ORIGINAL ARTICLE
Journal Section

A Comprehensive Survey on Secure Software defined Network for the Internet of Things

Monzir Babiker Mohamed[1] | Olasunkanmi Matthew Alofe [1] | Muhammad Ajmal Azad[1] | Harjinder Singh Lallie[2] | Kaniz Fatema[3] | Tahir Sharif[4]

[1]Discipline of Computer Science and Electronics, University of Derby

[2]Department of Computer Science, Aston University, Birmingham

[3]Faculty of Engineering, University of Derby

[4]WMG, University of Warwick, Coventry

Correspondence
Discipline of Computer Science and Electronics, University of Derby
Email: m.azad@derby.ac.uk

Funding information

The Internet of Things (IoT) is the network of smart devices, humans, and machines that continuously monitored the surrounding environment and execute meaningful decisions on the data or information they received. The Internet-enabled devices could facilitate computer-mediated strategies for various tasks e.g., smart healthcare, managing the cities or smart factories, smart manufacturing, automating the home and business, etc. IoT commonly uses the Internet technology for establishing communication among devices, thus inherits all the security threat that are currently affecting the Internet users along with security threat due to resources constrained nature of the smart devices. The greater footprint, the distributed nature of the network and the existence of a huge number of IoT devices has also attracted criminals, fraudsters and attackers to utilize this medium for spreading malicious content or making the devices unavailable for legitimate use. It is imperative to ensure that the Confidentiality, Integrity, Security, and Privacy of information and users remains intact while using these devices. Software-defined Networks (SDN) and Network

[*] Equally contributing authors.

Function are the way to control and configure devices from a central location and have been proven to offer scalability and versatility to their deployed systems. In this paper, we systematically reviewed the adoption of Software Defined Network (SDN) and Network Function Virtualization (NFV) in protecting the IoT network. To this extent, we provide a comprehensive survey on security solutions based on SDN, Blockchain, NFV and SDN/NFV IoT security mechanisms. We have also identified Open challenges in this domain which includes lack of standardisation, low cost and effective machine learning systems for identifying malicious traffic, and large attack surface. The deployed technologies exhibit positive strides in their usage for the provision of security in IoT environments offering security enhancements, scalability, and versatility.

KEYWORDS
IoT, Software Defined Network, Network Virtualization, IoT security

1 | INTRODUCTION

The influence of IoT in our daily lives has continually grown and expanded enormously into several aspects of our daily lives. The forecasted growth of connected devices has been 20 billion by 2020 and is expected to bolster a further 400,000 by 2022 [1, 2] with a further estimation due to reach 50 billion by 2030 [3]. The integration of these devices estimated in the expansion requires reliable methods to dynamically integrate the heterogeneous nature of the devices and the variation in the capability of the devices. Figure 1 presents the application areas of IoT in today's connected smart environment. The IoT environment compared with the traditional information technology environment is considered complex with regards to providing security and challenges encountered due to limitations within the environment [1, 2, 4]. The surge of IoT devices, the open nature of interconnection, and the lack of security policies have also attracted cyber attackers to use these devices for launching the cyberattack. It is estimated that currently more than 25% of identified attacks in enterprises involve the IoT devices which see a surge with the increase in the number of devices. For example, Mirai botnet [5] utilizes the common and simple trick i.e. scanning the devices [6] for default login name and password, and then launching Distributed Denial of Service attack (DDoS) by creating the botnet army of IoT device [5].

Standards for IoT architecture have not been clearly defined, however, researchers have classified them into three major layers: perception, network, and application layers [7, 8, 9], others have added an extra layer: data processing layers [2, 10, 11, 12]. Each layer is accompanied by several threats and vulnerabilities that undermine the efficiency of traditional security mechanisms [13, 14, 15]. The limitation of resources and capabilities of the devices within the environment plays a crucial part in foiling the extent to which traditional security mechanisms can work within the continuously changing and diverse environment. To provide security within the environment while considering the limitations of the devices, dynamic and customized security solutions are proposed for securing the low constrained interconnected devices [16, 17, 18, 19, 20].

The expanding nature of the IoT environment makes traditional security network architecture not suitable for handling attacks and threats directed at the IoT environment [21, 22] thus leading to the proposal of specialized security mechanisms such as based in emerging technologies such as SDN, NFV and Blockchain [23]. SDN deals with decoupling the network into two planes for managing the network and this makes a viable to become a flexible solution to cope with the security requirements of the IoT environment. These planes are control planes which is responsible for network logic, and the data planes which is responsible for network function. SDN provides robust control and traffic monitoring within the network and is potentially able to isolate IoT devices when malicious activities are discovered, identified, and handled by the device and network [24]. Network Functions Virtualization (NFV) like SDN decouples network functions, however proprietary hardware appliances are used as software in virtual machines (VMs). The combination of both mechanisms improves the network capability of the environment and provides innovative security mechanisms suitable for IoT environments such as rules for data availability, authentication, confidentiality, data security and authorization [4], [25].

This paper is based on an integrative research review methodology that highlights key issues, the current state of the mechanism, and the review of outcomes obtained from the mechanisms. In this paper, we provide a comprehensive analysis of the security aspect of IoT networks and the use of SDN/NFV-based systems to ensures the security of resource-constrained heterogeneous IoT networks. To this extent, we first provide a comprehensive discussion of the type of security threats the IoT devices are facing in today's interconnected environment and identify some core challenges towards ensuring the security and privacy of these devices. We provide detailed analysis on various security threats such as encryption for resource-constrained devices, access control mechanism for distributed and action-dependent devices, Intrusion and anomaly detection system for highly distributed and huge networks, and authentication challenges in these networks. We then focus on providing the detailed analysis of the SDN and NFV based solution that has been proposed for securing the IoT networks. To this extent, we identified a comprehensive set of features that we used to analyse the different aspects of SDN and NFV based solutions. This assessment inspires the development of new perceptions rather than symmetrical and semi-symmetrical approaches used for detailing the effects among several studies. The major contribution of this paper is:

- Review of present security requirements and challenges encountered for implementation of reliable security mechanisms for IoT devices and environments.
- Review of SDN and NFV technologies that provide security solutions in the IoT environment.
- Discuss the challenges, existing gaps and highlight future research directions regarding using SDN and/or NFV based IoT security mechanisms.

The rest of this paper is structured as follows. Section 2 reviews different challenges of IoT environment.Section 3 discuss the related work.Section 4 presents the research methodology used in this paper. Section 5 discuss the security solutions of SDN and section 6 discuss NVF security solution and section 7 provides discussion on heterogeneous SND and NVF based solution for securing IoT network. Section 8 presents analysis from the review. Section 9 presents challenges encountered by the SDN/NFV based IoT security mechanisms, and concluding remarks are drawn in Section 10.

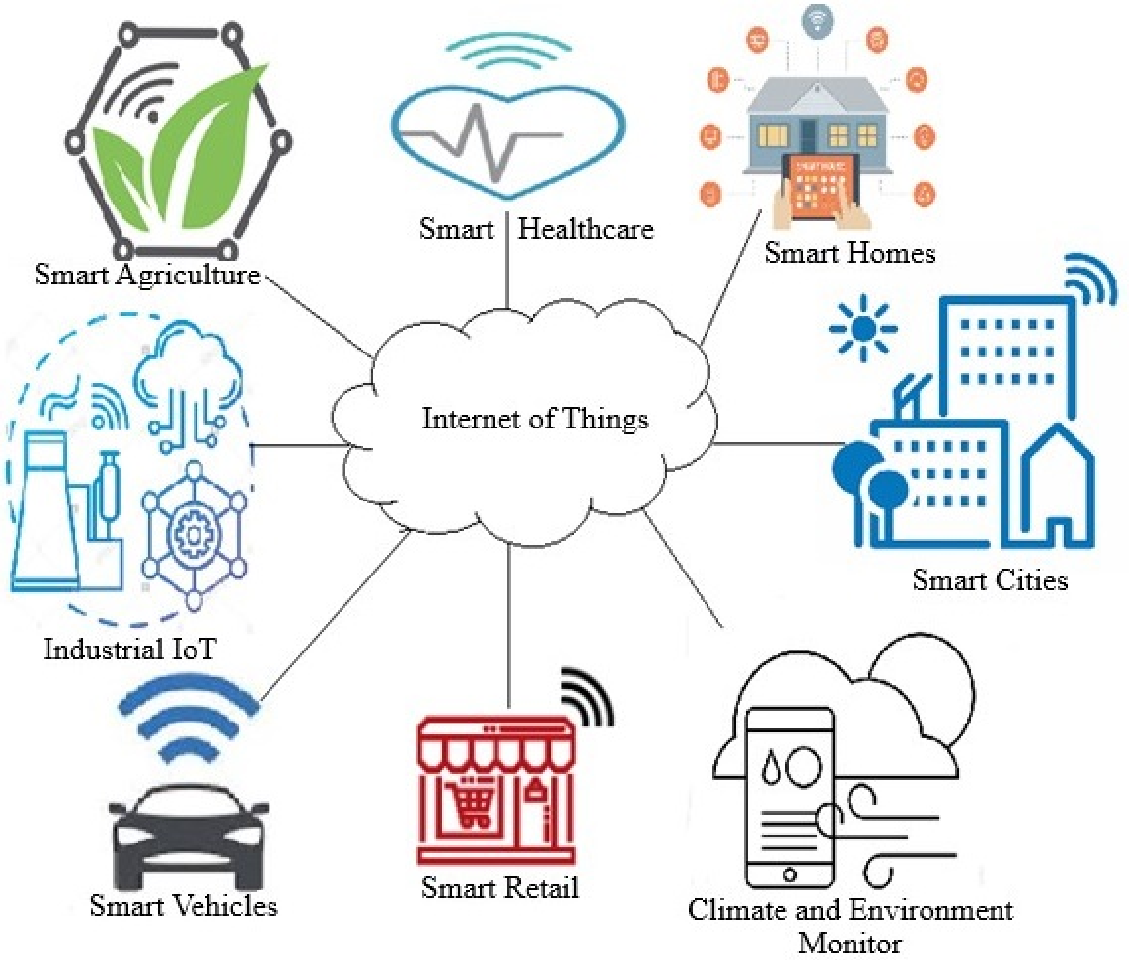

FIGURE 1 Application areas of Internet of Things

2 | SECURITY CHALLENGES IN IOT ENVIRONMENT

The consistent improvement provided by IoT in the daily lives of individuals cannot be over-emphasized, yet, in return, it creates a vulnerability that can adversely affect the security and privacy of users. Traditional hardware safety solutions have been reviewed [26, 27, 28] for providing security and privacy protection for IoT devices and have come short in various aspects. The shortcoming of the traditional system-specific security solutions can be attributed to the capabilities of resource-constrained IoT devices. The traditional hardware-based security solutions are not effective in providing security and privacy protection in the resource-constrained IoT devices, thus it became imperative to deploy intelligent solutions in the form of software-based secure solutions that are not dependent on the processing capabilities of resource-constrained devices in order to protect IoT devices from the external and internal cyber-attacks [29]. This allows deploying Software-defined and Virtualized systems, emerging blockchain technology as the proposed decentralized systems, use of lightweight artificial intelligence, and machine learning to enhance protection while trying to prevent the overloading of the limited resources available on the IoT devices in the dynamic environment. The main issue attributed to the shortcoming of the traditional hardware-based solutions in protecting devices in an IoT environment has been the limited resources of the devices and the dynamic nature of the network. The limited resources which could be limited power and processing capability, memory, communication bandwidth, energy requirements are the result of the small size of the IoT devices [16, 17].

