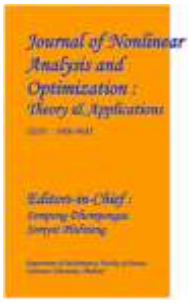
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2 : 2024
ISSN :**1906-9685**



A MULTI-LAYERED DEFENCE STRATEGY AGAINST DDOS ATTACKS

[1]T. RAVI KIRAN KUMAR,[2]A. KAMAL NAYAN ,[3]B. UDAY KIRAN,[4]S. PRANEETH REDDY,[5]K. SHIVA KUMAR

[1]ASSISTANT PROFESSOR, [2,3,4&5] UG STUDENTS

DEPARTMENT OF CSE, MNR COLLEGE OF ENGG. & TECHNOLOGY, MNR NAGAR, FASALWADIGUDA, SANGA REDDY-502294

ABSTRACT

The absence of standards and the diverse nature of the Internet of Things (IoT) have made security and privacy concerns more acute. Attacks such as distributed denial of service (DDoS) are becoming increasingly widespread in IoT, and the need for ways to stop them is growing. The use of newly formed Software-Defined Networking (SDN) significantly lowers the computational burden on IoT network nodes and makes it possible to perform more security measurements. This paper proposes an SDN-based, four module DDoS attack detection and mitigation framework for IoT networks called FMDADM. The proposed FMDADM framework comprises four main modules and five-tier architecture. The first module implements an early detection process based on the average drop rate (ADR) principle using a 32-packet window size. The second module uses a novel double-check mapping function (DCMF), that aids in earlier attack detection at the data plane level. The third module is an ML-based detection application comprising four phases: data preprocessing, feature extraction, training and testing, and classification. This module detects DDoS attacks using only seven features: two selected and five newly computed features. The last module introduces an attack mitigation process.We applied the proposed framework to three test cases: one single-node attack test case and two multi-node attack test cases, all with real IoT traffic generated and deployed in Mininet-IoT. The proposed FMDADM framework efficiently detects DDoS attacks at high and low rates, can discriminate between attack traffic and flash crowds, and protects both local and remote IoT nodes by preventing infection from propagating to the ISP level. The FMDADM outperformed most existing cutting-edge approaches across ten different evaluation criteria. According to the experimental results, FMDADM achieved the following accuracy, precision, F-measure, recall, specificity, negative predictive value, false positive rate, false detection rate, false negative rate, and average detection time benchmarks:- 99.79%, 99.43%, 99.77%, 99.79%, 99.95%, 00.21%, 00.91%, 00.23%, and 2.64 µs, respectively.

1.INTRODUCTION

The diffusion and integration of the Internet of Things (IOT) into several critical industries, including transportation, healthcare, energy, and agriculture, has become undeniable. IOT is a revolutionary technology that links numerous nodes via wireless technologies to automatically send and receive data. The IOT systems have transformed conventional systems into intelligent, economical, and scalable systems. The heterogeneous nature of IOT networks is a major challenge [1]. This is because various IOT applications have distinct network requirements that must be met to operate the system optimally [2]. In addition to the benefits of IOT services, we have recently noticed their negative consequences on network security. According to Sarker et al. [3], IOT nodes may be vulnerable to malware outbreaks that spread surreptitiously among unprotected nodes to form an enormous number of IOT bot nets. An IOT network's nodes are vulnerable to various attacks that attempt to obstruct the services offered by the IOT or control the entire network. Among these attack types, distributed denial of service (DDOS) attacks can be the IOT system's most challenging security risk [4]. When a DDOS attack is launched against an IOT network, the network immediately begins to allocate resources to handle these requests.

