A Survey on SDN-based Intrusion Detection Systems on the Internet of Thing: Concepts, Issues, and Blockchain Applications

Heba A. Hassan (✉ Ommolham2010@gmail.com )
Menoufia University

Ezz E. Hemdan
Menoufia University

Walid El-Shafai
Menoufia University

Mona Shokair
Menoufia University

Fathi E. Abd El-Samie
Menoufia University

Research Article

Keywords: Internet of Things, Software-defined networking, Intrusion Detection Systems, and Blockchain.

DOI: https://doi.org/10.21203/rs.3.rs-694000/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
**Abstract**

With the accelerated development of computer networks utilization and the enormous growth of the number of applications running on top of it, network security becomes more significant. Intrusion Detection Systems (IDS) is considered as one of the essential tools utilized to protect computer networks and information systems. Software-defined network (SDN) architecture is used to provide network monitoring and analysis mechanism due to the programming environment of the SDN controller. On the other hand intrusion detection system is developed to monitor incoming traffic to the SDN network; hence it enables SDN to adjust security service insertion. This paper presents a survey study for SDN with the Internet of Things (IoT) and its improved versions like SDN-based IDS and SDN-based IoT. Likewise, discussing the IoT and its problems, especially the security aspects and solutions to overcome these problems. Finally, a brief description of the Blockchain concept and how it can be merged with an SDN-based IoT system to further enhance its security aspects is provided.

**1. Introduction**

The Internet of things (IoT) network consists of many heterogeneous devices that are connected and to the internet. The IoT architecture contains three layers which are called perception layer, network layer, and application layer. First, the perception layer is composed of physical devices. Then, the functionality of the network layer is to provide the communication medium. Finally, the application layer is responsible for providing services to users. Figure 1 shows that data is generated by the devices in the perception layer then it can be forwarded to the network layer using the sink node. Finally, it can be transferred to a cloud that analyzes and stores data. Different applications/services can be provided to users using these data. The applications of IoT include smart home, smart healthcare, smart transport, smart grid, etc.

IoT has many advantages regarding time efficiency, money savings, and improved quality of life, but IoT devices make the system more vulnerable to risks that can give hackers and cyber criminals opportunities to exploit sensitive information. IoT includes many heterogeneous devices and each device uses a different access protocol that respond to user requirements to upgrade security measures and various access mechanisms. Hence each application has its performance and security requirements that differ from any application. So security, privacy, scalability, and interoperability are considered the main challenges in IoT.

The concept of SDN based security has been grown quickly in the area of IoT. SDN offers solutions to problems related to IOT security. The main property of an SDN architecture is that it has the ability to separate forwarding functions and network control. Hence, network control can be accomplished, directly [7]. This separation makes network management easy [2]. This feature of SDN introduces several advantages. First, it facilitates network system management and reduces human intervention. In addition, it enables IT administrators to manage network devices without limitation to a particular vendor. Finally, it decreases operation cost compared with those of the conventional networks, since no programming language is required for the underneath infrastructure devices [8]. To maintain a high level of security and
network monitoring, it is required to allow machine learning and deep learning (ML/DL) approaches to be merged with SDN controllers [6].

Due to continuous rise of cyber-attacks all over the world [1], the research in IDS grows quickly in the academic and industrial communities. Malicious insiders, denial of services, and web-based attacks are the main reasons that cause more dangerous cybercrimes. These cybercrimes may distribute country's critical national infrastructure by giving the opportunities for malicious software to creep into the system. Hence to avoid unauthorized access, some programs such as a firewall, antivirus software, and an intrusion detection system (IDS) are deployed by many organizations to protect them from losing their intellectual property. To determine cyber-attacks rapidly, first you should identify the attack process early [1] from the network utilizing IDS. Then you should use intrusion detection systems (IDS) to identify malicious activities including viruses, worm, DDOS attacks. Irregularity detection speed, accuracy, and reliability are the basic achievement factors for IDS. Therefore ML/DL approaches can be merged with SDN-based intrusion detection to introduce several advantages such as high Quality of Service (QoS), security enforcement, and virtual management. Other advantages introduced by SDN are enhancing the network security, eliminating hardware dependency and achieving flexibility to program network devices [4, 5]. The recent development concentrates on utilizing a new network architecture, namely, the software-defined network (SDN) to execute IDS with machine learning approaches [6]. A few researchers studied integrating SDN with IoT as shown in Table 1.

When services and devices are increased in the network, IoT should be scalable and feasible enough to accommodate these changes in the network. IoT system has limited resources, and hence security mechanisms may not be supportable. The combination of Blockchain (BC) [70] with IoT provides a solution to such difficulties. The advantage of using BC is that it has a scalable, distributed, and decentralized nature that makes it the perfect solution for the improvement of various IoT aspects. This paper introduces a review study on intrusion detection in software-defined networking as well as exploring the using Blockchain for SDN security. Therefore, the contribution of this paper can be summarized as the following:

- Study the concept and architecture of intrusion detection systems.
- Exploring the SDN architecture and its applications along with reviewing the IDS for SDN associated with applying ML/DL.
- Exploring the SDN-based IoT system.
- Presenting perceptions and concerns of Blockchain (BC) technology, BC-based IoT, and BC-SDN-IoT systems.
- Discussing open research directions of this innovative paper's subject.

The rest of this paper has organized as follows

Sect. 2 presents IDS followed by common datasets used in IDS. Section 3 provides ML approaches and consequently ML/DL based IDS observation. In Sect. 4, an outline of SDN architecture and applications is
provided. We likewise survey IDS for SDN related with applying ML/DL to SDN-based IDS are talked about. Section 5 discusses the SDN-based IoT system. A brief description of BC technology, BC-based IoT, and BC-SDN-IoT systems are given in Sect. 6. Section 7 provides the Open Issues and Future Research Directions while Sect. 8 concludes the paper with future works.