Various security challenges arise from the limitations of device resources within the environment. The challenges encountered include:

- **Energy and processing Limitation** - Batteries are the main power source of most IoT devices. Based on that, the computational and processing power of the devices has been made minimal while well-known security mechanisms and encryption mechanisms require high computational power, processing capabilities and memory to function properly [30]. A suitable security mechanism and encryption algorithm is required that must be suitable to function efficiently within the limitations of the IoT devices [31] thus requires a lightweight cryptosystem, Intrusion detection and analysis system that has been designed in accordance with the capabilities of the resource-constrained devices [32, 33, 34].
- **Memory restrictions:** Buffer overflow is a common form of attack that attempts to overrun the buffer boundaries [35] while processing buffers where data is stored. The attack is a result of the lack of proper inspection of buffers that store data [36]. IoT devices are designed to run on lightweight versions of operating systems empowered with restricted both flash and Random-Access Memory (RAM) memory capacity. Traditional security mechanisms demand high memory capacity which cannot be powered by the memory capability of IoT devices [30].
- **Heterogeneous Dynamic Environment:** IoT environments are combinations of different devices with diverse capabilities, capacities, and specifications. The environment deals with various options of operating systems, communication approaches, and transmission protocols [37, 38, 39]. The use of customized and versatile security solutions is vital to coping with the requirements for providing adequate security for the environment [40].
- **Technical and Big Data Concerns:** IoT devices continually generate data that are amassed to an enormous amount of data [41, 42, 43]. These data points require proper handling for storage, analysis, and safeguard. Handling of data within an IoT environment is of great concern as well as differentiating and verifying legitimate devices within the environment [44].
- **Lack of software patches and updates:** The concept of patching is to solve discovered issues and bugs that are identified in the running firmware, improve the current configuration and offer new services [45, 46, 47], providing solutions against newly discovered vulnerabilities in the system. The patch protects against new threats that arise from exploitable vulnerabilities that are discovered in currently running operating systems and software. The development of specialized mechanisms to consume low computational and processing resources is required to provide an efficient update and patch vulnerability [48].
- **End-to-End Security:** The protection of transmitted data between devices in an IoT environment to prevent interceptions or alteration to achieve end-to-end protection is very important for IoT devices and their users [49, 50, 51, 52]. The heterogeneity of the environment accounts for the differences in the ability and capability of devices; protocol sets, communication methods, and standards deployed in the environment. The provision of End-to-End security within the environment requires mechanisms that fit the variation of devices capabilities, communication technologies in the IoT environments [53, 54, 55].
- **User Awareness:** In the chain of security, the human factor is regarded as the most vulnerable aspect of security [56, 57, 58, 59]. The security of any system would be undermined if the security is not properly managed. Common mismanagement of system security includes default or low strength passwords, poor or misconfiguration of devices within the environment. The most common attack directed in this direction is the social engineering

attack. User awareness is required to prevent this form of attack as it aims at obtaining confidential information within the system exploiting the human factor within the system [31], [60].

To counter these challenges posed by the limitations of the devices, certain requirements should be fulfilled in ensuring the efficient security of an IoT environment. These requirements include:

- **Privacy:** Personal data identified by the Data privacy regulations (the General Data Protection Regulation (GDPR) or US data privacy Law) is any information that can be associated to recognize individual personal attributes. The users must know how their data is processed, who has access to their data, for what purpose their data is being collected, where their data is being processed within a particular jurisdiction or outside of particular jurisdiction, and request rights over their data. The guidelines as stated by European GDPR must be obeyed and sufficient protection must be provided to ensure the privacy of users while handling personal information. The IoT environment amasses a large amount of data about users and devices within the environment, which raises concerns about privacy within the environment. Tracking and profiling of information are the major compromises that occur which undermines privacy within the environment and the introduction of a compromised device into such an environment exposes valuable information that violates privacy [61].
- **Integrity:** This involves the assurance that the transmitted data within the environment is authentic and has not been modified [62, 63]. IoT devices are prone to several attacks either remotely or locally due to the widespread use of nodes that could be easily accessed by adversaries. If the adversaries successfully compromise a node, various components can be altered such as intended functions of the device, output product of device, and transmitted data within the environment. The environment must implement a proper means for the authentication and guarantee the integrity of devices and data transmitted within the environment and deter the transmission of data with compromised devices within the environment [64].
- **Network Security:** An IoT environment consists of a variety of connected devices that communicates with several communication technologies and standards [65, 66]. The environment exchanges an enormous amount of information at various layers of communication and the information is distributed between various device components which increases traffic within the environment [67]. The protection of the massive amount of data transmitted must be guaranteed against jamming and interception to ensure the service efficiency of the environment [68].
- **Authentication, Authorization, and Accounting:** Authentication involve the process of verifying users within the environment, authorization is the privileged access granted to users to specified assets within the environment while accounting serves to monitor and audit the environment [69, 70, 71, 72]. It is crucial to ensure a reliable means to provide authentication, authorization, and accounting for legitimate users to ensure the exact level of access is granted to resources [73].
- **Safety and Precautions:** The size and application areas covered by the sensors and actuators make the IoT devices easily accessible to adversaries. Identification of compromised devices in the environment is imperative based on the damage that could occur from the presence of such devices in the environment [68]. Ensuring the intended function of devices and transmitted data are unaltered is important and if altered, it is discovered before irreparable damage is done to the environment [74].
- **Attack Scenarios:** The IoT environment consists of different kinds of sensors, devices, and actuators communicating at different levels that are deployed in wider areas and across many systems that present an increased attack surface to the environment. Various attacks occur at different layers of the IoT such as hardware trojan [75], node capture [76], and battery draining attacks [77], [78] that occur at the perception layer; sniffing and eavesdropping attack [64], Denial of Service [79] and man-in-the-middle attack [80] that occurs at the network layer;

Malicious scripts [81], phishing attacks [82] and Distributed Denial of Service [83] that occurs at the application layer. Countermeasures have been implemented in attempts to mitigate challenges faced by the IoT environment with consideration based on different requirements that should be fulfilled. Some of the countermeasures include:

- **Side-channel Attacks:** Side-channel signals carry along with important details in regards to the operation of IoT devices and it allows for the discovery of irregular activities [84, 85, 86]. Malicious firmware and alteration of devices and data can be detected with this analysis providing insights and protection against side-channel attacks and many integrity-related attacks [75].
- **Transport layer security:** To provide end to end protection for communication within an IoT environment, the use of Secure Socket Layer (SSL) and Transport Layer Security (TLS) has been explored [87, 88, 89]. This helps maintain the integrity of data within the environment and provide network security for the environment. Based on the variations in the communication standards and technologies in the IoT environment, TLS is suitable to handle communication that runs on Transmission Control Protocol (TCP) and Datagram Transport Layer Security (DTLS) handles communication on User Datagram Protocol (UDP) [90]. A lighter version of these layer security has been proposed to offer end-to-end security that is efficient with the limited capabilities of the devices within the environment [91].
- **Intrusion Detection Systems:** There are various modes of operation employed by IDS. The most common in IoT environments are anomaly-based detection systems [92, 93, 94, 95] that compare the current behaviour of the environment against a benchmark score and signature-based detection that analyses traffic to match a specific pre-defined signature to determine the state of the traffic [75]. IDS works to enhance security by detecting intrusions into the environment and notifying the required authorities about the intrusions and added features can be used to deter node capture attacks [90],[96].
- **Best Practices:** The simplest and effective measure against the majority of attacks is the implementation of best practices within the environment such as changing of default credentials on new devices incorporated into the environment and raising awareness among users about best practices to implement [30, 60, 97, 98, 99].
- **Authorization control methods:** Access control list (ACL) contributes hugely in achieving authentication, authorisation, and accounting in the IoT environment. Security policies are usually deployed that filter traffic, permitting or blocking access based on specified rules in the policy [100, 101, 60]. The most commonly used access controls for these environments are Role-Based Access Control (RBAC) that assigns access based on the role of the user and Access Based Access Control (ABAC) that assign access based on the precise attributes assigned to the object [90, 102, 103].

3 | RELATED WORK

Several studies had been conducted about IoT security, with limited focus placed on SDN-based security solutions. This chapter provides a review of classic and emerging IoT security solutions exploring the studies been done to enhance the security of the IoT environment. Alaba et al. [80], explored the identification of current vulnerabilities and threats confronting IoT environments. Then a classification-based security system based on three categories namely application, perception, and communication were introduced. The potential attacks facing these categories were discussed without review of the detection methods of those attacks or covering the use of NFV and emerging solutions such as machine learning and Blockchain [80]. A holistic review of IoT security solutions discussing current security solutions and implementation was done by Kouicem et al. [104], categorising IoT security solutions into two groups namely Classic and emerging solutions. The survey provided a good classic IoT security review yet did

Paper	Attack Detection	SDN	NFV	Securing SDN/NFV	IoT Attacks	Authentication	Access Control	Encryption	Blockchain	ML	Security Countermeasures	Year
[2]	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	2019
[105]	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗	✓	2018
[104]	✓	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	2018
[80]	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✓	2017
[82]	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	2017
[106]	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	2017
Our paper	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2021

TABLE 1 Comparison between the main security aspects and features in the related work

not cover the deployment of emerging concepts such as machine learning, NFV, and SDN in IoT security solutions [104]. The survey on IoT security conducted by Hassija et al. [2] highlighted the threats within IoT layers and different IoT applications including their privacy dilemmas. However, IoT security countermeasures were reviewed with the concentration directed towards Blockchain, edge, and fog computing. The survey reviewed IoT security yet does not review the deployment of SDN or NFV based IoT security solutions [2].

Emerging technologies related to IoT such as SDN, NFV, Cloud computing, Fog computing, cellular IoT, and wireless sensor networks were explored by Salman et al. [105]. The process of standardisation by entities and organisations within IoT, SDN, NFV, and Edge computing to enhance utility was discussed. They focus on authentication, access control, and identity management for the handling of IoT security challenges. The threats and attacks faced by IoT networks were not included in their review alongside detection methods against attacks. The concept of combining SDN and NFV was introduced in the paper without narrowing down on any SDN/NFV based security solutions[105].

SDN-based approach for IoT was inspected by Bera et al. [106] providing outlines of using SDN with IoT to address requirements for security and provide capable solutions for challenges of IoT applications. Sets of the SDN-based approaches were compared based on two main perceptions which are access and edge networking. The challenges related to core networking and SDN-based technologies are illustrated. The paper was streamlined to the deployment of SDN-based solutions for the enhancement of IoT network efficiency rather than enhancing the security of IoT networks and applications [106]. This paper outlines IoT security requirements, challenges, and limitations that implementing reliable IoT security mechanisms encounters. A comprehensive review of emerging technologies such as SDN and NFV and their impact on IoT security solutions. Furthermore, challenges regarding the implementation of the technology are outlined with current implementation challenges and restrictions. Related studies about implementing SDN/NFV to provide security in IoT environment followed by current research gaps and future research directions are outlined.

Table 1 illustrates the topic covered for this paper. This includes attack detection methods; mitigation approaches; traditional security protection techniques such as encryption, authentication, and access control; emerging technologies such as Blockchain and machine learning. The table also shows a comparison of this work with other related work with topics and key issues covered.

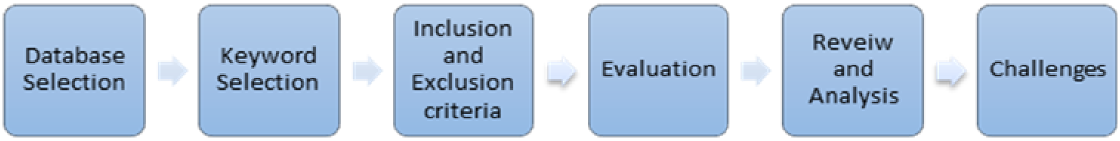

FIGURE 2 Research Methodology used in this paper

4 | RESEARCH METHODOLOGY

This paper used an integrative research approach for the review and elaborate on key issues and trends. The approach elaborates on the strengths and weaknesses of the reviewed topic and provides a critical evaluation of the literature based on the outcome of the method implemented. Assessment and analysis for the literature about the reviewed topic are developed on new perceptions rather than utilizing the commonly used symmetrical or semi-symmetrical approach. Researchers take on seven steps of research methodology, which was adopted for use in this paper. The methodology adopted is illustrated in figure 2 and explained in the sections that follow.

