnet).[3] Dyn is a company that provides Domain Name Services (DNS) service to companies like Netflix, GitHub, Reddit, and Twitter. In October 2016, the company experiences a botnet attack carried out with Mirai malware. Mirai malware is one of the popular real-life threats to IoT. It is used to hack IoT devices to create a botnet which is used to execute large scale DDoS attack. Mirai malware utilizes the poor authentication flaws on the devices using Linux. The hacked devices are used to look up for weaknesses in other IoT devices in order to increase the size of the botnet.

Another popular vulnerable IoT device is the thermostat, it was exploited to reduce the temperature of two buildings in Lappeenranta, Finland in November 2016.[4] Also, another group of hackers used the thermostat in an aquarium for data theft in a casino[3].

C. INTRUSION DETECTION SYSTEM

Intrusion detection systems detect unauthorized access by malicious users to a system or a network. An IDS is usually utilized at the host level or network level. The host IDS (HIDS) is usually installed on the host and it monitors the activities of its host such as system application files and the operating system e.g. a computer system or a node in IoT. The network IDS (NIDS) is usually placed on the border router and it monitors the network traffic flow to identify threats that occur over the network connection [24]. A network IDS (NIDS) can further be classified based on its deployments and detection method. Based on its deployment, NIDS can be deployed in a centralized, distributed or hybrid manner [25]. A centralized NIDS is placed on a central device such as a border router or a dedicated host. NIDS monitors the traffic between its network and the internet since all requests and responses pass through it. However, monitoring traffic between the network and the internet is insufficient to detect some attacks. A node can be compromised internally and it can cause some damage to the network. In a distributed deployment, the NIDS is deployed on each resource-constrained node of the network. In this type of deployment, nodes may be assigned to monitor each other. A hybrid deployment utilizes both placements to achieve maximum benefits. It groups nodes into regions or clusters and selects a cluster head in each group as a head that monitors or collects reports from the other nodes [21].

Based on the detection methodology, a NIDS can be a signature-based, anomaly-based or a hybrid. A signature-based IDS detects possible attacks by comparing and matching the network traffic flow characteristics with a predefined attack signature saved in its internal database. The signature-based IDS usually achieves a 100% detection rates for known attacks. The anomaly-based IDS detects an attack by comparing the network traffic flow with a model of a normal network traffic flow created by the system, a deviation from the normal behavior is considered an attack [26]. To detect unknown attacks, the anomaly-based IDS employs statistical or machine learning approaches to develop a model

[1] www.iotforall.com/5-worst-iot-hacking-vulnarabilities
[2] www.ophtek.com/4-real-life-examples-iot-hacked
[3] https://www.digikey.com/en/maker/blogs/2019/5-leading-iot-security-breaches-and-what-we-can-learn-from-them
[4] https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/

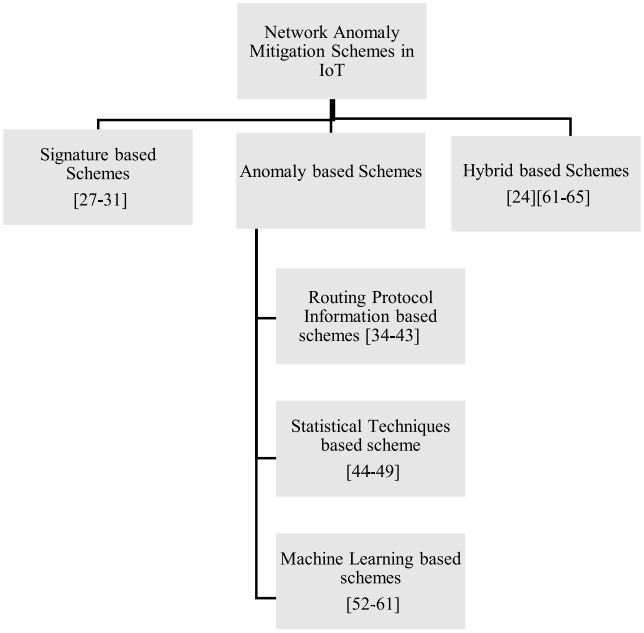

FIGURE 3. Taxonomy of network anomaly mitigation schemes.

of the normal traffic behavior used as a reference in monitoring and inspecting the network traffic flow. The hybrid IDS combines both signature-based and anomaly-based IDS in order to leverage the benefits of both and reduce their drawbacks [9].

In general, the signature-based IDS performs better than the anomaly-based IDS in detecting known attacks due to the signature of the attacks already saved in the database, however, it usually fails to detect unknown attacks and its application is limited in the resource-constrained IoT due to its operational needs. The anomaly-based outperforms the signature-based IDS in detecting zero-day (unknown) attacks due to its operation based on deviation from normal network traffic flow, although its application fits the IoT environment, it has its own challenges such as a high number of false-positive rate.

III. RELEVANT REVIEWS

This section presents a review of relevant literature on the IDS schemes in IoT. It contains a taxonomy based on the detection methodologies as shown in figure 3, a review of the proposed schemes and the comparison in tables 2-6. The review and the comparisons in this section are conducted based on the taxonomy.

A. SIGNATURE-BASED SCHEMES

The signature-based schemes detect possible attacks by comparing and matching the network traffic flow characteristics with a predefined attack signature saved in its database.

A Denial-of-Service detection scheme [27] is proposed for IPv6 over Low-power Wireless Personal Area Network protocol (6LoWPAN) based Internet of Things. The scheme is developed on the ebbits network framework, it uses probes that are placed in the area of interest and connected to an IDS in a wired mode. The probes operate in a promiscuous mode, it captures packets from network traffic for analysis in the adopted IDS system. The scheme employs Suricata which utilizes a packet threshold rule for detecting anomalies in the network traffic. The scheme was able to successfully detect a DoS attack (UDP flooding).

A Collaborative Blockchain Signature-Based Intrusion Detection System (CBSigIDS) in IoT environments is proposed [28]. The CBSigIDS integrates a collaborative signature-based IDS and a consortium blockchain (which allows selected users to write to the blockchain) to assist in increasingly sharing and building a trusted signature database. The nodes in CBSigIDS observe the network flows, identify attacks and share a set of signatures with other nodes by signing it with their respective private keys. The other nodes accept the set of signatures only after verification by the majority of the nodes. The scheme improves the effectiveness of signature-based IDS. However, the scheme will suffer from zero-day attacks because signature-based IDS can detect only attacks with known signatures.

A Real-time DDoS attack detection scheme [29] is proposed for IoT. The scheme employs on Complex Event Processing (CEP). The CEP scheme consists of three phases namely event filter, event processor (packet analyser & attack detection) and action engine. The event filter observes and gathers the network traffic flow, the event processor analyses the packets' characteristics to decide which type of attack is occurring. The action engine is in charge of controlling events that trigger the CEP rules on presumed intrusion activity. It subsequently denies the events' access to important services. The scheme achieves better performance than Bro IDS.

A Raspberry Pi Intrusion Detection System (RPiIDS) [30] is proposed for IoT. The system employs the Snort IDS. The full-pledged IDS was installed on the Raspberry Pi. The results obtained from experiments show that the Raspberry Pi is capable of hosting the Snort IDS.

A signature-based intrusion detection system [31] is proposed to detect DDoS attacks in IoT networks. The scheme consists of two modules: IDS router and IDS detectors, which are deployed in a hybrid manner. The IDS router is placed on the border router, it is utilized for detection as well as firewall functions. The IDS detectors placed as a sensor like devices are used to monitor traffic internally and forward information of suspicious or malicious nodes to the router for further action. The scheme can detect hello flooding and version number modification.

Table 2, presents a comparison table of network anomalies mitigation schemes based on signature-based detection methodology. The schemes are compared in terms of techniques used, performance metrics evaluated, anomalies detected, evaluation tools used, dataset utilized, the benchmark used for evaluation and the strengths of each scheme. The schemes rely on attack signatures stored in their database for attack detection. The signature-based schemes are evaluated using both simulation and experiments without using any

TABLE 2. Comparison table of network anomaly mitigation schemes based on signature based detection methodology.

S/No	Scheme Title	Technique	Performance Metrics Evaluated	Anomalies Detected	Evaluation Tools	Dataset	Benchmark	Strengths
1	A signature-based intrusion detection system,(2018) [31]	Routing protocol information	Not specified	i.Hello flooding ii.Version number modification	Simulation (Contiki/cooja)	N/A	None	Detect hello flooding and version number modification
2	A Raspberry Pi Intrusion Detection System (RPiIDS),(2016) [30]	Snort	i.CPU usage ii.RAM usage iii.Packet capture rate	Not specified	Experiment (Raspberry Pi)	N/A	Packet size	Raspberry Pi can host Snort.
3	A Real-time DDoS attack detection scheme, (2018) [29]	CEP	i.Accuracy ii.CPU usage iii.RAM usage iv.Packet loss	i.SYN flood ii.UDP flood iii.ICMP flood iv.Port scan	Experiment (Raspberry Pi)	N/A	i.Snort ii.Bro IDS	Achieves better performance than Bro IDS
4	A Denial-of-Service detection scheme (ebbits, 2013) [27]	Suricata (Packet threshold rule)	True positive rate	DoS	i.Penetration test system (Metspolit) ii.Contiki	N/A	None	Successfully detect DoS attack (UDP flooding).
5	CBSigIDS, (2019) [28]	i.Snort ii.Blockchain	i.Number of nodes infected ii.Number of survived node	i.Flooding attack ii.Worm attack iii.Insider exploration	i.Experiments ii. Simulations	N/A	None	Improves the effectiveness of signature-based IDS

dataset. The schemes were able to achieve their objectives. Although the operation of signature-based schemes does not fit in the IoT paradigm due to operational requirements.

It was shown that deploying a signature-based scheme is possible on IoT devices. However, these schemes will suffer from zero-day attacks because the schemes are limited to detecting known attacks or attacks within its database. In addition, majority of the schemes are not evaluated against any benchmark.

B. ANOMALY-BASED SCHEMES

The anomaly-based schemes detect an attack by comparing the network traffic flow with a model of a normal network traffic flow created by the system, a deviation from the normal behavior is considered an attack [9]. These schemes employ techniques such as routing protocol information, statistical or machine learning in its operations.

1) ROUTING PROTOCOL INFORMATION BASED SCHEMES

Routing Protocol for Low power and lossy networks (RPL) is utilized in IPv6 over Low-power Wireless Personal Area Network protocol (6LoWPAN) networks. It is also the existing routing protocol for IoT [32]. It creates a Destination-Oriented Directed Acyclic Graph (DODAG) between nodes in the network. Unidirectional traffic flow is supported in the direction of the root to the nodes or vice versa. A border router or gateway called 6LoWPAN Border Router (6BR) which supports a bi-directional traffic flow is placed between the nodes and the internet. The IDS usually resides on the 6BR [33].