Table 1 Summary of SDN based IoT.

| Research effort                                                                 | Technology | Summary                                                                                                                                 |
|--------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things[54] | SDN        | Discussed the challenges in SDN and IOT networks related to security and scalability perspectives and the usage of deep packet investigation (DPI) in that environment. |
| A Software Defined Networking Architecture for the Internet of Things[55]       | SDN        | Proposed SDN approach for IOT to accomplish separated quality levels to various IOT tasks in very heterogeneous wireless networking scenarios.   |
| A software defined based internet of things framework[56]                       | SDN        | Suggested SDIOT which is a software defined based IOT model, and hence difficulties in IOT management process from both storage and security are solved. |
| Software-defined internet of things for smart urban sensing[57]                 | SDN        | Suggested a software defined IOT architecture for smart urban sensing.                                                                 |
| Identity-Based Authentication Scheme for the Internet of Things[58]            | SDN        | Proposed identity-based authentication scheme for heterogeneous IOT that is resistant to masquerade, man-in-the-middle, and reply attacks.   |
| Black SDN for the Internet of Things[59]                                       | SDN        | Presented Black-SDN which is a software defined networking model for secure IOT networking and communications to improve routing and networking performance for broadband networks. |
| A Multi-Protocol Software-Defined Networking Solution for the Internet of Things[60] | SDN        | Discussed MINOS which is a multi-protocol SDN platform for IOT that execute service-awareness by using SDN controller.                    |
| SDN Controller Placement in IoT Networks[61]                                   | SDN-IOT controller | Optimize SDN controller to address problems with the distributed networks and introduced algorithms to increase the efficiency of the SDN Controller placement with the distributed IOT networks. |
| Enabling virtual AAA management in SDN-based IOT networks[62]                 | SDN/NFV    | Used SDN/NFV to propose a cyber-situational awareness security framework, and hence the authentication, authorization, and accounting (AAA) dynamic management are performed for IOT networks. |
| SDTCP: Towards datacenter TCP congestion control with SDN for IoT Applications[63] | SDN        | Proposed a software-defined network (SDN) based TCP congestion control mechanism (SDTCP), and hence high-traffic TCP control mechanism in cast problems for IOT is solved. |
| Security-Aware and Privacy Preserving D2D Communications in 5G[64]              | SDN        | Discussed an architecture for an LTE-D2D system and proposed security solutions from aspects of application-layer security and physical layer security on IOT devices based on SDN. |
| SDN based DDoS mitigation in IOT[65]                                           | SDN        | Leveraged SDN features to distinguish the malicious flows contributing to the DDoS flooding attack and effectively alleviate it.          |
| Man-in-the-Middle attack mitigation in IOT[66]                                 | SDN        | Proposed Counter measure by using Bloom filter in detecting MiM attacks on OpenFlow channel.                                           |
2. Intrusion Detection Systems

Intrusion Detection System (IDS) is a critical research achievement in the cybersecurity field, which can recognize an attack, which could be an ongoing attack or an attack that has already happened. Intrusion detection is like a classification problem, such as a binary or a multi-class classification problem. In binary classification, distinguish whether network traffic behavior is normal or anomalous, and in multi-class, i.e., a five-class classification problem, recognize whether it is normal or any one of the other four attack types such as DOS (Denial of Service), U2R (User to Root), Probe (Probing) and R2L (Root to Local). The major objective of intrusion detection is to successfully recognize the intrusive behavior and increasing the accuracy of classifiers.

2.1 Types of techniques of the Intrusion detection system

Techniques of intrusion detection can be divided into [14] into two primary types as shown in Fig. 2.

2.1.1 Anomaly Detection

The main idea in anomaly detection is that it detects both network and computer intrusions and misuse by monitoring system activity, and then classifying the types as either normal or anomalous. The classification here depends on heuristics or rules, as opposed to misuse detection which depends on patterns or signatures, and attempts.

Most anomaly detection systems have two phases. The first is training phase in which a profile of normal behaviors is built. The second is testing phase in which current traffic is compared with the profile created in training phase.

As we mentioned earlier that system activity must be classified as either normal or anomalous to detect both network and computer intrusions, there are several methods to detect anomalies. One of them is artificial intelligence type technique, while another method is called strict anomaly detection in which a strict mathematical mode is used to define what normal usage of the system comprises, and then any deviation is considered as an attack. Data mining methods, grammar based methods, and artificial immune system are considered as another methods used to detect anomalous.

2.1.2 Misuse Detection

The main idea in misuse detection is how to detect computer attacks. This is done by defining abnormal system behavior at first, and then any deviation is considered as normal. It seems as the opposite method to anomaly detection. Anything not known in misuse detection is considered as normal. Misuse detection depends on patterns, or signatures, and attempts. The advantage of using misuse detection is its simplicity of adding known attacks to the model, so it is used more generally to refer to all kinds of computer misuse. On the other hand the main disadvantage of misuse detection is that its inability to
recognize unknown attacks. Hence most intrusion detection systems utilize a combination of two techniques and are often deployed on the network, on a specific host, or even on an application within a host.

2.2 Types of the Intrusion detection system

Intrusion detection systems can be divided into the following:

2.2.1 Network-Based Intrusion Detection

Network-based intrusion detection systems (NIDS) are devices that are placed in different points within the network to analyze all traffic from all devices on the network. Hence, any attack can be identified. Once the attack is identified, the alert can be sent to the administrator. There are two network interfaces in NIDS. The first is used to listen to network conversation in promiscuous mode, while the second is used for control. NIDS have the ability to compare signatures for similar packets, and hence harmful detected packets are linked or dropped. On-line and off-line NIDS are considered as two main types of NIDS according to the system interactivity property. They are also called inline and tap mode. On-line NIDS is used in the network in real time to analyze the Ethernet packets to know the attack, but off-line NIDS is used to store data and make some processes on stored data to know the attack occur or not.

2.2.2 Host Based Intrusion Detection

Host-based intrusion detection systems (HIDS) are devices that run on individual hosts or devices on the network. They are used to analyze the inbound and outbound packets from the devices. Hence, if any suspicious activity is detected, HIDS will alert the user or administrator. Mission critical machines are considered as an example of HIDS usage. The main advantage of HIDS is that they have the ability to distribute the load associated with monitoring across available hosts on large networks. So, the load is spread evenly over the network which is very useful for cost and performance.

The main disadvantage in HIDS is that they can't see network traffic because they are designed to run on a single system.

2.3 Common Datasets used in IDS

Many datasets are not openly accessible in order to achieve security and privacy issues. Additionally, the data which are openly accessible are anonymous effort and don't examine the present network traffic variety. The details of different IDS datasets are mentioned in Table 2.