4.1 | Database Selection

Relevant studies related to IoT security, SDN, NFV, SDN/NFV integration, and SDN/NFV based IoT security mechanisms are selected from formally published studies pulled from well-known databases such as IEEE, Google Scholar, Springer link, Elsevier, ACM digital library, and the University of Derby library catalogue. IEEE Xplore and Google Scholar databases accounted for about 90% of the studies and the remaining database accounted for the remaining 10%. Table 2 presents the distribution of papers selected from each scholarly database.

Database	Phase 1	Phase 2
IEEE Xplore	648	67
ACM Digital Library	34	7
Elsevier ScienceDirect	27	11
Scilit	16	5
SpringerLink	28	8
Google Scholar	327	16
Total	**1080**	**114**

TABLE 2 Literature Database used along with the number of papers per database

4.2 | Keyword Selection

The keywords used in this paper are based on the articles covering the Internet of Things (IoT) along with SDN, IoT and Security; IoT, NFV and security; IoT, SDN/NFV and Security; IoT, SDN, and NFV. The keywords used in this paper are listed in 3 along with the number of retrieved results. Such a systematic approach gave results on a total of 1080 articles. Out of which we selected 114 papers for establishing the importance and novelty of our work. The paper are excluded and included based on the following criteria:

- The contribution has some focus on the security aspects of IoT using SDN and NVF
- associating the work done across different application architecture of IoT.
- The contribution which highlights the application of Block-chain related technology within a practical scenario.

The search resulted in 1080 document as illustrated in Table 3 with keywords that comprises of IoT, SDN and Security accounting for about 44% of the studies. The combination of IoT, SDN and NFV provided about 34% of the studies followed by the combination of IoT, NFV and Security that provided 12% of the studies. The number of studies regarding the IoT, SDN and Security combination shows the increased involvement in trying to incorporate IoT, SDN and Security together and that applies to IoT, SDN and NFV combination. In contrast to the IoT, SDN and Security combination, the IoT, NFV and Security combination has reduced studies.

Keywords	Number of Documents
IoT with SDN and NFV	362
IoT Security with SDN and NFV	475
IoT with NFV and security	125
IoT and SDN, NFV and security	88
Blockchain and IoT Security	15
Internet of things and security and & SDN/NFV	15
Total	1080

TABLE 3 Search results using the selected keywords

4.3 | Inclusion and exclusion criteria

The criterion for inclusion is typically based on titles and abstracts of relevant studies of IoT security that focused on SDN/NFV based solutions. The selected papers matching the studies could be modified throughout the selection process after they are summarised, compared, and discussed. To ensure state-of-the-art solutions and materials, exclusion criteria are selected based on the time frame of 2015 till 2020. Figure 3 presents the selected papers for this paper per year. There were 114 hits within the inclusion criteria and as indicated 2015 provided the least number of publications that goes up slightly in 2016. The publications in 2019 provided the highest number of hits and the year 2017, have the next high number of publication hits with 31 hits.

In this research, we consider the following topics to review the papers: application scenarios of the IoT system and related security challenges, network architecture of IoT and its usage along with SDN and NFV, Communication requirement of IoT, SDN and NVF and challenges involved in the secure deployment of the IoT network ensuring security and privacy of devices and their users. Figure 3 presents the number of papers we reviewed published in a different year. The papers are sorted by year, from 2015 to 2020. A deeper analysis over these years shows that most of the research has been carried out on securing the IoT network using the centralized network architecture

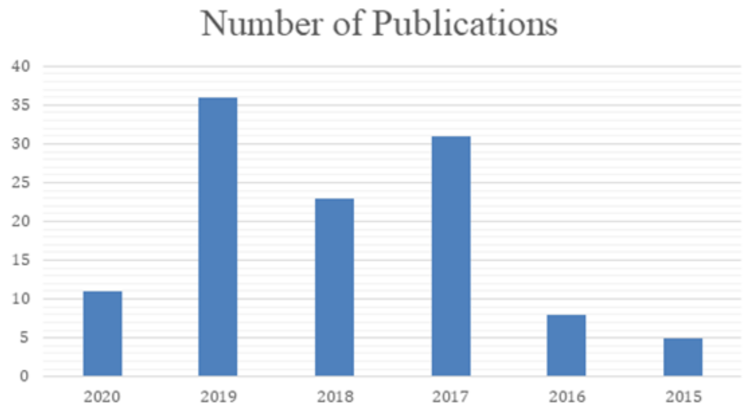

FIGURE 3 Trend Analysis of IoT Research over the years

focusing on the resource-constrained nature of the devices. There have been a number of a paper published that are also focusing on utilizing the usage of SDN/NFV in securing the network, however, this is the new trend and is continuously emerging over the past few years i.e. from 2018 to 2020. Another aspect that is gaining popularity over the last few years is the utilization of blockchain or decentralized technology for achieving the objectives of secure IoT deployment. In terms of system architecture, decentralized and distributed systems have been widely used for Intrusion detection and anomaly detection because of the resource-constrained nature of the devices.

5 | SOFTWARE DEFINED NETWORK (SDN)

SDN-based IoT architecture separates the network into two planes, the control plane and the data plane. The control plane handles the management features of the IoT network, and the data plane is responsible for routing the traffic between the source and the destination. SDN-based security specifies how the component of the SDN could be used to ensure the security of IoT of devices and the data exchange between the IoT network. It also ensures the implementation of authorization and access control mechanisms along with enabling the implementation of cryptosystem away from the end IoT devices. Furthermore, the SDN-based IoT solution could also be used to implement the functionality of firewall and Intrusion detection system which could provide efficient defence against attack to the dynamic and resource-constrained IoT network. The SDN based networks could also be used for deep packet analysis in order to ensure the device-specific and network-specific policies and routing the IoT traffic effectively and efficiently. The SDN-based solution could bring the benefit of not changing the security features of end-devices whenever the cyber attacker changes their attack mechanism, in this case only the controller would require enabling new rules and signatures with re-configuring each end device. Figure 4 represents the SDN based security architecture for IoT networks where different security functions could be moved away from the IoT devices and core network.

The impact of Software Defined Network (SDN) on IoT systems is to increase the manageability of the systems by decoupling the data plane from the control plane. The granular and dynamic operations of SDN provides a novel avenue for IoT environments to cope with security threats. IoT environments generate a massive amount of data traffic that could overwhelm the system, traditional security systems are unsuitable in dealing with security threats to the system, which led to the suggestion of deploying SDN to provide specialised security enhancement to meet the increased requirement of the environment [29],[107],[108],[109]. Components such as policy controller and execution

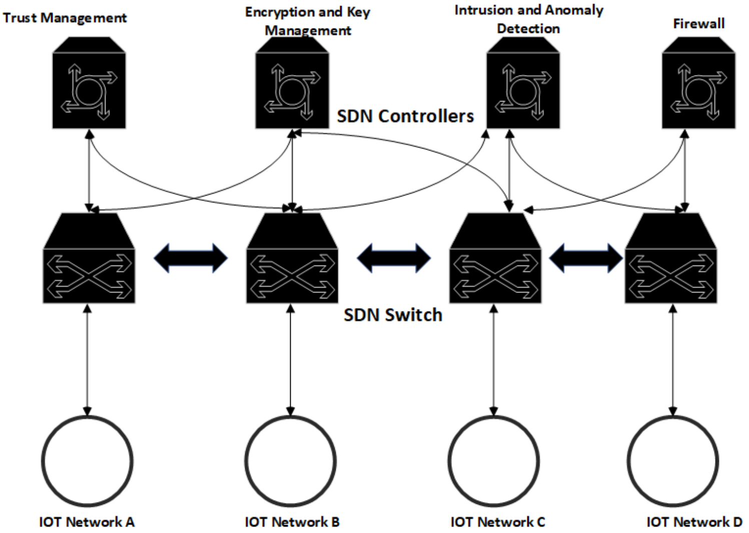

FIGURE 4 SDN-based Security architecture for the IoT Network

appliance are deployed within the network to prevent violation and exploitation based on the dynamic management afforded by these components [110]. The application layer, control plane, and data plane are the three layers that make up the SDN architecture.

The SDN application layer is the layer that faces the end-user where communication between the end-user and the controller occurs and accommodates services and external applications. The SDN controller resides in the control layer and controls the networks while forwarding commands to devices in the data plane. The data plane is like layer 3 of the OSI reference model. The similarities are observed in their operations with both layers empowered to transmit data traffic and fulfil data forwarding tasks. The communication between these 3 layers is carried out using the OpenFlow protocol and the SDN architecture API i.e. northbound and southbound interfaces. The Northbound interface defines how the controller and application are connected while the southbound interface defines the connection between the controller and network systems [7],[111].

SDN offers features capable of installing and updating rules dynamically for forwarding traffic to other network components to manage the flow of traffic within the network. These features improve the potential of implementing appropriate security mechanisms for the enhancement of the security of critical structures. Here we discuss potential solutions that have been designed for IoT security through SDN, summary and important characteristics of solutions is given in table 4. The benefits of incorporating SDN into a network system are stated below:

- **Isolation of traffic:** SDN can forward different network traffic for different clients within the network by creating routing paths for the network. Security policies can be deployed to the routing paths to accept or deny traffic as stated by the security configuration of the SDN controller. SDN controllers are capable of isolating traffic and when attached to an IoT environment as a gateway, they extend this into the traffic forwarded to devices in the environment. Flauzac et al. [112] presented a solution that characteristically enhanced the security of SDN controllers and is scalable to accommodate a large number of devices from different IoT networks. The proposed concept by [112] of expanding SDN to cover more than one domain shows the communication between domains is performed by the border controller located within each domain. These controllers implement access control among communicating nodes and domains. The mechanism proposed by [23] against new flow attacks on IoT environment benefits from the isolation of traffic yet SDN controllers and IoT devices are vulnerable to DoS attacks that terminate communication between devices due to resource limitation of these devices, and the proposed mechanism by [113] which monitors and analyse the flow of traffic which implements Self-Organising Map Algorithm at the gateway before isolating and denying traffic based on specified security rules [4].

- **Centralised System Monitoring:** The capacity of the SDN Controller to oversee the operation of the data plane and the control plane is extensive. The SDN controller is capable of obtaining certain details such as the updated status of infrastructure and flow request messages of applications running in the control plane. The protocols operating on these levels, OpenFlow that provide flow-oriented status and Flexam to enhance packet-level information allows for the extension of SDN controller capability in packet visibility and inreturn can be channelled into a centralised monitoring support system with low overhead. The centralised system is improved by the dynamism of SDN in providing installation and update of rules in network elements to manage traffic flow is a key feature in SDN. The potential of implementing appropriate security mechanisms is enhanced based on this dynamism [4].

The SDN has been used in combination with other technologies to enhance the security of the IoT environment. Derhab et al. [114] proposed a blockchain-based IDS security solution for industrial IoT systems that integrated an integrity checking system that is efficient against attacks such as misrouting and forged command attacks. Pourvahab and Ekbatanifard [115] proposed an architecture that is based on the algorithm that accomplishes validation in a blockchain-based SDN controller which is the Linear Homomorphic Signature (LHS). The architecture implements means for device authentication and user identification and deploys fuzzy logic for packet grouping to identify malicious packets and devices. The mechanism is effective against unauthorised access and reduces overhead in the environment as only suspected packets are further processed yet the logs of activities stored in the controller increase memory consumption. Rathore et al. [116] introduced a decentralised SDN security architecture that uses blockchain, fog, and edge computing for effective security management. Deep learning-based algorithms have been used to analyse and classify traffic for efficient attack detection before sending security rules to the switch to block malicious traffic and blacklist the source. The overhead generated due to the complex level of processing often outweighs the speed of attack detection. the system needs to use along with the firewall or intrusion detection systems. In a distributed network scenario, Gonzalez et al. [117] proposed an SDN-based firewall for the dynamic and distributed IoT network that monitors the flow of traffic to a group of IoT devices. The system uses the semantics of dynamic firewalls which have been implemented over the SDN controller which bring the benefit of not involving the input from IoT devices for the dynamic update of firewall rules. This type of setup could have the benefit of having a defence against the zero-day attack and involve different IoT networks into to collaborative update of firewall rules. Boudi et al. [118] proposed resource-constraints lightweight security as the service solution to protect the IoT devices from cyber-attacks. The solution is placed at the edge of the network near the IoT devices and shift the computation and processing load from the resource-constrained devices. The security decision is being imposed at the SDN based edge devices that provide an interface between IoT devices and their connection to the internet cloud.

