SDN based Intrusion Detection and Prevention Systems using Manufacturer Usage Description: A Survey

Noman Mazhar[1]
Faculty of Computer Science and Information Technology
University of Malaya, Lembah Pantai
50603 Kuala Lumpur Malaysia

Rosli Salleh[2]
Faculty of Computer Science and Information Technology
University of Malaya, Lembah Pantai
50603 Kuala Lumpur Malaysia

Mohammad Asif Hossain[3]
Faculty of Computer Science and Information Technology
University of Malaya, Lembah Pantai
50603 Kuala Lumpur Malaysia

Muhammad Zeeshan[4]
School of Electrical Engineering and Computer Science
National University of Sciences and Technology
Islamabad

***Abstract*—Internet of things (IoT) is an emerging paradigm that integrates several technologies. IoT network constitutes of many interconnected devices that include various sensors, actuators, services and other communicable objects. The increasing demand for IoT and its services have created several security vulnerabilities. Conventional security approaches like intrusion detection systems are not up to the expectation to fulfil the security challenges of IoT networks, due to the conventional technologies used in them. This article presents a survey of intrusion detection and prevention system (IDPS), using state of art technologies, in the context of IoT security. IDPS constitutes of two parts: intrusion detection system and intrusion prevention system. An intrusion detection system (IDS) is used to detect and analyze both inbound and outbound network traffic for malicious activities. An intrusion prevention system (IPS) can be aligned with IDS by proactively inspecting a system's incoming traffic to mitigate harmful requests. The alignment of IDS and IPS is known as intrusion detection and prevention systems (IDPS). The amalgamation of new technologies, like software-defined network (SDN), machine learning (ML), and manufacturer usage description (MUD), in IDPS is putting the security on the next level. In this study IDPS and its performance benefits are analyzed in the context of IoT security. This survey describes all these prominent technologies in detail and their integrated applications to complement IDPS in the IoT network. Future research directions and challenges of IoT security have been elaborated in the end.**

Keywords*—Intrusion Detection and Prevention Systems (IDPS); Internet of Things (IoT); Software Defined Network (SDN); Machine Learning (ML); Deep learning (DL); Manufacturer Usage Description (MUD)

I. Introduction

Internet revolutionizes our daily life and provides so many services that have become no more luxurious but the ultimate need for life. The Internet of things is the name of a smart environment that consists of many interconnected objects, to provide useful and instant services. These objects are not only traditional mobile devices or computers but also the gadgets of daily life like wearable devices, watches, and other smart articles. With the evolution of wireless sensor networks and recent improvement in the technology along with the expansion of low power devices, amplify the number of devices that can be connected to the Internet [1].

IoT inherits most of the conventional technologies for communication and so the security issues in them. The attacks such as worm attacks, denial of service attacks, etc. have become serious concerns [2]. There are many ways to address these security threats. A multitude of approaches used includes security systems and frameworks that have been adopted by the industry and research community. The intrusion detection and prevention systems (IDPS) is one of such systems.

The IDPS is not only capable to detect malicious activities like worms, viruses, distributed denial of services (DDoS), and others, but also capable to prevent the attacks before it happens. The detection system checks the traffic if it is normal or it should be blocked or regulate it to some different zone like a honeypot. Conventional IDPS has some limitations to defend against the latest security threats and also not feasible for devices with limited resources like IoT devices. Therefore, painstaking research has been done on developing the new generation of IDPS systems based on emerging technologies like Software Defined Networking (SDN) and Machine Learning (ML). A new contender, Manufacturer usage description (MUD), is also playing its role to reduce the attack surface for IoT devices.

SDN is recently a developing technology with different management and design approaches for networking. The design paradigm of this technology decouples the data and control planes. This gave the centralized and global view of the network. The controller is the decision-making authority while the switches and routers are the forwarding devices that handle data forwarding only. The controller and the forwarding devices work in a master and slave mode. The controller instructs the switches, how to handle the incoming and outgoing packets or flows. SDN is considered to be the best network model to address the heterogeneous changes in the overall network [3].

Along with the SDN technology, a new concept has been introduced for the identification of IoT devices known as "Manufacturer usage description" (MUD). MUD is a developing concept to define IoT device behaviour for network communication [4]. This automatically identifies the device and helps the security system to figure out the abnormal or malicious nodes within the network. For complete detection and monitoring of malicious activity in the network machine learning plays its role. For the detection of malware and malicious traffic, ML techniques have the primary role. In traditional networks, detection of malicious traffic and classification of a network attack is achieved using predefined rules and specifications which are limited to address new kinds of attacks. The main application of using ML in SDN networks is the control of the entire network rather than just focusing on localized policy or certain rules [5]. Such techniques show great potential for network traffic classification and solving prediction problems [6]. ML is used in the IDPS systems for the detection of security attacks and to predict future threats to the system.

In this paper, our research focuses on SDN based IDPS systems for IoT security using ML and device profile based techniques like MUD. Further, the study classifies IDPS systems based on the technology they use. Besides, we compare the conventional IDPS systems to new generation IDPS systems in the context of IoT security. Also, the study shows the performance of these new generation IDPS for IoT based networks. The overall research approach is shown in Fig. 1, we provide the future directions for upcoming secure systems along with the IDPS future perspectives in the domain of IoT security framework.

A. Contribution of this Survey Article

As the IoT scalability and heterogeneous increases over time, IDPS systems become inevitable. There is a lot of survey work done on the intrusion detection systems for the IoT but to the best of our knowledge, no work has been done on IDPS for IoT devices using the device profile base techniques like MUD for comprehensive security for IoT. As shown in Fig. 3. The contribution of this paper is to analyze the end to end IoT security solution based on IDPS using techniques like SDN and ML. The main points are given below:

1) Present the taxonomy of the IDPS for IoT using SDN and ML and hybrid approaches.
2) Investigate the IoT device profile standard like MUD in enhancing the IoT security in IDPS for IoT.
3) We analyse the performance of the IDPS systems based on SDN, ML, and MUD.

The paper is organized as shown in Fig. 2. Section II provides an overview of IoT, several security issues of IoT and their taxonomies, IDS and IPS and their integration. Section III presents the basic overview of SDN, ML and MUD technologies. Section IV describes the detail applications of SDN, ML and MUD in IDPS of IoT system. Section V outlines some open issues, challenges, and future research directions, and finally, Section VI concludes the paper. The acronyms used in this paper and their full forms are listed in Table I.

B. Related Works

Machine Learning applications have been proliferated in almost every field, especially in security. This gets the attention of many researchers and industrialists'. But ML requires a platform to unleash its potential. For network security IDPS provides a strong platform. Powering the IDPS system with ML, SDN, and MUD proving to be useful. IDPS system becomes a lot more effective and worthy for network security as in paper [7] presented an updated review on the IDPS systems. It shows the classification of IDPS systems and their role in securing the conventional network. The review did not talk about IoT security using IDPS systems. It also did not discuss SDN. Going further, paper [8] emphasized on the intrusion detection system in general and then specific to the context of IoT. Since IoT devices and systems are so diverse therefore they require proper security mechanisms to defend the system from cyberattacks. The study works more on the IDS for IoT networks and does not put any light on the latest technologies prevention techniques.

Much research focuses on the IoT security aspects like in [9] the author mostly focused on the IoT protocols and standards for different layers of network stack like medium access layer, Network Layer, and Session layer. Other than this the study explains different management and security standards, developed by the international engineering task force (IETF), Institute of electrical and electronics Engineers (IEEE), international telecommunication union (ITU), and other bodies. But the survey is more focused on IoT security, but not much explains about the new technologies like SDN and ML and their role in IoT security. Similarly, a study [10] focused on the state of art approaches like ML for IoT as well as intrusion detection for network security. But the focus of the study is on the ML approach and did not cover other technologies like SDN and MUD in this case. The study [11] explained the IoT architecture, IoT attacks. Then explain IDS technology and its types describing its use in IoT networks. It also classified different IDS systems used in IoT networks and the type of technology they use. Again, the issue is that they didn't consider the latest techniques like SDN and MUD for the security of IoT networks. Furthermore, they shed no light on the prevention systems along with the detection systems.

Further, the research shows the applicability of intrusion detection systems in IoT security as in research [12] showed the importance of IDS in defending IoT devices from cyber threats. It classifies different IDS systems based on the detection and deployment scenarios, explains different IoT attacks, and compares different IDS systems against the detection accuracy, false positive, resource consumption, and other attributes. The research work considers different IDS for the IoT defence systems but they were mostly based on conventional techniques, no state of art technique was considered like SDN and MUD techniques.

Next, the SDN comes into play and combining other techniques like ML provide security solutions as shown in a study [13] surveyed ML/DL techniques used in the SDN based IDS system. Also, the paper evaluates different deep learning techniques to analyses their impact on network security. The study evaluates that with the ML/DL approach there is a problem of the dataset for more accurate results. Also, with SDN the centralized controller is a bottleneck when we need to

TABLE I. SUMMARY OF MAJOR ACRONYMS USED

Acronym	Description	Acronym	Description
ACL	Access control list	MUD	Manufacturer Usage Description
CIAA	Confidentiality, Integrity, Authenticity and Availability	NFB	network function virtualization
CNN	convolutional neural network	RFID	radio frequency-based identification
DDoS	distributed denial of service	RNN	recurrent neural network
DL	Deep learning	SDN	Software Defined Network
IDPS	Intrusion Detection and Prevention Systems	SIEM	security incident and event management system
IDS	Intrusion Detection Systems	SOM	self-organizing maps
IoT	Internet of Things	SVM	support vector machine
IPS	Intrusion Prevention Systems	URL	Uniform Resource Locator
ML	Machine Learning		