https://doi.org/10.36893/JNAO.2024.V15I2.116

Any new requests would be rejected even if they came from a legitimate user, which would prevent the IOT network from providing its services as intended [5]. The most straightforward mitigation strategy is to develop cutting-edge security solutions that safeguard the IOT networks. The main obstacles in deploying any attack detection strategy are the limited power, processing, network bandwidth, and storage capacity resources over different IOT layers [6]. To avoid security breaches, it is critical to protect each layer of the IOT environment. IOT may be attacked at three different layers: he device layer, where data are gathered; the network layer, where data are transported for processing; and the cloud layer, where data are saved [7]. The proposed framework focuses on IOT network layer security. In recent years, a range of technologies, systems, and approaches have been proposed for solving security issues in IOT. Software-defined networking (SDN) and machine learning (ML) technologies have attracted the interest of researchers to address different IOT security concerns [8]. On the one hand, a new technique known as ‘‘State ful SDN’’ has expanded the basic functions of Open Flow, the most widely used protocol for communication between data and control planes [9], by adding the ability to apply multiple match-action rules depending on the distinct states detected in the switch’s SDN flow tables [10], [11], [12]. This feature gives the switch the ability to respond to events at the packet level. The switch can take appropriate action if the results of the packet analysis agree with the switch rules listed in the flow tables [13].Meanwhile, academics have developed many ML-based approaches and strategies for identifying DDOS attacks in SD-IOT. ML-based approaches have yielded good results in detecting DDOS attacks in SD-IOT networks [14]. Building a learned parameter model used to accurately forecast attacks requires training the system on both normal and attack behaviors. A substantial amount of data is produced by an IOT network. Choosing the most pertinent features of a dataset for model training and testing remains a challenging task. Using a large number of features in ML models increases both the cost and time complexity [15]. However, the inclusion of unrelated features renders the model less effective in detecting attacks. The construction of an effective ML-based DDOS detection model depends on the packet feature engineering approach, which is crucial [16], [17]. Considering these factors, we propose a new framework called FMDADM, which comprises four phases: data preprocessing, feature extraction, training and testing, and classification. The proposed FMDADM uses only five new computed features to detect an attack. By using fewer features, attacks can be detected more quickly. A variety of ML models for traffic classification, including Support Vector Machine (SVM), k-Nearest Neighbor (KNN), Gaussian Naive Bayes (GNB), Binomial Logistic Regression (BLR), Decision Tree (DT), and Random Forest (RF) classifiers, are used to construct the proposed detection model.

2.LITERATURE REVIEW

1. **FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks Walid I. Khedr, Ameer E. Gouda, Ehab R. Mohamed Published in IEEE Access 2023** The absence of standards and the diverse nature of the Internet of Things (IoT) have made security and privacy concerns more acute. Attacks such as distributed denial of service (DDoS) are becoming increasingly widespread in IoT, and the need for ways to stop them is growing. The use of newly formed Software-Defined Networking (SDN) significantly lowers the computational burden on IoT network nodes and makes it possible to perform more security measurements. This paper proposes an SDN-based, four-module DDoS attack detection and mitigation framework for IoT networks called FMDADM. The proposed FMDADM framework comprises four main modules and five-tier architecture. The first module implements an early detection process based on the average drop rate (ADR) principle using a 32-packet window size. The second module uses a novel double-check mapping function (DCMF), that aids in earlier attack detection at the data plane level. The third module is an ML-based detection application comprising four phases: data preprocessing, feature extraction, training and testing, and classification. This module detects DDoS attacks using only seven features: two selected and five newly computed features. The last module introduces an attack mitigation process.

We applied the proposed framework to three test cases: one single-node attack test case and two multi-node attack test cases, all with real IoT traffic generated and deployed in Mininet-IoT. The proposed FMDADM framework efficiently detects DDoS attacks at high and low rates, can discriminate between attack traffic and flash crowds, and protects both local and remote IoT nodes by preventing infection from propagating to the ISP level. The FMDADM outperformed most existing cutting-edge approaches across ten different evaluation criteria. According to the experimental results, FMDADM achieved the following accuracy, precision, F-measure, recall, specificity, negative predictive value, false positive rate, false detection rate, false negative rate, and average detection time benchmarks:- 99.79%, 99.43%, 99.77%, 99.79%, 99.95%, 00.21%, 00.91%, 00.23%, and $2.64 \mu \text{s}$, respectively.