A lightweight opinion metric based intrusion detection scheme is proposed in [34] to detect malicious attacks on routing protocol in the IoT network. The scheme calculates the opinion metric values (belief, disbelief, and uncertainty) of nodes in the network based on experience (positive or negative) of the traffic flow. The nodes send their respective opinion metric about their neighbors to the border router. The router aggregates the opinion of the nodes about their neighbors and detects a malicious node based on the calculated opinion values. A node with high disbelief value is considered a malicious node. Hence the scheme will generate an alert. The scheme was able to detect Sybil and DoS attacks.

A lightweight intrusion detection scheme based on energy consumption analysis is proposed to detect DoS in IoT networks [35]. The scheme uses mesh-under and route-over routing energy prediction models to analyses energy consumption. Consumption of more than 30% of the previous consumption of any node is considered an attack. The scheme achieves efficient and accurate detection of DoS attacks with 100% detection rate.

A real-time intrusion and wormhole attack detection scheme [36] is proposed for the Internet of Things. The scheme uses the neighbor validation to determine the location of a node. It detects an attack if the node is outside the transmission range. It also utilizes the Received Signal Strength Indicator (RSSI) to identify an attacker node. The scheme achieves a 94 % detection rate.

An intrusion detection scheme for sinkhole attacks on 6LoWPAN internet of things (INTI) [37] is proposed to detect sinkhole attacks on the routing services in IoT. The scheme employs watchdog, reputation and trust techniques for attack detection. The INTI schemes cluster the nodes and assign to them different network functions. It employs the watchdog strategy to monitor the behaviour of the nodes. This scheme utilizes the reputation and trust techniques to identify and isolate malicious nodes. The scheme achieves a sinkhole detection rate of 92% for fixed deployment and 75% in mobile deployments.

An Intrusion Detection and Response System (InDReS) [38] is proposed for 6LoWPAN based Internet of Things. The InDReS scheme employs the constrained based specification technique for sinkhole attack detection. It clusters the nodes into clusters and a node elects itself as a leader node of its cluster based on RSS and a probabilistic strategy. It then advertises its position to other nodes. The leader node monitors its adjacent nodes and records packet drop count of the nodes. It ranks each node and compares the result with a defined threshold to identify a malicious node.

The malicious node is isolated and the network is reconstructed. The InDReS scheme improves the Quality of Service (QoS) metric.

A distributed internal anomaly detection scheme is proposed for IoT [39]. The scheme enables each node to monitor its neighbor and report any anomaly upward to its parent node until the message reaches the root node (edge router). The anomaly messages are exchanged by employing a control message called Distress Propagation Object (DPO), which is integrated into the Routing Protocol for Low-power and lossy networks (RPL). The edge router performs the anomaly detection process and subsequently communicates with the nodes through its subsystems namely: Monitoring and Grading Subsystem (MGSS) & Reporting Subsystem (RSS) which operates at the network layer and Isolation Subsystem (ISS) which operates at the data link layer. The information collection, analysis, and scoring are done by the MGSS and message propagation is done by the RSS by utilizing DPO. The ISS is in charge of isolating a node in an event of an anomaly. The identified malicious node is isolated and its packets discarded.

A DDoS attack mitigation framework [40] is proposed for the Internet of Things. The framework is embedded in the border router and consists of two stages namely analysis and monitoring stages. The analysis stage monitors the inbound traffic and determine if it is suspicious or not. First, by checking its blacklist saved on a dedicated server. Secondly, it analyses the packets by checking the bit rate and the payload size. It drops the packet with bit rates above a threshold and saves their source in a blacklist and forwards the packets with payload size above a threshold to a grey list on the dedicated server. The monitoring stage monitors packets on the grey list. It drops the packets if they keep coming from the same source, adds the source address in the blacklist and classifies them as DoS or DDoS attack packets. The framework fits the IoT environment and can adapt to different applications.

A trust-based distributed intrusion detection scheme [41] is proposed for the Internet of Things. The scheme employs the subjective logic for trust evaluation among the nodes in the network based on opinions in traffic flow. It utilizes three different algorithms for managing reputation among the nodes, which are: Neighbour Based Trust Dissemination (NBTD), Clustered Neighbour Based Trust Dissemination (CNTD) and Tree-Based Trust Dissemination (TTD). In the NBTD algorithm, the border router computes trust values sporadically based on information from the nodes. In the CNTD algorithm, reputations are computed in a distributed manner by the cluster heads instead of the border router. While in the TTD algorithm, the reputations are computed by using the same topology with the CNTD but with less observation on the nodes. Each node only observes its parent node in order to reduce overhead. The nodes are blocked when their reputation exceeds a defined threshold. The scheme can detect an RPL protocol based attack. It is also flexible due to its ability to adapt to other attacks.

A Multidimensional Trust-Based Anomaly Detection (MTBAD) scheme [42] is proposed for IoT network. The MTBAD scheme evaluates trust based on reputation, Quality of Service (QoS), and social relationship. The trust level of each node is evaluated using a fuzzy approach. The anomalies are detected when the trust value is above a threshold. In the event of an anomaly, the system is prompted to re-evaluate the trust of the whole system. The MTBAD scheme achieves a very low false alarm rate with a proper trust level threshold.

A DDoS attack detection and prevention scheme [43] is proposed for IoT networks. The scheme employs agent-based technology for attack detection. The scheme deploys the agent on the border router to stop attacks from outside the network. The scheme maintains a greylist and blacklist for monitoring and blocking access temporarily or permanently, respectively. The greylist is updated every 40s while the blacklist is updated every 300s. The scheme is suitable for small IoT networks.

Table 3, presents a comparison table of network anomalies mitigation schemes based on routing protocol information. The schemes are compared in terms of techniques used, performance metrics evaluated, anomalies detected, evaluation tools used, dataset utilized, the benchmark used for evaluation and the strengths of each scheme. These schemes rely on routing protocol information to make decisions on network traffic flow. The schemes achieve their objectives with acceptable performance. The schemes are widely evaluated using simulation without utilizing any dataset. However, these solutions are limited to attack detection for a specific protocol. Furthermore, most of the schemes are not validated with other IoT schemes.

2) STATISTICAL BASED SCHEMES

Statistical techniques used for anomaly detection seeks unusual events in the traffic flow characteristics. It utilizes first-order statistical approaches such as standard deviation and means, second-order like correlation measures, or the third order, such as hypothesis testing, mixture models and inference approaches [21].

A fog empowered anomaly detection scheme [44] is proposed for IoT to harness the computational abilities of the fog layer in anomaly detection. It utilizes the hyper ellipsoidal Clustering for Resource-Constrained Environments algorithm (HyCARCE) for clustering the data obtained from the sensor nodes and Ellipsoidal neighbourhood outlier factor (ENOF) a scoring mechanism for differentiating normal and anomalous clusters. The scheme consists of four phases namely HyCARCE clustering, ENOF computation, cluster information transmission, and anomaly detection process. The fog layer receives data from the nodes and executes the clustering, outlier computation, and anomaly detection processes. The scheme ensures anomaly detection in a timely manner, with minimal overhead and also decreases energy consumption. However, the scheme fails to provide security and privacy during information exchange between sensor nodes, fog, and cloud layers.

TABLE 3. Comparison table of network anomaly mitigation schemes based on routing protocol information.

S/No	Scheme Title	Technique	Performance Metrics Evaluated	Anomalies Detected	Evaluation Tools	Dataset	Benchmark	Strengths
1	A distributed internal anomaly detection scheme, (2016) [39]	Routing protocol information messages	None	Not specified	None	N/A	None	Identifies malicious nodes
2	A lightweight opinion metric based intrusion detection scheme, (2018) [34]	Opinion metric value (based routing protocol information messages)	i.Detection rate ii.False-positive iii.False-negative	i.Sybil attack ii.DoS attack	Simulation (Contiki/cooja	N/A	None	Detect Sybil and DoS attack
3	An intrusion detection scheme (INTI),(2015) [37]	Routing protocol information messages	i.Detection rate ii.False positive iii.False negative iv.Packet delivery rate	Sinkhole attack	Simulation (contiki/cooja)	N/A	SVELTE	Detects sinkhole attack
4	A trust based distributed intrusion detection scheme,(2017) [41]	Routing protocol information messages	i.Number of intruders detected ii.False positive iii.False negative	RPL based attacks	Simulation (MATLAB)	N/A	i.NBTD ii.CNTD iii.TTD	i.Detect RPL based attacks ii.Flexibility
5	A DDoS attack mitigation framework ,(2017) [40]	Routing protocol information messages	Packet delivery ration	DDoS	Simulation (Contiki/cooja)	N/A	None	Adaptable to different applications.
6	A lightweight intrusion detection scheme based on energy consumption analysis,(2014) [35]	Routing protocol information messages	Energy Consumption	DDoS	Simulation (Qualnet)	N/A	Normal and Abnormal traffic	Detects DDoS with 100% detection rate.
7	A real-time intrusion and wormhole attack detection scheme, (2015) [36]	i.Neighbor validation (Routing protocol information messages) ii.RSSI	i.Detection rate ii.Energy consumption iii.Packets overhead iv.Memory consumption	Wormhole	Experiments and simulation (cooja and Contiki)	N/A	None	Achieves a 94 % detection rate.
8	A Multidimensional Trust-Based Anomaly Detection (MTBAD) scheme,(2017) [42]	i.Routing messages ii.Fuzzy logic	False-positive	DDoS	Simulation	N/A	Percentage of malicious nodes	Low false alarm rate.
9	An Intrusion Detection and Response System (InDReS),(2016) [38]	Routing protocol information	i.Packet drop ratio ii.Throughput iii.Energy consumption iv.Normalized overhead	Sinkhole	Simulation (NS 2)	N/A	INTI	Improves QoS
10	A DDoS attack detection and prevention scheme, (2016) [43]	i.Agent technology ii. Routing protocol information	i.Packet delivery ratio ii.Number of dropped packets iii.True positive iv.False-positive v.Packet rate	DDoS	Simulations (Contiki/cooja)	N/A	i.Learning period ii.Attack with a different number of attackers.	Suitable for small IoT networks.

A Principal Component Analysis (PCA) approach for network anomaly detection in IoT is proposed [45]. The schemes employ the Minkowski formula to compute the distance between the principal components (PC) and Empirical Cumulative Distribution Function (ECDF) for defining the threshold. The scheme has three stages which are gathering network data (which captures the data and transform it into PCA space), analysis and anomaly detection. It gives an alert when the observed instances threshold is at a far distance from the PCs which translates to an anomaly. The scheme achieves an acceptable detection rate with minimal computational overhead.