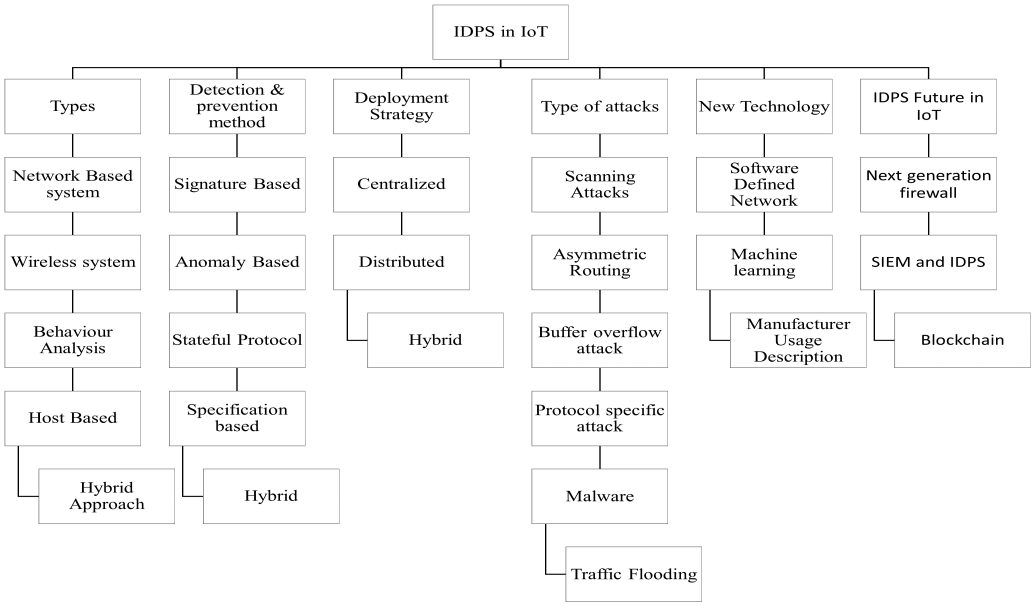

Fig. 1. Taxonomy of IDPS in IoT

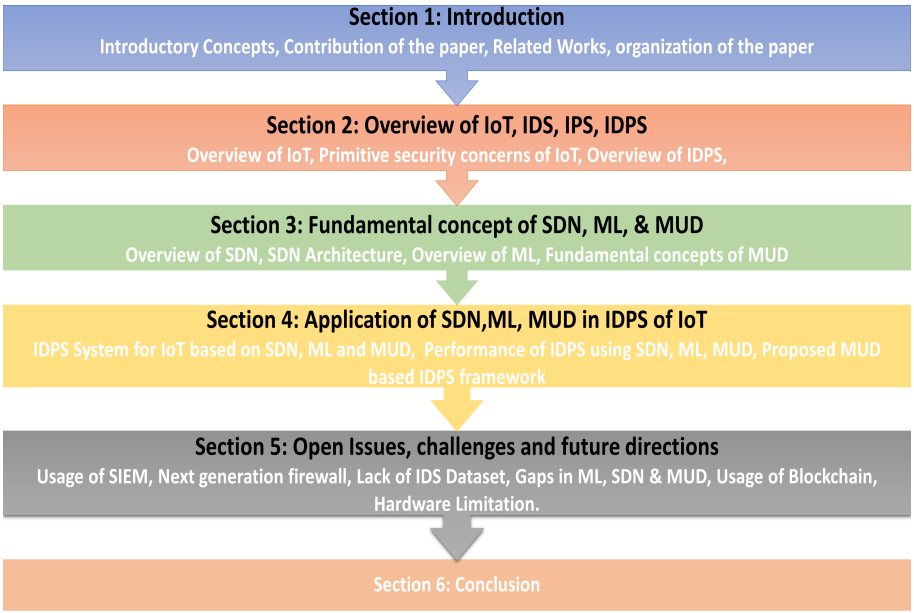

Fig. 2. Organization of the Paper

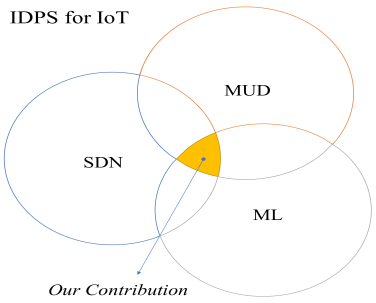

Fig. 3. Contribution of this Paper

do real-time intrusion detection. The study, however, focusses on ML and SDN based IDS but did not give any statistical analysis of their performance. Also, it did not explain the effectiveness of these IDS systems in the context of low power and resource-constrained devices like IoT devices. In this [14] the author focused on the SDN and its application to secure the computer network. The study explains SDN issues like scalability, resilience, security, incorporation with the conventional network. Further, the author shows a little description of the IDS based on the SDN and what type of IDS is more effective in securing the network against the threats. The research [15] showed the role of SDN in IoT to defend against the DDoS attacks. Discuss the different detection techniques that are possible in the SDN for attack detection like ML, traffic analysis, and connection-oriented. However, the study only uses ML techniques for the detection of attacks and did not consider other techniques like signature-based, specification-based, and stateful protocol analysis. It also did not describe any authenticated model for IoT devices like MUD.

However, a new dimension for security has been discussed in the research [16] suggested that the traditional security techniques where security is provided as a pre-emptive measure against known attacks are not sufficient for future attacks on IoT devices. The study proposes a secure by design thinking, for proactive defence system rather than passive systems. This paper has not given much description of the detection system as they are gaining importance in IoT security due to the heterogeneity and scalability of IoT devices. It also did not cover much about the authentication technique in IoT security. The summary of the related works and additional contributions of our paper compared to those related works is given in Table II.

II. Overview of IOT, IDS, IPS, IDPS

This section describes the basic overview of IoT and its various security concerns. It also discusses the concept of IDS, IPS, and IDPS along with their limitations.

A. Overview of IOT

IoT objects are intelligent devices, not dump objects. These smart things use different communication mediums for interacting with each other and outside world over the Internet. These intelligent things have certain properties in common as shown in Fig. 4 [17].

Identification: is required for every device to communicate with each other, IPv6 protocol can be used for this purpose.

Sensing: is the capability of the device to get some physical world data.

Communication: is the ability of the device to be able to communicate with the user and the other devices in the network and outside world.

Computation: is required for information processing.

Services: is the functionality provided to the users by these devices based on the data they acquire from the outer world.

Semantics: is the concept that the devices are supposed to get the right information from the environment and give them services in a timely fashion. Example for these devices are beagle boards [18], [19], Arduino [18]–[20], cubie Board [20], [21], Raspberry Pi [20]–[22] and radio frequency-based identification (RFID) [23]. There are some security concerns as discussed in the coming sections.

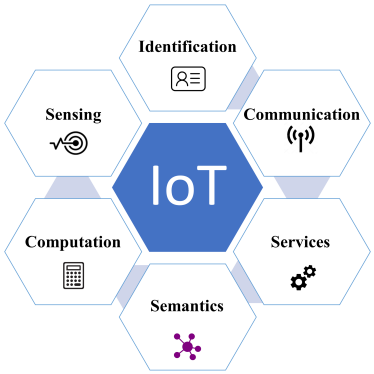

Fig. 4. IoT Device Attributes

1) Primitive Security Concerns of IOT: IoT security has become a big challenge for the industry and academia. With every passing day, new devices come in the market with a plethora of new useful applications. But this exposes more risk towards the security and privacy of the data. Before going to discuss IoT security threats first few basic security requirements are described below known as CIAA (Confidentiality, Integrity, Authenticity, and Availability) [8], [15], [24].

Confidentiality: is the concept that assures no unauthorize service should access the private information and it maintains the privacy and proprietary of the information.

Integrity: is the concept in which the information of the IoT devices should not be modified by any unauthorized user or object.

Authenticity: is the concept that validates the fact that the partner involves in the information transaction is genuine and as in the same what they claim to be.

Availability: is the feature that determines the service is available to the user when and where it is required. In this context, all the storage, processing, and communication medium should work reliably.

TABLE II. RELATED WORKS AND COMPARISONS WITH OUR PAPER

Reference	IDS	IPS	ML	SDN	Signature	Anomaly	Specification	Entropy	Hybrid	topics not covered
Azeez, et al. [7]	✓	✓	✓	✗	✗	✗	✗	✗	✗	IDP
da Costa, et al. [10]	✓	✗	✓	✗	✗	✗	✗	✗	✗	SDN, MUD
Tiwari and Mishra [8]	✓	✗	✗	✗	✓	✓	✗	✗	✗	SDN and authorization techniques.
Sultana, et al. [13]	✓	✗	✓	✓	✗	✗	✗	✗	✗	IDP and IDS for IoT networks
Sahay, et al. [14]	✓	✗	✓	✓	✗	✗	✗	✓	✗	SDN based detection for IoT
Pajila and Julie [15]	✗	✗	✓	✓	✗	✗	✗	✗	✗	Focus on IDS systems
Hajiheidari, et al. [12]	✓	✗	✓	✓	✓	✓	✓	✗	✗	SDN based IDS and authorization techniques
Choudhary and Kesswani [11]	✓	✗	✓	✗	✓	✓	✓	✗	✗	Classification of IDS systems for IoT
Restuccia, et al. [16]	✓	✗	✓	✓	✗	✗	✗	✗	✗	IDPS for IoT networks Using MUD

2) IOT Attack Vectors: The Open Web Application Security Project (OWASP) has published a detailed draft regarding the attack surfaces of IoT, these are the areas in IoT systems and applications that are vulnerable and prone to threats. Fig. 5 shows a summary of these attack surface areas [25].

Attacks on Devices: devices are the primary sources from where the attack can be initiated. The main parts of the device like memory, firmware, physical interface, web interface, and network surfaces are vulnerable. The attackers can further exploit the default setting, old components, and insecure update mechanism.

Attacks on Communication: communication channels are another area of security concern. The channel connects the IoT devices and the outside world. The protocol used for communication in the IoT networks has security issues and can affect the entire system. IoT systems get vulnerable to attacks like Denial of the Service (DoS) and spoofing.

Attacks on Application software: in this the vulnerabilities of web application and software used in IoT systems can become a great cause of a compromised system. The web application can steal user data and insert malicious updates in the system. To defend these challenges, many techniques have been developed and are being used in the industry, intrusion detection and prevention system is one of them.

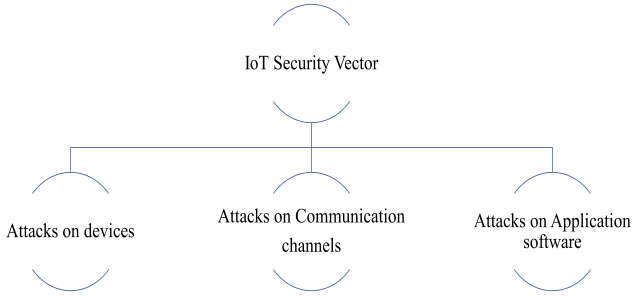

Fig. 5. OWASP Taxonomy of IoT Security

B. Overview of Intrusion Detection and Prevention System

The working principle of the IDS is to monitor the data packets to determine abnormal traffic. There are three major parts of IDS system monitoring, analysis, and detection [26]. The core modules of IDS are the analysis and detection based on the algorithm, which also generates the alarms on the detection of any intrusion [27]. As the detection systems become more common nowadays, attackers find covert ways to exploit the loopholes in the system, like bypassing the system and disabling the system. This results in a DoS kind of attack. To mitigate these kinds of attacks, the researchers suggest the IDPS. This system is not visible to the attackers thus restricts the communication to the other components of the network [7]. The taxonomy of IDPS in IoT is given in Fig. 1.

The IDPS system can be classified using different perspectives as shown in the figure. One way is the application-specific types of IDPS like for network-based applications, wireless applications, behaviour analysis based applications, Host-based and hybrid approaches. Next, we can classify the IDPS based on the detection and prevention techniques used by them like anomaly, signature, specifications, protocol analysis, and hybrid approaches. One of the important aspects of such systems is the deployment strategy, like centralized and distributed deployment of IDPS systems. If required hybrid mode deployment can be used according to the application requirement. One interesting IDPS classification is regarding the security coverage provided by the IDPS systems.

Complete range of security coverage is not discussed here, however, three main areas are discussed like security coverage for IoT devices, communication medium, and application layer. Further, the IDPS systems are discussed in the context of the conventional use of technologies versus new state of art technologies. IDPS constitutes of many building blocks like the type of data network used for IDPS, protocols for the communication, detection and prevention techniques, and application software.

The general IDPS architecture contains sensors, firewalls, management server and console as shown in Fig. 6. Typical

IDPS systems use sensors in the network to monitor the network traffic. At the input of the network, there is a firewall installed as the first line of defence after that there is IDPS sensor which monitors incoming network traffic and passes the information to the management server and the console, while at the same time, it sends network traffic to the local network. Many security techniques discussed above put a focus on the defensive strategy against the attacks.

However, there is a need for the method to detect the ongoing attack. Heavy and complex antivirus and firewalls cannot be used in IoT devices. In this context, lightweight IDS has been devised [28]. One of the examples of attack detection is to monitor different parameters like CPU usage, storage usage, and throughput usage, etc. [24]. Another way to check the energy profiles of power consumption may lead to detecting attacks [29]. Many anomaly detection techniques can be used like the one described in [30] to test the packet drops, send rate, and signal strength. One of the latest methods is to use an ML approach for intrusion detection. Like in [31] random forest technique has been used for the monitoring of traffic flows. An attack is detected when some flows exhibit not according to the normal standard. The goal of IDS is to detect any intrusion in the network or detect any malicious node. Also, it alerts the users about it timely. IDS works like an alarm system and monitors the whole system and generate an alarm when some malicious activity is observed. It gave protection from internal and external threats. The following sections discuss different aspects of IDPS in detail.

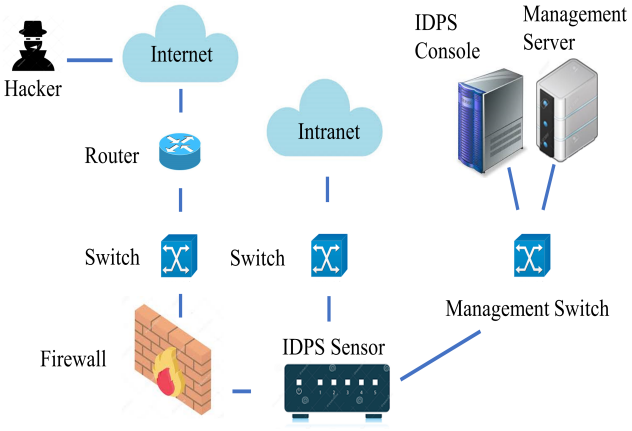

Fig. 6. Working Principle of IDPS

1) IDPS based on application type: The IDPS can be classified based on the kind of applications in which they are used [32]. They are [33] discussed as follow:

Network-Based IDPS (NIDPS) this type checks the network traffic for devices or specific network and application protocol for the detection of malicious traffic. It can detect many interesting events in the network. The deployment of these systems is mostly at the edge of networks like the boundary of router or firewall, remote access servers, virtual private network servers, and wireless networks.

Wireless IDPS (WIDPS) these devices monitor the wireless network traffic and the wireless network protocols for monitoring of suspicious activity. The WIDPS compose of the almost same components like the network IDPS like database servers, sensors, and management servers. The only difference is sensors in both types of IDPS. The wireless sensors have to perform more complex functions of wireless networks.