Figure 5 shows the distribution of defence mechanisms offered by the deployment of SDN based security solutions in network security. Detection and mitigation defence mechanisms mode of operation are the most deployed among the studies, this is because the Intrusion detection and anomaly detection system are resource intensive and it would be good to separate the control and data plane. This would ultimately not only reduce the load from the devices but would also incorporate some level of collaboration among devices for effective intrusion and anomaly detection. The prevention-based system has also seen popularity in the research community as these systems are most likely to integrate with SDN based Intrusion detection systems.

Paper	Environment	System Design	Security Method	Architecture	Strength	Defense Mechanism	Security Objective	Performance
[112]	Simulation	Distributed	Access control, Authentication	Collaborative	The deployment of Controller for controlling communication and device authentication	Prevention	Unauthorized access	Not Available
[23]	Simulation	Centralised	Dynamic access control	Collaborative	New flow attack identification and mitigation	Detection and Mitigation	New-flow attack	85% Accuracy
[117]	Simulation	Distributed	Packet inspection	Network Based	Protocol extension to enhance the end device protection	Prevention	Unauthorized access	Not Available
[119]	Simulation	Centralised	Anomaly based detection	Network Based	Identification and mitigation of DoS attacks with entropy-based solution	Detection and Mitigation	DoS and DDoS attacks	97.5% Detection rate
[120]	Real-world deployment and Simulation	Centralised	Anomaly based detection	Network Based	Devices and communication protection against DDoS attacks	Detection and Mitigation	DDoS attacks	80% Detection rate
[10]	Simulation	Centralised	Packet inspection	Collaborative	HTTP protocol for device security	Mitigation	MITM attack	100% mitigation rate
[121]	Real-world deployment and Simulation	Centralised	Anomaly based detection	Network Based	SDN based flow analysis approach for IoT traffic monitoring	Detection and Mitigation	ICMP and TCP based flooding attacks	Not Available
[122]	Simulation	Centralised	Anomaly based detection	Network Based	Traffic analysis with self-similarity factor	Detection	DDoS attack	Not Available
[113]	Simulation	Centralised	Anomaly based detection	Network Based	Self-Organising Map neural network algorithm for malicious device detection and mitigation.	Detection and mitigation	Ping flood DDoS attack	100% detection ratio
[123]	Simulation	Centralised	Honeypots	Network Based	DDoS attacks identification and Mitigation with honeypots and Moving Target Devices	Detection and Mitigation	Telnet and SSH based DDOS attacks	High Mitigation
[124]	Real World deployment	Centralised	Update devices of attacks	Collaborative	The controller updates connected switches with information of the attack reported by the IoT device	Detection and Mitigation	Malicious traffic	Better result with hardware implementation than Virtual implementation.

TABLE 4 Comparison of SDN Based IoT security solutions

6 | NETWORK FUNCTION VIRTUALIZATION (NFV)

Network Function Virtualization changes the landscape of the network environment. It boycotts the traditional set up of hardware devices in executing required network tasks by setting up virtual mediums for performing these tasks

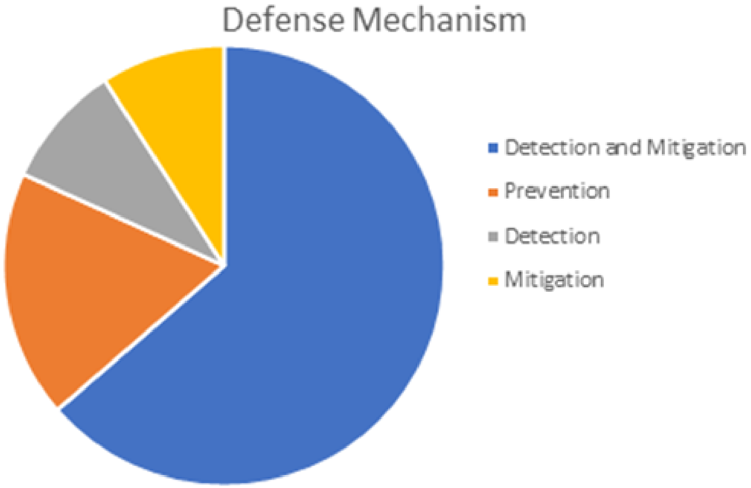

FIGURE 5 Categorization of SDN based defense mechanism Designed for IoT Security

[125]. Software-based functions hosted on existing devices in the network can replace a hardware device required to perform services within the network, thereby reducing cost and enhances network flexibility and scalability [126]. The architectural implementation consists of various technologies that execute network functions virtually and carry out efficient communication between these functions. Figure 6 represent the system architecture of an NFV-based IoT network. The security attribute can be configured at the application layer of the architecture. The main blocks for NFV implementation are :

- **Network Function Virtualization Infrastructure (NFVI):** these are essential for the execution of virtual functions as the software and hardware components required for the establishment of a virtual environment are contained in the infrastructure [127], [128].
- **Virtual Network Functions (VNFs):** these are deplorable components that could be hosted individually and interconnected through different interfaces. The implementation consists of well-defined functional behaviours and external interfaces and is deployed over virtual resources [127], [128].

The enhanced flexibility provided by the underlying complex network of NFVs are controlled by the efficient deployment of VNF and is composed of three main components:

- **Virtualized Infrastructure Manager (VIM)** that serves as the coordinating unit for the hardware resources that are provided by the NFVI in the network. The task of VIM is carried out across several geo-distributed resources and tasks can include obtaining information regarding the infrastructure for monitoring, energy efficiency, fault, and performance analysis [127], [128].
- **VNF Manager (VNFM)** is accountable for the lifecycle of VNF from creation, configuration, maintenance, performance, and security management of implemented instances [127], [128].
- **NFV Orchestrator (NFVO)** orchestrates the deployment of resources and services within the framework. NFVO combines with VIMs and VNFM in a coordinating capacity to ensure the smooth operation of the framework. Resources required for VNF hosting are provided by the interactivity of VIMs and NFVO and the configurations

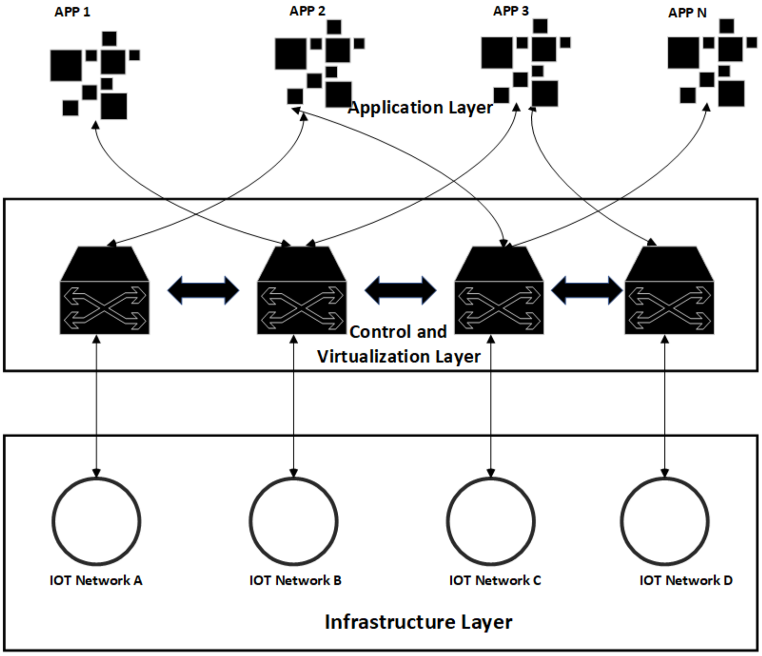

FIGURE 6 NFV-based Security architecture for the IoT Network

required for managing VNF are provided by the NFVO linkage with VNFM [127], [128].

Sairam et al. [129] proposed a lightweight architecture implemented at the network edge deploying a machine learning algorithm for anomaly detection of incoming traffic. Replicating a network device with limited capabilities, a docker container was used for the deployment of the mechanism that achieves efficiency in the detection of ICMP and SYN flood attacks without generating overhead. Mattos et al. [130] deployed an NFV infrastructure for malignant traffic detection offering traffic degradation prevention against DoS attack while isolating the overhead generated from the system and communicating processes of devices and gateways. The combination of NFV infrastructure with blockchain, fog, and cloud computing was proposed by Salahuddin et al. [131] to provide elastic and secure deployment in a smart healthcare environment. Blockchain enhances the security for the proposed mechanism deploying asymmetric key cryptography for data authorisation and authentication. A lightweight solution proposed by Massonet et al. [132] for network edge nodes using the VNF block of the NFV infrastructure and service function to offer security services to IoT devices and networks. Thangavelu et al. [133] proposed NFV based architecture that enhances security with the locally implemented machine learning algorithm at the gateway. The mechanism demonstrated potency in the identification and detection of malicious behaviour among devices in the environment. A honeynet based solutions have got lots of attention in traditional networks. Zarca et al. [134] proposed a novel virtual IoT HoneyNets based on NFV for securing IoT devices in the network. The successful deployment of such would help in identifying the malicious traffic at the early stage of the attack. Zarca et al. [135] proposed a security architecture for the IoT networks that are based on the NFV setup. The system provides security scenarios for different architectural setups. The system has been tested against different types of intrusions and malware attacks on IoT systems. The security components of the proposed system enable the manager to configure the security properties on demand and reactively and proactively.

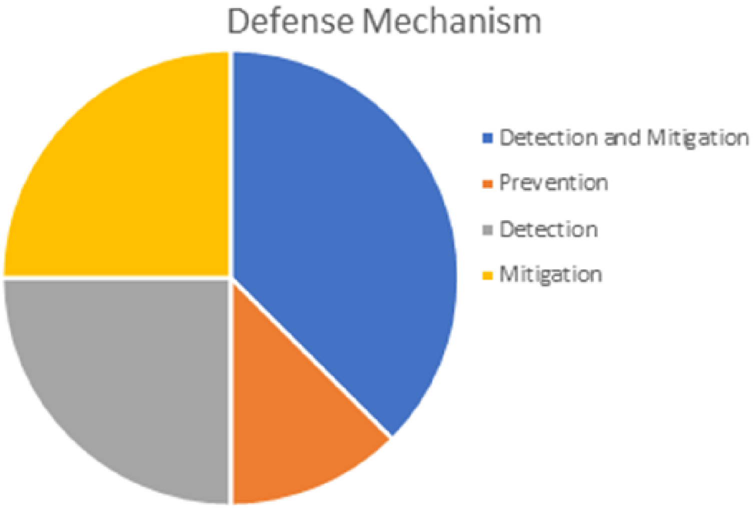

FIGURE 7 Distribution of defense mechanism Designed for SDN Based IoT security solutions

Table 5 shows a comparison among the analysed NFV based solution design for IoT architecture focusing on the type of system (collaborative, centralized or distributed), environment in which the system has been deployed and test, what type of security mechanism the system is designed for and the performance analysis of the system. From the table 5, the deployment of these solutions has indicated improved detection and mitigation defence mechanism on centralised or distributed system designs. Figure 8 shows the distribution of defence mechanisms offered by the deployment of NFV based IoT network security solutions. Detection and mitigation defence mechanism mode of operation is the most deployed among the studies. Deploying the detection and mitigation mechanism individually, accounted for the next deployed mode of operation.

