Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.052994

REVIEW

Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions

Ahmad Rahdari[1,6], Ahmad Jalili[2], Mehdi Esnaashari[3], Mehdi Gheisari[1,4,7,8,*], Alisa A. Vorobeva[5], Zhaoxi Fang[1], Panjun Sun[1,*], Viktoriia M. Korzhuk[5], Ilya Popov[5], Zongda Wu[1] and Hamid Tahaei[1]

[1]Institute of Artificial Intelligence, Shaoxing University, Shaoxing, 312000, China

[2]Department of Computer Engineering, Gonbad Kavous University, Gonbad-e Kavus, 49717-99151, Iran

[3]Faculty of Computer Engineering, K. N. Toosi University of Technology, Tehran, 196976-4499, Iran

[4]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, 602105, India

[5]Secure Information Technologies Department, National Research University ITMO, St. Petersburg, 197101, Russia

[6]School of Electrical and Computer Engineering, Shiraz University, Shiraz, 71946–84334, Iran

[7]Department of Computer Science and Engineering, Islamic Azad University, Damavand, 1477893855, Iran

[8]Department of R&D, Shenzhen BKD Co., Ltd., Shenzhen, 518000, China

*Corresponding Authors: Mehdi Gheisari. Email: mehdi.gheisari61@gmail.com; Panjun Sun. Email: sunpanjun2008@163.com

Received: 21 April 2024 Accepted: 26 June 2024 Published: 15 August 2024

ABSTRACT

Software-Defined Networking (SDN) represents a significant paradigm shift in network architecture, separating network logic from the underlying forwarding devices to enhance flexibility and centralize deployment. Concurrently, the Internet of Things (IoT) connects numerous devices to the Internet, enabling autonomous interactions with minimal human intervention. However, implementing and managing an SDN-IoT system is inherently complex, particularly for those with limited resources, as the dynamic and distributed nature of IoT infrastructures creates security and privacy challenges during SDN integration. The findings of this study underscore the primary security and privacy challenges across application, control, and data planes. A comprehensive review evaluates the root causes of these challenges and the defense techniques employed in prior works to establish sufficient secrecy and privacy protection. Recent investigations have explored cutting-edge methods, such as leveraging blockchain for transaction recording to enhance security and privacy, along with applying machine learning and deep learning approaches to identify and mitigate the impacts of Denial of Service (DoS) and Distributed DoS (DDoS) attacks. Moreover, the analysis indicates that encryption and hashing techniques are prevalent in the data plane, whereas access control and certificate authorization are prominently considered in the control plane, and authentication is commonly employed within the application plane. Additionally, this paper outlines future directions, offering insights into potential strategies and technological advancements aimed at fostering a more secure and privacy-conscious SDN-based IoT ecosystem.

KEYWORDS

Security; privacy-preserving; software-defined network; internet of things

1 Introduction

The Internet of Things (IoT) encompasses a framework of computing devices, objects, mechanical and electronic machines, animals, and humans equipped with distinctive identifiers, facilitating data transmission within the network without the need for direct connections between them [1]. The SDN paradigm aims to simplify network management by separating control and data planes. The SDN architecture initiates changes in IoT network communication patterns, thus shaping a new approach for powering IoT networks. With a significant amount of data in these systems, efficient traffic management and load balancing reduce the additional effects of data-flow generation. Implementing dynamic traffic management enables operators to independently monitor and coordinate bandwidth fluctuations, which is particularly advantageous for global IoT service providers anticipating exponential growth in both the number of IoT devices and the associated data. The inherent capabilities of SDN, including automation, resource provisioning, programmability, and coordination, can provide substantial value in an IoT environment [2]. Software-driven analysis and traffic control by SDN can be applied to IoT for efficient traffic management. Fig. 1 illustrates the broad concept of an SDN-enabled IoT system, along with an SDN architecture.