Network Behavior Analysis (NBA) this system analyzes the network traffic and its statistics to determine malicious traffic like DDoS, malware, and any policy violation in the network. The NBA components consist of consoles, sensors, and analyzers.

Host-Based IDPS (HIDPS) this type of system is designed to monitor a single host and all the activities within the single host. These kinds of systems monitor both wired and wireless connections. Most of the host-based systems use agents that are installed on a single host for the detection of malicious activity.

2) Detection Type: Based on the detection method, there are normally four types of IDS. Each one of them is explained below.

Signature-Based: this type of system detects the attack by determining the incoming network behaviour and match it with the attack signature stored in the internal database. If the match occurs then an alert is generated. It is also known as rule-based detection. This compares the present profile of the network from the previously-stored profiles containing different attacks [34]. This type of IDPS is accurate in determining the known attacks whose signature is stored in the database. But for new kinds of attacks, this approach is not suitable because the matching signature of attack is not available [35], [36].

Anomaly-Based: this type of IDS defines normal network behaviour and any activity not conforming to this is an intrusion or threat [34]. If the network behaviour deviated from the normal profile it generates alert. This approach is good for the detection of new attacks. But this type of IDPS has high false-positive [32], [37], [38].

Stateful Protocol Analysis: this type of system works by comparing the established profile of the protocol and against their behaviour. This standard behaviour is provided by the vendor, just like the signature-based system that compares the behaviour from the given list. This stateful analysis of protocol requires a very deep understanding of the protocol and applications they interact with [39].

Specification-Based: this type of IDS is based on the physically defined polices by the users. Any activity that is against such rules is considered a threat to the system [34]. It is the system in which set of rules and their thresholds are defined for all the network elements like nodes, protocols, and routing tables. If the network behaviour deviates from the set specifications then the threat is detected.

Hybrid Approaches: this approach combines all these types of systems specification-based, signature-based and anomaly-based systems to get the maximum advantage from their strength and lesson the weakness in those systems. SVELTE is an example of a hybrid system [40]This system combines the signature-based and anomaly-based methods.

3) Deployment Strategy Type: We discuss different ways to deploy the IDS in a network, based on the security application scenario.

Distributed IDS: In this strategy, the IDS is placed in every node. IDS needs to be efficient and optimize for the IoT devices due to resource constraints.

Centralized IDS: In this kind of strategy, the IDS is placed at the centre of the network such as at the border router or some specific host. All the Internet traffic from the low power and lossy networks (LLN) nodes pass through the border router, therefore the border router can monitor all the traffic from the Internet and the LLN nodes [40], [41].

Hybrid Approach: In this approach, both methods are followed like a centralized and distributed approach to have the benefits of both approaches. One of the practical approaches for this is to transform all the network into regions and clusters so that each sub region and the cluster can have one node that acts as a host and responsible to monitor all the nodes in the cluster.

C. Conventional IDPS Systems for IoT

Since the IoT devices are resource constraints, therefore conventional IDS system is not suitable for them. A hybrid scheme is required to suit the needs of these resource-limited devices. One of the studies [42] concluded that in signature-based IDS the headers of the incoming packet are compared to the set of the rules. If the number of packets increases the computation will more CPU cycles. Therefore, signature-based IDS are not suitable for IoT devices. Dynamic encoding scheme [43] uses a distributed signature-based IDS system among the ubiquitous sensor networks based on IP, making it lightweight and suitable for low power devices. The study proposed an outlier algorithm TAOOD for the fact that the majority of IoT devices have power constraints and have low quality. So, the resource limitation must be taken into consideration of the outlier algorithm. The TAOOD "Tolerance based adaptive online outlier detection" technique shows higher performance in terms of accuracy to the tolerance and outlier parameters.

The Finite State Machine (FSM) [44] approach has been used to detect the rank and local repair attacks. However, research [45] shows that resource constraint and heterogeneity the IoT networks are causing vulnerability in IoT networks and become a cause of too many threats. So, the study proposes an algorithm based on anomaly detection at the perceptual layer. The algorithm uses anomaly mining techniques. Similarly, a system [46] uses the artificial immune technique in the IoT environment. The study uses the concept of immature, mature, and memory detectors for attack detection.

Service-based approaches [47] presents an architecture constitute of services known as service-oriented architecture SOA used in the IoT system. It uses to prevent the DDoS attacks using learning automata concept. However, conventional methods are not adequate for IoT security [48], so an artificial immune system concept has been used containing the antigen, non-self, and detector in an IoT environment. Hybrid scheme [49] uses a two-layer strategy for protection. One is cryptography and the other is the IDS technique. TESLA [50] protocol is used for DoS attack prevention, as it uses few resources.

Some network-based approaches [51] address the DoS detection using IDS architecture based on the IDS probe. The IDS monitor the sixLoWPAN traffic for the detection of attacks. However, the SVELTE [40] a real-time IDS implemented in Contiki OS. This IDS also works for 6LoWPAN based border router. Some system uses a "security incident and event management system" (SIEM) and "frequency agility manager" (FAM) [52] for the detection of flooding, jamming, and DoS attacks.

Performance of the detection system is very important, a new lightweight protocol known as heartbeat protocol [53] has been introduced in the IDS of IoT networks. Also for real-time detection, a proposed scheme [54] event-based IDS system for real-time detection in IoT networks has been introduced. The IDS works on the event processing model (EPM). The model proposes a rule base scheme, the rules are stored in a repository. Device authentication is another way to protect the devices, a research [55] presents an authentication scheme for IoT devices using XOR manipulation. It is used for counterfeiting and privacy protection of the IoT devices.

Attack categorization is also important, as this research [56] works on the categorization of the Sybil attack in the social aspect of the IoT. The study proposes defence schemes for Sybil using "social graph-based Sybil detection" (SGSD) and "behaviour classification-based Sybil detection" (BCSD). Similarly, [57] shows IDS capable of detecting wormhole attacks and the attacker uses the Contiki OS and Cooja simulator. The IDS can be used in a centralized and distributed scenario. Another research [58] purpose an intrusion detection system against the sinkhole attack known as "intrusion detection of sinkhole attacks on 6LoWPAN for the Internet of things" (INTI).

RFID can be used for authentication of IoT devices, as an interesting study [59] used the RFID authentication mechanism for IoT devices. Also, propose the elliptical curve cryptography (ECC) based on protocols using RFID authentication and the author propose three extended RFID protocols based on ECC. This study [60] proposes a cloud-based antimalware system known as CloudEyes capable of providing reliable and efficient security for resource constraint devices.

Some modelling techniques [61] describes a behavioural modelling IDS (BMIDS). This IDS based on immunity inspired algorithm to distinguish between behaviour changes. The use of artificial intelligence is also quite useful against cyber threats, as a work [62] proposes IDS based on the neural network approach to detect the DDoS and DoS. In the same direction, this work [63] uses compressed sensing technology to monitor the network data, also uses the "support vector machine" (SVM) for the detection of anomalous compressed data. The author [64] proposes a semi-auto building to protect the network topology based on RPL using a specification-based IDS system. The model can detect attacks on topology and RPL like a wormhole, black hole, and selective forwarding. Table III shows the summary of the conventional IDPS systems for the IoT systems as discussed above, it also shows the scheme and the techniques used in such systems along with the security impact of such systems.

TABLE III. CONVENTIONAL IDPS SYSTEMS

References	Signature	Anomaly	Specification	Hybrid	Other	Results	Remarks
Amin, et al. [42]	✗	✗	✗	✓	✗	Work well for a large number of the signature set.	Has limitation to detect new kind of attacks
Shen, et al. [43]	✗	✓	✗	✗	✗	TAOOD perform better than normal sliding window based detection.	The scheme is restricted to detect few attacks.
Le, et al. [44]	✗	✗	✓	✗	✗	Detect the attacks with some processing overhead	No real-time implementation has been done.
Fu, et al. [45]	✗	✓	✗	✗	✗	Theoretical results are 100% detection.	The system is not tested in real-time scenarios.
Liu, et al. [46]	✓	✗	✗	✗	✗	Shows better performance over the other conventional detection systems.	The study does not show what new types of attacks the system can detect.
Misra, et al. [47]	✗	✗	✗	✗	✓	Using LA shows better results to detect DDoS as compared to without LA.	LA requires a lot of processing power, also to detect the runtime attacks will be a question mark for the system.
Chen, et al. [48],Le, et al. [49]	✗	✗	✗	✓	✗	———	The system didn't show any actual results.
Kasinathan, et al. [51]	✓	✗	✗	✗	✗	The results show detection of flood attacks increase as the nodes increases.	The system is not implemented in an actual scenario.
Raza, et al. [40]	✗	✗	✗	✓	✗	True positive rate is 100%	Need to test against a broader range of attacks
Kasinathan, et al. [52],Jun and Chi [54]	✗	✗	✓	✗	✗	AS the traffic increase the system Akeeps normal processing as compare to traditional IDS.	Require more resources to process CEP.
Pongle and Chavan [57]	✗	✗	✗	✓	✗	The attack detection is more than 90%.	Require more attributes of the nodes other than location to detect more attacks.
Arrington, et al. [61],Chen, et al. [63]	✗	✗	✗	✗	✓	The results show efficient detection results.	Now in the future trend behavior attribute is bypassed using smart techniques.

III. FUNDAMENTAL CONCEPT OF SDN ML & MUD

A. Software Defined Network

Traditional computer networks consist of many devices like switches, routers, middleboxes, servers, and hosts. Network operators are responsible for the configuration and maintenance of the network. As the network configuration requires manual low-level device-specific syntax to configure the network, making it more complex, time-consuming, and error-prone. This becomes the big reason for the network downtime [65], [66]. To address these issues software-defined network (SDN) technology emerges. SDN decouples the control plane from the data plane of the network devices [67]. All the intelligence is centralized in SDN and the device is known as a controller, the rest of the devices like switches, routers, etc. are known as forwarding devices and come under the category of the data plane. The devices at the data plane use flow rules to handle the incoming packets. The rules are programmed in these forwarding devices from the controller using a standard interface such as OpenFlow [68]–[70]. In addition to this, the controller can get the flow information of all the devices attached to the network to provide the network administrator's global network status [71]–[74]. This makes network management simple and transparent.

1) SDN Architecture: SDN Architecture is composed of three layers and three interfaces [75] as shown in Fig. 7

Application Plane: This layer contains the business applications that use SDN communication and network services. Examples of such applications are security application, management, and monitoring applications and network virtualization applications.

Control Plane: This plane consists of SDN controllers responsible for the control of the network and defining the network forwarding behaviour using open interfaces. The controller uses three interfaces northbound, southbound, and east/westbound interfaces. The northbound interface helps the developers to develop the SDN application while hiding the lower layer details is known as the northbound interface. The southbound interface provides the communication between the SDN controller and the data devices like switches and routers at the data plane. It also specifies the communication protocol between the controller and the data plane devices. While the Westbound API's are responsible for the controller communicates with the legacy network devices.

Data plane: Consist of network devices like router, switches, IDS, and firewall their main responsibility is to forward the data and filter it.

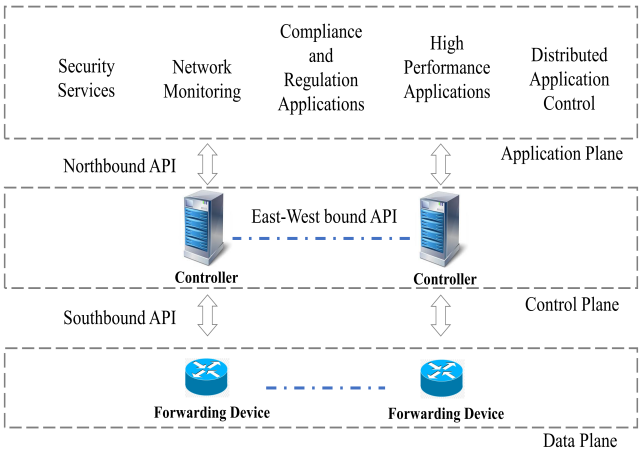

Fig. 7. SDN Architecture

B. Machine Learning

The concept of ML is to make machines to learn automatically from the given data [76]. Also, detect patterns without explicitly programmed the device [77]. The ML algorithm classification is based on the type of data they learn from and what function they perform [77]. Mainly the ML approaches can be categorized in supervised learning, unsupervised learning, and semi-supervised learning [78]. The ML classification is shown in Fig. 8.

Supervised learning: In this the algorithm input the label data, base on this it will predict the unknown cases. Random forest and support vector machine is the example of this type of algorithms used for regression and classification problems respectively [76]. Support vector machine (SVM) and random forest both are used for network intrusion detection system (NIDS). However, SVM is more resource-hungry in the context of memory and computational power [77].