A Lightweight Anomaly Mining Algorithm (LAMA) [46] is proposed for IoT. The LAMA employs a Jaccard coefficient for detecting data sequence similarity and detecting distance between data sequence. It consists of two phases: training and detection phases. The training phase obtains a normal pattern of the data sequence by calculating the Jaccard coefficient of a sequence of data streams. A sliding window is employed to fine-tune to a specific threshold for the normal pattern. The detection phase also uses the Jaccard coefficient to compare a new data sequence with the normal pattern obtained from the training phase, a coefficient above the threshold indicates an abnormality. The algorithm decreases misjudgments in detecting abnormal data sequence.

An Intelligent Maintenance and Lightweight Anomaly Detection System (IMLADS) is proposed in [47] to decrease the computational complexity and enhance scalable and stable systems in the internet of things. The IMLADS system utilizes mobile agents for data collection and analysis on the node and system level. At the node level, the system employs PCA for dimension reduction of the collected data and Density-based Spatial Clustering of Applications with Noise (DBSCAN) for clustering to differentiate normal data from abnormal data. While at the system level, the system utilizes sketch (probabilistic dimension reduction method) for dimension reduction of features in the captured traffic packets and Exponentially Weighted Moving-Average (EWMA) technique to estimate the changes and choose upper and lower limits to execute anomaly detection. A continuous sliding time window is used to further increase the detection accuracy at the system level. The system achieves efficiency and accuracy in detecting anomalies.

An intrusion detection system for constrained WSN and IoT nodes called mIDS is proposed [48]. The mIDS scheme employs a statistical tool based on Binary Logistic Regression (BLR) for monitoring the network and detecting anomalies. The scheme comprises two steps; training and evaluation steps. During the training, the scheme uses a run-time monitoring tool to obtain node parameters (local) for normal and abnormal behaviours as well as developing a model using (BLR). The evaluation step of mIDS tests the model in real-time to detect attacks. The mIDS scheme achieves an accuracy of 96% -100%.

TABLE 4. Comparison table of network anomaly mitigation schemes based on statistical techniques.

S/No	Scheme Title	Technique	Performance Metrics Evaluated	Anomalies Detected	Evaluation Tools	Dataset	Benchmark	Strengths
1	A fog empowered anomaly detection scheme for IoT, (2017) [44]	i.HyCARCE ii.ENOF	i.Accuracy ii.Energy consumption ratio iii.Time delay ratio	Not specified	Experiments	i.S12 ii.Banana iii.Melbourne IoT data iv.Intel Berkeley Research Laboratory IBRL(IBRL)	i.Centralized ii.Distributed schemes	i.Fast anomaly detection ii.Minimal overhead iii.Decreases energy consumption
2	PCA approach for network anomaly detection, (2018) [45]	i.PCA ii.Minkowski formula iii.ECDF	Accuracy	Not specified	Experiments	i.Kyoto 2006+	Cases with different thresholds	i.Fast anomaly detection ii.Minimal overhead iii.Decreases energy consumption
3	mIDS, (2018) [48]	BLR	Accuracy	i.Selective forwarding ii.Blackhole attack.	Simulation (Contiki/cooja)	N/A	Evaluation based on different topologies	Achieves an accuracy of 96% -100%.
4	GARUDA, (2018) [49]	Gaussian function	i.Accuracy ii.Detection rate iii.False alarm	i.U2R ii.R2L	Experiments	i.KDD-CUP99 ii.NSL-KDD	i.CANN ii.CLAPP iii.CSVAC iv.CSOCACN	Achieves better results in detecting low frequency attacks
5	LAMA, (2014) [46]	Jaccard Coefficient	Difference in attributes value between normal and abnormal data sequence	Not specified	Simulation (MATLAB)	N/A	None	Decreases misjudgments in detecting abnormal data sequence.
6	IMLADS, (2019) [47]	i.PCA ii.DBSCAN iii.Sketch iv.EWMA	i.Detection rate ii.False positive rate iii.False negative rates.	Virus attacks	Experiments	Data from authors lab	i.DBSCAN ii.Avast	Achieves efficiency and accuracy in detecting anomalies

A Gaussian dissimilarity measure for feature representation and anomaly detection scheme (GARUDA) [49] is proposed for the internet of things. The GARUDA scheme uses a Gaussian function for distance measure. It also employs an incremental feature clustering technique for dimension reduction by specifying a threshold based on a dissimilarity value. The distance measure is used to evaluate several classifiers (*k*-NN, J48, SVM, naive Bayes, and Bayes net) in detecting anomalies. The GARUDA scheme achieves better results than Cluster Center and Nearest Neighbor (CANN), CLustering APProach (CLAPP), Combining Support Vectors with Ant Colony (CSVAC) and CSOCACN in detecting low-frequency attacks (U2R and R2L).

Table 4, presents a comparison table of network anomalies mitigation schemes based on statistical techniques. The schemes are compared in terms of techniques used, performance metrics evaluated, anomalies detected, evaluation tools used, dataset utilized, the benchmark used for evaluation and the strengths of each scheme. The schemes employ statistical techniques at the core of their operation in detecting attacks. These schemes utilize both simulations and experiments for evaluation using available datasets. The schemes achieve their objectives, even though 50% of these schemes fail to mention the anomaly type detected. These schemes may experience high false alarm when legitimate traffic flow is classified as illegitimate due to reliance on historical behavior. Also, most of the schemes are not evaluated against other IoT schemes.

3) MACHINE LEARNING-BASED SCHEMES

Machine learning techniques used for anomaly detection distinguish malicious traffic flows based on characteristics of network traffic [50] and utilize models that learn automatically from these experiences. It uses supervised learning algorithms such as support vector machine (SVM), Decision tree, etc. and unsupervised learning algorithms like K-means [51].

A machine learning-based IDS schemes [52] are proposed to detect wormhole attacks in IoT. The author proposed three schemes by utilizing unsupervised K-means clustering, supervised decision tree algorithm and hybridizing the two schemes. The first scheme using K-means scheme clusters nodes into safe zones. Any routing update to the router between the nodes in different safe zones is considered an attack. The second scheme employs a Decision Tree (DT) algorithm, it computes a safe distance between nodes. An update to the router about any neighbor above the safe distance is considered an attack. The third scheme is a hybrid of the K-means and Decision tree scheme. In an attempt to update the routing table, it first uses the K-means scheme to check if the nodes are in the safe zone and then utilize the Decision tree to check if the distance between the nodes is within the safe distance even if the nodes are not in the same safe zone. The K-means scheme achieves a detection rate of 70-93%, the DT achieves 71-80% and the hybrid achieves 71-75%. Although the hybrid scheme has a lower detection rate it was able to reduce false-positive alerts.

A Naïve Bayesian Classification technique in Multi-Agent system-enriched IDS scheme (NBC-MAIDS) [53] is proposed for securing IoT against DDoS attacks. The NBS-MAIDS scheme employs the Naïve Bayesian classification technique to classify data from the traffic flow. The scheme also uses multiple agents namely: collector agent, system monitoring agent, actuator agent and communication agent for the functionality of the scheme. The collector agent

collects the data (classified data) from the data source and forwards it to the system monitoring agent. The system monitoring agent monitors the whole multi-agent system network. It decides if the data is normal or abnormal by comparing it to an earlier detected data if it's available or collaborates with other IDS. The actuator agent responds to intrusion alerts by cutting off the malicious node. The communication agent shares information about the detected attack among the agents and other distributed IDSs. The NBC-MAIDS scheme enhances the performance of the IDS.

A Two-layer Dimension Reduction and Two-tier Classification (TDTC) scheme is proposed in [54] to detect malicious activities such as User to Root (U2R) and Remote to Local (R2L) attacks. The TDTC scheme consists of two modules namely dimension reduction and classification. The scheme employs supervised Linear Discriminant Analysis (LDA) and unsupervised Principal Component Analysis (PCA) for dimension reduction and Naïve Bayes (NB) and Certainty-Factor version of K-Nearest Neighbour (CF-KNN) for classification. In the dimension reduction module, the high dimension of the dataset is reduced and feature selection and extraction are performed in order to avoid making incorrect decisions and improving the computational complexity of the classifier. In the classification module, the trained data is classified as normal or abnormal using the two-tier classification. The scheme detects low-frequency attacks such as U2R and R2L, it also outperforms similar schemes in terms of detection rate.

A hybrid approach for detecting anomaly in IoT is proposed [55]. The scheme employs K-means clustering and Sequential Minimal Optimization (SMO) classification to improve the detection with low complexity. The scheme has three phases namely: pre-processing, clustering and classification. The pre-processing phase consists of two steps: feature selection and removing null records. It prepares the data and reduces the ambiguity of the dataset by removing the redundant part of the data. The clustering phase utilizes the K-Means clustering algorithm to group similar data in clusters. The classification phase uses the SMO to build a predictor model, which is used to test the dataset for normal or abnormal data. The scheme achieves 100% accuracy and detection rate as well as a 0% false-positive rate.

An intrusion detection scheme [56] based on anomaly mining is proposed for the internet of things. The scheme utilizes a Symbolic Aggregate Approximation (SAX) algorithm to change perception layer reading to symbolic representations which are utilized in computing similarity between new traffic and normal traffic pattern. It then uses an unsupervised mining algorithm to learn normal traffic and also differentiate normal from abnormal traffic. The scheme is self-adaptive and can ensure low false-positive alerts.

A cross layer-based intrusion detection scheme [57] based on network behavior is proposed for IoT. The scheme consists of two detection levels namely local and global. The local detection level employs a dedicated sniffer trained using a supervised machine learning approach to create correctly classified instances (CCIs) of the network traffic. The global detection level utilizes a super node that gathers the CCIs and performs iterative linear regression in order to create a time-based profile named the Accumulated Measure of Fluctuation (AMoF) for malicious and normal nodes. Then, it uses the profiles to distinguish between the normal and malicious nodes. The scheme achieves malicious node identification after three iterations with 100% accuracy.

A distributed attack detection scheme [58] is proposed for the internet of things. The scheme employs a deep learning approach. The scheme utilizes the fog nodes for training the models and hosting the detection schemes. It also employs a coordinator (master node) to enhance collaboration in sharing parameters and optimization between the fog nodes. The scheme achieves a better result than centralized models in terms of attack detection.