Table 2: Datasets used in IDS
### Dataset Description

| Dataset     | Description                                                                                                                                 |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| KDDCup 99   | MIT Lincoln Labs are responsible for preparing and managing 1998 DARPA intrusion detection evaluation program. The goal was to overview and assess research in intrusion detection. It provided a standard set of data which incorporates a wide variety of intrusions that can be simulated in a military network environment. The 1999 KDD intrusion detection is considered to be the upgraded version of DARAP98. Take into mind that there are two forms in KDDCup99 which are full dataset and 10% dataset. There are 41 features and 3 classes ('Normal', 'DoS', 'Probe', 'R2L', 'U2R') in this dataset. Features counting from [1-9] are known as basic features. Features counting from [10-22] are known as content features. Features counting from [23-41] are known as time-based traffic features. |
| NSL-KDD     | NSL-KDD [14, 50, 51] is a dataset proposed to solve some of inherent problems of the KDDCup99 dataset. The advantage of NSL-KDD is that the number of records in train and test sets is reasonable that makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Hence, evaluation results will be consistent and comparable. NSL-KDD can be used to protect machine learning algorithms but from being biased. NSL-KDD has selected records of the complete KDD Cup 99 dataset, but suffers from representing the real-time network traffic profile characteristics. |
| UNSW-NB15   | UNSW-NB15 was published by cyber security research team of Australian Centre for Cyber Security (ACCS) in 2015. There are 9 attack types, 49 features, and a variety of normal and attacked activities that are included in this dataset. There are 6 groups of features in UNSW-NB15. These groups are Basic Features, Flow Features, Time Features, Content Features, Additional Generated Features, and Labeled Features. These features can be classified into General Purpose Features [36-40], and Connection Features [41-47]. On the other hand, the nine attack types exist in this dataset are named as Analysis, Fuzzers, Backdoors, DOS, Exploits, Reconnaissance, Generic, Shellcode, and Worms. |
| Kyoto       | Network traffic data in the honeypot systems of Kyoto University includes 24 statistical features. These features are divided into 14 conventional features and 10 additional features. As we mentioned earlier that KDDCup 99 dataset has 41 original features, the first 14 features of Kyoto are extracted based on KDDCup 99 dataset from the raw traffic data obtained by honeypot systems. On the other hand, additional 10 features are extracted to enable us to know more about the network. These 10 features can be used for training and testing data with 14 conventional features. |
| WSN-DS      | It is a specialized dataset designed for wireless sensor networks (WSN). It is designed to enable us to detect and classify four types of 'DoS' attacks such as Blackhole, Grayhole, Flooding, and Scheduling. Low-energy adaptive clustering hierarchy (LEACH) protocol is used in this dataset, and hence data is collected from network Simulator 2 (NS-2). The collected data is then preprocessed to produce 23 features in WSN-DS dataset. |
| CICIDS2017  | It is a new dataset that was designed to overcome the problems existed in previous datasets since 1998 such as lack of traffic diversity and volumes. This new dataset is designed to include benign and the most up-to-date common attacks. It additionally incorporates the results of the network traffic analysis. This is done by using CICFlowMeter with labeled flows dependent on the timestamp, source, and destination IPs, source and destination ports. In this dataset, benign traffic was built to have the characteristics of 25 users based on the HTTP, HTTPS, FTP, SSH, and email protocols. On the other hand, the different attacks infused were Brute Force FTP, Brute Force SSH, 'DoS', Heartbleed, Web Attack, Infiltration, Botnet and 'DDoS'. |

### 3. Machine Learning For Intrusion Detection

Machine learning (ML) introduces many advantages. These advantages are improvement the detection rate, reduction the false alarm rate, and decreasing the cost [19]. As shown in Fig. 3, machine learning approaches can be classified according to their learning styles to supervised, unsupervised learning, and semi-supervised learning [3].
Firstly in supervised learning to predict unknown cases, there are many algorithms used to learn representations from labeled input data. These algorithms are support vector machine (SVM) that used for classification problems and random forest that used for classification and regression problems [17]. The main property for SVM algorithms that makes it broadly utilized in NIDS research and appropriate for high dimensional data is its powerful classification power and practicality in computation. SVM has a problem for choosing a reasonable kernel function as it requires computational processing units and memory [18]. On the other hand the Random forest algorithm [20] is considered a powerful approach when dealing with uneven data but its shortcoming is that it is exposed to over-fitting.

Secondly in the unsupervised learning scheme, unlabeled input data is used by algorithms as opposite to supervised learning. To predict unknown data, unsupervised learning algorithms model the fundamental structure or distribution in the data [17]. Principal component analysis (PCA) and self-organizing map (SOM) are considered as examples of unsupervised learning algorithms. Principal Component Analysis (PCA) is an algorithm of feature reduction techniques that is utilized to significantly accelerate unsupervised feature learning [21]. PCA is used for feature selection by many researches before applying classification [22]. On the other hand self-organizing map (SOM) is one of clustering techniques that was utilized to reduce payload in NIDS. K-means and other distance-based learning algorithms are other clustering algorithms that utilized for anomaly detection because they are exposed to initial conditions such as centroid, and may produce a high false-positive rate [24].

Finally, Semi-supervised learning is considered as a kind of supervised learning because a small amount of labeled data converged with a large number of unlabeled data to form the training data such as photo archives [25]. Keeping in your mind that Semi-supervised support vector machine [26] is another way to improve the accuracy of NIDS [27]. Spectral Graph Transducer and Gaussian Fields approach are two examples of semi-supervised classification that are used to distinguish unknown attacks while MPCK-means is an example of semi-supervised clustering method [28].

### 3.1 Deep learning for network intrusion detection system

With the accelerated development of machine learning, deep learning has become more popular, so it has been applied for intrusion detection. Recent studies have presented that deep learning has the potential to generate better models than traditional methods. Table 3 shows different datasets used in the intrusion detection system using a deep learning approach.

**Table 3** Comparison of Datasets used in IDS using the DL approach.
Deep Learning algorithms can be considered as a new version of artificial neural networks that exploit abundant, affordable computation [38]. We can use a deep learning algorithm to learn a representation of data with various levels of generalization. Object detection, detecting network intrusion, and visual object recognition [39] are some applications that use deep learning algorithms. Supervised and unsupervised ways are used to train a deep learning algorithm [12]. The CNN [39] is illustrated as an example of deep learning algorithms that uses a supervised way for training. The CNN architecture is utilized in general in applications such as face recognition [39] and 2D images [40].