Paper	Environment	System Design	Security Method	Architecture	Strength	Defense Mechanism	Security Objective	Performance
[129]	Real world virtual implementation	Centralised	Firewall, Anomaly Detection	Network Based	Network edge traffic analysis	Detection and Mitigation	ICMP and SYN flood attacks	Approximately 95% detection accuracy
[130]	Simulation	Centralised	Machine learning algorithm	Collaborative	Malicious traffic analysis at the gateway	Detection and Mitigation	DoS Attack	99.8% traffic classification
[131]	Real World implementation	Decentralised	Authentication and Authorisation	Collaborative	Authentication and authorisation with blockchain and asymmetric key encryption	Prevention	Unauthorised access	Not Available
[133]	Real World implementation	Distributed	Anomaly-based detection	Network Based	Analysis and detection of Malicious behaviour	Detection	Malicious behaviour detection	Around 97% accuracy
[136]	Simulation	Centralised	VNFs	Host Based	Device protection with VNFs at network edge	Mitigation	DDoS Attack	Not Available
[137]	Real-world implementation and Simulation	Centralised	Access control	Network Based	Access control provision	Mitigation	ARP spoofing attack, MiTM	High mitigation rate
[138]	Simulation	Distributed	Virtual IPS	Collaborative	IPS in combination with external resources defend against DDoS attack	Detection and Mitigation	SYN Flood DDoS attack	Enhance protection rate
[118]	Real-world implementation	Centralised	Intrusion Detection	Network based	Security solution application at network edge	Detection	Malicious traffic	Edge security show enhance security

TABLE 5 Comparison of SDN Based IoT security solutions

7 | HETEROGENEOUS SDN AND NFV BASED SOLUTIONS

The Software-defined networking and network function virtualization both offer the functionality of network abstraction, however, SDN provides the function of the separation of network control logic from the physical devices (router, switches or other network nodes) that route or forward traffic from the individual network nodes. The NFV is the implementation of network service by virtualizing networking devices and appliances from the hardware on which they run. The heterogeneous approach combines both the features of SDN and NFV together to achieve the objective of an effective and reliable security system.

Zolotukhin and Hämäläinen [139] proposed a mechanism that combined SDN and NFV with machine learning to enhance IoT security. Reinforcement Machine Learning was deployed for identification of malware with the design including SDN controller and several NFV which serves as honeypots and firewalls. The mechanism adopts an AI machine for the analysis of traffic and security policies by the NFV for threat mitigation. If malicious traffic is discovered, the traffic is rerouted or bandwidth is altered and sent to the SDN controller to the required procedure to be performed. The mechanism was demonstrated to be efficient against brute force and DDoS attacks. Kim et al. [140] use NFV to provide security services within the gateway and SDN controller to manage traffic flow. The mechanism seems to handle policy resolution automatically, achieve access control and perform security functions that are successful at Botnet and brute force attack mitigation.

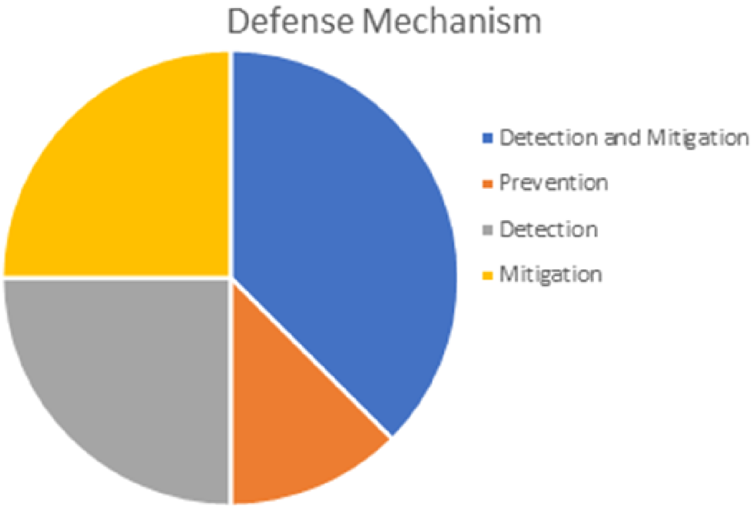

FIGURE 8 Distribution of defense mechanism Designed for SDN Based IoT security solutions

Zarca et al. [141] proposed an SDN and NFV architecture that focuses on Authentication, Authorization, and Accounting (AAA). The AAA framework control is deployed at the network edge using virtual EAP servers at the network edge for verification management and a virtual proxy is deployed to manage safeguarding of communication channels via DLTS. The framework achieves high scalability in a large IoT network environment [141]. Alharbi et al. [142] proposed a mechanism that conducts flow screening to classify the nature of the traffic and define the process required to be implemented and executed automatically by the NFVs to the delivery of security functions. The mechanism does not show enough evidence to demonstrate the efficiency against DDoS attacks despite the scalability of the mechanism. Table 6 shows comparison of combined SDN/NFV based IoT security solutions.

From the table above, the deployment of these solutions has indicated improved detection and mitigation defence mechanism on centralised or distributed system designs. Figure 9 shows the distribution of defence mechanism offered by the deployment of combined SDN/NFV based IoT network security solution. Detection and mitigation defence mechanism mode of operation is the most deployed among the studies. Deploying the detection and mitigation mechanism individually, accounted for the next deployed mode of operation.

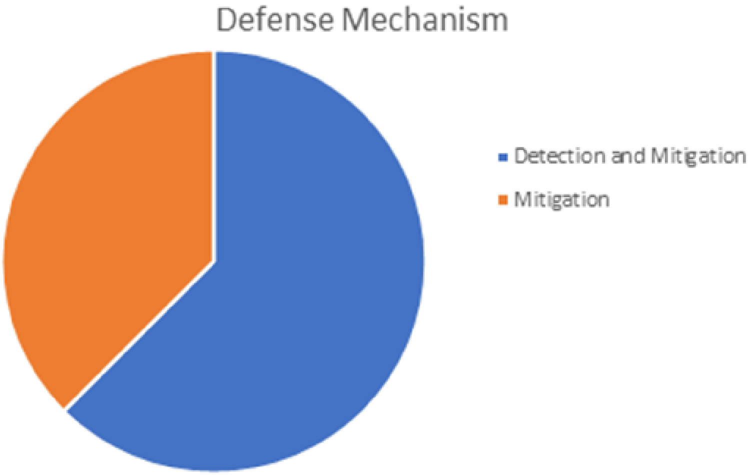

FIGURE 9 Distribution of Heterogeneous defense mechanisms

Paper	Environment	System Design	Security Method	Architecture	Strength	Defense Mechanism	Security Objective	Performance
[140]	Real World environment	Centralised	Anomaly based detection, IPS, Dynamic access control	Network Based	SDN and NFV act as access control system and security management for IoT devices, detecting remote exploitation	Detection and Mitigation	Botnet, Brute Force Attacks	99% mitigation rate
[128]	Simulation	Distributed	Firewall, Anomaly based detection	Collaborative	MiTM detection and mitigation	Detection and Mitigation	MITM Attack, Infected nodes detection	Efficient Mitigation
[139]	Simulation	Distributed	Anomaly based detection, honey bots	Collaborative	Attacks identification with reinforcement learning algorithm in mitigating attacks	Detection and Mitigation	HTTP based DOS attack, SSH -Brute force attack	Efficient detection and mitigation
[141]	Simulation	Centralised	Authentication, Authorization and Accounting	Collaborative	Access control management and communication channel protection	Detection and Mitigation	Internal attack	Increase protection speed
[143]	Simulation	Centralised	Flow Control	Network Based	Service availability with better response time and DDoS attack mitigation	Mitigation	DDoS attack	Not available
[144]	Simulation	Distributed	Authorisation, Confidentiality	Network Based	Reduced energy consumption and improved confidentiality with SDN/NFV architecture	Mitigation	DDoS attack	Improved performance
[145]	Simulation	Distributed	Anomaly-based detection	Collaborative	Distributed framework for DDoS botnet attacks	Detection and Mitigation	Botnet	Improved botnet discovery and mitigation
[29]	Simulation	Distributed	Encrytion	Collaborative	Multiple controller with distributed role-based security functions	Mitigation	Unauthorised access	Not Available

TABLE 6 Comparison of Heterogeneous SDN Based IoT security solutions

8 | COMPARATIVE ANALYSIS

The implementation of SDN and NFV either separately or together provides the flexibility of establishing multiple security approaches and methods for the safeguarding of IoT networks and the environment. Here we briefly review some security challenges associated with SDN and NFV that could impede the efficiency of these mechanisms in offering security to the IoT environment and review the efficiency of the proposed mechanism. The benefits exhibited by SDN and NFV in the performance and security of IoT environments make these technologies an extended point of attack to the environment. Multiple controller implementation was proposed by some papers [29], [112] to conquer the effect that could occur from DoS and DDoS attacks on environments with a centralised system that could lead to a single point of failure. Some papers [116], [146] suggested the use of distributed system approach architecture which in some cases is combined with blockchain, fog, and edge computing to overcome the challenge of a single point of failure. Attacks on NFV can cause damages to various aspects such as exploitation of VNF to compromise and access the hypervisor which contains network resources. Lai et al. proposed the signing of the VNF image digitally and verification of the signature in an attempt to maintain the integrity of the system [125]. While in some cases, IDS has been suggested to implement a means of safeguarding virtual machines from attacks [147] A critical review of the efficiency of the proposed mechanisms in providing security for IoT environment using SDN/NFV based technologies was analysed and broken down based on different features that are presented as follows:

- **The environment used:** This is the environment used for deploying the proof of concept for the proposed mechanisms reviewed in the paper. The most utilised implementation approach adopted for the mechanism is the use of simulation which accounts for 69% of the reviewed mechanisms, mixed implementation of simulation and/or hardware components, and/or virtual implementation account for 21% of the mechanisms with 5% implemented in a virtual environment and the remaining 5% were based on hardware implementation. The flexibility of the simulation environment such as Cooja Contiki, Ganache, and MATLAB is responsible for its increased use in deploying the solution mechanisms.
- **System Design:** This involves the identification of the architecture used for implementation and the status of the architecture. The centralised system is the most deployed approach accounting for 55.3% of the reviewed proposed mechanisms. The deployment of Distributed system design accounts for the remaining 44.7% of the reviewed mechanisms. Multiple controllers and/or various decentralised systems such as blockchain, machine learning, and/or VNFs are deployed in the suggested architecture. Figure 12 shows the types of SDN controllers deployed in achieving the system design. The distributed system conquers the single point of failure challenge faced by the centralised design but the design of the system becomes complex in the process. The consideration for the use of a centralised system in system design despite the challenge of a single point of failure is based on the default architecture of SDN using a centralised controller in achieving its objective.
- **Architecture:** this illustrates the architecture taken into consideration for ensuring a secure environment or enhancing the security of the IoT environment. From the solutions reviewed, there are three main security architectures discovered. The architecture is collaborative which combines various technologies such as blockchain, machine learning, and/or VNF to provide layers of numerous security methods that detect, mitigate and prevent different attacks and threats. The other architectures are network-based which entail security solutions that are based on the network and host-based is a security architecture that is based on the host. The collaborative and network-based architecture both accounts for an equal share of 97% of the reviewed solution with each architecture possessing 48.5%. The high implementation of this architecture is based on the SDN and NFV architecture deployed.
- **Performance:** This is the evaluation of the security practices used in the reviewed solutions. The assessment is based on the obtained result of the efficiency of the solutions, and elements involved in the operation of the solution. The evaluation aims at the procedures that the solutions deploy against attacks and threats in the IoT environment. Figure 10 shows the security operation performed by the solutions against attacks and threats. 47.7% of the solution provides both detection and mitigation mechanisms while 11.6% state prevention techniques and 26.6% of the reviewed solutions included mitigation procedures. 28.5% of the reviewed solutions focused on protection against DDoS attacks followed by 11.9% that concentrate on the prevention of unauthorised access and malicious traffic detection and mitigation with the remaining focusing on threats such as DoS, Malware injection, Misrouting. Figure 11 provides insight into the attacks and threats encountered by the reviewed solutions while Figure 13 shows attacks mitigated by the solutions. Despite the performance of the solutions, 36.9% indicates

that resources overhead is not generated with 18.4% indicating generation of overhead and 44.7% of reviewed solutions does not indicate any information regarding the generation of resource overhead.