An intelligent intrusion detection scheme [59] in low-power IoT devices is proposed for the detection and prevention of numerous performance and integrity attacks. The scheme is placed on the IoT network base station and it comprises two phases. The first phase employs the Random Neural Network (RNN) for training the detection model. The second phase uses a lightweight compile-time code instrumentation technique for detection of illegal memory access. In addition, the scheme also serves as a health monitoring system for the nodes in the IoT network by monitoring the data transmission between the nodes and the base station. The scheme achieves a 97.3 % detection rate with an acceptable performance overhead.

A distributed anomaly detection scheme [60] using autoencoder neural networks is proposed for IoT. The scheme detects anomalies by utilizing two algorithms that are placed on the sensors (Distributed Anomaly Detection using Autoencoders-S) and the IoT cloud (Distributed Anomaly Detection using Autoencoders-C). The cloud side performs the required computations for learning traffic behaviour. While the sensor side performs detection in a distributed manner without interactions with other sensors or the cloud layer. The scheme achieves anomaly detection with high accuracy.

An ensemble intrusion detection scheme [23] based on statistical flow features for protecting network traffic is proposed to detect botnet attacks on the internet of things. The scheme employs an Adaboost ensemble learning technique comprising of three machine learning algorithms: Decision Tree (DT), Naive Bayes (NB) and Artificial Neural Network (ANN). The ensemble technique evaluates a set of statistical features obtained from Domain Name Service (DNS), Message Queuing Telemetry Transport (MQTT) and HyperText Transfer Protocol (HTTP) protocols to detect attacks. The scheme offers a higher detection rate and lowers the false positive rate.

Table 5, presents a comparison table of network anomalies mitigation schemes based on machine learning algorithms. The schemes are compared in terms of techniques used, performance metrics evaluated, anomalies detected, evaluation tools used, dataset utilized, the benchmark used for

TABLE 5. Comparison table of network anomaly mitigation schemes based on machine learning algorithms.

S/No	Scheme Title	Technique	Performance Metrics Evaluated	Anomalies Detected	Evaluation Tools	Dataset	Benchmark	Strengths
1	TDTC scheme, (2016) [54]	i. LDA ii.PCA iii.NB iv.CF-KNN	i.Detection rate ii.False alarm rate	i.U2R ii.R2L	Experiments	NSL-KDD	Similar Schemes	Detects low-frequency attacks
2	A hybrid approach for detecting anomaly in IoT, (2018) [55]	i.K-means clustering ii.SMO for classification	i.Accuracy ii.Detection rate iii.False positive rate	Not specified	Experiment	Intel Lab dataset	i.K-Means ii.SMO.	i.Achieves 100% accuracy and detection rate ii.0% false positive rate.
3	A distributed anomaly detection scheme,(2018) [60]	Autoencoder Neural Network	i.True positive ii.ROC iii.AUC	Not specified	Experiments	Dataset from experiment setup	None	Achieves anomaly detection with high accuracy.
4	An intelligent intrusion detection scheme,(2016) [59]	Random Neural Network	Detection accuracy	Integrity attacks	Experiment	Features generated from experiment setup	Test cases	Achieves 97.3% detection rate with acceptable overhead.
5	A distributed attack detection scheme,(2018) [58]	Deep learning	i.Accuracy ii.Detection rate iii.False positive	i.DoS ii.Probe iii.R2L iv.U2R	Experiment	NSL-KDD	i.Centralized model ii.Shallow learning model	Achieves better result than centralized model
6	A cross layer-based intrusion detection scheme, (2018) [57]	Decision Tree algorithm	Detection rate	Not specified	Simulation (Contiki/Cooja)	N/A	Profile of nodes	Achieves 100% detection of the malicious node after three iterations.
7	An intrusion detection scheme based on anomaly mining,(2012) [56]	Unsupervised mining algorithm	False-positive rate	Botnet attacks	Experiment	Intel dataset	None	i.Self-adaptive ii.Low false positive alert.
8	An ensemble intrusion detection scheme, (2018) [23]	Adaboost ensemble learning technique	i.Accuracy ii.Detection rate iii.False-positive rate iv.ROC curve	Botnet attacks	Experiment	i.UNSW-NB15 ii.NIMS botnet datasets	i.DT ii. NB iii.ANN	Higher detection rate and lower false-positive rate.
9	NBC-MAIDS, (2018) [53]	i.Naïve Bayesian classification technique ii.Multi-agent system	i.Detection rate ii.Delays iii.End to end packet forwarding iv.Packet drop	DDoS	Simulation (NS 2.35)	NSL-KDD	Generic IDS	Enhance the performance of the IDS.
10	Machine learning based IDS schemes, (2017) [52]	i.K-means clustering, ii.Decision tree algorithm	Detection rate	Wormhole attack	Simulation (C++)	N/A	i.Different topologies ii.SVELTE	i.K-means scheme achieves a detection rate of 70-93%, ii.Decision tree achieves 71-80% and iii. Hybrid achieves 71-75%.

evaluation and the strengths of each scheme. The schemes utilize different machine learning algorithms (supervised and unsupervised) for making decisions on traffic flow to either normal or abnormal.

The machine learning schemes require training data and time for effective operation. Majority of the schemes utilize available public datasets with few generating their own datasets. The schemes achieve their objectives but may suffer from low accuracy and false-positive rates when legitimate traffic flow is tagged illegitimate. Similarly, most of the schemes are not validated with other IoT schemes.

C. HYBRID BASED SCHEMES

The hybrid based schemes leverage on the strengths of the other schemes to achieve better performance by hybridizing them. Majority of these schemes combine the signature-based and anomaly-based scheme to achieve its objectives.

A Real-time intrusion detection scheme (SVELTE) [24] is proposed for the internet of things. The SVELTE scheme consists of three modules located in the border router (6BR) namely: 6LoWPAN Mapper (6Mapper), intrusion detection component and a distributed mini-firewall. The 6Mapper collects node information (Node ID, node rank, parent ID, and all neighbour IDs and ranks) from the nodes about the RPL network by using the response of the mapping request and reconstruct the network in the 6BR. The intrusion detection component comprises of three types of attack detection techniques (spoofed or altered information, sinkhole, and selective forwarding attacks). It also detects routing inconsistencies by checking each node's information and comparing it with information in the 6Mapper. A node is removed from the whitelist of the 6Mapper if it fails the consistency check two times. The distributed mini-firewall module is used to protect the network from external attackers. The SVELTE scheme detects all malicious nodes that launch sinkhole and/or selective forwarding attacks. In addition, it has an acceptable overhead with low energy consumption.

An intrusion detection scheme [61] is proposed for the RPL-connected 6LoWPAN networks. The scheme improves on the SVELTE scheme [24] by incorporating an Expected Transmissions (ETX) and a geographical hint for attack detection. The ETX indicates the communication quality of neighbour nodes. The geographical detection algorithms which enhance the scheme to detect ETX and rank attacks by providing the location of the nodes. The scheme improves attack detection in schemes that use ranking for anomaly detection.

A hybrid lightweight anomaly detection scheme for low-resource IoT devices using a game-theory approach is proposed [62]. The scheme employs a signature-based and anomaly-based detection (Back Propagation Network) schemes on the IoT devices. It utilizes a Nash equilibrium to decide when to activate the anomaly-based detection technique in order to save energy of the constrained IoT devices. The scheme achieves a high detection rate and low false-positive rates with low energy consumption. But using both signature-based and anomaly-based schemes on an IoT device will limit the performance of the device due to its lack of resources.

TABLE 6. Comparison table of network anomaly mitigation schemes based on hybrid detection methodologies.

S/No	Scheme Title	Technique	Performance Metrics Evaluated	Anomalies Detected	Evaluation Tools	Dataset	Benchmark	Strengths
1	A hybrid lightweight anomaly detection scheme using a game-theory approach, (2016) [62]	i.Back Propagation Network ii.Nash Equilibrium iii.Signature-based IDS	i.Accuracy ii.Energy consumption	DoS	Simulation (TOSSIM simulator)	N/A	Scheme without game theory approach	i.High detection rate ii.Low false positive rates iii.Low energy consumption
2	An Adaptive Intrusion Detection scheme (PULSE),(2018) [65]	i.Naïve Bayes ii.Signature based IDS	i.Precision ii.Recall iii.F-measure	i. Probing attacks ii.SYN flooding iii.UDP flooding	Experiment	Data from experiment testbed	None	Detects probing attacks
3	A hybrid of anomaly-based and specification-based IDS scheme, (2017) [64]	i.Optimum-Path Forest (OPF) clustering algorithm ii.MapReduce	Accuracy	i.Sinkhole ii.Selective forwarding iii.Wormhole attacks	Simulation (MATLAB)	N/A	Different network size	Satisfactory results in detecting attacks.
4	SVELTE, (2013) [24]	i.Routing protocol information ii. Signature based IDS	i.True positive rate ii.Energy iii.Memory consumption	i.Sinkhole ii.Selective forwarding attacks	Simulation (Contiki)	N/A	Number of nodes	Detects all malicious nodes that launch attacks
5	CHA – IDS, (2018) [63]	i.Best first search algorithm ii. Greedy stepwise algorithm iii.Correlation-based features selection iv. Signature-based IDS	i.Accuracy ii.Energy consumption iii.Memory consumption	i.Hello flooding attack, ii.Sinkhole attack iii.Wormhole	Experiments and simulation (cooja and contiki)	N/A	SVELTE	Detect hello flooding attack, sinkhole attack or wormhole attack or a combination of the attacks
6	An intrusion detection scheme for the RPL-connected 6LoWPAN networks,(2017) [61]	Routing protocol information	i.True positive ii.Power consumption	i.ETX and ii.Rank attacks	Simulation (contitki/cooja)	N/A	i.Rank only scheme ii.ETX based scheme	Enhance detection in rank only schemes

A Compression Header Analyser Intrusion Detection Scheme (CHA - IDS) [63] is proposed for 6LoWPAN Communication Protocol. The scheme utilizes signature-based and anomaly-based intrusion detection systems to detect attacks. The CHA – IDS is placed on the router and it uses machine learning algorithms to learn and classify attacks by utilizing the compression header features. The scheme employs the best-first search and greedy stepwise algorithms for feature selection and a correlation-based feature selection to differentiate normal from the abnormal traffic flow. The scheme consists of four modules that use different agents namely: Sensor Agents (SA), Aggregator Agent (AGA), Analyser Agent (ANA) and Actuator Agent (ACA). The SA is in charge of gathering packets from the traffic flow of all nodes. The AGA identifies the feature that will be utilized in behavior classification (normal or abnormal). The ANA label the data as normal or abnormal (hello flooding attack, sinkhole attack or wormhole). Finally, the ACA sends an alert to the user when malicious activity is detected. The CHA-IDS was able to detect hello flooding attack, sinkhole attack or wormhole attack or a combination of attacks.