2. **DDoS Attack Detection System Using Semi-supervised Machine Learning in SDNM. Etman Published 2018** Distributed Denial of Service (DDoS) attacks is one of the most dangerous cyber-attack to Software Defined Networks (SDN). It works by sending a large volume of fake network traffic from multiple sources in order to consume the network resources. Among various DDoS attacks, TCP SYN flooding attack is one of the most popular DDoS attacks. In this attack, the attacker sends large amounts of half-open TCP connections on the targeted server in order to exhaust its resources and make it unavailable. SDN architecture separates the control plane and data plane. This separation makes it easier to the controller to program and manage the entire network from single device to make better decisions than when the control is distributed among all the switches. These features will be utilized in this thesis to implement our detection system. Researchers have proposed many solutions to better utilize SDN to detect DDoS attacks, however, it is still a very challenging problem for quick and precise detection of this kind of attacks. In this thesis, we introduce a novel DDoS detection system based on semi-supervised algorithm with Logistic Regression classifier. The algorithm is implemented as a software module on POX SDN controller. We have conducted various test scenarios, comparing it with the traditional approach in the literature. The approach presented in this thesis manages to have a better attack detection rate with a lower reaction time.
3. **Watching Smartly from the Bottom: Intrusion Detection revamped through Programmable Networks and Artificial Intelligence S. Guti'errez, J. Branch, +1 author J. F. Botero Published in arXiv.org 1 June 2021** The advent of Programmable Data Planes represents an outstanding evolution and complete revolution of the Software- Defined Networking paradigm. The capacity to define the entire behavior of forwarding devices by controlling the packet parsing procedures and executing custom operations enables offloading functionalities traditionally performed at the control plane. A recent research line has explored the possibility of even offloading to the data plane part of Artificial Intelligence algorithms, and more specifically, Machine Learning ones, to increase their accuracy and responsiveness (by having more detailed visibility of the traffic). This introduces a significant opportunity for evolution in the critical field of Intrusion Detection. However, offloading functionalities to the data plane is not a straightforward task. In this paper, we discuss how Programmable Data Planes might complement different stages of an Intrusion Detection System based on Machine Learning. We present two use cases that make evident the feasibility of this approach and highlight aspects that must be considered when addressing the challenge of deploying solutions leveraging data-plane functionalities.
4. **Detecting Multi-Step Attacks: A Modular Approach for Programmable Data Plane Abir Laraba, J. François, +2 authors R. Boutaba Published in IEEE/IFIP Network Operations… 25 April 2022**

The increasing sophistication of attacks over the last years such as the proliferation of complex multi-steps attacks, calls for new monitoring models and methods for diagnosing the attacks' severity and mitigating them in a timely manner. In this paper, we propose an in-network monitoring approach capable of detecting a set of composed behaviors and consequently triggering different levels of alerts and reactions. Our approach is based on a Petri Net model capable of aggregating individual attacks into a multi-step composition. To this end, we propose a method for deriving a Match-Action Table (MAT) abstraction from a Petri net model. MATs can be then deployed on a P4 programmable data plane, enabling flexible re-composition of attack detection steps at runtime. We demonstrate the feasibility of our proposal by modeling the detection of a multi-step DNS cache poisoning attack and implementing the model on a P4 programmable data plane.

5. **An Intelligent Cloud Data Protection Technique Based on Multi Agent System Using Advanced Cryptographic Algorithms Mohammed Amine Yagoub, A. Laouid, +1 author M. Alshaikh Published in International Conference on… 1 July 2019** In last decade, cloud computing has been envisioned as the next generation architecture of Information Technology (IT). This advent motivates the data owners to outsource their complex systems from local sites to the cloud for great flexibility and economic savings. However, the protected data should to be encrypted before outsourcing. The main objective of this paper is to implement properly this approach. The solution must provide an encryption scheme such that the user may maintain some functions such as arithmetic operations, research, update requests and preserving order, i.e., the homomorphism, on the encrypted cloud data. Moreover, even if another tenant can access to the stored data, all the stored data will appear is gibberish to the unknown users. We look to propose a strong solution that combines obfuscation technique for securing user interface, hybrid encryption algorithms for securing transport, communication operations and fully homomorphic encryption approach for securing storage operations. Then, this work is a new security architecture based on multi-agent system for cloud computing communications and storage environment that considers the intelligent various security gaps as much as possible.