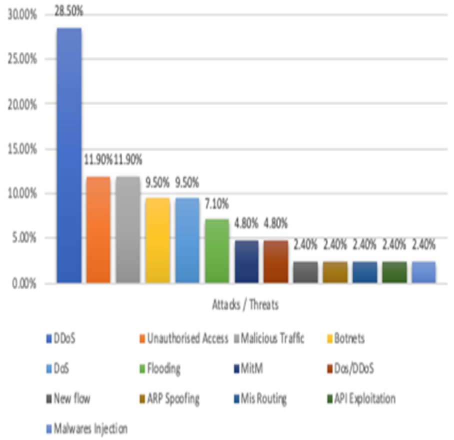

FIGURE 10 Attacks and Threats to IoT environment Do we have clearer figures?

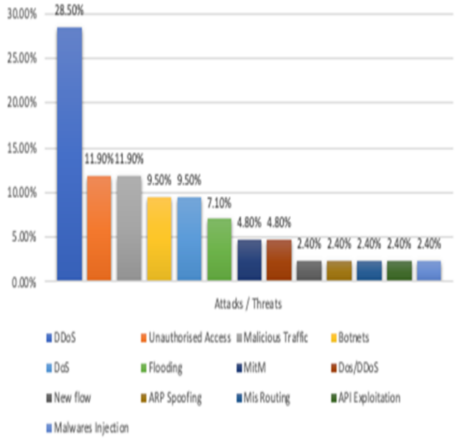

FIGURE 11 Attacks Mitigated by SDN/NFV IoT security solutions

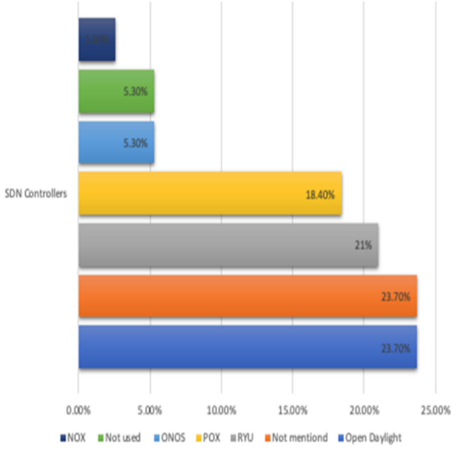

FIGURE 12 Types of SDN controller used in the security solutions

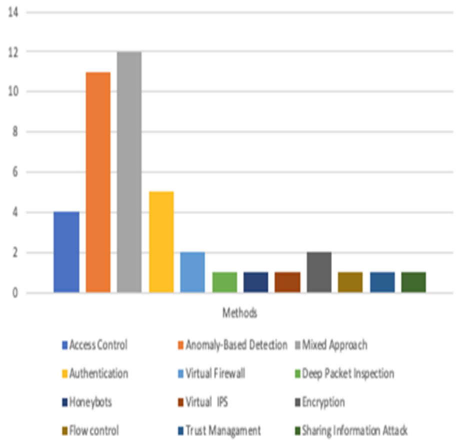

FIGURE 13 Security operations performed by the solutions

9 | CHALLENGES

The reviewed SDN/NFV based IoT security mechanisms do offer benefits and enhance the security of the IoT environment. In the implementation of the solutions, there are various challenges identified and key issues which require more research in enhancing its efficiency. Some of the challenges identified in the review are as follows:

- **Large Attack Surface and Comprehensive Security Solutions:** - IoT environment consists of widespread application domains and is connected to the Internet for remote access. The inclusion of SDN and NFV technologies such as SDN controllers, switches, VNFs, and components like hypervisors offers an additional attack surface. The extra technologies added increases the complexities of the network especially with collaborative and distributed systems which could lead to trust issues among devices and weaken the security of the environment. Comprehensive SDN/NFV IoT security solutions should take into consideration the security of the SDN and NFV components alongside IoT devices when designing the security architecture of the IoT environment to avoid exploitation at any level of the environment. The management and orchestration of SDN and NFV solution enablers and rapid reaction to attacks and threats require more research in enhancing the efficiency of the security mechanism.
- **Artificial Intelligence and Machine Learning Algorithm:** The implementation of artificial intelligence and Machine learning offer better performance and protection in anomaly-based detection systems. With 10.5% of the reviewed solution deploying machine learning algorithms for traffic analysis and detection. High accuracy for detection was obtained with [129] achieving 95% accuracy and [130] showing 99.8% traffic classification accuracy. The model must be updated regularly as re-training is crucial to provide efficient protection for the identification of new attacks. The implementation of AI and machine learning algorithms in SDN/NFV implementation has been hampered by the lack of real-time or available datasets and limited access to network resources.
- **Patching and Updates:** The provision of secured firmware updates and patches is crucial in ensuring security in the IoT environment. The management for the provision of updates and patches for IoT devices still needs further research and implementation of SDN/NFV could enhance the delivery of the patch and updates to the IoT environment and use VNF or controller for ensuring secured communication.
- **Standardisation:** IoT environments consist of different types of devices with different communication mechanisms and capacities which leads to an absence of standardised communication mechanisms unlike in the traditional environment. The lack of standardisation in the environment increases the complexity of the environment and with the expansion of the environment with SDN/NFV technologies, standardisation within the environment should be researched further to reduce complexities and improve communication within the environment.

10 | CONCLUSION

The demand and usage of IoT devices in multiple application domains keeps increasing with over 1.3 billion connected devices in 2019. The increase in connected devices means the devices are prone to various attacks and threats. The limited capabilities of these devices do not provide a suitable platform for the implementation of extensive security measures that generate overheads when in operation. Efficient lightweight security mechanisms that do not generate overheads and are suitable for the capability of the devices are to be deployed to provide security. In the bid to enhance the security mechanism deployed in the IoT environment, research into extensive security solutions that do not generate too much overhead has been proposed [119].

In this paper, we have explored common security challenges and requirements of the IoT environment. We further reviewed the customised features and scenarios that SDN and NFV offer in the security enhancement of IoT environment when deployed in a centralised or distributed systems [10], [23]. The implementation of these technologies has been shown to perform threat and attack detection, prevention, and mitigation with some generating overheads and others do not generate overheads. The features of the SDN and NFV technologies permit the deployment of appropriate and efficient security solutions and leveraging these features to overcome resource limitations and provide efficient, effective scalable, and elastic IoT security solutions.

The combination of both technologies for security deployment in IoT environments has demonstrated their potency in enhancing security especially for edge devices in the environment [128]. When NFV or SDN are implemented with AI, machine learning and/or blockchain they provide intelligent security solutions and have proven to exhibit improved detection accuracy and enhance security mechanism efficiency. Future research can be in the direction of integrating intelligent solutions into SDN and NFV incorporated IoT environments. The deployment of machine learning algorithms to SDN and NFV based IoT security systems in implementing intelligent security solutions still require further research in the aspect of available real-time data to enhance anomaly-based detection and establishment of standardised protocols within the environment.

references

[1] Krishnan P, Najeem JS, Achuthan K. SDN Framework for Securing IoT Networks. In: Kumar N, Thakre A, editors. Ubiquitous Communications and Network Computing Cham: Springer International Publishing; 2018. p. 116–129.

[2] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019;7:82721–82743.

[3] Ahmed Z, Danish SM, Qureshi HK, Lestas M. Protecting IoTs from Mirai Botnet Attacks Using Blockchains. In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD); 2019. p. 1–6.

[4] Farris I, Taleb T, Khettab Y, Song J. A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. IEEE Communications Surveys Tutorials 2019;21(1):812–837.

[5] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, et al. Understanding the Mirai Botnet. In: 26th USENIX Security Symposium (USENIX Security 17) Vancouver, BC: USENIX Association; 2017. p. 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[6] Port scanning /0 using insecure embedded devices;. Accessed: 2021-07-30. http://census2012.sourceforge.net/paper.html.

[7] Tayyaba SK, Shah MA, Khan OA, Ahmed AW. Software Defined Network (SDN) Based Internet of Things (IoT): A Road Ahead. In: Proceedings of the International Conference on Future Networks and Distributed Systems ICFNDS '17, New York, NY, USA: Association for Computing Machinery; 2017. https://doi.org/10.1145/3102304.3102319.

[8] Bilal M, A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers; 2017.

[9] Farhan L, Shukur ST, Alissa AE, Alrweg M, Raza U, Kharel R. A survey on the challenges and opportunities of the Internet of Things (IoT). In: 2017 Eleventh International Conference on Sensing Technology (ICST); 2017. p. 1–5.

[10] Al Hayajneh A, Bhuiyan MZA, McAndrew I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). Computers 2020;9(1). https://www.mdpi.com/2073-431X/9/1/8.

[11] Sikder AK, Petracca G, Aksu H, Jaeger T, Uluagac A. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications. ArXiv 2018;abs/1802.02041.

[12] Fernandes E, Rahmati A, Eykholt K, Prakash A. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? IEEE Security Privacy 2017;15(4):79–84.

[13] Blythe JM, Sombatruang N, Johnson SD. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? Journal of Cybersecurity 2019 06;5(1). https://doi.org/10.1093/cybsec/tyz005, tyz005.

[14] Blythe JM. The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. IET Conference Proceedings 2018 January;p. 4 (7 pp.)–4 (7 pp.)(1). https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0004.

[15] Blythe JM, Johnson SD. A systematic review of crime facilitated by the consumer Internet of Things. Security Journal 2019;34:97–125.

[16] DAZINE J, MAIZATE A, HASSOUNI L. Internet of things security. In: 2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD); 2018. p. 137–141.

[17] Iskhakov S, Shelupanov A, Mitsel A. Internet of Things: Security of Embedded Devices. 2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC) 2018;p. 1–4.

[18] Raza S, Wallgren L, Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks 2013;11(8):2661–2674. https://www.sciencedirect.com/science/article/pii/S1570870513001005.

[19] Arshad J, Azad MA, Amad R, Salah K, Alazab M, Iqbal R. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Electronics 2020;9(4). https://www.mdpi.com/2079-9292/9/4/629.

[20] Arshad J, Azad MA, Abdeltaif MM, Salah K. An intrusion detection framework for energy constrained IoT devices. Mechanical Systems and Signal Processing 2020;136:106436. https://www.sciencedirect.com/science/article/pii/S0888327019306570.

[21] Yu T, Sekar V, Seshan S, Agarwal Y, Xu C. Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things. In: Proceedings of the 14th ACM Workshop on Hot Topics in Networks HotNets-XIV, New York, NY, USA: Association for Computing Machinery; 2015. https://doi.org/10.1145/2834050.2834095.

[22] Ambrosin M, Compagno A, Conti M, Ghali C, Tsudik G. Security and Privacy Analysis of National Science Foundation Future Internet Architectures. IEEE Communications Surveys Tutorials 2018;20(2):1418–1442.

[23] Ren J, Guo H, Xu C, Zhang Y. Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing. IEEE Network 2017;31(5):96–105.

[24] 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(2). https://www.mdpi.com/1424-8220/19/2/295.

[25] Ojo M, Adami D, Giordano S. A SDN-IoT Architecture with NFV Implementation. In: 2016 IEEE Globecom Workshops (GC Wkshps); 2016. p. 1–6.

[26] Jurcut A, Niculcea T, Ranaweera P, Le-Khac NA. Security Considerations for Internet of Things: A Survey. SN Computer Science 2020 06;1.