A hybrid of anomaly-based and specification-based IDS scheme [64] is proposed for the internet of things. The scheme employs a Specification Agent (SA-IDS) and Anomaly Agent (AA-IDS) based IDSs. The SA-IDS is utilized at each node to monitor traffic flow, whenever it identifies a potential malicious node, a message inserted in the packets is sent to the border router. The AA-IDs at the border router employs the unsupervised optimum-path forest (OPF) clustering algorithm to form a cluster from the collected results in order to detect anomalies. The scheme finally makes its decision about detecting attacks (it assumed that the attack traffic is much less than the normal traffic) using a voting mechanism by comparing results of the SA-IDS and AA-IDS. The scheme uses the MapReduce technique to enable it to process the messages from the nodes in parallel. The hybrid scheme achieves satisfactory results when selective forwarding and sinkhole attacks are initiated concurrently. Similarly, it achieves a true positive rate of 96.02% and a false-positive rate of 2.08% in detecting wormhole attack.

An Adaptive Intrusion Detection scheme (PULSE) [65] is proposed for IoT network. The PULSE scheme employs an anomaly and signature-based detection schemes. The anomaly base scheme uses a supervised machine learning algorithm (Naïve Bayes) for learning the behaviour of traffic flow and classifications while the signature-based detection scheme consists of a combination of rule-based algorithms formed from the outcome of the machine learning results. The scheme achieves a good level of detection rates for probing attacks.

Table 6, presents a comparison table of network anomalies mitigation schemes based on machine learning algorithms. The schemes are compared in terms of techniques used, performance metrics evaluated, anomalies detected, evaluation tools used, dataset utilized, the benchmark used for evaluation and the strengths of each scheme. These schemes leverage the benefits of different methodologies to make decisions, hence it achieves good results. The schemes are evaluated using simulations. However, the scheme may inherit the shortcoming of the adopted methodologies when deployed on the IoT devices. For example, most of the hybrid schemes are a combination of signature-based and anomaly-based schemes, hence lack of enough resources such as storage may hinder the effective operation of the schemes. Also, most of the schemes are not validated with other IoT schemes.

In summary, we learned the following from the reviews and comparisons:

- The network anomalies mitigation schemes in IoT can largely be divided into signature-based IDS and anomaly-based IDS based as well as a hybrid based.
- There are several security threats in the IoT network which are solved by utilizing the different IoT based IDS schemes.
- The most important performance metric evaluated in the proposed schemes is the accuracy rate in attack detection.
- The proposed schemes are widely evaluated using simulations and experiments using available public datasets with few authors generating their dataset. However, none of the available public datasets is IoT based. Additionally, majority of the proposed network anomalies mitigation schemes in IoT are not evaluated against other schemes. Hence this shows a lack of effective validation techniques that will enhance research reproducibility and continuity in the research community.
- The signature-based schemes can be deployed on the IoT devices. However, it is limited to detect known attacks only and suffer from zero-day attacks. In addition, the operational requirements will stretch the resources of the IoT device, which will affect the general performance of the schemes. To solve the limitation of the signature-based schemes, anomaly-based schemes are used. The anomaly-based schemes can be categorized into three classes: i) routing protocol information based, ii) statistical techniques based, and iii) machine learning-based. These schemes achieved acceptable accuracy in detecting attacks. However, the routing protocol information based schemes are limited to attack detection for a specific protocol while the statistical techniques and machine learning-based techniques may suffer from false-positive rates and low accuracy when legitimate traffic flow is misclassified.
- The hybrid schemes combine more than one detection methodology to achieve better results in the accuracy rate in attack detection. However, the hybrid schemes may inherit the weakness of the adopted detection methodologies which will affect its performance. These problems may include i) lack of enough resources in the IoT and ii) the need for a labeled and up to date training data that consist of all attack classes.

In addition, the process of combining different detection methodologies to obtain an effective and operational hybrid scheme is challenging [66].

IV. PERFORMANCE EVALUATION

In this section, a performance evaluation of some classification algorithms widely used in IDS schemes in IoT is conducted. It discusses the dataset used, algorithms utilized, performance metrics evaluated as well as the results and discussion.

Performance evaluation is fundamental in the development of IDS schemes. The evaluation assists in ascertaining the effectiveness and efficiency of the schemes, which are usually developed using statistical techniques or machine learning algorithms.

TABLE 7. Distribution of the extracted sample.

S/No	Class	Number of Extracted Sample
1	Normal	64778
2	Fuzzers	22186
3	Analysis	2445
4	Backdoors	2222
5	DoS	13199
6	Exploits	37504
7	Generic	45173
8	Reconnaissance	11742
9	Shellcode	1298
10	Worms	149

A. DATASET AND CLASSIFICATION ALGORITHMS UTILIZED

In this paper, three supervised machine learning algorithms (classification algorithms) used in IDS schemes namely Naïve Bayes (NB), Decision Tree (DT) and k-Nearest Neighbor (k-NN) were evaluated on the UNSW-NB15 dataset [67].

The UNSW-NB15 dataset was created at the University of New South Wales in 2015. It was developed using the IXIA Perfect Storm tool. The UNSW-NB15 dataset consists of a hybrid of modern normal and synthesized malicious network traffic. It was extracted from 100GB of raw network packets acquired using tcpdump [6]. The dataset is stored in four CSV files, it contains 2,540,044 records with 49 features extracted using Bro-IDS, Argus tools and twelve algorithms developed using C# programming language. It contains nine different classes of attacks which are fuzzers, analysis, backdoors, DoS, exploits, generic, reconnaissance, shellcode, and worms. The description of the attacks in the dataset can be found in [67]. Majority of the attacks are executed to check or exploit the weakness or vulnerabilities of computer systems. The vulnerabilities and weaknesses can further be utilized to perform other attacks such as Botnet attacks which are discussed in section 2.

The dataset was chosen because its traffic contains properties of modern networks. For the experiments in this paper, 200,696 samples were randomly extracted from the UNSW-NB15 dataset. Table 7 provides the distribution of the extracted sample of the dataset.

Machine learning algorithms are one of the widely used techniques in developing IDS schemes. In this paper, supervised machine learning algorithms also called classification algorithms are utilized because intrusion detection challenges are usually classification problems and also the dataset includes predefined classes. The classifiers utilized are briefly explained below:

- Naïve Bayes [23], [51]: The Naive Bayes makes an assumption about the independence of all features in its operation. It utilizes the Bayes theorem during the classification process. It searches for the maximum likelihood

TABLE 8. Confusion matrix.

	Predicted Class Label	
	Positive	**Negative**
Actual Class Label		
Positive	True positive	False-negative
Negative	False-positive	True negative

hypothesis that classifies a class label. The implementation time of NB is short and also it performs well in practical applications.

- Decision Tree [23], [51]: The decision tree refers to structural techniques like a tree with branches and leaves. The branches represent features that result in classes while the leaves symbolize the class. The J48 used in this paper is a variant of the DT which improves the C 4.5. It was implemented by Ross Quinlan [68] in 1993.
- k-Nearest Neighbor [69]: The k-NN also referred to as an instance-based learning classifier classifies new unknown data by observing the K data points in a training set that is near to it in the input space. Hence it needs a distance measuring technique such as Manhattan or Euclidean distance measuring technique. The k-NN is also called a lazy learner because it doesn't learn anything during the training phase.

B. PERFORMANCE METRICS

The evaluations of IDS schemes are based on an estimation of a confusion matrix [70]. The aim of the confusion matrix is to relate actual and predicted labels. The intrusion detection is defined by a 2 by 2 confusion matrix as shown in table 8 for its evaluations because it consists of two classes i.e. normal and abnormal (attack).

The performance metrics are derived from the terms in the confusion matrix. These terms are described below:

i. True Positive (TP): Total predicted classes as true that are actually true.
ii. False Positive (FP): Total predicted classes as true that are actually false.
iii. True Negative (TN): Total predicted classes as false that are actually false.
iv. False Negative (FN): Total predicted classes as false that are actually true.

Given the True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN). The performance metrics can be defined below:

- **Accuracy** is a metric that estimates the overall percentages of detection and false alarms an IDS model produces, it reflects the overall success rate of any IDS, and is computed as,

$$\text{Accuracy} = (\text{TN} + \text{TP})/(\text{TP} + \text{FP} + \text{TN} + \text{FN}) \quad (1)$$

- The **Detection Rate (DR)**, also called the true positive rate (TPR) or recall, is the proportion of correctly classified malicious instances of the total number of malicious vectors and is computed as,

$$\text{DR} = \text{TP}/(\text{FN} + \text{TP}) \quad (2)$$

- The **False Positive Rate (FPR)** also called false alarm rate is the percentage of normal vectors of the total number of normal vectors misclassified as attacks and is computed as,

$$\text{FPR} = \text{FP}/(\text{FP} + \text{TN}) \quad (3)$$

- The **False Negative Rate (FNR)** also called precision is the percentage of misclassified attack vectors of the total number of attack instances, given as,

$$\text{FNR} = \text{FN}/(\text{FN} + \text{TP}) \quad (4)$$

An additional performance metric of IDS is the **Receiver Operating Characteristics (ROC)** curve. It represents the relationship between TPR and FPR. A value closer to 100% or 1 indicates good performance in attack detection and lower value shows the weakness of the attack detection.

The performance evaluation was performed using Waikato Environment for Knowledge Analysis (WEKA) [71] on a windows 10 operating system with 8GB RAM and i7 processor @ 2.70 GHz.

C. RESULTS AND DISCUSSION

In order to perform the experiments on WEKA. The extracted sample comprises of the nine classes of attacks within the UNSW-NB15 dataset. We further employed correlation coefficient and information gain methods for feature selections in order to remove irrelevant and redundant features and also obtain good performance from the classification algorithms [72]. The features with values closer to 1 are selected as it signifies more information or better relation. The features selected are presented in tables 9 and 10. A 10 fold cross-validation was used in the evaluation process using the default settings of each algorithm. The algorithms are evaluated in terms of accuracy, false-positive rate, and ROC curve area. The results of the comparison between the two feature selection methods and the accuracy results of each algorithm in the classification of attacks are presented below.

Figure 4, presents the accuracy rate for the classification between normal and abnormal instances. The k-NN records the highest accuracy both in the correlation coefficient and the information gain feature selection methods with 94.71% and 94.38% respectively. The Naïve Bayes records the lowest accuracy rate with 85.43% and 85.11% for correlation coefficient and information gain respectively. The J48 achieves 93.16% and 91.79% for correlation coefficient and information gain respectively. The higher accuracy of the classifiers signifies a better detection rate.