| Publication               | Method                                                                 | Dataset used               |
|---------------------------|------------------------------------------------------------------------|---------------------------|
| Chuanlong Yin[29]         | Proposed a deep learning approach for intrusion detection system based on recurrent neural networks for intrusion detection (RNN-IDS) and discussed the performance of the model in both binary classification and multiclass classification. | NSL-KDD                   |
| OzgurDcprcn [30]          | Proposed Intrusion Detection System (IDS) architecture that utilized both anomaly and misuse detection approaches. This architecture utilized a Self-Organizing Map (SOM) structure for the proposed anomaly detection module to demonstrate normal behavior and the deviation from the normal behavior is classified as an attack. | KDD Cup '99               |
| Nathan Shone [31]         | Proposed deep learning classification model built utilizing stacked non-symmetric deep autoencoder (NDAE) for unsupervised feature learning in a network intrusion detection system. | KDD Cup '99 and NSL-KDD    |
| Ping Wang [32]            | Introduced a network intrusion detection system utilizing convolutional neural networks (CNN) based classifier for enhancing the precision of model dependent on LeNet-5 to classify the network threat. | KDD Cup '99               |
| BhupendraIngre [33]       | Utilized NSL-KDD dataset to assess the performance of Artificial Neural Network and obtained a result for the binary class as well as five class classification (normal vs four types of attack). | NSL-KDD                   |
| Howon Kim[34]             | Proposed a deep learning approach to construct an IDS, and applied Long Short Term Memory (LSTM) architecture in a Recurrent Neural Network (RNN). | KDD Cup '99               |
| MalbodTavallae [35]       | Examined the performance of KDD CUP 99 and introduced NSI-KDD dataset which comprises of selected records of the complete KDD data set, but has the ability to overcome difficulties existed in KDD CUP 99. | KDD Cup '99 and NSL-KDD    |
| Sang-Hyun Choi and Hec-Su Chae[36] | Proposed another feature selection method attribute ratio that utilizes the attribute average of total and each class data to enhance the efficiency of data mining algorithms by removing the redundant or irrelevant feature. | NSL-KDD                   |
| Anna Buczak [37]          | Introduced machine learning (ML) and data mining (DM) methods that are utilized in cyber analytics in support of intrusion detection, provided a short description of each ML/DM method, and addressed the complexity of ML/DM algorithms when they are used for cyber security. | Some well-known cyber datasets such as DARPA 1998, DARPA 1999, DARPA 2000, or KDD 1999 data sets |
On the other hand an autoencoder [41] is considered as example of deep learning algorithms that can be trained in an unsupervised way. An autoencoder achieves dimensionality reduction by learn a representation (encoding) for a set of data. A Deep Belief Network (DBN) [42] is another example of deep learning algorithms that can be trained at first in an unsupervised way to learn how to reconstruct its inputs then it can be trained in a supervised way to achieve classification. The goal of using DBNs that include restricted Boltzmann machines (RBMs) [43] or auto-encoders is to achieve collaborative filtering, topic modeling, feature learning, regression, and dimensionality reduction, etc.

Recurrent neural network (RNN) [44] is an example of deep learning algorithms that can be trained in a supervised or unsupervised way to process random orders of inputs by using internal memory. The main property of RNN is that it has the ability to predict character in the text and learn dependencies and actual evidence stored for a long time [39]. A typical application for RNN is speech recognition [45].

### 3.1.1 Recurrent Neural Network

The recurrent neural network is presented in Fig. 4, which contains three different types of units such as input units, output units, and hidden units. Hidden units are considered the most important work is completed be, and because they also remember the end-to-end information i.e., hidden units are the storage of the whole network. There is a single flow of information in the RNN model, from the input units to the hidden units. At the point when we unfold the RNN, we can find that it encapsulates deep learning. For supervised classification learning, we can utilize RNNs based approach as mentioned in [46]. The fundamental difference between Recurrent Neural Networks and traditional Feed-forward Neural Networks (FNNs) is that RNN has presented a directional loop which is utilized to retain the preceding information and hence it can be applied to the present output. The previous output is additionally associated with the present output of a sequence, and the nodes between the hidden layers also have connections. The output of the input layer, as well as the output of the last hidden layer, can be considered as the input of the hidden layer.

### 3.1.2 Convolutional Neural Network

The convolutional neural network (ConvNet) [47] is a class of deep neural networks that is applied in image and video recognition, recommender systems, image classification, medical image analysis, and financial time series. ConvNet has three main layers: input layer, output layer, and multiple hidden layers which consist of a series of convolutional layers such as pooling layers, fully connected layers, and normalization layers. These layers are called hidden layers because their inputs and outputs are masked by the activation function and final convolution. The most activation function used is a Relu layer.

As we mentioned earlier that image recognition is one of applications used for ConvNet, Fig. 5 shows an example for image recognition. First, the feature extraction network is used to extract feature signals from input image, and then classification neural network produces the output from the features of the image.
The feature extraction neural network as shown in the figure has many digital filters that convert the image by using the convolution operation. On the other hand, the main property in the pooling layer is that it decreases the dimension of the image from many pixels to a single pixel.

4. Software-defined Networking (SDN) Based Intrusion Detection System

This section presents the intrusion detection system for SDN.

4.1 Overview of Software-Defined Networking

SDN [7] is a new technology concerned with planning, constructing, and overseeing systems. Separating the network's control (brains) and forwarding (muscle) planes is the main property for SDN to make it simpler to advance each. In this condition, a Controller goes about as the "brains," giving a conceptual, concentrated perspective of the general system. Through the Controller, organize chairmen can rapidly and effectively settle on and push out choices on how the fundamental frameworks (switches, routers) of the forwarding plane will deal with the activity. The most widely-used SDN protocol that manages the relation between the controller and the switches is the OpenFlow [52, 53]. An SDN depends on Application Programming Interfaces (APIs). These APIs, usually called northbound APIs, empower effective administration coordination and computerization. Accordingly, the SDN empowers a system to shape movement and send administrations to address-changing business needs, without touching any individual switch or any switch in the sending plane. The SDN is another system that tends to empower more agile and financially savvy systems. The Open Networking Foundation (ONF) leads the pack in SDN standardization [7]. Figure 6 introduces a simple logical representation of SDN architecture. The ONF/SDN engineering comprises three layers that are available through open APIS:

- The application layer is specialized for expanding the SDN communication services. Both application layer and control layer are separated by the northbound API.
- The control layer is specialized for overseeing the network forwarding behavior through an open interface by leveraging from the centralized control.
- The infrastructure layer is specialized for packet switching and forwarding by using Network Elements (NEs) and devices.

A software-defined network is a new technology that has the ability to separate the network control and forwarding functions. Hence, programming of the network control can be achieved, directly [7]. The separation feature of SDN makes network management easy [2] and introduces several advantages. First, it facilitates innovative applications. Then, it helps for dictating a new networking paradigm with the ability to implement IDS [8]. To maintain a high level of security and network monitoring, it is required to allow machine learning and deep learning (ML/DL) approaches to be merged with SDN controllers [6]. On the other hand, ML/DL approaches can be merged with SDN-based intrusion detection to introduce several advantages such as high Quality of Service (QoS), security enforcement, and virtual
management. Other advantages introduced by SDN are enhancing the network security, eliminating hardware dependency and achieving flexibility to program network devices.

4.2 SDN Applications

There are many applications for SDN. These applications tend to increase the flexibility of a network and at the same time reduce both the total time required to market and total cost of ownership of future IT network infrastructures. Some of the applications of SDN are discussed in this part [48].

- **Wireless Communication**: Mobile communication networks leverage from the programmability feature of the SDN that can be used to fine-tune mobile communication performance. Hence, new applications for mobile communication networks are developed. On the other hand internet of things (IOT), Wi-Fi access network, wireless mesh network, and wireless cellular communication are other applications that leverage from SDN architecture. SDN presents many advantages. For example SDN introduces scalability in the IOT paradigm and creates opportunities for bandwidth sharing and network connectivity in wireless mesh networks.