[27] Sha K, Yang TA, Wei W, Davari S. A survey of edge computing-based designs for IoT security. Digital Communications and Networks 2020;6(2):195–202. https://www.sciencedirect.com/science/article/pii/S2352864818303018.

[28] Lv Z, Qiao L, Kumar Singh A, Wang Q. AI-Empowered IoT Security for Smart Cities. ACM Trans Internet Technol 2021 Jul;21(4). https://doi.org/10.1145/3406115.

[29] Islam MJ, Mahin M, Roy S, Debnath BC, Khatun A. DistBlackNet: A Distributed Secure Black SDN-IoT Architecture with NFV Implementation for Smart Cities. In: 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE); 2019. p. 1–6.

[30] Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST); 2015. p. 336–341.

[31] Oh SR, Kim YG. Security Requirements Analysis for the IoT. In: 2017 International Conference on Platform Technology and Service (PlatCon); 2017. p. 1–6.

[32] Omrani T, Rhouma R, Becheikh R. LICID: a lightweight image cryptosystem for IoT devices. Cryptologia 2019;43(4):313–343. https://doi.org/10.1080/01611194.2018.1563009.

[33] Goyal TK, Sahula V. Lightweight security algorithm for low power IoT devices. In: 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI); 2016. p. 1725–1729.

[34] Chaudhary R, Aujla GS, Kumar N, Zeadally S. Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions. IEEE Internet of Things Journal 2019;6(3):4897–4909.

[35] Xu B, Wang W, Hao Q, Zhang Z, Du P, Xia T, et al. A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device. IEEE Access 2018;6:72862–72869.

[36] Mullen G, Meany L. Assessment of Buffer Overflow Based Attacks On an IoT Operating System. In: 2019 Global IoT Summit (GIoTS); 2019. p. 1–6.

[37] Luo X, Yin L, Li C, Wang C, Fang F, Zhu C, et al. A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment. IEEE Access 2020;8:67192–67204.

[38] Siddiqui F, Beley J, Zeadally S, Braught G. Secure and lightweight communication in heterogeneous IoT environments. Internet of Things 2021;14:100093. https://www.sciencedirect.com/science/article/pii/S2542660519301921.

[39] Zhang ZK, Cho MCY, Wang CW, Hsu CW, Chen CK, Shieh S. IoT Security: Ongoing Challenges and Research Opportunities. In: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications; 2014. p. 230–234.

[40] Sha K, Wei W, Andrew Yang T, Wang Z, Shi W. On security challenges and open issues in Internet of Things. Future Generation Computer Systems 2018;83:326–337. https://www.sciencedirect.com/science/article/pii/S0167739X17324883.

[41] Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ahmed E, Nainar ASM, et al. Deep learning and big data technologies for IoT security. Computer Communications 2020;151:495–517. https://www.sciencedirect.com/science/article/pii/S0140366419315361.

[42] Sollins KR. IoT Big Data Security and Privacy Versus Innovation. IEEE Internet of Things Journal 2019;6(2):1628–1635.

[43] Stergiou C, Psannis KE, Gupta BB, Ishibashi Y. Security, privacy efficiency of sustainable Cloud Computing for Big Data IoT. Sustainable Computing: Informatics and Systems 2018;19:174–184. https://www.sciencedirect.com/science/article/pii/S2210537918300490.

[44] Singh S, Singh N. Internet of Things (IoT): Security challenges, business opportunities amp; reference architecture for E-commerce. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT); 2015. p. 1577–1581.

[45] Hong BK, Huang JW, Ban T, Isawa R, Cheng SM, Inoue D, et al. Measurement Study Towards a Unified Firmware Updating Scheme for Legacy IoT Devices. In: 2019 14th Asia Joint Conference on Information Security (AsiaJCIS); 2019. p. 9–15.

[46] Simpson AK, Roesner F, Kohno T. Securing vulnerable home IoT devices with an in-hub security manager. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops); 2017. p. 551–556.

[47] Alladi T, Chamola V, Sikdar B, Choo KKR. Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine 2020;9(2):17–25.

[48] Yaqoob I, Ahmed E, ur Rehman MH, Ahmed AIA, Al-garadi MA, Imran M, et al. The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks 2017;129:444–458. https://www.sciencedirect.com/science/article/pii/S1389128617303468, special Issue on 5G Wireless Networks for IoT and Body Sensors.

[49] Hossain MS, Muhammad G, Rahman SMM, Abdul W, Alelaiwi A, Alamri A. Toward end-to-end biomet rics-based security for IoT infrastructure. IEEE Wireless Communications 2016;23(5):44–51.

[50] Pérez S, Hernández-Ramos JL, Raza S, Skarmeta A. Application Layer Key Establishment for End-to-End Security in IoT. IEEE Internet of Things Journal 2020;7(3):2117–2128.

[51] Bugeja J, Vogel B, Jacobsson A, Varshney R. IoTSM: An End-to-end Security Model for IoT Ecosystems. In: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops); 2019. p. 267–272.

[52] Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, et al. End-to-end security scheme for mobility enabled healthcare Internet of Things. Future Generation Computer Systems 2016;64:108–124. https://www.sciencedirect.com/science/article/pii/S0167739X16300334.

[53] Elkhodr M, Shahrestani S, Cheung H. The Internet of Things: New Interoperability, Management and Security Challenges. ArXiv 2016;abs/1604.04824.

[54] binti Mohamad Noor M, Hassan WH. Current research on Internet of Things (IoT) security: A survey. Computer Networks 2019;148:283–294. https://www.sciencedirect.com/science/article/pii/S1389128618307035.

[55] da Costa KAP, Papa JP, Lisboa CO, Munoz R, de Albuquerque VHC. Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks 2019;151:147–157. https://www.sciencedirect.com/science/article/pii/S1389128618308739.

[56] Zeng E, Mare S, Roesner F. End User Security and Privacy Concerns with Smart Homes. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) Santa Clara, CA: USENIX Association; 2017. p. 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng.

[57] Xu G, Cao Y, Ren Y, Li X, Feng Z. Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things. IEEE Access 2017;5:21046–21056.

[58] Alkhariji L, Alhirabi N, Alraja MN, Barhamgi M, Rana O, Perera C. Synthesising Privacy by Design Knowledge Toward Explainable Internet of Things Application Designing in Healthcare. ACM Trans Multimedia Comput Commun Appl 2021 Jun;17(2s). https://doi.org/10.1145/3434186.

[59] Perera C, Barhamgi M, Bandara AK, Ajmal M, Price B, Nuseibeh B. Designing privacy-aware internet of things applications. Information Sciences 2020;512:238–257. https://www.sciencedirect.com/science/article/pii/S0020025519309120.

[60] Angrishi K. Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. ArXiv 2017;abs/1702.03681.

[61] Voigt P, Bussche Avd. The EU General Data Protection Regulation (GDPR): A Practical Guide. 1st ed. Springer Publishing Company, Incorporated; 2017.

[62] Chamarajnagar R, Ashok A. Integrity Threat Identification for Distributed IoT in Precision Agriculture. In: 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON); 2019. p. 1–9.

[63] Hossain M, Hasan R, Skjellum A. Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems. In: 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW); 2017. p. 220–225.

[64] Andrea I, Chrysostomou C, Hadjichristofi G. Internet of Things: Security vulnerabilities and challenges. In: 2015 IEEE Symposium on Computers and Communication (ISCC); 2015. p. 180–187.

[65] Lam KY, Mitra S, Gondesen F, Yi X. ANT-Centric IoT Security Reference Architecture – Security-by-Design for Satellite-Enabled Smart Cities. IEEE Internet of Things Journal 2021;p. 1–1.

[66] Lv Z, Qiao L, Kumar Singh A, Wang Q. AI-Empowered IoT Security for Smart Cities. ACM Trans Internet Technol 2021 Jul;21(4). https://doi.org/10.1145/3406115.

[67] Hashem IAT, Chang V, Anuar NB, Adewole K, Yaqoob I, Gani A, et al. The role of big data in smart city. International Journal of Information Management 2016;36(5):748–758. https://www.sciencedirect.com/science/article/pii/S0268401216302778.

[68] Sehrawat D, Gill NS. Security Requirements of IoT Applications in Smart Environment. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI); 2018. p. 324–329.

[69] Li N, Liu D, Nepal S. Lightweight Mutual Authentication for IoT and Its Applications. IEEE Transactions on Sustainable Computing 2017;2(4):359–370.

[70] Aman MN, Basheer MH, Sikdar B. Two-Factor Authentication for IoT With Location Information. IEEE Internet of Things Journal 2019;6(2):3335–3351.

[71] Aman MN, Chua KC, Sikdar B. Mutual Authentication in IoT Systems Using Physical Unclonable Functions. IEEE Internet of Things Journal 2017;4(5):1327–1340.

[72] Lagutin D, Kortesniemi Y. Enabling Decentralised Identifiers and Verifiable Credentials for Constrained Internet-of-Things Devices using OAuth-based Delegation; 2018. .

[73] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems 2018;82:395–411. https://www.sciencedirect.com/science/article/pii/S0167739X17315765.

[74] Minoli D, Sohraby K, Kouns J. IoT security (IoTSec) considerations, requirements, and architectures. In: 2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC); 2017. p. 1006–1007.

[75] Mosenia A, Jha NK. A Comprehensive Study of Security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing 2017;5(4):586–602.

[76] K SK, Sahoo S, Mahapatra A, Swain AK, Mahapatra KK. Security Enhancements to System on Chip Devices for IoT Perception Layer. In: 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS); 2017. p. 151–156.

[77] Smith R, Palin D, Ioulianou PP, Vassilakis VG, Shahandashti SF. Battery draining attacks against edge computing nodes in IoT networks. CoRR 2020;abs/2002.00069. https://arxiv.org/abs/2002.00069.

[78] Dabbagh M, Rayes A. In: Internet of Things Security and Privacy; 2017. p. 195–223.

[79] Deogirikar J, Vidhate A. Security attacks in IoT: A survey. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC); 2017. p. 32–37.

[80] Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Things security: A survey. Journal of Network and Computer Applications 2017;88:10–28. https://www.sciencedirect.com/science/article/pii/S1084804517301455.

[81] Virat MS, Bindu SM, Aishwarya B, Dhanush BN, Kounte MR. Security and Privacy Challenges in Internet of Things. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI); 2018. p. 454–460.

[82] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal 2017;4(5):1125–1142.

[83] Vishwakarma R, Jain A. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication Systems 2020 01;73.

[84] Sayakkara A, Le-Khac NA, Scanlon M. Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices. Digital Investigation 2019;29:S94–S103. https://www.sciencedirect.com/science/article/pii/S1742287619301616.

[85] Park J, Rahman F, Vassilev A, Forte D, Tehranipoor M. Leveraging Side-Channel Information for Disassembly and Security. J Emerg Technol Comput Syst 2019 Dec;16(1). https://doi.org/10.1145/3359621.

[86] Devi M, Majumder A. Side-Channel Attack in Internet of Things: A Survey. In: Mandal JK, Mukhopadhyay S, Roy A, editors. Applications of Internet of Things Singapore: Springer Singapore; 2021. p. 213–222.

[87] Ha DA, Nguyen KT, Zao JK. Efficient Authentication of Resource-Constrained IoT Devices Based on ECQV Implicit Certificates and Datagram Transport Layer Security Protocol. In: Proceedings of the Seventh Symposium on Information and Communication Technology SoICT '16, New York, NY, USA: Association for Computing Machinery; 2016. p. 173–179. https://doi.org/10.1145/3011077.3011108.

[88] Granjal J, Monteiro E, Silva JS. End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. In: 2013 IFIP Networking Conference; 2013. p. 1–9.

[89] Haroon A, Akram S, Shah MA, Wahid A. E-Lithe: A Lightweight Secure DTLS for IoT. In: 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall); 2017. p. 1–5.