Figure 5, presents the false-positive rates for the evaluated classifiers, low false positive rate values indicate good performance of the classifiers. The k-NN achieves the lowest

TABLE 9. Features selected using correlation coefficient.

S/No	Selected feature	Description
1	proto	Transactional protocol
2	service	Service type, e.g., http, ftp, ssh, dns
3	sttl	Source to destination time to live
4	sload	Source bits per second
5	ct_srv_src	No. of connections that contain the same service and source address connections according to the last time
6	ct_state_ttl	No. for each state according to specific range of values for source/destination time to live
7	ct_src_dport_ltm	No of connections of the same source address and the destination in 100 connections
8	ct_dst_sport_ltm	No of connections of the same destination address and the source port in 100 connections
9	ct_dst_src_ltm	No of connections of the same source and the destination address in 100 connections
10	ct_src_ltm	No. of connections of the same source address in 100 connections
11	ct_srv_dst	No. of connections that contain the same service and destination address in 100 connections

TABLE 10. Features selected using information gain.

S/No	Selected feature	Description
1	dur	Record total duration
2	sbytes	Source to destination bytes
3	dbytes	Destination to source bytes
4	sttl	Source to destination time to live
5	sload	Source bits per second
6	dload	Destination bits per second
7	sintpkt	Source inter-packet arrival time (mSec
8	dintpkt	Destination inter-packet arrival time (mSec)
9	sjit	Source jitter (mSec)
10	djit	Destination jitter (mSec)
11	stcpb	Source TCP sequence number
12	dtcpb	Destination TCP sequence number
13	tcprtt	The sum of 'synack' and 'ackdat' of the TCP

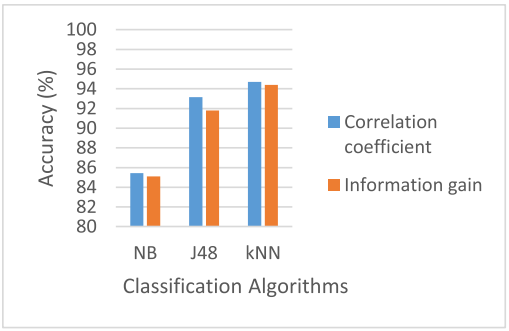

FIGURE 4. Accuracy rate of kNN, J48, and Naïve Bayes.

value with 0.079 and 0.084 for the correlation coefficients and information gain, respectively. J 48 records the highest values with 0.138 and 0.172 for the correlation coefficients

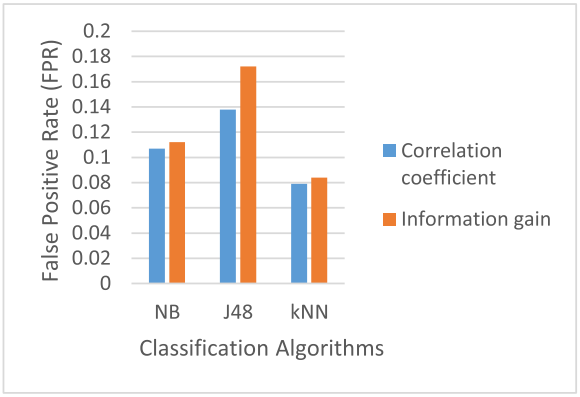

FIGURE 5. False-positive rate of kNN, J48, and Naïve Bayes.

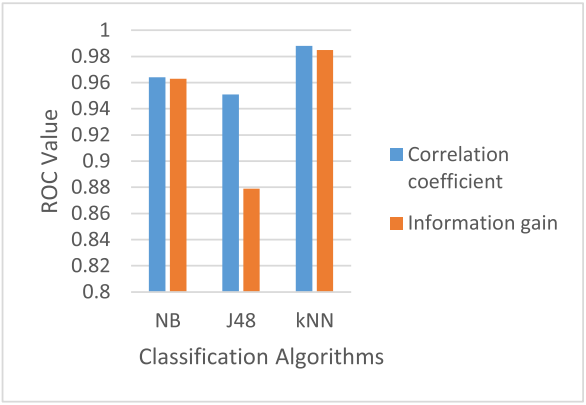

FIGURE 6. ROC curve values of k-NN, J48, and Naïve Bayes.

and information gain, respectively while Naïve Bayes records 0.107 and 0.112 or the correlation coefficients and information gain, respectively.

Figure 6, presents the ROC curve values for the k-NN, J48 and Naïve Bayes. The ROC curves values closer to 1 signifies good performance of the classifier.

The k-NN achieves the highest value with 0.988 and 0.985 for the correlation coefficients and information gain, respectively. J48 records the lowest value with 0.951 and 0.879 for the correlation coefficients and information gain, respectively. The Naïve Bayes classifier records 0.964 and 0.963 for the correlation coefficients and information gain, respectively.

The results obtained from the evaluations show that features selected using the correlation coefficients provide a slightly better result than the features selected using the information gain with k-NN recording the highest accuracy and lowest false positive rate. Both feature selection methods provide information or relation about the features, correlation coefficients give information on how the change in the one variable affects other variables, similarly, the information gain also gives information about the relationship between the features and the output.

Figure 7, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the backdoor attacks. The J48 recorded

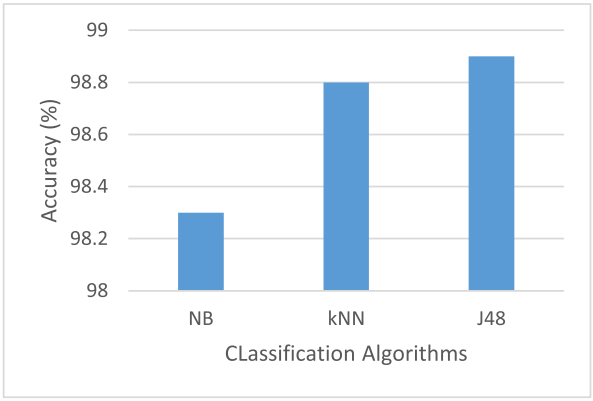

FIGURE 7. Classification accuracy on Backdoor attack.

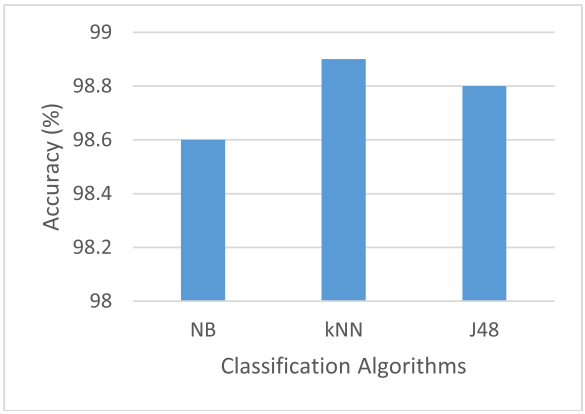

FIGURE 8. Classification accuracy on Analysis attack.

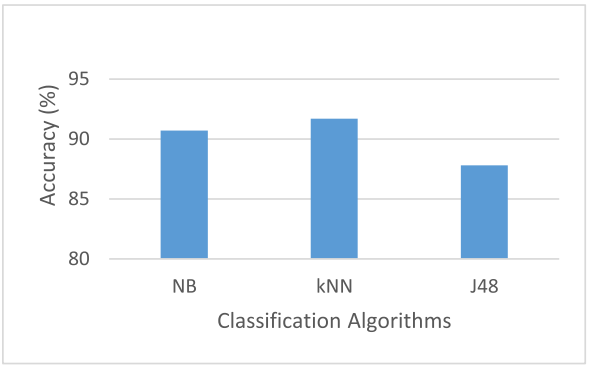

FIGURE 9. Classification accuracy on Fuzzers attack.

the highest accuracy with 98.9 %, while NB and k-NN recorded 98.3%, and 98.8%, respectively.

Figure 8, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the analysis attacks. The k-NN recorded the highest accuracy with 98.9 %, while NB and J48 recorded 98.6%, and 98.8%, respectively.

Figure 9, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the fuzzers attacks. The k-NN recorded the highest accuracy with 91.7 %, while NB and k-NN recorded 90.7%, and 87.8%, respectively.

Figure 10, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the shellcode attacks.

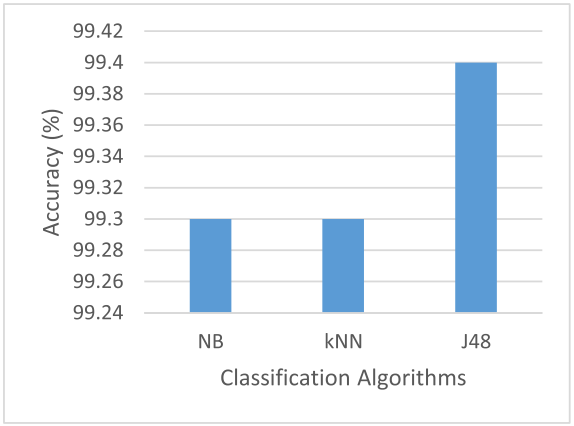

FIGURE 10. Classification accuracy on Shellcode attack.

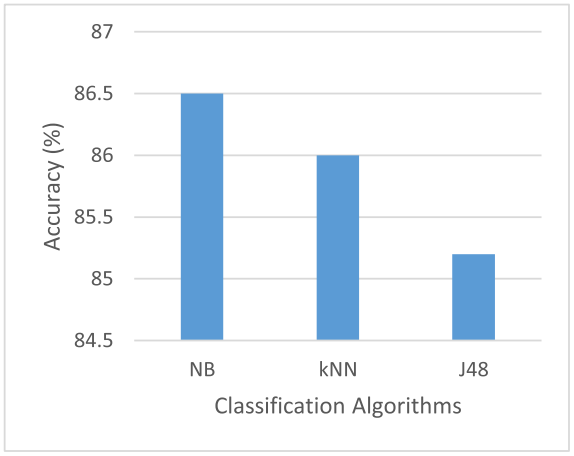

FIGURE 11. Classification accuracy on Exploits attack.

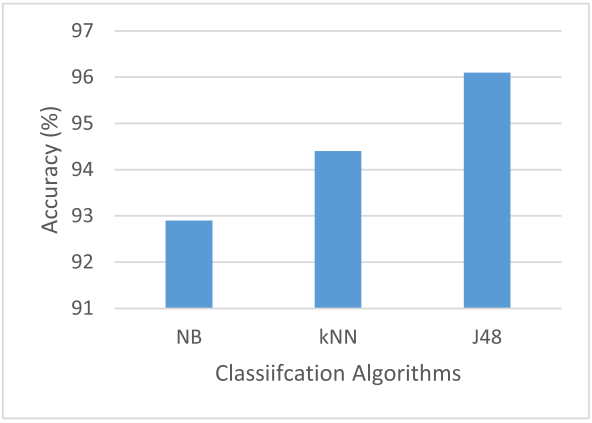

FIGURE 12. Classification accuracy on Reconnaissance attack.