Unsupervised Learning: This kind of algorithm gets the unlabeled data, they learn from the data distribution and data pattern to determine the unknown data [76]. Examples of this are the principal component analysis (PCA) and self-organizing maps (SOM). PCA is mostly used for feature extraction before applying the classification [79]. Other algorithms based on the clustering technique as K-means and other distance-based algorithms are used for anomaly detection. SOM is developed to reduce the payload in NIDS [80]. The main disadvantage of the clustering algorithm is its dependency on the initial conditions like centroid that produces high false-positive results [81].

Semi-Supervised Learning: In this learning process there is a small portion of labelled data and a large chunk of unlabeled data. It is a useful scheme when a large amount of data is unlabeled. For example, photo archives where few images are available [82]. A semi-supervised support vector machine is used for the improvement of the NIDS [83], [84].

Deep Learning algorithms an update on the artificial neural networks use the computation available [85]. The DL technique permits the algorithm to represent the data at various levels of generalization. The main application is object detection, detect the network intrusion detection and many different domains [86]. DL can be learned and trained both ways supervised and unsupervised [76]. Deep learning in a supervised way has an example of a convolutional neural network (CNN). The main application of the CNN is in face recognition and 2D images [86], [87]. DL in an unsupervised way has the example for autoencoder [88] used to learn the representations for the application of dimensionality reduction. A deep belief network (DBN) [89] is another example that is learned using unlabeled and labelled data for the feature extraction and classification purpose. DL in a supervised and unsupervised way has an example recurrent neural network (RNN) [90]. Speech recognition is the main application of the RNN algorithm.

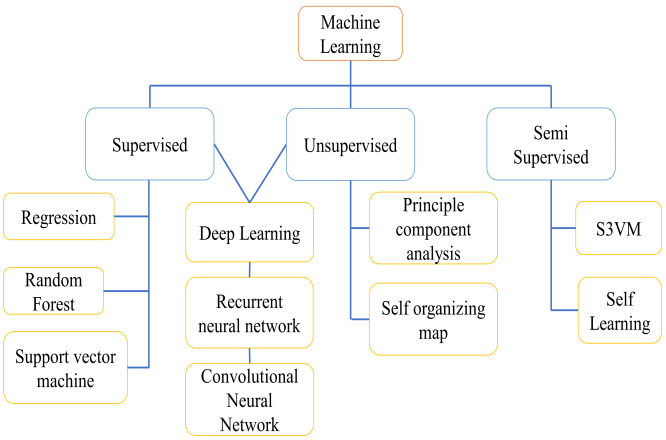

Fig. 8. Taxonomy of Machine Learning

C. Manufacturer Usage Description (MUD)

IoT devices are specialized devices with specific tasks to perform. These devices need to communicate over the network and have special communication requirements that the vendor only knows. For example, the printer only requires to print on the LPT port and the local access port for HTTP is 80. Therefore, it should deny all the other means of access to the network. For this purpose, an idea of MUD [91] has been introduced. MUD declares the intended communication pattern by the manufacturer for the network infrastructure using a network access control list. The MUD works as shown in Fig. 9.

The IoT devices also called things wanted to join the IoT network, they emit Uniform Resource Locator (URL) to the MUD manager. The manager sends this URL to the MUD server. The server sends the device profile file to the MUD manager. Based on the device profile, the manager configures the switch and installs the policy for the device. After this verification process, the device got permission to enter the network. MUD provides a defence system against the malicious agents that got into the network and try to launch an attack on the network infrastructure. This technology also provides defence against compromised devices to attack other devices. MUD helps to reduce the overall threat vector surface. ACLs [92] are normally defined using classes, these are based on the MAC and IP address when deployed on the network switches. MUD working principle is as: the device is

allocated with the MUD URL. This MUD URL is used for accessing the MUD ACL file. This service is given by the MUD server, MUD server fetches the MUD ACL file from the vendor or manufacturer website. Then install this ACL file for this particular device in the switches. Only after this authentication process, the device is allowed to communicate over the network.

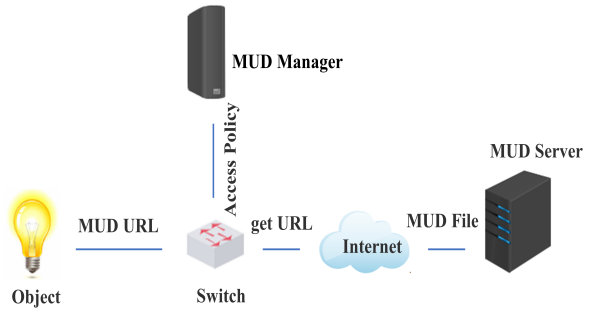

Fig. 9. MUD Working Principal

IV. Application of SDN, ML and MUD in IDPS of IoT

A. Detection using SDN based on Anomaly and Entropy

Attack detection is a crucial aspect of network management. The SDN feature of global network visibility plays a vital rule in network security. This feature helps in monitoring network real-time status. This helps entropy-based detection techniques to become more effective in SDN networks. SDN uses a set of protocols to communicate between the application layer and the controller and vice versa, such as RESTapi, XML and netconf, etc. also controller uses certain communication protocols to talk to the data layer and vice versa like sflow and OpenFlow, etc.

Anomaly Detection covers range of detection systems, as shown in the study [93] communication protocol OpenFlow and sampled flow (sflow) can be used for anomaly detection. The study uses threshold random walk with a connection-based algorithm for the entropy-based anomaly detection. The study also compares the flows required for anomaly detection in the case of sflow and OpenFlow. For sflow the number is 217 and for OpenFlow, it is 5184. This concludes that the sflow is better than OpenFlow in the context of traffic collection for anomaly detection. Another study [94] uses a two-stage scheme for the detection of DDoS attacks. The study first set some threshold value for the flows after that is if some flow crosses the limit it is sent to the detection stage. As in the experiments the author set 3000 packets for five seconds is allowed if some flow exceeds the limit then the 800 packets per second (PPS) for 5 s is imposed. Also, the packet filtering mechanism is activated. One of the research [95] implement anomaly detection algorithms at the border router of the home network. The study uses the NOX SDN controller. The algorithms were also based on threshold random walk with credit-based, rate limiting, maximum entropy detector, and NETAD. And the results show that the algorithms perform better in small networks like home networks.

Another study [96] developed a bidirectional sketch algorithm to detect attacks. It identifies the IP address of the destination for the asymmetric traffic pattern depends on the threshold value to detect some anomaly. once the malicious traffic is identified the controller instructs the switch to drop the malicious flows. In this, once the malicious traffic is identified it is detected and blocked at the ingress points of the network to avoid collateral damage. The author [97] present a distributed algorithm for anomaly detection based on the entropy technique.

Entropy detection is one way to detects attacks, as the study suggests that most of the entropy detection is based on the collection of flows from the network, so if the network is big then due to a large number of flows may overload the network. Therefore, the study processes the flows at the switch and present filters for the DDoS attack at the edge switches. The study in [98] introduces the NetFuse device between the switch and the controller to monitor the network load. This instructs the switches to reroute the flows causing the congestion. StateSec [99] a novel algorithm to detect the DDoS attacks using the port scans. Anomaly is measured by the abrupt changes in the traffic features. However, the study shows no implementation for this algorithm. Few industrial solutions have been proposed Radware [100] developed DefenseFlow to detect the DDoS attacks. This technique measures some key attributes like packet rate, average packet size, bandwidth connection distribution, and connection rate. In case of attack, the device instructs the controller to reroute the traffic to the specialized devices to handle the traffic.

B. Detection using ML

ML techniques in SDN networks help against the detection of the malicious flow as in the study [101] detect the anomalous flows in the SDN network. The information is taken from the flow tables from the switches and gets the flow of information. The DPTCM-KNN algorithm in the detection module process these anomalous flows. The only issue here is the processing overhead as the process is repeated after 10 seconds. In another study proposed a trust-based approach for the detection of malicious devices using the packet data and device profile.

Another study [102] proposed DDoS detection using OpenFlow by proposing the self-organizing maps (SOM) for attack detection. The SOM is an unsupervised neural network method for classifying the traffic as normal or abnormal. In this method, the controller continuously collects the data from the switches and other devices and monitor the attributes like average packets in the flow, average number of bytes in the flows, and the average duration of flows. The data is then fed into the classifier for the detection of DDoS attacks. All the process also adds some overhead on the processing of the controller. One of the studies [103] analyzes the ML algorithms in the context of the SDN for providing security, resource optimization, traffic classification, and quality of service. This further shows that ML brings intelligence to the controller for the detection and prevention of attacks.

The study [104] shows that ML can be used for DDoS and intrusion detection also shows the pros and cons of the surveyed mechanism in handling the intrusion detection in SDN networks. Another study [105] analyzes the traffic scheduling problem in the SDN network in a hybrid data centre environment. In this, the edge devices are responsible for the ML-based elephant flow traffic classification. This reduces the burden on the SDN controller. However, the scope is limited it is unable to give the network-wide information having multiple switches and controllers.

A study EUNOIA [106] proposes a system to detect the threat and respond in the SDN system. The framework has multiple modules like data preprocessing, decision making, response system, and predictive data modelling. For predictive data modelling, the system uses the decision tree and random forest algorithms, to monitor malicious and suspicious traffic. Response module works based on alerts. While the decision-making module is responsible for the routing path computation and implements new flow rules for each flow type. The experimental results display high detection accuracy and reduce data preprocessing time. However, if the data is increased from any node then the processing time also jumps up showing degradation in overall performance also the scalability is an issue in this framework.

Another study presents a management framework for classification, anomaly detection, and mitigation within the SDN network. The system works in two phases for classification and detection. First is the lightweight phase in this light computation is done to detect any suspicious or malicious activity. In the second phase, SVM, an ML algorithm, is applied for the classification and abnormal flow detection. Again, the controller requires a lot of processing power to poll all the switches in the network. In [107], propose a scheme using the DL algorithm for the detection of DDoS within an SDN network. The study develops stack autoencoder using the SoftMax classifier and unsupervised deep learning algorithm. The results based on the NSL-KDD dataset shows around f-score 75.76% and 69% accuracy. Again, this technique requires to monitor each packet that limits the controller performance.

A similar study [108] uses deep neural networks in the SDN network for intrusion detection. The author developed the neural network. The network constitutes one input, three hidden, and one output layer. The SDN controller receives data from the switches in the network and sends the data to the detection module. The results using the NSL-KDD data set is about 75.75%. The scalability of SDN has been tried to handle in [109] by proposing the framework called Athena. The main concept of this framework is to implement the detection mechanism not only on the edges but to deploy this at network-wide switches and controllers for better results. Athena doesn't require special hardware for the deployment of the detection modules. But the framework doesn't provide adaptive measurement for resource optimization.

C. Detection using MUD

The researchers provide IoT security solutions using MUD as in [110] implement MUD over the OpenFlow switches in the SDN network. In another study, [111] they developed a machine for the detection of anomalous patterns in a MUD compliant network. Also analyzing the IoT network behaviour after volumetric attacks happen in the network. When they compare the results for attack detection with other systems its detection is much superior. Similarly, in [112] translated the MUD policies into the flow rules and implement these policies using SDN technology. The study also showed the limitations of MUD based policies in the context of securing the network. The author in [113] sorted out the validation and integration problems of the MUD profiles with the network. Further, the study validates the MUD profile for each device also makes sure that the profile is confirmed under the organization policy.

D. Prevention using SDN and ML

The ability of the SDN controller to be programmed and change the rules on the fly made it suitable for attack mitigation. As the security notification can be shared across the network. Based on the context flow rules that can be generated and implemented on the edge devices. Also, the anomaly detection capability of the ML technique made it possible to develop the defence system based on the collaboration of ML and SDN. One of the study Drawbridge [114] proposes a framework for ISP used for attack mitigation. The main objective of the framework is to stop the dropping of the customer traffic from the ISP due to heavy load. The detection in the framework is performed at the end devices like switches. The controller and the switches in the ISP share the rules. The responsibility of the validity check of the rules lies on the controller before deploying them on the switches.

In another study proposes the SENSS [115] that offer an interface for the attack mitigation. When the attack happens, the victim sends the information to the controlling body, which is ISP in this case, with all the routes and traffic details. However, the system allows the victim to request for the rerouting the network traffic. In this study, Bohatei [116] the author leverages the strength of network function virtualization (NFV) along with SDN to detect the DDoS attacks. The authors make use of NFV technology to place and start the defence virtual machine at the required location in the network. This developed architecture pushes all the network traffic at these initiated VMs. This framework works for the ISP network. The kind of architecture of ISP provides support to create a service for the customers to defend them from DDoS attacks. After detecting the anomaly in the network another process of estimation starts on the suspicious traffic. This estimation is sent to the resource manager module to find out the number, type, and location for the instantiation of virtual machines. The process is based on a couple of algorithms namely server selection and data centre algorithm used in the data centre. The results show that the system can mitigate the DDoS attacks in one minute. But this put quite a workload on the ISP as it must handle hundreds and thousands of customers.