- **Data centers**: SDN introduces many advantages when used in network control, data center environment, optimal traffic engineering, and policy implementations especially when operated at large scales. These advantages are concerned with network latency reduction and security in an automated and dynamic fashion in the data centers [48].

- **SDN-Based Cloud**: The main advantage of using SDN in cloud techniques is that it has the ability to defeat cloud intrusions. On the other hand, the service scalability in cloud environments is increased when the SDN paradigm is joined with cloud techniques [49].

- **Residential environment**: SDN framework achieves greater visibility for users and service providers in residential and small office networks. On the other hand SDN achieves greater accuracy and scalability by using anomaly detection systems in a SOHO network [4].

4.3 SDN Based Intrusion Detection System using ML/DL

The programming environment of the SDN controller allows SDN architecture to provide network monitoring and analysis mechanism. On the other hand intrusion detection system [IDS] is developed to monitor incoming traffic to the SDN network; hence it enables SDN to adjust security service insertion. Taking into account that SDN-based intrusion detection system (IDS) is concentrated on an SDN controller as shown in Fig. 7. This IDS is utilized to recognize the malicious flow by analyzing the traffic intended to the SDN network. After analyzing traffic, SDN switches receive the traffic coming from outside networks. Then SDN switches check flow table entries that is concerned with transmitted packets which are characterized by the controller. Keeping in your mind that if flow entry for respective packets does not exist in the periodically updated flow table then, respective packets take a path to the controller that is responsible for setting the data path to the corresponding packets.
The architecture of the system is shown in Fig. 6. First, preprocessing is applied to the given input which includes numericalization and normalization [46]. In numericalization, non-numeric features are converted into numeric features by using encoding and in normalization, features are scaled i.e. the value of every feature is mapped to [0,1] range. In the feature selection step, optimal features are selected a given to the training of the neural network.

4.4 System Analysis

The recurrent neural network is trained using NSL-KDD, KDDCUP 99, and UNSW-NB15 Datasets. Three datasets are available for both binary and multiclass classification. The detailed statistics of these datasets are reported in Table 5 and Table 6.

| Attack Type | Description                                                        |
|-------------|--------------------------------------------------------------------|
| Normal      | Normal connection records                                          |
| DoS         | Attacker aims at making network resources down                     |
| Probe       | Obtaining detailed statistics of system and network configuration details |
| R2L         | Illegal access from remote computer                                |
| U2R         | Obtaining the root or super-user access on a particular computer    |
Table 6  
Types of attacks for the UNSW-NB15 dataset.

| Class     | Description                                                                 |
|-----------|-----------------------------------------------------------------------------|
| Normal    | Normal connection records                                                   |
| Fuzzers   | Attacks related to spams, html files penetrations and port scans             |
| Analysis  | Attacks related to port scan, html file penetrations and spam                |
| Backdoors | Backdoors is a mechanism used to access a computer by evading the background existing security. |
| DoS       | Intruder aims at making network resources down and consequently, resources are inaccessible to authorized users |
| Exploits  | The security hole of operating systems or the application software is understand by an attacker with the aim to exploit vulnerability |
| Generic   | Attacks are related to block-cipher                                          |
| Reconnaissance | A target system is observe by an attacker to gather information for vulnerability |
| Shell code| A small part of program termed as payload used in exploitation of software    |
| Worms     | Worms replicate themselves and distributed to other system through the computer network |

The performance of the model is evaluated using accuracy which is calculated by using the confusion matrix. The value of accuracy is considered as performance indicator of the RNN model. Table 7 shows the accuracy of RNN with a different number of features for binary classification with different datasets. The number of epochs is given 100.

Table 7 The accuracy of RNN with a different number of features for binary classification with different datasets.
5. Sdn-based Iot

The concept of SDN has been grown quickly in the area of the Internet of Things (IoT). SDN offers solutions to problems concerned with IoT security. In SDN architecture controller becomes an intelligent resource in the network. The controller is decoupled from the networking element and set in the control plane. This gives different points of interest to design the network with less time and resources. As IoT has many drawbacks, many researchers propose a new architecture that merges SDN with IoT to enhance their performance. The combination of SDN with IoT is shown in Fig. 8 where the SDN controller is used to monitoring all devices in the network such as the sink node of IoT and OpenFlow switch to achieve better performance. SDN controller can program all devices in the network according to the requirement and hence, it helps in solving many of the difficulties of IoT. On the other hand, the proper installation of OpenFlow switches and SDN controllers helps in enhancing the reliability of the IoT network. Using programmable OpenFlow protocol introduces many advantages. First it helps the IoT system to manage its devices more efficiently. Then, it increases the overall network performance in terms of low bandwidth utilization and high throughput of the network. SDN-based IOT can be additionally enhanced by merging fog computing with. This allows computations to occur at the edge of the network. So, decentralized computing infrastructure is obtained and hence, the overall computation load is reduced [71]. The architecture of SDN-based IoT and fog computing is shown in Fig. 9 where data of IoT application is processed on the edge of the network itself and hence, network latency and bandwidth will be reduced.

6. Blockchain

| No. of features | NSL-KDD | KDDCup 99 | UNSW-NB15 |
|-----------------|---------|-----------|-----------|
| 16              | 0.0264  | 0.0264    | 0.0264    |
| 17              | 0.0283  | 0.0283    | 0.0264    |
| 18              | 0.0283  | 0.0283    | 0.0260    |
| 19              | 0.0263  | 0.0263    | 0.0263    |
| 20              | 0.2766  | 0.2766    | 0.2993    |
| 21              | 0.2878  | 0.2881    | 0.2974    |
| 22              | 0.2882  | 0.2882    | 0.3022    |
| 23              | 0.3474  | 0.3537    | 0.4067    |
| 24              | 0.3765  | 0.3765    | 0.4279    |
| 25              | 0.3772  | 0.3775    | 0.4287    |
| 26              | 0.3777  | 0.3789    | 0.4237    |
| 27              | 0.3774  | 0.3775    | 0.3987    |
| 28              | 0.0260  | 0.0260    | 0.0260    |
| 29              | 0.3894  | 0.3893    | 0.0260    |
Blockchain (BC) is a new technology that has already been implemented in cryptocurrencies such as Bitcoin, Ethereum, etc. BC technology provides a way to record transactions or any digital interaction securely. BC has a distributed and decentralized nature that makes it a secure solution over IOT and Artificial Intelligence (AI). BC can be classified into three types. They are public, private, and permissioned [70]. Public BC can make anyone join the BC network without the agreement of third parties. On the other hand, the owner in private BC has the ability to control access of the nodes in the network because network access is restricted. Keep in mind that in private BC, authorized nodes can only maintain consensus. Finally, permission BC is a combination of public and private BCs.