3.SYSTEM ANALYSIS

3.1. EXISTING SYSTEM

Recently, relevant AI-based studies have been presented for DDoS attack detection in Software-Defined IoT (SD-IoT) networks, where SDN was used to improve the security aspects of IoT networks. A DDoS detection solution for an SDN-based IoT network, called LEDEM, was suggested in [18]. The main issue with this model is its lack of adaptability, as LEDEM uses only one classification method and is incapable of dealing with various types of DDoS attacks. Yin et al. [19] proposed a broad architecture for the SDIoT. The proposed SD-IoT architecture analyzes IoT network traffic and detects DDoS attacks based on the network attributes. The SD-IoT is further constrained by insufficient ML-based categorization algorithms. Xie et al. [20] employed traffic-flow patterns to identify DDoS attacks. This solution shows efficient DDoS information detection with a comparably low overhead compared with other approaches. However, this solution falls short when dealing with heavy network traffic, necessitating the implementation of a more sophisticated security solution. In [21], a new SVM-based security mechanism for IoT networks was proposed. Their model uses learning algorithms for both observing and reacting agents. Their proposed method achieved a general accuracy rate of 99.71% for anomaly identification. The authors of [22] suggested a feed-forward neural network model for attack detection in IIoT networks. The proposed model performed well in terms of accuracy; however, the dataset was not designed for the IIoT domain. Ullah and Mahmoud [23] developed a new anomaly-based detection system for IoT networks. They devised a multiclass classification technique using a convolutional neural network (CNN) algorithm. This classification technique was admirably performed. However, ML approaches are preferred in intrusion detection systems (IDSs) for implementing highly secure capabilities [24]. The

authors of [24] examined several ML models to conduct both binary and multiclass classification. They concluded that, compared with other classifiers, the XGBoost technique produced higher performance outcomes. Another CNN-based DDoS attack detection system for IoT networks, which restricts attacks at the source end, was proposed by the authors of [25]. They evaluated the proposed CNN using the freely accessible dataset CIC-DDoS2019 [26]. Two test cases were used to obtain the performance results; however, this dataset was insufficient for analyzing the behavior of IoT network traffic. Using a recurrent neural network (RNN),Yousuf and Mir [27] proposed an algorithm called DALCNN. DALCNN employs OpenDayLight (ODL) as a suitable SDN controller to address the problem of identifying DDoS attacks in IoT. The gap in DALCNN is that the RNN algorithm was trained using the NSL-KDD dataset, which is unfortunately inadequate for IoT network traffic characteristics. Another detection mechanism for abnormalities in IoT environments was proposed by Alanazi and Aljuhani [28]. The proposed mechanism uses several ML techniques for feature selection and an ensemble learning approach for traffic classification. Numerous constraints were considered in this study. For instance, detection accuracy may be affected by employing custom datasets instead of real-time IIoT traffic. Another problem is that obsolete datasets are restricted to particular types of cyber attacks and cannot recognize contemporary attack scenarios. Another RNN-based deep learning solution termed ‘‘Deep Defense’’ was proposed by Yuan et al. [29] for detecting DDoS attacks in IoT. This solution employs a series of consecutive network packets to extract low-level features to discriminate between normal and attack packets. However, the authors still need to test their model under numerous realtime scenarios.ADeep Neural Network (DNN) approachwas proposed in [30] to identify DDoS attack in SDN scenarios. The tests results show that the Deep IDS system is a workable solution with a low network load. The proposed approach does not affect the functionality of the POX controller. Furthermore, the authors needed to improve the model to obtain better detection rates with low false alarm rates across multiple OpenFlow Controllers. Zhang et al. [31] presented a technique for detecting low rate (LR) DoS attacks based on the Power Spectral Density (PSD). In [31], an SVM model was used to extract features from the KDD99 dataset.

Disadvantages:

- The system never proposes a new double-check mapping function called DCMF, which is used to provide early attack detection at the switch level.
- An existing system has the following problems 1) missing values replacement, 2) encoding categorical data, and 3) feature scaling.

3.2. PROPOSED SYSTEM

The proposed framework consisted of four modules: three detection modules and one mitigation module. The first module uses a small window size of 32 packets. This window size was then employed in the third detection module to achieve an earlier and more efficient attack detection. The second detection module presents a new mapping function to help detect DDoS attacks at the data plane level. The third module provides an ML-based detection application that is implemented and deployed at the controller level. The last module is a mitigation technique that operates at both switch and controller levels. Most related research uses a conventional, stateless approach to design detection and mitigation processes. The switch scans its flow table to match the incoming packets. If no match was found, the packets were treated as new and routed to the controller for processing. However, this approach lacks scalability and efficiency. In this paper, we make use of the aforementioned ‘‘Stateful SDN,’’ where the switches are given stateful packet analysis privileges by the SDN network. Therefore, when new packets arrive at the network, the switch considers the packets that have already been received in addition to the new packet features.