In other research, [117] a framework is proposed for collaborated defending against the DDoS attacks. In this, the customer requests to ISP to provide the service against the DDoS attack. Upon request, the suspicious flows are sent to the middleboxes for further processing. But the implementation of the said framework has not been done. One of the frameworks proposed called ArOMA [118] it tries to mitigate the DDoS attacks automatically using the SDN strengths like centralized manageability and programmability at the ISP. This framework

brings all the three stages like monitoring, detection, and mitigation against DDoS attacks under one automated umbrella. This framework also enables the collaboration between the customers and ISP to defend against DDoS attacks. The author provided the implementation and evaluation of the proposed framework.

In the research, [119] presented a framework based on the collaboration of SDN and content-based data network (CDN) to manage the high volume video traffic flows. Normally this application is deployed at the controller to get the hidden knowledge of the network like topology end-users to optimize the network. The ISP uses the application to manage the huge traffic emanating from CDN. The CAPTCHA [120] is used for the protection of the services. The server runs these services. The results in this process are based on weak programming of the bots. Also, they believe that the bots cannot perform the IP spoofing which is not the case.

E. IDPS Systems for IoT based on SDN, ML and MUD

IDPS has become a very eye-catching technique especially with the involvement of a new state of art techniques. Fig. 10 shows the integration usage of MUD, SDN, and ML in IDPS of IoT [111]. IoT devices have their local network in which they communicate with each other and also communicate with the Internet through a gateway. The SDN switch manages the flow-table rules dynamically. The MUD engine works with the SDN controller and App. The architecture also contains the MUD collector along with an anomaly detector and IDPS. These elements work combinely to manage the flow-table rules embedded in the switch and also monitor the device activities inside the network [112].

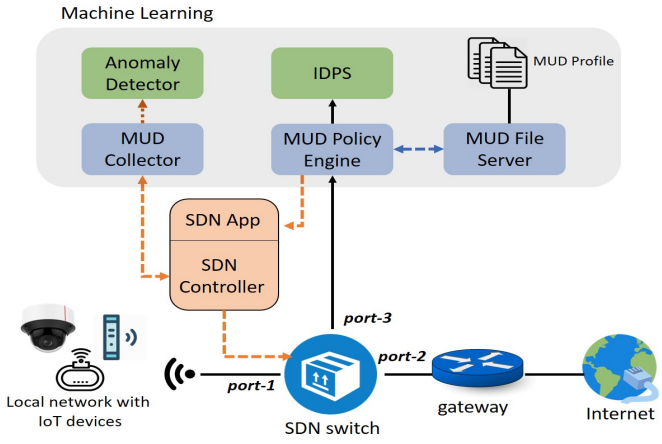

Fig. 10. Network Architecture of IoT based on SDN, MUD and ML (redrawn from [111])

In this network architecture, default rules are initially configured in the SDN switch to mirror packets that are intended to use for the device identity. MAC addresses are generally used for the identification of the device. Application for example DHCP contains this MAC of the device and provides MUD-URL which adapts the MUD standard. This is used by the MUD policy engine to discover new IoT devices making a connection with that network. The MUD engine already has a record of discovered devices. The MUD engine retrieves the MUD profile from a MUD file server and stores it till its validity. To be noted here that the manufacturer operates and manages the MUD file server. The MUD policy engine makes the ACLs (access control lists) of the MUD profile into the set of flow rules. The packets intended to be sent are mirrored and send to the IDPS for the inspection. IDPS confirms the traffic that does not follow the MUD specification. Some traffic still can pass to the network by using spoofing techniques. Therefore, an anomaly detector has been used. For these, MUD collector pulls flow counters from the SDN switch, then compute each device's attributes, and stream them to that anomaly detector. ML is used to learn the policy, anomaly detection, and flow rules for the smooth operations of the whole architecture. ML is also used to train the system to determine the attack flow. The system is also trained by using ML to detect the abnormality of the expected traffic (defined by the MUD profile). This helps the system to detect attacks.

These technologies like SDN, ML, and MUD are getting attention from the researchers and industrialists to be used in intrusion detection systems. This improves the overall performance of the system and able them to meet future challenges. As in [143], the study proposes an IDPS system for the protection of the command and control system for unmanned vehicles (UV). There are attacks like anti-drone and anti-autonomy on these UVs and these attacks disturb their autonomous decision-making system. The system uses a hybrid IDS system approach. Another study [144] more focused on wireless sensor networks shows the need for IDPS system to protect the network from growing cyber-attacks. Further, the author compares the ML and DL approaches in the context of the IDPS. Another paper [121] proposes a secure model for smart cities based on the IDPS and DL approaches. They propose a deep migration learning model and use KDD-CUP 99 data set for the model evaluation. The results show shorter detection time and higher detection efficiency. One of the studies [122] proposes a security model for the IoT devices based on the strength of the SDN network. It combines the power of firewall and IPS to detect anomaly in the network traffic and detect the attack in the IoT network.

A new concept known as Manufacturer Usage Description (MUD) has been used with SDN [111] for intrusion detection. MUD is a device description for its expected behaviour, provided by the vendor. The system based on SDN, MUD, and ML approaches to defend against benign and volumetric attacks in IoT devices. In this study, [112] the author implements the MUD in the SDN network and analyzes the effect of this new technology against the volumetric attacks in IoT networks. A similar work [113] generates MUD profiles based on the behaviour of the device, the work also validates the generated profiles with the organizational policies. Another study [110] presents the MUD implementation in SDN based network. It also shows the implementation scenario in a scalable fashion. An interesting study [123] shows that the MUD is not completely defining the IoT devices, so they propose their security framework with few extensions in a MUD. The author presents their learning model that extracts the IoT device feature by analyzing the network traffic. Based on these features develop a normal behaviour profile of the device. Thus, the claim that the specification of the device using this framework is tighter and clearer.

TABLE IV. TAXONOMY OF IDPS SYSTEMS FOR IOT BASED ON TECHNOLOGY

References	SDN	ML	MUD/ Device profile	Technique	Tools	Remarks
Li, et al. [121]	✗	✓	✗	Migration Learning	KDD CUP 99 Ubuntu MATLAB	The IDPS does not consider the resource limitation of the IoT devices. Also, the vulnerabilities of the IoT devices itself.
Gonçalves, et al. [122]	✓	✗	✗	NIDS	Snort Linux Nmap OVS	Use SNORT IDS for detection and prevention is done by SDN. Limiting the system capability for the detection of a few attacks.
Hamza [111]	✓	✓	✓	MUD SDN ML	OpenFlow switch Faucet SDN controller MUD policy engine	Rely on MUD for IoT security. But MUD has its limitation for completely defining the IoT device profile.
Hamza [112]	✓	✗	✓	MUD SDN	MUDgee PCAP	Only focus on MUD implementation rather than the comprehensive security solution for IoT.
Hamza [113]	✗	✗	✓	MUD	MUDgee	Only provide proof of concept for the MUD profile generation and did not focus on IoT security.
Ranganathan [110]	✓	✗	✓	SoftMUD	ODL YANG	The security solution is only able to test the DDoS. Attacks like malware are real threats to IoT devices.
Singh, et al. [123]	✗	✗	✓	MUD Clustering Technique	Multitech Conduit LoRa Gateway Ettus USRP B210 Linux containers LXD TShark	Only focus on removing the weakness of the MUD. Did not address how to handle the diverse cyber-attacks on IoT devices.
Kumar and Lim [124]	✗	✓	✗	Random Forest k-NN Gaussian Naive Bayes	scikit-learn Wireshark	Due to the absence of the MUD like technique the solution capability to secure diverse IoT devices is a question mark.
Amangele, et al. [125]	✓	✓	✗	decision-tree LR LDA KNN CART NB SVC	Scikit-learn Python package CICIDS2017 Dataset	In this solution, scalability will be an issue. As the number of IoT devices increases there is more processing load on the SDN controller that effects the real-time detection of the system against intrusion detection.
Wani and Revathi [126]	✓	✓	✗	BPNN	NSL-KDD Dataset RYU Controller	The proposed solution has not been tested in a real-time environment. Also, only a flood attack has been tested, the system performance for another kind of DDoS attacks is not tested.
Chang [127]	✓	✓	✓	Self-Organizing Map (SOM)	YANG data model Mininet Ryu SDN controller	The proposed solution results are not compared with any other existing detection and prevention system.
Wu, et al. [128]	✗	✓	✓	Signature based Device Profile	NS-3	Effective only against the EEA attacks
Venkatraman and Surendiran [129]	✗	✓	✗	Automata Technique	Automata controller	The IDS system is designed for the home security systems
Soe, et al. [130]	✗	✓	✗	ML Correlated-Set Thresholding on gain-ratio (CST-GR) algorithm	Raspberry Pi system Botnet DataSet	Only works for the known attacks.
Putra, et [131] al	✗	✓	✗	SVM, Block Chain	Raspberry Pi system	This IDS make additional overhead of blockchain
Li, et al. [132]	✗	✓	✗	DL	NSL-KDD Keras	The system has limitation for the new cyber-attacks
Ferrag, et al.	✗	✓	✗	ML	CICIDS2017 BoT-IoT	Shows little effectiveness on some attacks
Ferrag, et [133] al.	✗	✓	✗	specification heuristic	CUPCORBAN JAVA Platform	It adds to the overhead for the IoT devices
Nguyen, et [134] al	✗	✓	✓	federated learning approach	Kali Linux tcpdump	The System just talk about the detection but didn't give much about prevention from such attacks
Cervantes, et al [135]	✗	✓	✓	Behavior Based	Cooja	The study focuses only on sinkhole attack. Need to test against new attacks types
Eskandari, et al. [136]	✗	✓	✓	Behavior Based	Raspberry Pi 3 model B AGILE gateway software	The work does not describe the overhead and the performance plenty for the IDS system used in the IoT based networks
Bhale, et al. [137]	✗	✗	✓	Device profile	Contiki OS Coja Simulator	The IDS system just focuses on one type of attack sinkhole attack. Its role against other attacks need to be tested.
Babu and Reddy [138]	✗	✓	✓	Specification based	CUPCORBAN JAVA Platform	The IDS can lead to more false positive as compare to signature based technique
Ambili and Jose	✗	✗	✓	Behavior Based Blockchain	IoT Devices	The performance of the IDS system is not very commendable
Al-Duwairi, et al [139]	✗	✗	✗	SIEM	Splunk SIEM	The IDS system is not compared with other IDS in terms of performance
Mudgerikar, et al [140]	✗	✓	✓	Anomaly base Profile Base	IoT Device	This is system level IDS tailored for IoT devices. But its comparison with network IDS system is not mentioned.
Kumar, et al. [141]	✗	✓	✗	ML Decision Tree	UNSW-NB15 data set	Limited for other kind of attacks like zero day attacks.
Breitenbacher, et al. [142]	✗	✗	✓	host based	Linux kernel	The system overhead has not been measured

EDIMA [124] as an early detection system for the IoT devices. Thus, the system helps in detecting malware in the network, especially for large-scale networks. The system uses an ML algorithm at the edge devices for traffic classification. One of the studies [125] proposes a hierarchical ML approach in the SDN network to reduce processing load at the edge devices for anomaly detection. The results show that the two-level classifier significantly reduce the packet processing at the edge. The research [145] shows the pons and cons of different IDS and IPS systems in the context of cloud computing. The author in [126] presents an IDS system SDIoT-IDS based on SDN for the IoT devices such that the maximum load is taken off from the edge devices. The system is tested only with few attacks like flood attack and ICMP based attacks. Table IV summaries the IDPS systems discussed with addition to the classification of systems based on the technology used in them.

1) Role of SDN, ML AND MUD in IDPS: The IDPS system based on the MUD, ML and SDN become more robust and dynamic. The MUD provides the system first line of defence by verifying the ID and the role of the device within the network. This reduces the threat surface for the IoT devices. The second line of defence, the ML/DL techniques helps not only to detect the established cyber threats but also the unknown threats that can cause the system to malfunction. Finally, the last line of defence is the SDN technology that helps in taking realtime actions to rectify the damage caused by the threats and prevent them to happen again by enforcing new rules and policies within the network. All these layers are shown in the Fig. 11.