As shown in Fig. 10, a digital ledger is composed of recorder blocks. The role of blocks is to record transactions across many computers. A blockchain database is controlled automatically utilizing a peer-to-peer network. Blocks include batches of valid transactions. These batches are hashed and encoded into a Merkle tree. Each block keeps the copyright hash of the prior block and the hash of the previous block that confirms integrity in the BC. Additionally, each block includes the Merkle root in the block header. Keep in mind that, if multiple copies have the same Merkle root, all transactions in that block are the same.

6.1 Blockchain-based IoT

Due to changes existed in the network such as increasing services and devices, IOT should have enough scalability and feasibility to be able to face these changes. IOT system has limited resources, and hence security mechanisms may not be supportable. The main advantage of BC-based IoT is that it helps in tracking billions of connected devices. Hence, the processing of transactions and coordination between devices can be executed. Figure 11 shows the architecture of BC-based IoT. The perception layer as shown has various devices for every application. Hence, the local miner in each application enable it to store transactions from the other devices in local BC [72].

6.2 Blockchain-based SDN and IoT architecture

BC can be merged with SDN for improving the overall security and privacy of IoT. The advantage of using this architecture is that it has a distributed and decentralized nature that makes the system more resilient and reduces the impact of attacks. The architecture is shown in Fig. 12 where the edge networks include edge nodes. On the other hand, the blockchain layer contains core miner nodes that provide high computation and high storage resources. Miner nodes are responsible for creating blocks and achieve consensus [73, 74].

Although the combination of BC with IoT has many advantages in terms of security and privacy, it has many challenges [68]. Firstly, the algorithms for cryptographic and consensus used in the current implementation of BC require significant computational resources, and existing IoT can't provide the same. Secondly, BC reduces the need for the server to store transactions, but the size of the global ledger
increases with the increasing blocks. This conflicts with IoT devices that have very low storage capacity. Thirdly, the current implementation of BC requires an increase in the number of nodes and this means more scalability, but SDN and IoT suffer from scalability issues. So, the combination of BC-SDN-IoT will be affected by this problem that needs to be resolved to improve the performance. Finally, consensus protocols used in BC such as PoW and PoS require significant and energy-consuming. Therefore, researchers try to solve these difficulties and develop improved IoT architecture to the extent that even the BC concept can be merged with it.

7. Open Issues And Future Research Directions

Although SDN has many advantages concerned with its flexibility, features, and suitability to control and manage IoT networks. The combination of SDN and IoT has several limitations that need to be solved by researches. The following research areas need to be discussed as shown in Fig. 13:

- **SDN-based IoT controller**: SDN controller's south bound APIs need to be changed to communicate with IoT devices and this requires lots of effort.

- **Limited table sizes of switches**: Since the IoT network consists of millions of devices, this requires large flow tables at SDN-enabled switches. Each unknown flow needs a new entry in the switch's memory. Hence, this becomes the main challenge to store the flow rules.

- **Communication traffic between the gateway and the controller**: There is a large number of IoT devices that generate huge amounts of traffic that will be taken into consideration in traffic management to ensure network availability. Hence, new security mechanisms for the SDN-IoT environment should be considered to overcome the problems caused by the huge amount of traffic.

- **Mobility issues**: The nature of IoT infrastructure component differs from the variety of smart objects which are static and mobile. Thus, the diversity in the mobility patterns should be taken into consideration when including the mobility challenge in the transmission rules updating process.

- **Interoperability**: As we mentioned before about the diversity of existing devices nature, common standards, and protocols is required to integrate communication among these devices. Therefore, the interaction between heterogeneous equipment, dependable transport, and routing are considered challenges.

8. Conclusion

The usage of the IoT system has increased in recent years due to the need for applications such as smart homes and smart cities. Hence, a suitable protection system is required to adapt with a large amount of produced data, but this conflicts with IoT. The data are vulnerable to various attacks. IDS systems are intended to identify attacks early. Due to the dynamic nature of the attacks, we should take into account various issues while implementing IDS such as the adaptability of the detection method, but there are many challenges. One of them is that the dimensions of the dataset should be reduced, so feature selection method with classification should be developed to classify dataset properly using deep learning
techniques. On the other hand designing a centralized SDN controller is another challenge that can monitor and implement real-time intrusion detection in high-speed networks. In the SOHO network [39], most of malicious activities should be identified, so SDN-based IDS architectures should be developed. Keep in your mind that none of the approaches that implement SDN-based IDS are applied to critical infrastructure and high-speed network infrastructure. SDN can be merged with IoT because SDN provides opportunities to solve issues related to IoT security. Another problem related to IoT is that IoT devices are resource and energy-constrained. Hence, the traditional security mechanism required for this implementation is very difficult. The combination of BC with IoT can solve this problem due to the scalable, distributed, and decentralized nature of BC. The combination of BC with IoT has many advantages in terms of security and privacy.

9. Declarations

1. Funding: There are no funding source for this work.
2. Conflict of interest: There are no conflict of interest for this manuscript.
3. Availability of Data and Material: Not applicable for this manuscript.
4. Code Availability: The codes are available and can be provided only by request.
5. Authors’ contributions: Security and Intrusion Detection for recognizing attacks.

10. References

1. Hewlett Packard Enterprise (2015) 2015 cost of cyber crime study: global, independently conducted by Ponemon institute LLC publication, Ponemon Institute research report. Available https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf. Accessed 26 June 2017
2. Kreutz D, Ramos FMV, Verissimo PE, Rothenberg CE, Azodolmolky S (2015) Software-defined network- a comprehensive survey. Published in Proceedings of the IEEE, 103, 1
3. Aburomman AA, Reza MBI (2016) Survey of learning methods in intrusion detection systems. International conference on advances in electrical, electronic and system Engineering(ICAEES), Putrajaya, pp 362–365. https://doi.org/10.1109/ICAEES.2016.7888070
4. Mehdi SA, Khalid J, Khaiyam SA (2011) Revisiting traffic anomaly detection using software defined networking. In: Sommer R, Balzarotti D, Maier G (eds) Recent Advances in Intrusion Detection. RAID 2011. Lecture Notes in Computer Science, vol 6961. Springer, Berlin, Heidelberg
5. García-Teodoroa P, Díaz-Verdejo J, Macía-Fernaández G, Vázquez E (2009) Anomaly-based network intrusion detection: Techniques, systems and challenges. J Comput Secur 28(1-2):18–28
6. Tuan TA, Mhamdi L, Mclernon D, Zaidi SAR, Ghogho M (2016) Deep learning approach for network intrusion detection in software defined networking. Int Conf Wirel Netw Mob Commun. https://doi.org/10.1109/WINCOM.2016.7777224
7. Open Networking Foundation (2013) SDN architecture overview, Version 1.0. Available https://www.opennetworking.org/images/stories/downloads/sdnresources/technical-reports/TR_SDNARCH-Overview-1.1-11112014.02.pdf. Accessed 27 June 2017