ADVANTAGES:

1. The proposed FMDADM framework employs feature engineering to identify DDoS attacks using only five new computed features. The model can successfully overcome the over-fitting problem and provides a good fit as a result.
2. The second detection module, which uses a novel proposed mapping function called DCMF, provides two crucial features:- (a) detecting the attack at the data plane level before overwhelming the controller, and (b) discriminating between attack traffic and flash crowds. As a result, the controller has an extra layer of protection against the attack.
3. A small 32-packet window size is used for feature extraction in the third detection module. The three

detection modules resulted in a reduction in the amount of time needed for training, testing, and detection.

4. FMDADM effectively detects DDoS in multi-node attack scenarios. This is a crucial area of strength for the proposed framework because it is generally known that conventional defenses fall short in the face of these attack scenarios.

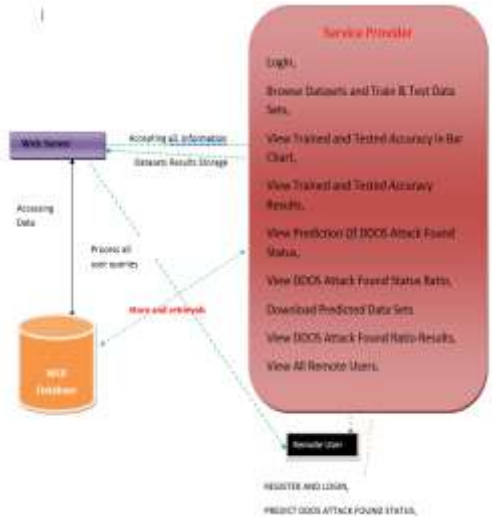
5. FMDADMprotects both local and remote IoT nodes by preventing infections from spreading to the ISP level. By protecting the controller and remote nodes in this form, we can stop DDoS attacks before they reach the Internet.

6. FMDADM uses actual IoT traffic features to build the detection model. Most literature-based studies deal with either simulated traffic or network traffic that is not extracted from actual IoT networks.

7. According to the experimental results, FMDADM outperformed most of the existing cutting-edge approaches across ten different evaluation criteria.

4.IMPLEMENTATION

4.1. SYSTEMARCHITECTURE



4.2. MODULES

- **Service Provider**

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Browse Datasets and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of DDOS Attack Found Status, View DDOS Attack Found Status Ratio, Download Predicted Data Sets View DDOS Attack Found Ratio Results, View All Remote Users.

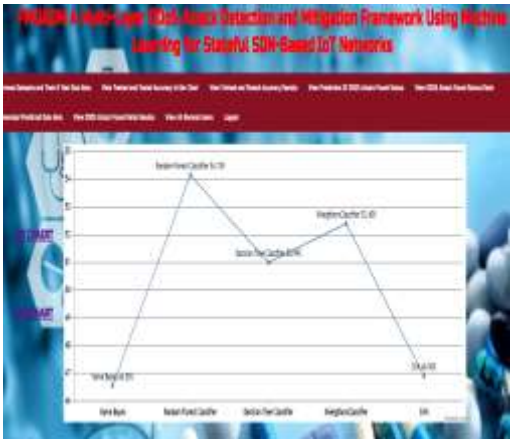
- **View and Authorize Users**

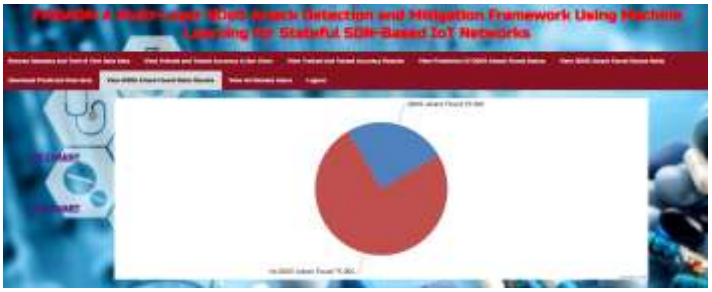
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

- **Remote User**

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT DDOS ATTACK FOUND STATUS, VIEW YOUR PROFILE.