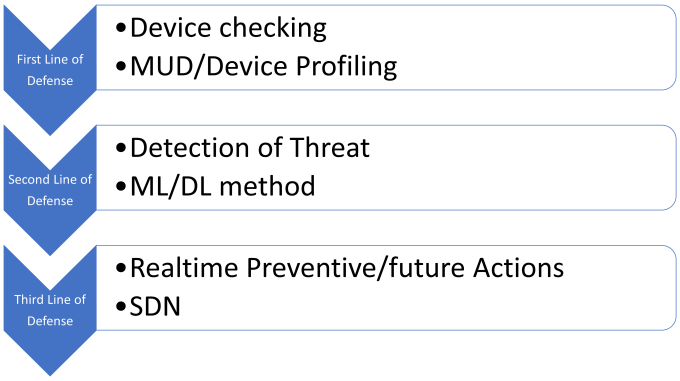

Fig. 11. Role of MUD, ML and SDN in IDPS

2) Performance of IDPS in IoT: Research [127] shows the advantages of using MUD and SDN together against the flood attack in IoT. The results show 98% detection for TCP attacks and 90% detection for UDP attacks. With the introduction of the IoT device profile for the IDPS systems will reduce the attack surface. The [128] study used graph theory to describe the network. They used centralized and malicious node detection (CAMD) IDS. It uses the genetic algorithm to analyze the nodes data gathering behaviour. This node profile helps for the distribution and passive EEA resistance (DPER) module used as the second part of IDS to lower the Energy Exhaustion attack (EEA). The accuracy for detection is 100%. Also in [142] the author purpose HADES-IoT is a host-based IDS system for the IoT devices. This is a lightweight IDS system that requires very few resources. It defends the IoT devices using profiling techniques. Profiling is performed on every IoT device to detect malware like VPNFilter, Persirai, Marai, and IoTReaper. The results are 100% detection. As there is a serious need for the including MUD in IDPS systems for the end to end security of the IoT devices.

Little work has been on the MUD and its implementation for IoT as the standard is relatively new as compared to other technologies. However, the ML and SDN usage in IDPS systems are showing convincing results. In this research, [130] a lightweight ML-based IDS system has been proposed for the IoT devices. In this, a novel feature selection algorithm has been implemented known as correlated-set thresholding on gain-ratio (CST-GR) algorithm. Giving the detection accuracy of 99.4%. Similarly in [133], the study proposes an intrusion detection system based on tree-based and rule-based classifiers. It uses EP Tree, JRip algorithm, and Forest PA. It shows good performance in the context of accuracy, false alarm, detection rate, and false alarm. The detection is some times vary between 30% to 100% depend on the attack type. Table V summaries the IDPS systems performance based on the detection of specific cyberattacks.

The performance of the IDPS system as shown in Table V is very interesting as few systems show the 100% detection accuracy. As we can see that [128] shows 100% detection accuracy, similarly, in [142] the detection rate is 100% for the latest attacks. However the minimum detection in the current sample is close to 80% depend on the attack type as shown in [140], which is still quite encouraging. Keeping the fact that using the new technologies in the IDPS system made them more dynamic and up to date to handle the upcoming cyber threats, as compared to the conventional techniques that require predefined rules and signatures to identify the threat. The range and application of the IDPS systems were limited. Also, the response to those threats was not real-time and it took long to rectify the system and update it to counter such attacks. As the technology gets more mature the IDPS systems will get more effective and applicable to provide end to end security for IoT networks.

V. Open Issues, Challenges and Future Research Directions

In the previous sections, we have reviewed some aspects of the combined use of SDN, ML, and MUD in IDPS of IoT. Together these techniques provide several common research issues in different aspects of IDPS of IoT. In this section, we highlight some of the future research issues and challenges in this domain.

A. End to End Security for IoT using IDPS and SIEM

All the types of IDPS discussed above for the security of the IoT has some drawbacks too. Like network-based, NBA, wireless, and host-based all have different characteristics. Each of the technology can detect a set of attacks that the other cannot. So, if we use multiple types of IDPS together it will produce much better results against the malicious activity. Also, as each IDPS works independently so there is no fear of a single point of failure. But if all the IDPS systems are not integrated then their effectiveness is limited.

TABLE V. PERFORMANCE OF IDPS SYSTEMS FOR IOT BASED ON TECHNOLOGY

References	Attacks	Performance
Li, et al. [121]	DoS Probe	97.2%
Gonçalves, et al. [122]	Port Scanning DoS	—
Hamza [111]	port scanning, TCP/UDP/ICMP flooding ARP spoofing TCP/SSDP/SNMP reflection	92.82%
Hamza [113]	DoS	—
Ranganathan [110]	DDoS	—
Singh, et al. [123]	Malicious Nodes	—
Kumar and Lim [124]	Mirai, Hajime, Remaiten, Linux.Wifatch Brickerbot, Satori, Masuta, Linux.Darlloz, Reaper, Amnesia	94.44%
Amangele, et al. [125]	Slowloris, Hulk, Golden Eye, Heartbleed Slowhttptest , DDOS, BOT	99%
Wani and Revathi [126]	TCP flood ICMP Attack	99%
Chang [127]	TCP SYN Attacks UDP Attacks	90%
Wu, et al. [128]	Energy Exhaustion attack (EEA)	100%
Venkatraman and Surendiran [129]	DoS Hijacking attacks, Zero day attacks Replay attacks	99.06%
Soe, et al. [130]	DDoS attacks, probing attacks (reconnaissance), information theft attack	99.4%
Putra, et al [131]	DoS, Man-in-the-middle, Spoofing Reconnaissance, Replay attacks	—
Li, et al. [132]	DoS, Probe, R2L, U2R	82.62%
Ferrag, et al. [133]	DOS, Brute, force, web, Attack, SQL injection	30%-100% depend on the attack type
Babu and Reddy [138]	malicious traffic	91%
Nguyen, et [134] al	malware , attacks	95.6%
Cervantes, et al [135]	Sinkhole attack	Mobile Devices 75% Fixed Devices 92%
Eskandari, et al. [136]	Port, Scanning, HTTP and SSH Brute Force, SYN Flood attacks	98%
Bhale, et al. [137]	Sinkhole attacks	TPR 95.86% TNR 94.31%
Babu and Reddy [138]	malicious traffic	91%
Al-Duwairi, et al [139]	botnet, Attacks, Flood Attack	—
Mudgerikar, et al [140]	malware, attacks, brute-forcing, DDoS, crypto-mining	78% - 99%
Kumar, et al. [141]	DoS, attacks, Probe, attacks	88.92%
Breitenbacher, et al. [142]	VPNFilter, IoTReaper	100%

The IDPS can be directly or indirectly integrated for overall improved performance. Direct integration involves using multiple IDPS from the same vendor. This integration shows quite an improvement in the accuracy of the system to detect the threats. But this approach has a flaw if any single module failed the whole system will be compromised. To address this issue an indirect integration approach is used to achieve the same result. In this scheme, all types of the IDPS report to one system called security information and event management (SIEM) software [146].

SIEM [147] can be used to complement to IDPS system. This system can analyze the data from different IDPS and detect the attack more efficiently. To protect the future-critical applications based on IoT requires an end to end security management system. This paradigm requires to orchestrate and manage security across all the connected domains, like connected devices, networks of communication, cloud, apps up to the users. This is only possible by using existing Intrusion Detection and Prevention Systems (IDPS) and Security Incident and Event Management (SIEM).

B. Next Generation Firewall over IDPS

With the advent of ML techniques in IDS and IPS, the predictive mechanism becomes very efficient in changing rules based on previous history. This model helps to detect the unseen attacks. But the scheme fails in the generative policy model, as IDS and IPS generate new policies based on the context. This scenario becomes a challenge for automated and reliable policy-based management systems. Especially in distributed and coordinated systems.

Firewalls in this case use packet information and directly block the suspicious packets rather than to detect and block the attack. But IDS and IPS can handle many unseen attacks that the firewall cannot detect. But at the cost of time and resources. That is not acceptable to the IoT devices having a limited resource. Therefore, a next-generation firewall using ML and SDN approaches to analyze the IP packets for malicious packet detection and block unseen attacks rite at the edge before entering into the network will be more efficient and suitable for the IoT based networks [148].

C. Lack of Intrusion Detection Dataset

The available intrusion detection dataset is not up to the mark for the research predictions as the academic's research require proper classification of data. For this reason, the network researcher uses artificial datasets for the network intrusion detection because of the unavailability of the realistic datasets. So, the importance of realistic datasets cannot be undermined for the accurate and more realistic testing and evaluation of the intrusion detection systems. The most common dataset used nowadays are KDD cup 1999 with a new version and NSL-KDD for network-based intrusion detection system [13].

D. Gaps in Machine Learning, SDN and MUD

Deep learning is expected to improve the security of the network, but infect it is also vulnerable to cyber-attacks. As if the input to the DL algorithms is changed the output of the system could be drastically different [149]. As an example, the use of DL in IDPS if the input to these algorithms is changed then the IDPS system will be in the control of the adversaries. Therefore, more investigation and care are required while using deep learning algorithms in critical security applications. One of the issues with the SDN networks is the logically centralized controller. In this context, the attacks on the controller pose a more serious threat over all the networks.

Moreover, the communication channel between the controller and the switch can also be compromised. There are other challenges involved with SDN is scalability and compatibility with the conventional networks [150]. Similarly, MUD also has few weaknesses, as shown in [112], when the MUD translated to the flow rules it has vulnerabilities against the internal and external attacks on the IoT devices. This MUD profile needs to add on a few additional attributes regarding the devices for shortening the attack surface.

E. Usage of Blockchain

Blockchain has revolutionized the cryptocurrency industry. The main design is consisting of the secure distributed database (a.k.a public ledger) all the participants do their transactions from this. The cryptocurrency like Bitcoin and Ethereum do their transactions in peer to peer architecture. The working principle of blockchain is such that when one peer wants to make a transaction to another peer it makes transaction requests to all the peers in the blockchain network. This way every node gets periodic transaction updates and puts them into a single block. After that, the validation of each block is done by a special consensus algorithm that is executed by special nodes in the network known as miners.

The new IoT emerging applications can take advantage of the secure communication architecture of blockchain [151]. Since in the IoT world more and more devices and sensors need to communicate to provide real-world applications, Blockchain gave a tamper-resistant record allowing the participants to have secure and consistent access. Additionally, the blockchain provides flow management. It provides an efficient way to automate the business and creating smart contracts [152]. IoT takes benefit from blockchain due to the certain feature of the technology;

Decentralization: Due to the decentralized architecture of IoT blockchain suits as a security solution. The default decentralized architecture of IoT solves the problem of single failure and at the same time gives robustness against DoS attacks. Pseudonymity the public keys are the identifications of the nodes in the blockchain. But these Pseudonyms don't give any information regarding the identity of the node.

Secure Transaction: every transaction send is first signed by the node itself, then it gets verified and validated by the miners. Once this transaction got verified it cannot be altered and whole proof of the traceable events is stored in the network.

F. Software Watermarking

Watermarking is a technique used for software protection from the cyber-attacks [153]. As the algorithms use keywords within the code to produce a key. Further, there are extraction algorithms that extract the key and compare it with the original key to check the amount of tempering in the software. if the tampering reaches to certain threshold the intrusion detection system can take certain action to eliminate the malicious software or block it from further execution. This technique can be used in the intrusion detection and protection systems to enhance the overall system security and reduce the attack surface, especially when used with MUD.

G. Hardware Limitation

The use of IDPS including ML, MUD, and SDN, we need a more sophisticated computational capability, more memory resource, energy or power, etc. However, the smaller IoT devices still have a resource constraint. The IoT network requires more computational power and better network infrastructure to fully benefit from the applications of these latest technologies. Further, the requirements for real-life implementation and real-time monitoring are more resource-demanding approaches in the context of IoT network security. Therefore, more research needs to be performed in the hardware part to include the integrated application of SDN, ML, and MUD for the IDPS in IoT.

VI. Conclusion

This paper discusses the security issues of the Internet of things (IoT) and the role of the Intrusion Detection and Prevention System (IDPS) to address these challenges. These IDPS are not new in network security, whereby many conventional IDPS systems are already being used for security purposes. However, in this study, we focus on IDPS systems based on modern and state of art technologies like Software Defined Network (SDN), Machine Learning (ML) and Manufacturer Usage Development (MUD) techniques. Further, we analyze the application and the effects of the latest IDPS systems on the security of the IoT networks and devices. The new concept of security design is evolving among the researcher communities and industries to provide comprehensive security in IoT networks. MUD is one of the latest standards developed in this direction. This study also analyzes the integration of MUD with IDPS systems to study their effect on network security. For the future of IoT networks, the importance of the IDPS system is irrefutable. Systems like security information and event management (SIEM) and IDPS using the power of modern technology are the future of security in IoT networks.