8. Sezer S, Scott-Hayward S, Chouhan PK (2013) Are we ready for SDN? Implementation challenges for software-defined networks. In: IEEE Communication Magazine, vol. 51, no. 7, pp 36–43. https://doi.org/10.1109/MCOM.2013.6553676

9. Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen, S., Isoaho, J.: Distributed internal anomaly detection system for internet-of-things. In: 13th IEEE Annual Consumer Communications Networking Conference (CCNC), pp. 319–320 (2016)

10. Pongle, P., Chavan, G.: Real time intrusion and wormhole attack detection in Internet of Things. Int. J. Comput. Appl. 121(9), 1–9 (2015)

11. Raza, S., Wallgren, L., Voigt, T.: SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw. 11, 2661–2674 (2013)

12. Sforzin, A., Conti, M., Marmol, F.G., Bohli, J.-M.: RPiDS: raspberry Pi IDS a fruitful intrusion detection system for IoT. In: International IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, pp. 440–448 (2016)

13. Kasinathan, P, Costamagna, G., Khaleel, H., Pastrone, C., Spirito, M.A.: DEMO: an IDS framework for internet of things empowered by 6LoWPAN, pp. 1337–1339 (2013)

14. K. Lahre, T. Diwan, S. Kashyap, P. Agrawal, "Analyze Different approaches for IDS using KDD 99 Data Set", International Journal on Recent and Innovation Trends in Computing and Communication , Volume: 1, Issue: 8, AUG 2013, pages 645-651

15. N. Sultana, N. Chilamkurti, W. Peng, R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches", Peer-to-Peer Networking and Applications, Springer, (2019) 12:493–501

16. Vinayakumar R, Mamoun Alazab, Soman KP, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman, "Deep Learning Approach for intelligent Intrusion Dection System", 10.1109/ACCESS.2019.2895334, IEEE access

17. Supervised and unsupervised machine learning algorithms http://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/. Accessed 20 June 2017

18. Atkinson RC, Bellekens XJ, Hodo E, Hamilton A, Tachtatzis C (2017) Shallow and deep networks intrusion detection system: a taxonomy and survey. CoRR, arXiv preprint arXiv:1701.02145.2017 Jan 9

19. Zamani M, Movahedi M (2015) Machine learning techniques for intrusion detection. CoRR, arXiv preprint arXiv:1312.2177. 2017 Jan 9

20. Thaseen S, Kumar Ch (2013) An analysis of supervised tree based classifiers for intrusion detection system. In: Proceedings of the international conference on pattern recognition, informatics and
mobile engineering (P RIME). Pp. 21–22

21. Eid HFA, Darwish A, Hassanien AE, Abraham A (2010) Principal components analysis and support vector machine based intrusion detection system. International conference intelligent systems design and applications (ISDA)

22. Niyaz Q, Sun W, Javaid AY, Alam M (2016) A deep learning approach for network intrusion detection system. International conference wireless networks and mobile communications (WINCOM)

23. Zanero S, Savaresi SM (2004) Unsupervised learning techniques for an intrusion detection system. In: Proceedings of the ACM symposium on applied computing. Pages 412–419

24. Syarif I, Prugel-Bennett A, Wills G (2012) Unsupervised clustering approach for network anomaly detection. In: Benlamri R (eds) Networked Digital Technologies. NDT 2012. Communications in Computer and Information Science, vol 293. Springer, Berlin, Heidelberg

25. Tsai C, Hsu Y, Lin C, Lin W (2009) Intrusion detection by machine learning: a review. Expert Syst Appl 36:11994–12000

26. Bennett KP, Demiriz A (2017) Semi-supervised support vector machines. Neural Comput & Applic 28(5):969–978

27. Haweliya J, Nigam B (2014) Network intrusion detection using semi supervised support vector machine. Int J Comput Appl 85, 9

28. Chen C, Gong Y, Tian Y (2008) Semi-supervised learning methods for network intrusion detection. Int Conf Sys, Man Cybern, IEEE. https://doi.org/10.1109/ICSMC.2008.4811688

29. Chuanlong Yin, Yuefei Zhu, Jinlong Fei, And Xinzheng He, “A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks”, vol. 05, pp. 21954-21961, oct 2017.

30. Depren, Ozgur, et al., "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks", Expert systems with Applications 29.4, pp. 713-722, 2005

31. Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi, "A Deep Learning Approach to Network Intrusion Detection", vol. 2, pp. 41-50 no. 1, feb 2018

32. Wen-Hui Lin1, Hsiao-Chung Lin, Ping Wang, Bao-Hua Wu, Jeng-Ying Tsai, "Using Convolutional Neural Networks to Network Intrusion Detection for Cyber Threats", ISBN 978-1-5386-4342-6, pp.1107-1170, 2018

33. B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN", in Proc. Int. Conf. Signal Process. Commun. Eng. Syst., Jan. 2015, pp. 92-96.

34. Jihyun Kim, Jaehyun Kim, Huong Le Thi Thu, and Howon Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection", Platform Technology and Service (PlatCon), 2016 International Conference on. IEEE, 2016.

35. M. Tavallaee, E. Bagheri, W. Lu, and A. A. A. Ghorbani, "A detailed analysis of the KDDCUP 99 data set", in Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl., Jul. 2009, pp. 1-6.

36. Sang-Hyun Choi and Hee-Su Chae, "Feature Selection using Attribute Ratio in NSL-KDD data", International Conference Data Mining, Feb 4-5, 2014 Bali (Indonesia), pp. 90-92
37. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection", IEEE Commun. Surveys Tuts, vol. 18, no. 2, pp. 11531176, 2nd Quart, 2016

38. Deep learning stand to benefit to data analytics and HPC expertise
   http://www cio com/article/3180184/analytics/deep-learningstands- to- benefit-from-data-analytics- and-high-performance-computing- hpc-expertise.html. Accessed 3 July 2017

39. LeCun Y, Bengio Y, Hinton G (2015) Deep learning review. Weekly journal of science in nature international. Nature 521, doi: https://doi.org/10.1038/nature14539

40. Convolutional Neural Networks (2017) http://eric-yuan.me/cnn/. Accessed 10 July 2017

41. Deng L, Yu D (2014) Deep learning methods and applications. Microsoft Research. Available https://www.microsoft.com/en-us/ research/publication/deep-learning-methods-and-applications/. Accessed 10 July 2017