The J48 recorded the highest accuracy with 99.4 %, while NB and k-NN both recorded 99.3%.

Figure 11, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the exploits attacks. The NB recorded the highest accuracy with 86.5 %, while k-NN and J48 recorded 86%, and 85.2%, respectively.

Figure 12, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the reconnaissance attacks.

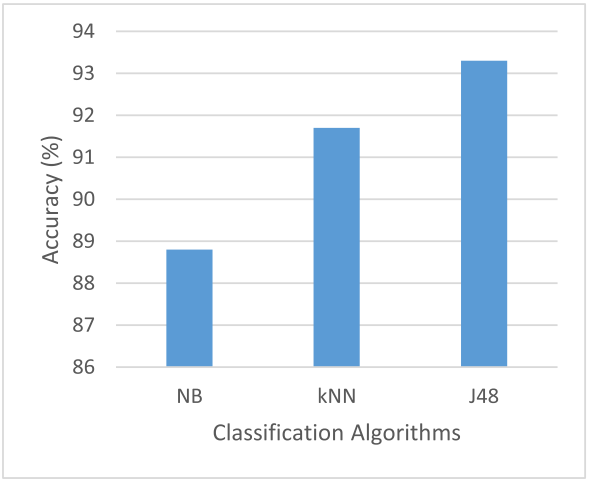

FIGURE 13. Classification accuracy on DoS attack.

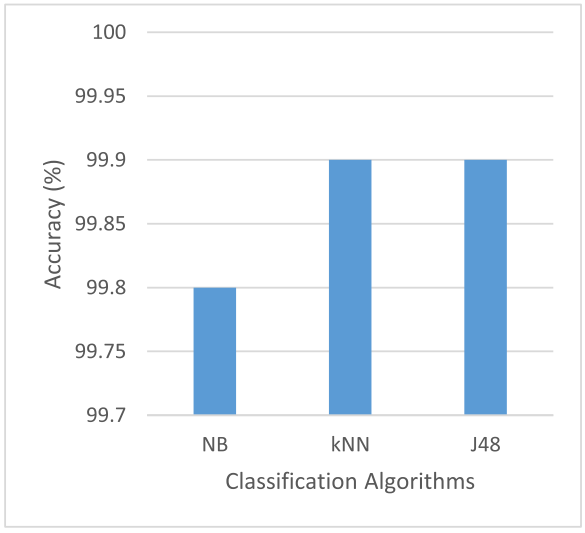

FIGURE 14. Classification accuracy on Worms attack.

The J48 recorded the highest accuracy with 96.1 %, while k-NN and NB recorded 94.4 %, and 92.9 %, respectively.

Figure 13, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the DoS attacks. The J48 recorded the highest accuracy with 93.3 %, while k-NN and NB recorded 91.7 %, and 88.8 %, respectively.

Figure 14, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the Reconnaissance attacks. Both J48 and k-NN recorded 99.9 %, while NB recorded 99.8 %.

Figure 15, presents the accuracy of the k-NN, J48 and Naïve Bayes in classifying the generic attacks. Both k-NN and J48 recorded 99.3 %, while NB recorded 98.3%.

The classification algorithms evaluated performed satisfactorily in the classification of attacks based on the classes as described in the dataset. Results from figure 3 show that k-NN has higher accuracy in distinguishing normal and abnormal traffic. However, the J48 performs better in classification based on the class of the attack. Results from

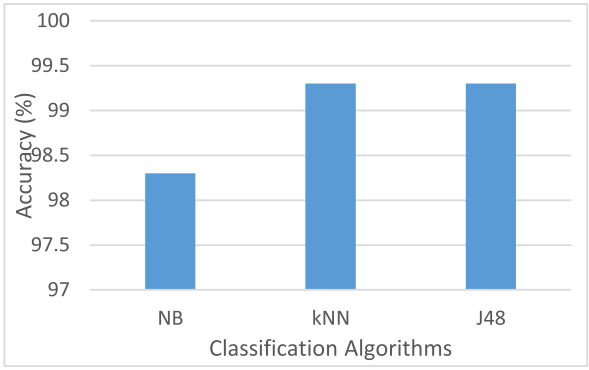

FIGURE 15. Classification accuracy on Generic attack.

TABLE 11. Summary of accuracy rates of k-NN, J48, and NB.

S/No	Attack classes	Classification Algorithms		
		k-NN (%)	**J48 (%)**	**NB (%)**
1	Backdoor	98.8	98.9	98.3
2	Analysis	98.9	98.8	98.6
3	Shellcode	99.3	99.4	99.3
4	Reconnaissance	94.4	96.1	92.9
5	DoS	91.7	93.3	88.8
6	Fuzzers	91.7	87.8	90.7
7	Worms	99.9	99.9	99.8
8	Exploits	86	85.2	86.5
9	Generic	99.3	99.3	98.3

figure 7 -15 show that J48 has achieved higher accuracy in classifying the backdoor, shellcode, reconnaissance and DoS attacks. While k-NN recorded higher accuracy in classifying the analysis and fuzzers attacks. Similarly, NB achieved higher accuracy in classifying the exploits attack. Both k-NN and J48 recorded the same accuracy in classifying worm and generic attacks. Table 11, presents the summary of the accuracy of k-NN, J48 and NB algorithms on attack classification.

In summary, the results show that features selected using the correlation coefficients provide a marginally better result than the features selected using the information gain. Similarly, k-NN has higher accuracy in distinguishing normal and abnormal traffic while J48 performs better in classification based on the class of the attack. While NB has the highest accuracy in detecting the exploits attack. The performance of k-NN, J48 and NB algorithms is attributed to their operational procedure and nature of the selected features utilized from the dataset.

The k-NN performs classification on the test sample by measuring the closest distance between the test sample and the majority of similar samples using the k-nearest neighbor. Parameters such as the Euclidian distance technique as the distance measurement technique and the value of $K = 5$ were selected. Hence, the reason for good performance in binary classification, the features selected provide a considerable difference between the normal and attack traffic instances.

The J48 performs its classification decisions based on tree rules where the branches represent the features and the leaves represent the class. The utilization of relevant features helps in achieving good results in the multiclass classification.

The NB performs its classification by assuming all features are independent. However, there is a dependence between the selected features in the dataset. This assumption of independence in the features attributed to the lower accuracy recorded by NB compared to the other evaluated classification algorithms (k-NN and J48).

V. CHALLENGES AND FUTURE DIRECTION

The IoT is characterized by limited resources such as memory and computational capabilities as well as the heterogeneity of standards and protocols. These factors contribute largely to challenges in the research on security issues of IoT, anomaly mitigation using intrusion detection systems (IDS) inclusive. Despite numerous research in the area of anomaly detection within IoT networks, there are several important open issues that need further studies. Some of these issues are:

i. Lack of technology and protocol coverage in proposing of anomaly mitigation schemes.
Several proposed IDS schemes in IoT utilize popular protocols and technologies such as the 6LoWPAN and HTTP. While protocols and technologies such as Z-wave, Bluetooth Low Energy (BLE), and Constrained Application Protocol (CoAP) among others are excluded, which also contributes to building the IoT landscape. Hence, for proper protection of the entire IoT environment, the research community, on one hand, should make efforts in proposing solutions that will cover other protocols and technologies used in the IoT. On the other hand, a platform can be proposed to integrate various solutions across different protocols and technologies.

ii. Lack of public IoT network traffic datasets.
The unavailability of public IoT datasets poses another challenge. Since evaluating and validating the anomaly mitigation schemes will be difficult on the real network, efforts in creating an IoT dataset are required. This will ease the evaluation and validation of the proposed anomaly mitigation schemes in IoT.

iii. Lack of standard validation applications for IoT.
The validation of proposed schemes is vital because it ensures the schemes are satisfactorily developed. The proposed schemes are widely evaluated using simulation or experiments. However, majority of the proposed IDS schemes in the IoT are not evaluated/benchmarked against other IDS schemes in the IoT due to the lack of enough standard validation applications. Hence efforts are required in developing standard validation, which will ensure replication or reproducibility and continuity of research.

iv. Effective deployment of anomaly mitigation schemes on IoT despite the lack of enough resources.
Deployment and effective operation of the IDS schemes in the IoT depends on the availability of resources such as computation and storage. However, the lack of enough resources is one of the main challenges in the IoT. In order to solve the operational requirement challenges in terms of computation and storage of the IDS schemes in the IoT, the fog or edge devices could be employed. This will help in reducing the burden of the computational overhead on the resource-constrained IoT nodes and will further make the IoT network more efficient and effective.

VI. CONCLUSION

With the growth in the adoption of IoT in our daily activities, protecting the network cannot be overemphasized. A successful attack can cause devastating or negative consequences in our activities. In this paper, a brief overview of the IoT concept, security threats, and intrusion detection systems are discussed. A review of network anomaly mitigation schemes in IoT networks is also presented. The review focused on the objectives, operational procedures and strengths of each scheme. A comparison table of the reviewed schemes, as well as a taxonomy based on the detection methodology, is provided. Furthermore, unlike other surveys that perform a qualitative evaluation, our survey provides both qualitative and quantitative evaluations. Performance evaluation of k-NN, J48, and Naïve Bayes classification algorithms using the Waikato Environment for Knowledge Analysis (WEKA) application was conducted on the UNSW-NB15 dataset. Results from the performance evaluation show that the k-NN achieves the highest accuracy and lowest false positive rates in distinguishing normal and abnormal traffic while J48 performs better than k-NN and NB in classification according to the class of attack. Lastly, challenges and future directions in the development of network anomaly mitigation schemes in IoT are highlighted.

ACKNOWLEDGMENT

The authors would like to thank King Abdulaziz University Jeddah, Saudi Arabia, for providing necessary facilities for conducting their research.