5.RESULTS





CONCLUSION

In this paper, we introduced FMDADM, an ML-based DDOS detection, and mitigation framework for SDN-enabled IOT networks. The proposed framework comprises three detection modules and a mitigation module. The first module employs a 32-

packet window size used for feature extraction in the third detection module. The second detection module introduces a novel mapping function called DCMF. The DCMF provides two crucial features:- (a) detecting the attack at the data plane level before overwhelming the controller, and (b) discriminating between attack traffic and flash crowds. As a result, the controller has an extra layer of protection against the attack. The third detection module employs feature engineering to identify DDOS attacks using only five new computed features. As a result, the model gives a good fit and can successfully handle the over-fitting problem. The three detection modules resulted in a reduction in the amount of time needed for training, testing, and detection.We thoroughly tested the proposed framework by employing trained BLR, GNB, SVM, KNN, DT, and RF models to assess their performance outcomes and select the best model. The RF model performed best across all ten evaluation metrics. Three different test scenarios were used to evaluate the performance of the proposed framework. According to the experiments, the FMDADM can detect DDOS with high accuracy in multi-node attack scenarios. This is a crucial area of strength for the proposed framework because it is generally known that conventional defences fall short in the face of these attack scenarios. The proposed framework is designed to prevent local DDOS attacks produced by IOT Bot nets inside compromised LANs from propagating to the ISP level. By protecting the controller and remote nodes in this form, we can stop DDOS attacks before they can reach the Internet. The proposed FMDADM framework can effectively identify DDOS attacks at both high and low ratesThe experimental results show that the proposed framework performed better than most cutting-edge solutions currently available with the following benchmarks for accuracy, precision, F-measure, recall, specificity, negative predictive value, false positive rate, false detection rate, false negative rate, and average detection time: 99.79%, 99.09%, 99.43%, 99.77%, 99.79%, 99.95%, 00.21%, 00.91%, 00.23%, and 2.64 µs. In the future, we plan to deploy and evaluate the proposed framework in a multi-controller SD-IOT environment. Additionally, we plan to test the proposed framework with other controllers to determine which one works best for the IOT network. In addition, we will test increasingly sophisticated test scenarios. Finally, the detection of more attack types on an SDN-based IoT network may be added to this study.

REFERENCES

[1] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, W. H. Alshoura, and H. Arshad, ‘‘The Internet of Things security: A survey encompassing unexplored areas and new insights,’’ *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102494, doi: 10.1016/j.cose.2021.102494.

[2] R. Ahmad and I. Alsmadi, ‘‘Machine learning approaches to IoT security: A systematic literature review,’’ *Internet Things*, vol. 14, Jun. 2021, Art. no. 100365, doi: 10.1016/j.iot.2021.100365.

[3] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, ‘‘Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions,’’ *Mobile Netw. Appl.*, pp. 1–17, Mar. 2022, doi: 10.1007/s11036-022-01937-3.

[4] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, ‘‘Federated-learning-based anomaly detection for IoT security attacks,’’ *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2545–2554, Feb. 2022, doi: 10.1109/JIOT.2021.3077803.

[5] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, ‘‘Internet of Things security: Challenges and key issues,’’ *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Sep. 2021, doi: 10.1155/2021/5533843.

[6] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, ‘‘A survey on federated learning for resource-constrained IoT devices,’’ *IEEE Internet Things J.*, vol. 9, no. 1, pp. 1–24, Jan. 2022, doi: 10.1109/JIOT.2021.3095077.

[7] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, ‘‘Smart home security: Challenges, issues and solutions at different IoT layers,’’ *J. Supercomput.*, vol. 77, no. 12, pp. 14053–14089, Dec. 2021, doi: 10.1007/s11227-021-03825-1.

[8] S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba, D. Draheim, and S. Dustdar, ‘‘Towards software-defined networkingbased IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects,’’ *IEEE Access*, vol. 10, pp. 70850–70901, 2022, doi: 10.1109/ACCESS.2022.3188311.

[9] B. Isyaku, K. B. A. Bakar, F. A. Ghaleb, and A. Al-Nahari, ‘‘Dynamic routing and failure recovery

approaches for efficient resource utilization in OpenFlow-SDN: A survey,'' *IEEE Access*, vol. 10, pp. 121791–121815, 2022, doi: 10.1109/ACCESS.2022.3222849.

[10] X. Zhang, L. Cui, K. Wei, F. P. Tso, Y. Ji, and W. Jia, ''A survey on stateful data plane in software defined networks,'' *Comput. Netw.*, vol. 184, Jan. 2021, Art. no. 107597, doi: 10.1016/j.comnet.2020.107597.