[90] Abdul-Ghani HA, Konstantas D. A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. Journal of Sensor and Actuator Networks 2019;8(2). https://www.mdpi.com/2224-2708/8/2/22.

[91] Nastase L. Security in the Internet of Things: A Survey on Application Layer Protocols. In: 2017 21st International Conference on Control Systems and Computer Science (CSCS); 2017. p. 659–666.

[92] Violettas G, Simoglou G, Petridou S, Mamatas L. A Softwarized Intrusion Detection System for the RPL-based Internet of Things networks. Future Generation Computer Systems 2021;125:698–714. https://www.sciencedirect.com/science/article/pii/S0167739X21002752.

[93] Ge M, Syed NF, Fu X, Baig Z, Robles-Kelly A. Towards a deep learning-driven intrusion detection approach for Internet of Things. Computer Networks 2021;186:107784. https://www.sciencedirect.com/science/article/pii/S138912862031358X.

[94] Kan X, Fan Y, Fang Z, Cao L, Xiong NN, Yang D, et al. A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network. Information Sciences 2021;568:147–162. https://www.sciencedirect.com/science/article/pii/S002002552100311X.

[95] Mishra N, Pandya S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. IEEE Access 2021;9:59353–59377.

[96] Smache M, El Mrabet N, Gilquijano JJ, Tria A, Riou E, Gregory C. Modeling a node capture attack in a secure wireless sensor networks. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT); 2016. p. 188–193.

[97] Ngo QD, Nguyen HT, Le VH, Nguyen DH. A survey of IoT malware and detection methods based on static features. ICT Express 2020;6(4):280–286. https://www.sciencedirect.com/science/article/pii/S2405959520300503.

[98] Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Communications Surveys Tutorials 2019;21(3):2702–2733.

[99] Ngo QD, Nguyen HT, Le VH, Nguyen DH. A survey of IoT malware and detection methods based on static features. ICT Express 2020;6(4):280–286. https://www.sciencedirect.com/science/article/pii/S2405959520300503.

[100] Chifor BC, Bica I, Patriciu VV, Pop F. A security authorization scheme for smart home Internet of Things devices. Future Generation Computer Systems 2018;86:740–749. https://www.sciencedirect.com/science/article/pii/S0167739X17311020.

[101] Ghosh N, Chandra S, Sachidananda V, Elovici Y. SoftAuthZ: A Context-Aware, Behavior-Based Authorization Framework for Home IoT. IEEE Internet of Things Journal 2019;6(6):10773–10785.

[102] Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart Contract-Based Access Control for the Internet of Things. IEEE Internet of Things Journal 2019;6(2):1594–1605.

[103] He W, Golla M, Padhi R, Ofek J, Dürmuth M, Fernandes E, et al. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In: 27th USENIX Security Symposium (USENIX Security 18) Baltimore, MD: USENIX Association; 2018. p. 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he.

[104] Kouicem DE, Bouabdallah A, Lakhlef H. Internet of things security: A top-down survey. Computer Networks 2018;141:199–221. https://www.sciencedirect.com/science/article/pii/S1389128618301208.

[105] Salman O, Elhajj I, Chehab A, Kayssi A. IoT survey: An SDN and fog computing perspective. Computer Networks 2018;143:221–246. https://www.sciencedirect.com/science/article/pii/S1389128618305395.

[106] Bera S, Misra S, Vasilakos AV. Software-Defined Networking for Internet of Things: A Survey. IEEE Internet of Things Journal 2017;4(6):1994–2008.

[107] Sood K, Pokhrel SR, Karmakar K, Vardharajan V, Yu S. SDN-Capable IoT Last-Miles: Design Challenges. In: 2019 IEEE Global Communications Conference (GLOBECOM); 2019. p. 1–6.

[108] Shakil M, Fuad Yousif Mohammed A, Arul R, Bashir AK, Choi JK. A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering. Transactions on Emerging Telecommunications Technologies;n/a(n/a):e3622. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3622, e3622 ett.3622.

[109] Yurekten O, Demirci M. SDN-based cyber defense: A survey. Future Generation Computer Systems 2021;115:126–149. https://www.sciencedirect.com/science/article/pii/S0167739X20303277.

[110] Lin YD, Lin PC, Yeh CH, Wang YC, Lai YC. An extended SDN architecture for network function virtualization with a case study on intrusion prevention. IEEE Network 2015;29(3):48–53.

[111] Tselios C, Politis I, Kotsopoulos S. Enhancing SDN security for IoT-related deployments through blockchain. In: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN); 2017. p. 303–308.

[112] Flauzac O, González C, Hachani A, Nolot F. SDN Based Architecture for IoT and Improvement of the Security. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops; 2015. p. 688–693.

[113] Meng Y, Huang Z, Wang S, Shen G, Ke C, SOM-based DDoS Defense Mechanism using SDN for the Internet of Things; 2020.

[114] Derhab A, Guerroumi M, Gumaei A, Maglaras L, Ferrag MA, Mukherjee M, et al. Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security. Sensors 2019;19(14). https://www.mdpi.com/1424-8220/19/14/3119.

[115] Pourvahab M, Ekbatanifard G. An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology. IEEE Access 2019;7:99573–99588.

[116] Rathore S, Wook Kwon B, Park JH. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications 2019;143:167–177. https://www.sciencedirect.com/science/article/pii/S1084804519302243.

[117] Gonzalez C, Charfadine SM, Flauzac O, Nolot F. SDN-based security framework for the IoT in distributed grid. In: 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech); 2016. p. 1–5.

[118] Boudi A, Farris I, Bagaa M, Taleb T. Assessing Lightweight Virtualization for Security-as-a-Service at the Network Edge. IEICE Transactions on Communications 2018 11;E102.B.

[119] Galeano-Brajones J, Carmona-Murillo J, Valenzuela-Valdés JF, Luna-Valero F. Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. Sensors 2020;20(3). https://www.mdpi.com/1424-8220/20/3/816.

[120] Rebecchi F, Boite J, Nardin PA, Bouet M, Conan V. DDoS protection with stateful software-defined networking. International Journal of Network Management 2019;29(1):e2042. https://onlinelibrary.wiley.com/doi/abs/10.1002/nem.2042, e2042 nem.2042.

[121] Bull P, Austin R, Popov E, Sharma M, Watson R. Flow Based Security for IoT Devices Using an SDN Gateway. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud); 2016. p. 157–163.

[122] Zheng S. Research on SDN-based IoT Security Architecture Model. In: 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC); 2019. p. 575–579.

[123] Luo X, Yan Q, Wang M, Huang W. Using MTD and SDN-based Honeypots to Defend DDoS Attacks in IoT. In: 2019 Computing, Communications and IoT Applications (ComComAp); 2019. p. 392–395.

[124] Grigoryan G, Liu Y, Njilla L, Kamhoua C, Kwiat K. Enabling Cooperative IoT Security via Software Defined Networks (SDN). In: 2018 IEEE International Conference on Communications (ICC); 2018. p. 1–6.

[125] Lal S, Taleb T, Dutta A. NFV: Security Threats and Best Practices. IEEE Communications Magazine 2017;55(8):211–217.

[126] Velasco Esteban L, Casellas R, Llana S, Gifre L, Martinez R, Vilalta R, et al. A control and management architecture supporting autonomic NFV services. Photonic Network Communications 2019 02;37.

[127] Zerifi M, Ezzouhairi A, Boulaalam A. Overview on SDN and NFV based architectures for IoT environments: challenges and solutions. In: 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS); 2020. p. 1–5.

[128] Molina Zarca A, Bernal Bernabe J, Farris I, Khettab Y, Taleb T, Skarmeta A. Enhancing IoT security through network softwarization and virtual security appliances. International Journal of Network Management 2018;28(5):e2038. https://onlinelibrary.wiley.com/doi/abs/10.1002/nem.2038, e2038 nem.2038.

[129] Sairam R, Bhunia SS, Thangavelu V, Gurusamy M. NETRA: Enhancing IoT Security Using NFV-Based Edge Traffic Analysis. IEEE Sensors Journal 2019;19(12):4660–4671.

[130] Menezes D, Braconnot Velloso P, M B Duarte OC. An agile and effective network function virtualization infrastructure for the Internet of Things. Journal of Internet Services and Applications 2019 03;10:6.

[131] Salahuddin MA, Al-Fuqaha A, Guizani M, Shuaib K, Sallabi F. Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare. Computer 2017;50(7):74–79.

[132] Massonet P, Deru L, Achour A, Dupont S, Croisez LM, Levin A, et al. Security in Lightweight Network Function Virtualisation for Federated Cloud and IoT. In: 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud); 2017. p. 148–154.

[133] Thangavelu V, Divakaran DM, Sairam R, Bhunia SS, Gurusamy M. DEFT: A Distributed IoT Fingerprinting Technique. IEEE Internet of Things Journal 2019;6(1):940–952.

[134] Zarca AM, Bernabe JB, Skarmeta A, Alcaraz Calero JM. Virtual IoT HoneyNets to Mitigate Cyberattacks in SDN/NFV-Enabled IoT Networks. IEEE Journal on Selected Areas in Communications 2020;38(6):1262–1277.

[135] Molina Zarca A, Bernabe JB, Trapero R, Rivera D, Villalobos J, Skarmeta A, et al. Security Management Architecture for NFV/SDN-Aware IoT Systems. IEEE Internet of Things Journal 2019;6(5):8005–8020.

[136] Cziva R, Pezaros DP. Container Network Functions: Bringing NFV to the Network Edge. IEEE Communications Magazine 2017;55(6):24–31.

[137] Al-Shaboti M, Welch I, Chen A, Mahmood MA. Towards Secure Smart Home IoT: Manufacturer and User Network Access Control Framework. In: 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA); 2018. p. 892–899.

[138] Rashidi B, Fung C. CoFence: A collaborative DDoS defence using network function virtualization. In: 2016 12th International Conference on Network and Service Management (CNSM); 2016. p. 160–166.

[139] Zolotukhin M, Hämäläinen T. On Artificial Intelligent Malware Tolerant Networking for IoT. In: 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN); 2018. p. 1–6.

[140] Kim Y, Nam J, Park T, Scott-Hayward S, Shin S. SODA: A software-defined security framework for IoT environments. Computer Networks 2019;163:106889. https://www.sciencedirect.com/science/article/pii/S1389128619307522.

[141] Molina Zarca A, Bernabe JB, Trapero R, Rivera D, Villalobos J, Skarmeta A, et al. Security Management Architecture for NFV/SDN-Aware IoT Systems. IEEE Internet of Things Journal 2019;6(5):8005–8020.

[142] Alharbi T, Aljuhani A, Liu H, Hu C. Smart and Lightweight DDoS Detection Using NFV. In: Proceedings of the International Conference on Compute and Data Analysis ICCDA '17, New York, NY, USA: Association for Computing Machinery; 2017. p. 220–227. https://doi.org/10.1145/3093241.3093253.

[143] Hyun D, Kim J, Hong D, Jeong J. SDN-based network security functions for effective DDoS attack mitigation. 2017 International Conference on Information and Communication Technology Convergence (ICTC) 2017;p. 834–839.

[144] Rahman A, Islam MJ, Sunny FA, Nasir MK. DistBlockSDN: A Distributed Secure Blockchain Based SDN-IoT Architecture with NFV Implementation for Smart Cities. In: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET); 2019. p. 1–6.

[145] Krishnan P, Duttagupta S, Achuthan K. SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure. Mobile Networks and Applications 2019 12;24.

[146] Faizullah S, Khan MA, Alzahrani A, Khan I. Permissioned Blockchain-Based Security for SDN in IoT Cloud Networks. In: 2019 International Conference on Advances in the Emerging Computing Technologies (AECT); 2020. p. 1–6.

[147] Pattaranantakul M, He R, Song Q, Zhang Z, Meddahi A. NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures. IEEE Communications Surveys Tutorials 2018;20(4):3330–3368.