REFERENCES

[1] M. Burhan and R. A. Rehman, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, pp. 1–37, 2018.
[2] D. Reinsel, J. Gantz, and J. Rydning, "The digitization of the world from edge to core," Int. Data Corp., Framingham, MA, USA, IDC White Paper Doc# US44413318, 2018. [Online]. Available: https://www.seagate.com/em/en/our-story/data-age-2025/
[3] D. M. Hawkins, *Identification of Outliers*, vol. 11. London, U.K.: Chapman & Hall, 1980.
[4] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," in *Proc. IEEE 15th Int. Symp. Intell. Syst. Informat. (SISY)*, Sep. 2017, pp. 277–282.
[5] I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," *Inf. Sci.*, vol. 239, pp. 201–225, Aug. 2013.
[6] TCPDUMP/LIBPCAP. *Tcpdump/Libpcap Public Repository*. Accessed: Apr. 15, 2019. [Online]. Available: https://www.tcpdump.org/
[7] G. Combs. *Wireshark*. Accessed: Apr. 15, 2019. [Online]. Available: https://www.wireshark.org/
[8] J. P. Anderson, *Computer Security Threat Monitoring and Surveillance*. Fort Washington, PA, USA: Anderson, 1980.
[9] 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.

[10] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3496–3509, Jun. 2018.

[11] 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.

[12] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, Dec. 2018.

[13] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," *IEE Internet Initiat.*, vol. 1, pp. 1–86, May 2015.

[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[15] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[16] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Gener. Comput. Syst.*, vol. 100, pp. 144–164, Nov. 2019.

[17] A. Al-fuqaha, S. Member, M. Guizani, M. Mohammadi, and S. Member, "Internet of Things?: A survey on enabling," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 2015.

[18] Z. A. Baig, S. Sanguanpong, S. N. Firdous, V. N. Vo, T. G. Nguyen, and C. So-In, "Averaged dependence estimators for DoS attack detection in IoT networks," *Future Gener. Comput. Syst.*, vol. 102, pp. 198–209, Jan. 2020.

[19] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[20] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[21] N. Moustafa, J. Hu, and J. Slay, "A holistic review of network anomaly detection systems: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 128, pp. 33–55, Feb. 2019.

[22] S. Plaga, N. Wiedermann, S. D. Anton, S. Tatschner, H. Schotten, and T. Newe, "Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions," *Future Gener. Comput. Syst.*, vol. 93, pp. 596–608, Apr. 2019.

[23] N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, Jun. 2019.

[24] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.

[25] R. A. Shaikh, H. Jameel, B. D'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Intrusion-aware alert validation algorithm for cooperative distributed intrusion detection schemes of wireless sensor networks," *Sensors*, vol. 9, no. 8, pp. 5989–6007, Jul. 2009.

[26] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial Internet of Things based on deep learning models," *J. Inf. Secur. Appl.*, vol. 41, pp. 1–11, Aug. 2018.

[27] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in *Proc. IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2013, pp. 600–607.

[28] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Gener. Comput. Syst.*, vol. 96, pp. 481–489, Jul. 2019.

[29] A. Marques da Silva Cardoso, R. Fernandes Lopes, A. Soares Teles, and F. Benedito Veras Magalhaes, "Poster abstract: Real-time DDoS detection based on complex event processing for IoT," in *Proc. IEEE/ACM 3rd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2018, pp. 273–274.

[30] A. Sforzin, F. G. Marmol, M. Conti, and J.-M. Bohli, "RPiDS: Raspberry pi IDS—A fruitful intrusion detection system for IoT," in *Proc. Intl IEEE Conferences Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul. 2016, pp. 440–448.

[31] P. P. Ioulianou, V. G. Vassilakis, I. D. Moscholios, and M. D. Logothetis, "A signature-based intrusion detection system for the Internet of Things," in *Proc. Inf. Commun. Technol. Forum (ICTF)*, 2018, pp. 1–7.

[32] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019.

[33] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Jan. 2013, Art. no. 794326.

[34] A. Nikam and D. Ambawade, "Opinion metric based intrusion detection mechanism for RPL protocol in IoT," in *Proc. 3rd Int. Conf. for Converg. Technol. (ICT)*, Apr. 2018, pp. 1–6.

[35] T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, and M.-C. Hsieh, "A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN," in *Proc. Adv. Technol., Embedded Multimedia Hum.-centric Comput.*, vol. 260, no. 77, pp. 1257–1268, 2014.

[36] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in Internet of Things," *Int. J. Comput. Appl.*, vol. 121, no. 9, pp. 1–9, Jul. 2015.

[37] 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.

[38] 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.

[39] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for Internet-of-Things," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 319–320.

[40] V. Adat and B. B. Gupta, "A DDoS attack mitigation framework for Internet of Things," in *Proc. Int. Conf. Commun. Signal Process.*, 2017, pp. 2036–2041.

[41] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for Internet of Things," in *Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2017, pp. 1169–1176.

[42] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Multidimensional trust-based anomaly detection system in Internet of Things," in *Wireless Algorithms, Systems, and Applications* (Lecture Notes in Computer Science), vol. 10251. Cham, Switzerland: Springer, 2017, pp. 302–313.

[43] K. Sonar and H. Upadhyay, "An approach to secure Internet of Things against DDoS," in *Proc. Int. Conf. ICT Sustain. Develop.*, vol. 408, 2016, pp. 367–376.

[44] L. Lyu, J. Jin, S. Rajasegarar, X. He, and M. Palaniswami, "Fog-empowered anomaly detection in IoT using hyperellipsoidal clustering," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1174–1184, Oct. 2017.

[45] D. H. Hoang and H. D. Nguyen, "A PCA-based method for IoT network traffic anomaly detection," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 381–386.

[46] Y. Liu and Q. Wu, "A lightweight anomaly mining algorithm in the Internet of Things," in *Proc. IEEE 5th Int. Conf. Softw. Eng. Service Sci.*, Jun. 2014, pp. 1142–1145.

[47] T. Qin, B. Wang, R. Chen, Z. Qin, and L. Wang, "IMLADS: Intelligent maintenance and lightweight anomaly detection system for Internet of Things," *Sensors*, vol. 19, no. 4, p. 958, Feb. 2019.

[48] C. Ioannou and V. Vassiliou, "An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression," in *Proc. 21st ACM Int. Conf. Model., Anal. Simul. Wireless Mobile Syst. (MSWIM)*, 2018, pp. 259–263.

[49] S. A. Aljawarneh and R. Vangipuram, "GARUDA?: Gaussian dissimilarity measure for feature things," *J. Supercomput.*, to be published.

[50] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, and R. Dash, "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," *Future Gener. Comput. Syst.*, vol. 89, pp. 685–697, Dec. 2018.

[51] P. Dangeti, *Statistics for Machine Learning*. Birmmingham, U.K.: Packt, 2017.

[52] P. Shukla, "ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things," in *Proc. Intell. Syst. Conf. (IntelliSys)*, Sep. 2017, pp. 234–240.

[53] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," *J. Supercomput.*, vol. 74, no. 10, pp. 5156–5170, May 2018.
[54] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K.-R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 314–323, Apr. 2019.
[55] M. Hosseini and H. R. S. Borojeni, "A hybrid approach for anomaly detection in the Internet of Things," in *Proc. Int. Conf. Smart Cities Internet Things (SCIOT)*, 2018, pp. 1–6.
[56] R. Fu, K. Zheng, D. Zhang, and Y. Yang, "An intrusion detection scheme based on anomaly mining in Internet of Things," in *Proc. 4th IET Int. Conf. Wireless, Mobile Multimedia Netw. (ICWMMN)*, 2011, pp. 315–320.
[57] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "Cross layer-based intrusion detection based on network behavior for IoT," in *Proc. IEEE 19th Wireless Microw. Technol. Conf. (WAMICON)*, Apr. 2018, pp. 1–4.
[58] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, May 2018.
[59] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Intelligent intrusion detection in low-power IoTs," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–25, Dec. 2016.
[60] T. Luo and S. G. Nagarajan, "Distributed anomaly detection using autoencoder neural networks in WSN for IoT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[61] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks," in *Proc. 3rd ACM Int. Workshop IoT Privacy, Trust, Secur. (IoTPTS)*, 2017, pp. 31–38.
[62] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.
[63] M. N. Napiah, M. Y. I. Bin Idris, R. Ramli, and I. Ahmedy, "Compression header analyzer intrusion detection system (CHA–IDS) for 6LoWPAN communication protocol," *IEEE Access*, vol. 6, pp. 16623–16638, 2018.
[64] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," *Comput. Commun.*, vol. 98, pp. 52–71, Jan. 2017.
[65] E. Anthi, L. Williams, and P. Burnap, "Pulse: An adaptive intrusion detection for the Internet of Things," in *Proc. Living Internet Things, Cybersecurity*, 2018, p. 35.
[66] Z. D. M. Seifeddine. *Hybrid Intrusion Detection System*. Adelaide SA, Australia: The University of South Australia, 2014.
[67] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. MilCIS*, 2015, pp. 1–6.
[68] J. R. Quinlan, *C4. 5: Programs for Machine Learning*. San Francisco, CA, USA: Morgan Kaufmann, 1993.
[69] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 161–175, Aug. 2018.
[70] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 303–336, 1st Quart., 2014.
[71] E. Frank, Mark A. Hall, and I. H. Witten, *Data Mining: Practical Machine Learning Tools and Techniques*. 4th ed. San Mateo, CA, USA: Morgan Kaufmann, 2016.
[72] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, and H. Karimipour, "Cyber intrusion detection by combined feature selection algorithm," *J. Inf. Secur. Appl.*, vol. 44, pp. 80–88, Feb. 2019.

MUHAMMAD AMINU LAWAL received the B.Eng. degree in electrical and computer engineering from the Federal University of Technology Minna, Nigeria, in 2006, and the M.S. degree in distributed computing from Universiti Putra Malaysia, in 2014. He is currently pursuing the Ph.D. degree in computer science with King Abdulaziz University, Jeddah, Saudi Arabia. His research interest includes network security and privacy in smart city environment.

RIAZ AHMED SHAIKH received the Ph.D. degree from the Computer Engineering Department, Kyung Hee University, South Korea, in 2009. He is currently an Associate Professor with the Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia. He wrote more than 50 research articles published in peer-reviewed journals and conferences. The two U.S. and one Korean patents are issued to him. His research interests include privacy, security, trust management, risk estimation, sensor networks, vehicular networks, and the IoT. He has served as a Technical Program Committee member of more than 35 international conferences. He was also an Editor of the book entitled *Secure Cyber-Physical Systems for Smart Cities* (USA: IGI Global).

SYED RAHEEL HASSAN received the Ph.D. degree in network security from he Universite de Franche-Comte, France. Before his Ph.D. degree, he worked four years in the industry as a Network Administrator. He has been working in academia for last seven years. He has completed a Research Fellowship with Emory University, USA. He is currently affiliated with the Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia, which is ranked 186 according to QS world ranking of the universities for 2019. He is also involved in multiple projects related to Network Security, such as Intrusion Detection Systems in distributed networks and Smart Authentication for future networks.