Acknowledgment

The authors would like to thank the sponsor as this work was supported by the University of Malaya, Malaysia (Grant No. GPF017D-2019).

References

[1] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the internet of things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, 2019.

[2] K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Communications Magazine*, no. 99, pp. 1–7, 2017.

[3] O. Flauzac, C. González, A. Hachani, and F. Nolot, "Sdn based architecture for iot and improvement of the security," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*. IEEE, 2015, Conference Proceedings, pp. 688–693.

[4] "Rfc-8519 - proposed standard mud," 2019. [Online]. Available: https://datatracker.ietf.org/doc/rfc8519/

[5] S. Gangadhar and J. P. Sterbenz, "Machine learning aided traffic tolerance to improve resilience for software defined networks," in *2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE, 2017, Conference Proceedings, pp. 1–7.

[6] S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa, and B. Yang, "Predicting network attack patterns in sdn using machine learning approach," in *2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. IEEE, 2016, Conference Proceedings, pp. 167–172.

[7] N. A. Azeez, T. M. Bada, S. Misra, A. Adewumi, C. Van der Vyver, and R. Ahuja, *Intrusion Detection and Prevention Systems: An Updated Review*. Springer, 2020, pp. 685–696.

[8] M. T. S. P. Tiwari and P. Mishra, "Review of intrusion detection system," *International Journal of Scientific Research & Engineering Trends*, 2019.

[9] T. Salman and R. Jain, "A survey of protocols and standards for internet of things," *arXiv preprint arXiv:1903.11549*, 2019.

[10] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[11] S. Choudhary and N. Kesswani, "A survey: Intrusion detection techniques for internet of things," *International Journal of Information Security and Privacy (IJISP)*, vol. 13, no. 1, pp. 86–105, 2019.

[12] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the internet of things: A comprehensive investigation," *Computer Networks*, vol. 160, pp. 165–191, 2019.

[13] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on sdn based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2019.

[14] R. Sahay, W. Meng, and C. D. Jensen, "The application of software defined networking on securing computer networks: A survey," *Journal of Network and Computer Applications*, vol. 131, pp. 89–108, 2019.

[15] P. B. Pajila and E. G. Julie, "Detection of ddos attack using sdn in iot: A survey," in *Intelligent Communication Technologies and Virtual Mobile Networks*. Springer, 2019, Conference Proceedings, pp. 438–452.

[16] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *Ieee Internet of Things Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[17] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys and tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[18] M. Sharma and S. C. Gupta, "An internet of things based smart surveillance and monitoring system using arduino," in *International Conference on Advances in Computing and Communication Engineering (ICACCE)*. IEEE, 2018, Conference Proceedings, pp. 428–433.

[19] G. Coley, "Beaglebone black system reference manual," *Texas Instruments, Dallas*, vol. 5, 2013.

[20] U. Isikdag, *Internet of Things: Single-board computers*. Springer, 2015, pp. 43–53.

[21] D. K. Rahmatullah, S. M. Nasution, and F. Azmi, "Implementation of low interaction web server honeypot using cubieboard," in *International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*. IEEE, 2016, Conference Proceedings, pp. 127–131.

[22] G. Chu, N. Apthorpe, and N. Feamster, "Security and privacy analyses of internet of things children's toys," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 978–985, 2018.

[23] A. Khattab, Z. Jeddi, E. Amini, and M. Bayoumi, *RFID security threats and basic solutions*. Springer, 2017, pp. 27–41.

[24] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Z. Song, "System statistics learning-based iot security: Feasibility and suitability," *IEEE Internet of Things Journal*, 2019.

[25] "The iot attack surface: Threats and security solutions," 2019. [Online]. Available: https://www.trendmicro.com/vinfo/gb/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions

[26] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 167575, 2013.

[27] M. R. Thakur and S. Sanyal, "A multi-dimensional approach towards intrusion detection system," *arXiv preprint arXiv:1205.2340*, 2012.

[28] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[29] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Z. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, 2019.

[30] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An accurate security game for low-resource iot devices," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381–9393, 2017.

[31] J. Li, Z. Zhao, R. Li, and H. Zhang, "Ai-based two-stage intrusion detection for software defined iot networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2093–2102, 2018.

[32] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," National Institute of Standards and Technology, Report, 2012.

[33] K. Letou, D. Devi, and Y. J. Singh, "Host-based intrusion detection and prevention system (hidps)," *International Journal of Computer Applications*, vol. 975, p. 8887, 2013.

[34] J. P. Amaral, L. M. Oliveira, J. J. Rodrigues, G. Han, and L. Shu, "Policy and network-based intrusion detection system for ipv6-enabled wireless sensor networks," in *IEEE International Conference on Communications (ICC)*. IEEE, 2014, Conference Proceedings, pp. 1796–1801.

[35] J. R. Vacca, *Computer and information security handbook*. Newnes, 2012.

[36] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[37] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 46, no. 4, p. 55, 2014.

[38] H. Debar, "An introduction to intrusion-detection systems," *Proceedings of Connect*, vol. 2000, 2000.

[39] K. A. Scarfone and P. M. Mell, "Sp 800-94. guide to intrusion detection and prevention systems (idps)," National Institute of Standards & Technology, Report, 2007.

[40] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[41] A. H. Farooqi and F. A. Khan, "Intrusion detection systems for wireless sensor networks: A survey," in *International Conference on Future Generation Communication and Networking*. Springer, 2009, Conference Proceedings, pp. 234–241.

[42] S. O. Amin, M. S. Siddiqui, C. S. Hong, and J. Choe, "A novel coding scheme to implement signature based ids in ip based sensor networks," in *IFIP/IEEE International Symposium on Integrated Network Management-Workshops*. IEEE, 2019, Conference Proceedings, pp. 269–274.

[43] Q. Shen, Z. Zhao, W. Niu, Y. Liu, and H. Tang, "Tolerance-based adaptive online outlier detection for internet of things," in *Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications and Int'l Conference on Cyber, Physical and Social Computing*. IEEE Computer Society, 2010, Conference Proceedings, pp. 560–565.

[44] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing rpl from topology attacks," in *2011 IFIP Wireless Days (WD)*. IEEE, 2011, Conference Proceedings, pp. 1–3.

[45] R. Fu, K. Zheng, D. Zhang, and Y. Yang, "An intrusion detection scheme based on anomaly mining in internet of things," 2011.

[46] C. Liu, J. Yang, R. Chen, Y. Zhang, and J. Zeng, "Research on immunity-based intrusion detection technology for the internet of things," in *Seventh International Conference on Natural Computation*, vol. 1. IEEE, 2011, Conference Proceedings, pp. 212–216.

[47] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in internet of things," in *International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011, Conference Proceedings, pp. 114–122.

[48] R. Chen, C. M. Liu, and C. Chen, "An artificial immune-based distributed intrusion detection model for the internet of things," in *Advanced materials research*, vol. 366. Trans Tech Publ, 2012, Conference Proceedings, pp. 165–168.

[49] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6lowpan: a study on qos security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189–1212, 2012.

[50] N. Ruan and Y. Hori, "Dos attack-tolerant tesla-based broadcast authentication protocol in internet of things," in *International Conference on Selected Topics in Mobile and Wireless Networking*. IEEE, 2012, Conference Proceedings, pp. 60–65.

[51] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*. IEEE, 2013, Conference Proceedings, pp. 600–607.

[52] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "An ids framework for internet of things empowered by 6lowpan," in *Proceedings of the 2013 ACM SIGSAC conference on Computer and communications security*. ACM, 2013, Conference Proceedings, pp. 1337–1340.

[53] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 794326, 2013.

[54] C. Jun and C. Chi, "Design of complex event-processing ids in internet of things," in *Sixth International Conference on Measuring Technology and Mechatronics Automation*. IEEE, 2014, Conference Proceedings, pp. 226–229.

[55] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in *2014 International Symposium on Next-Generation Electronics (ISNE)*. IEEE, 2014, Conference Proceedings, pp. 1–2.

[56] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[57] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in internet of things," *International Journal of Computer Applications*, vol. 121, no. 9, 2015.

[58] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things," in *IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2015, Conference Proceedings, pp. 606–611.

[59] R. An, H. Feng, Q. Liu, and L. Li, "Three elliptic curve cryptography-based rfid authentication protocols for internet of things," in *International Conference on Broadband and Wireless Computing, Communication and Applications*. Springer, 2016, Conference Proceedings, pp. 857–878.

[60] H. Sun, X. Wang, R. Buyya, and J. Su, "Cloudeyes: Cloud-based malware detection with reversible sketch for resource-constrained internet of things (iot) devices," *Software: Practice and Experience*, vol. 47, no. 3, pp. 421–441, 2017.

[61] B. Arrington, L. Barnett, R. Rufus, and A. Esterline, "Behavioral modeling intrusion detection system (bmids) using internet of things (iot) behavior-based anomaly detection via immunity-inspired algorithms," in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2016, Conference Proceedings, pp. 1–6.

[62] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat analysis of iot networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2016, Conference Proceedings, pp. 1–6.

[63] S. Chen, M. Peng, H. Xiong, and X. Yu, "Svm intrusion detection model based on compressed sampling," *Journal of Electrical and Computer Engineering*, vol. 2016, p. 12, 2016.

[64] A. Le, J. Loo, K. Chai, and M. Aiash, "A specification-based ids for detecting attacks on rpl-based network topology," *Information*, vol. 7, no. 2, p. 25, 2016.

[65] R. J. Colville and G. Spafford, "Configuration management for virtual and cloud infrastructures," *Gartner2010*, 2010.

[66] O. Networking, "Open networking foundation," 2019.

[67] S. Brief, "Sdn security considerations in the data center," 2013.

[68] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[69] R. Enns, M. Bjorklund, and J. Schoenwaelder, "Network configuration protocol (netconf)," *Network*, 2011.

[70] A. Doria, J. H. Salim, R. Haas, H. M. Khosravi, W. Wang, L. Dong, R. Gopal, and J. M. Halpern, "Forwarding and control element separation (forces) protocol specification," *RFC*, vol. 5810, pp. 1–124, 2010.

[71] H. Zhong, Y. Fang, and J. Cui, "Lbbsrt: An efficient sdn load balancing scheme based on server response time," *Future Generation Computer Systems*, vol. 68, pp. 183–190, 2017.

[72] N. L. Van Adrichem, C. Doerr, and F. A. Kuipers, "Opennetmon: Network monitoring in openflow software-defined networks," in *2014 IEEE Network Operations and Management Symposium (NOMS)*. IEEE, 2014, Conference Proceedings, pp. 1–8.

[73] V. Mann, A. Vishnoi, K. Kannan, and S. Kalyanaraman, "Crossroads: Seamless vm mobility across data centers through software defined networking," in *2012 IEEE Network Operations and Management Symposium*. IEEE, 2012, Conference Proceedings, pp. 88–96.

[74] A. Tootoonchian, M. Ghobadi, and Y. Ganjali, "Opentm: traffic matrix estimator for openflow networks," in *International Conference on Passive and Active Network Measurement*. Springer, 2010, Conference Proceedings, pp. 201–210.

[75] Z. Latif, K. Sharif, F. Li, M. M. Karim, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *arXiv preprint arXiv:1902.07913*, 2019.

[76] J. Brownlee, "Supervised and unsupervised machine learning algorithms," *Machine Learning Mastery*, vol. 16, no. 03, 2016.

[77] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," *arXiv preprint arXiv:1701.02145*, 2017.

[78] A. A. Aburomman and M. B. I. Reaz, "Survey of learning methods in intrusion detection systems," in *2016 International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES)*. IEEE, 2016, Conference Proceedings, pp. 362–365.

[79] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*. ICST (Institute for Computer Sciences, Social-Informatics and ..., 2016, Conference Proceedings, pp. 21–26.

[80] S. Zanero and S. M. Savaresi, "Unsupervised learning techniques for an intrusion detection system," in *Proceedings of the 2004 ACM symposium on Applied computing*. ACM, 2004, Conference Proceedings, pp. 412–419.

[81] I. Syarif, A. Prugel-Bennett, and G. Wills, "Unsupervised clustering approach for network anomaly detection," in *International conference on networked digital technologies*. Springer, 2012, Conference Proceedings, pp. 135–145.

[82] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *expert systems with applications*, vol. 36, no. 10, pp. 11 994–12 000, 2009.