42. Alom MZ, Bontupalli VR, Taha TM (2015) Intrusion detection using deep belief networks. Aerospace and electronics conference, NAECON. IEEE

43. Tutorial http://ufldl.stanford.edu/tutorial/supervised/ ConvolutionalNeuralNetwork/. Accessed June 15 2017

44. Vyas A (2017) Deep learning in natural language processing" in mphasis, deep learning- NL_whitepaper

45. Hughes T, Mierle K (2013) Recurrent neural networks for voice activity detection IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, pp 7378–7382. https://doi.org/10.1109/ICASSP.2013.6639096

46. Prajyot S. Autade, Prakash N. Kalavadekar. "Intrusion Detection System using Recurrent Neural Network with Deep Learning", International Journal of Innovative Research in Computer and communication Engineering. Vol. 7, Issue 4, April 2019

47. Phil Kim, " MATLAB Deep Learning: With Machine Learning, Neural Networks and Artificial Intelligence", DOI 10.1007/978-1-4842-2845-6

48. Bakshi T (2017) State of the art and recent research advances in software defined networking. In Wireless Communications and Mobile Computing, 2017, 1530-8669, Hindawi Publishing Corporation

49. Yan Q, Yu FR, Gong Q and Li J (2016) Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp 602– 622 Firstquarter 2016. https://doi.org/10.1109/COMST.2015.2487361

50. Mohammad K.Siddiqui and Shams Naahid, "Analysis of KDD CUP 99 Dataset using Clustering based Data Mining", International Journal Of Database Theory and Application, Vol.6. No.5 (2013), pages.23-34

51. M. Tavallaee, E. Bagheri, Wei Lu, Ali A.Ghorbani. "A Detailed Analysis of the KDD Cup 99 Data Set", http://nsl.cs.unb.ca/NSL-KDD/
52. Adrian Lara, Anisha Kolasani, and Byrav Ramamurthy "Network Innovation using OpenFlow: A Survey "IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION. 1553-877X/13/$31.00 c_ 2013 IEEE.

53. McKeown, Nick, Tom Anderson, HariBalakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. "OpenFlow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review 38, no. 2 (2008): 69-74.

54. Sood, K.; Yu, S.; Xiang, Y. Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A review. IEEE Int. Things J. 2015, 3, 453–463.

55. Zhijing, Q.; Denker, G.; Giannelli, C.; Bellavista, P; Venkatasubramanian, N. A Software Defined Networking Architecture for the Internet-of-Things. In Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–9.

56. Yaser, J.; Al-Ayyoub, M.; Benkhelifa, E.; Vouk, M.; Rindos, A. SDIoT: A software defined based internet of things framework. J. Ambient. Intell. Humaniz. Comput. 2015, 6, 453–461.

57. Liu, J.; Li, Y.; Chen, M.; Dong, W.; Jin, D. Software-defined internet of things for smart urban sensing. IEEE Commun. Mag. 2015, 53, 55–63.

58. Salman, O.; Abdallah, S.; Elhajj, I.H.; Chehab, A.; Kayssi, A. Identity-Based Authentication Scheme for the Internet of Things. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Wroclaw, Poland, 7–9 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1109–1111.

59. Chakrabarty, S.; Engels, D.W.; Thathapudi, S. Black SDN for the Internet of Things. In Proceedings of the 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, Dallas, TX, USA, 19–22 October 2015; IEEE: Piscataway, NJ, USA; pp. 190–198.

60. Theodorou, T.; Violettas, G.; Valsamas, P; Petridou, S.; Mamatas, L. A Multi-Protocol Software-defined Networking Solution for the Internet of Things. IEEE Commun. Mag. 2019, 57, 42–48.

61. Tran, A.K.; Piran, M.; Pham, C. SDN Controller Placement in IoT Networks: An Optimized Submodularity-Based Approach. Sensors 2019, 19, 5474.

62. Molina Zarca, A.; Garcia-Carrillo, D.; Bernal Bernabe, J.; Ortiz, J.; Marin-Perez, R.; Skarmeta, A. Enabling virtual AAA management in SDN-based IoT networks. Sensors 2019, 19, 295.

63. Lu, Y.; Ling, Z.; Zhu, S.; Tang, L. SDTCP: Towards datacenter TCP congestion control with SDN for IoT applications. Sensors 2017, 17, 109.

64. Zhang, A.; Lin, X. Security-Aware and Privacy-Preserving D2D Communications in 5G. IEEE Netw. 2017, 31, 70–77.

65. Ahmed, M.E., Kim, H.: DDoS attack mitigation in Internet of Things using software defined networking. In: 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService) (2017)

66. Li, C., Qin, Z., Novak, E., Li, Q.: Securing SDN infrastructure of IoT-fog networks from MitM attacks. IEEE Internet Things J. 4, 1156–1164 (2017)
67. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor. 2015;17(4):2347-2376.

68. Pohrmen FH, Das RK, KhongbuhW, Saha G. Blockchain-based security aspects in Internet of Things network. In: Advanced Informatics for Computing Research: Second International Conference, ICAICR 2018, Shimla, India, July 14-15, 2018, Revised Selected Papers, Part II. Berlin, Germany: Springer; 2018.

69. Pohrmen FH, Das RK, Saha G. Blockchain-based security aspects in heterogeneous Internet-of-things networks: A survey. Trans Emerging Tel Tech.2019;30:e3741.https://doi.org/10.1002/ett.3741

70. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. Paper presented at: 2017 IEEE International Congress on Big Data (BigData Congress); 2017; Honolulu, HI.

71. Salman O, Elhajj I, Chehab A, Kayssi A. IoT survey: an SDN and fog computing perspective. Computer Networks. 2018;143:221-246.

72. Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of Things: challenges and solutions. 2016. arXiv preprint arXiv:1608.05187.

73. Sharma PK, Singh S, Jeong Y-S, Park JH. DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun Mag. 2017;55(9):78-85.

74. Sharma PK, Chen M-Y, Park JH. A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access. 2018;6:115-124.

11. Tables

Table 4 is not available with this version

Figures
Figure 1

Layers for IoT and its security issues [67].
Figure 2

Overview of the intrusion detection system.
Figure 3

Overview of machine learning approaches.

Figure 4

Recurrent Neural Network [46].
Figure 5

the architecture of ConvNet [47].
Figure 6

SDN architecture [7].
Figure 7

SDN-based intrusion detection system.
Figure 8

SDN-based IoT architecture [69].
Figure 9

SDN-based IoT and Fog architecture [69].

Figure 10

Blockchain architecture [68].
Figure 11

Blockchain-based IoT architecture [69].
Figure 12

Blockchain-based SDN and IoT architecture [69].
Figure 13

Research Areas