[83] J. Haweliya and B. Nigam, "Network intrusion detection using semi supervised support vector machine," *International Journal of Computer Applications*, vol. 85, no. 9, 2014.

[84] K. P. Bennett and A. Demiriz, "Semi-supervised support vector machines," in *Advances in Neural Information processing systems*, 1999, Conference Proceedings, pp. 368–374.

[85] "Deep learning stand to benefit to data analytics and hpc expertise," 2017. [Online]. Available: https://www.cio.com/article/3180184/deep-learning-stands-to-benefit-from-data-analytics-and-high-performance-computing- hpc-expertise.html

[86] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, p. 436, 2015.

[87] "Convolutional neural networks," 2014. [Online]. Available: http://eric-yuan.me/cnn/

[88] L. Deng and D. Yu, "Deep learning: methods and applications," *Foundations and Trends® in Signal Processing*, vol. 7, no. 3–4, pp. 197–387, 2014.

[89] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in *2015 National Aerospace and Electronics Conference (NAECON)*. IEEE, 2015, Conference Proceedings, pp. 339–344.

[90] A. Vyas, "Deep learning in natural language processing," 2017.

[91] E. Lear, D. Romascanu, and R. Droms, "Manufacturer usage description specification," *IETF*, 2019.

[92] M. Jethanandani, L. Huang, S. Agarwal, and D. Blair, "Network access control list (acl) yang data model," *IETF Draft*, 2018.

[93] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, "Combining openflow and sflow for an effective and scalable anomaly detection and mitigation mechanism on sdn environments," *Computer Networks*, vol. 62, pp. 122–136, 2014.

[94] C. YuHunag, T. MinChi, C. YaoTing, C. YuChieh, and C. YanRen, "A novel design for future on-demand service and security," in *2010 IEEE 12th International Conference on Communication Technology*. IEEE, 2010, Conference Proceedings, pp. 385–388.

[95] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in *International workshop on recent advances in intrusion detection*. Springer, 2011, Conference Proceedings, pp. 161–180.

[96] K. Giotis, G. Androulidakis, and V. Maglaris, "Leveraging sdn for efficient anomaly detection and mitigation on legacy networks," in *2014 Third European Workshop on Software Defined Networks*. IEEE, 2014, Conference Proceedings, pp. 85–90.

[97] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed ddos detection mechanism in software-defined networking," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, Conference Proceedings, pp. 310–317.

[98] Y. Wang, Y. Zhang, V. K. Singh, C. Lumezanu, and G. Jiang, "Netfuse: Short-circuiting traffic surges in the cloud," in *ICC*. Citeseer, 2013, Conference Proceedings, pp. 3514–3518.

[99] J. Boite, P.-A. Nardin, F. Rebecchi, M. Bouet, and V. Conan, "Statesec: Stateful monitoring for ddos protection in software defined networks," in *2017 IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2017, Conference Proceedings, pp. 1–9.

[100] S. McGillicuddy, "Radware adds open source ddos protection to opendaylight project," Technical report, Radware, Report, 2013.

[101] H. Peng, Z. Sun, X. Zhao, S. Tan, and Z. Sun, "A detection method for anomaly flow in software defined network," *IEEE Access*, vol. 6, pp. 27 809–27 817, 2018.

[102] R. Braga, E. de Souza Mota, and A. Passito, "Lightweight ddos flooding attack detection using nox/openflow," in *LCN*, vol. 10, 2010, Conference Proceedings, pp. 408–415.

[103] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (sdn): Research issues and challenges," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 393–430, 2018.

[104] J. Ashraf and S. Latif, "Handling intrusion and ddos attacks in software defined networks using machine learning techniques," in *2014 National Software Engineering Conference*. IEEE, 2014, Conference Proceedings, pp. 55–60.

[105] M. Glick and H. Rastegarfar, "Scheduling and control in hybrid data centers," in *IEEE Photonics Society Summer Topical Meeting Series (SUM)*. IEEE, 2017, Conference Proceedings, pp. 115–116.

[106] C. Song, Y. Park, K. Golani, Y. Kim, K. Bhatt, and K. Goswami, "Machine-learning based threat-aware system in software defined networks," in *26th international conference on computer communication and networks (ICCCN)*. IEEE, 2017, Conference Proceedings, pp. 1–9.

[107] Q. Niyaz, W. Sun, and A. Y. Javaid, "A deep learning based ddos detection system in software-defined networking (sdn)," *arXiv preprint arXiv:1611.07400*, 2016.

[108] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 2016, Conference Proceedings, pp. 258–263.

[109] S. Lee, J. Kim, S. Shin, P. Porras, and V. Yegneswaran, "Athena: A framework for scalable anomaly detection in software-defined networks," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2017, Conference Proceedings, pp. 249–260.

[110] M. Ranganathan, "Soft mud: Implementing manufacturer usage descriptions on openflow sdn switches," in *International Conference on Networks (ICN)*, 2019, Conference Proceedings.

[111] A. Hamza, H. H. Gharakheili, T. A. Benson, and V. Sivaraman, "Detecting volumetric attacks on lot devices via sdn-based monitoring of mud activity," in *Proceedings of the 2019 ACM Symposium on SDN Research*, 2019, pp. 36–48.

[112] A. Hamza, H. H. Gharakheili, and V. Sivaraman, "Combining mud policies with sdn for iot intrusion detection," in *Proceedings of the 2018 Workshop on IoT Security and Privacy*, 2018, pp. 1–7.

[113] A. Hamza, D. Ranathunga, H. H. Gharakheili, M. Roughan, and V. Sivaraman, "Clear as mud: Generating, validating and applying iot behavioral profiles," in *Proceedings of the 2018 Workshop on IoT Security and Privacy*, 2018, pp. 8–14.

[114] J. Li, S. Berg, M. Zhang, P. Reiher, and T. Wei, "Drawbridge: Software-defined ddos-resistant traffic engineering," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 591–592, 2014.

[115] M. Yu, Y. Zhang, J. Mirkovic, and A. Alwabel, "SENSS: Software defined security service," in *Presented as part of the Open Networking Summit 2014 (ONS 2014)*, 2014, Conference Proceedings.

[116] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey, "Bohatei: Flexible and elastic ddos defense," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, Conference Proceedings, pp. 817–832.

[117] R. Sahay, G. Blanc, Z. Zhang, and H. Debar, in *Towards autonomic DDoS mitigation using software defined networking*, 2015, Conference Proceedings.

[118] ——, "Aroma: An sdn based autonomic ddos mitigation framework," *Computers and Security*, vol. 70, pp. 482–499, 2017.

[119] M. Wichtlhuber, R. Reinecke, and D. Hausheer, "An sdn-based cdn/isp collaboration architecture for managing high-volume flows," *IEEE Transactions on Network and Service Management*, vol. 12, no. 1, pp. 48–60, 2015.

[120] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard ai problems for security," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2003, Conference Proceedings, pp. 294–311.

[121] D. Li, L. Deng, M. Lee, and H. Wang, "Iot data feature extraction and intrusion detection system for smart cities based on deep migration learning," *International Journal of Information Management*, 2019.

[122] D. G. Gonçalves, F. L. de Caldas Filho, L. M. E. Martins, G. d. O. Kfouri, B. V. Dutra, R. d. O. Albuquerque, and R. T. de Sousa, "Ips architecture for iot networks overlapped in sdn," in *2019 Workshop on Communication Networks and Power Systems (WCNPS)*. IEEE, 2019, Conference Proceedings, pp. 1–6.

[123] S. Singh, A. Atrey, M. L. Sichitiu, and Y. Viniotis, "Clearer than mud: Extending manufacturer usage description (mud) for securing iot systems," in *International Conference on Internet of Things*. Springer, 2019, Conference Proceedings, pp. 43–57.

[124] A. Kumar and T. J. Lim, "Edima: Early detection of iot malware network activity using machine learning techniques," *arXiv preprint arXiv:1906.09715*, 2019.

[125] P. Amangele, M. J. Reed, M. Al-Naday, N. Thomos, and M. Nowak, "Hierarchical machine learning for iot anomaly detection in sdn," 2019.

[126] A. Wani and S. Revathi, *Analyzing Threats of IoT Networks Using SDN Based Intrusion Detection System (SDIoT-IDS)*. Singapore: Springer Singapore, 2018, vol. 828, pp. 536–542.

[127] L. Chang, "A proactive approach to detect iot based flooding attacks by using software defined networks and manufacturer usage descriptions," Thesis, Arizona State University, 2018.

[128] C. Wu, Y. Liu, F. Wu, F. Liu, H. Lu, W. Fan, and B. Tang, "A hybrid intrusion detection system for iot applications with constrained resources," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 12, no. 1, pp. 109–130, 2020.

[129] S. Venkatraman and B. Surendiran, "Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems," *Multimedia Tools and Applications*, vol. 79, no. 5, pp. 3993–4010, 2020.

[130] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a lightweight detection system for cyber attacks in the iot environment using corresponding features," *Electronics*, vol. 9, no. 1, p. 144, 2020.

[131] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Towards scalable and trustworthy decentralized collaborative intrusion detection system for iot," *arXiv preprint arXiv:2002.07512*, 2020.

[132] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, Y. Zhao, and L. Cui, "Robust detection for network intrusion of industrial iot based on multi-cnn fusion," *Measurement*, vol. 154, p. 107450, 2020.

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

[134] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏot: A federated self-learning anomaly detection system for iot," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, Conference Proceedings, pp. 756–767.

[135] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2015, Conference Proceedings, pp. 606–611.

[136] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban ids: An intelligent anomaly based intrusion detection system for iot edge devices," *IEEE Internet of Things Journal*, 2020.

[137] P. Bhale, S. Dey, S. Biswas, and S. Nandi, "Energy efficient approach to detect sinkhole attack using roving ids in 6lowpan network," in *International Conference on Innovations for Community Services*. Springer, 2020, Conference Proceedings, pp. 187–207.

[138] M. J. Babu and A. R. Reddy, "Sh-ids: Specification heuristics based intrusion detection system for iot networks," *Wireless Personal Communications*, pp. 1–23, 2020.

[139] B. Al-Duwairi, W. Al-Kahla, M. A. AlRefai, Y. Abdelqader, A. Rawash, and R. Fahmawi, "Siem-based detection and mitigation of iot-botnet ddos attacks," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, 2020.

[140] A. Mudgerikar, P. Sharma, and E. Bertino, "E-spion: A system-level intrusion detection system for iot devices," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 2019, Conference Proceedings, pp. 493–500.

[141] V. Kumar, A. K. Das, and D. Sinha, "Uids: a unified intrusion detection system for iot environment," *Evolutionary Intelligence*, pp. 1–13, 2019.

[142] D. Breitenbacher, I. Homoliak, Y. L. Aung, N. O. Tippenhauer, and Y. Elovici, "Hades-iot: A practical host-based anomaly detection system for iot devices," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 2019, Conference Proceedings, pp. 479–484.

[143] J. Straub, "An interdiction detection and prevention system (idps) for anti-autonomy attack repulsion," in *2019 IEEE Aerospace Conference*. IEEE, 2019, Conference Proceedings, pp. 1–8.

[144] P. R. Chandre, P. N. Mahalle, and G. R. Shinde, *Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis*. Springer, 2020, pp. 95–120.

[145] S. Alam, M. Shuaib, and A. Samad, "A collaborative study of intrusion detection and prevention techniques in cloud computing," in *International Conference on Innovative Computing and Communications*. Springer, 2019, Conference Proceedings, pp. 231–240.

[146] K. Scarfone and P. Mell, *Intrusion detection and prevention systems*. Springer, 2010, pp. 177–192.

[147] B. JOSEFSSON, *Securing your Industrial IoT ecosystem against cyber threats*, 2019. [Online]. Available: https://www.ericsson.com/en/blog/2019/4/securing-your-industrial-IoT-network-against-cyber-threats

[148] S. Arunkumar, S. Pipes, C. Makaya, E. Bertino, E. Karafili, E. Lupu, and C. Williams, "Next generation firewalls for dynamic coalitions," in *2017 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computed, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 2017, Conference Proceedings, pp. 1–6.

[149] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: Current solutions and future challenges," *arXiv preprint arXiv:1904.05735*, 2019.

[150] R. Sahay, W. Z. Meng, and C. D. Jensen, "The application of software defined networking on securing computer networks: A survey," *Journal of Network and Computer Applications*, vol. 131, pp. 89–108, 2019.

[151] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, p. 533, 2016.

[152] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[153] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy, R. Kaluri, G. Srivastava, and O. Jo, "Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72 650–72 660, 2020.