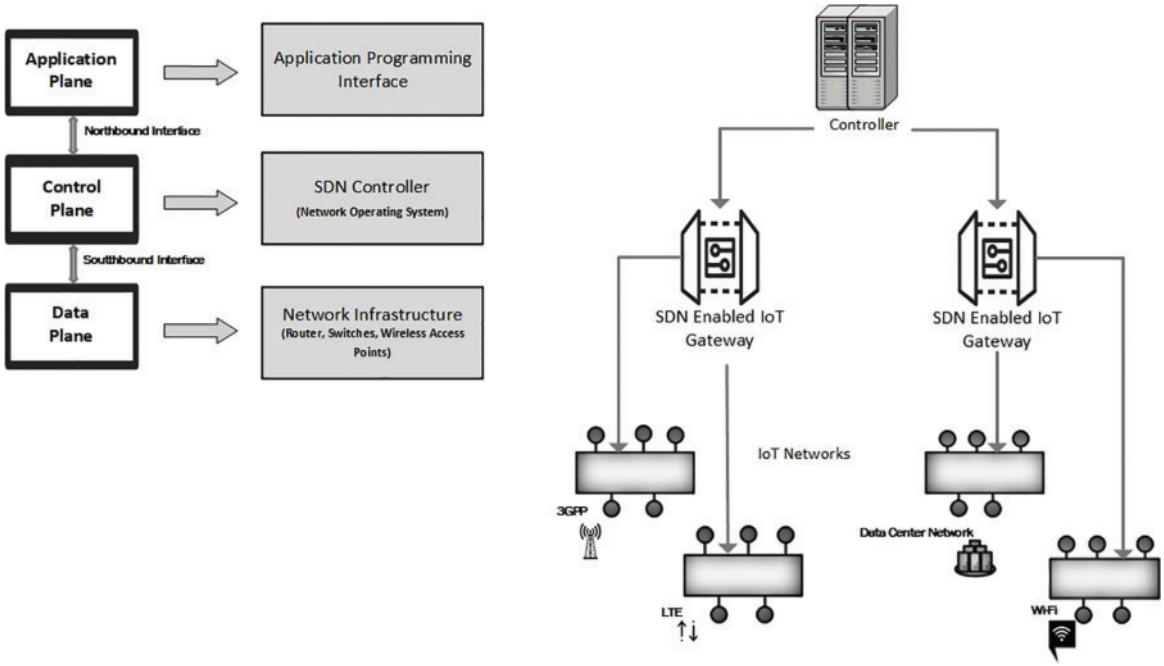

Figure 1: SDN-enabled IoT architecture

In SDN architecture, three planes exist. The lowest one is the data plane, housing SDN-enabled switches, functioning solely as packet forwarders without involvement in decision-making. Control plane, encompassing the controller, handles routing decisions and is responsible for forming routing rules upon request from the data plane. Additionally, the controller is responsible for making various decisions regarding data packets. The third plane incorporates an application programming interface that hosts applications for controlling the network. The link between the application plane and the control plane is termed the northbound interface, while the connection between the control plane and the data plane is known as the southbound interface [3]. Communication within the southbound interface is governed by protocols such as OpenFlow [4], which has become the standard since its

inception. Typically, packets are routed according to predefined flow rules listed in the flow table on an OpenFlow enabled switch. The inputs to these flow tables include actions, statistics, and match fields. As can be guessed, the actions field determines the performance of each packet, the statistics field tracks the packets matching each flow entry, and the matching field analyze the received packets.

Ensuring the secrecy of devices and networks is crucial to accommodate diverse devices, vendors, and users on a unified platform [5]. SDN enhances security in IoT deployments by providing centralized control, dynamic segmentation, policy-based access control, and deep visibility into network traffic, thereby improving the overall resilience of IoT networks against cyber threats [6,7]. However, challenges still persist in SDN-IoT, primarily stemming from evolving hacker capabilities [8,9]. This paper furnishes current insights into the ongoing research developments on security and privacy challenges in SDN-enabled IoT systems, along with approaches aimed at protecting and ensuring the stability of these systems. The resilience and integrity of SDN-enabled IoT environments against dynamic cyber threats requires a comprehensive security strategy, including device security, network infrastructure protection, data privacy, and continuous monitoring implementation.

1.1 Summary of Contributions

The contributions outlined in this review paper encompass the following:

A) Analyzing and discussing the core security and privacy challenges faced by SDN-enabled IoT systems, along with their underlying causes.
B) Exploring the main security attacks in SDN-enabled IoT and outlining the solutions adopted by researchers and industry professionals.
C) Mapping out a clear trajectory and identifying research challenges in this domain that merit attention for future exploration.

1.2 Organization

Section 2 reviews existing surveys on SDN-IoT security and emphasizes differences with them. Section 3 presents the categorization of literature on the security and privacy of SDN-IoT, highlighting key research contributions in this domain. In Section 4, the Analytical Questions (AQs) used to identify and analyze literature information is initially introduced, followed by the presentation of research outcomes in a classification table and the discussion. Finally, Section 5 concludes this paper.

2 Existing Surveys on SDN-IoT Security

Numerous studies have extensively examined the security challenges related to IoT from an SDN perspective in the literature. In [6], the authors tackled security concerns and proposed solutions for SDN-based IoT systems. This paper examined the defensive techniques employed in prior research to ensure adequate security and privacy in SDN-based IoT systems, offering a statistical analysis of the current literature. Multiple vulnerabilities and potential attacks within the IoT landscape have been outlined in [10]. This survey emphasized the critical importance of SDN security in safeguarding IoT systems and identified several areas where SDN and Network Function Virtualization (NFV) could be improved. It also shared insights gained from implementing SDN-based security methods in IoT environments and provided a comparison with conventional security measures. In [11], an examination of various SDN-based technologies was conducted, focusing on their relevance in meeting the demands of IoT across core, access, and data center networking domains. The discussion encompassed the benefits of SDN-based technologies in these areas, along with the challenges and prerequisites they entail within the scope of IoT applications. According to [12], various types of

DDoS attacks were categorized into three layers of SDN. Thereupon, this study presented an analysis of recent progress in DDoS detection and mitigation research designed to address these vulnerabilities.

The survey in [7] provided an overview of several studies that leveraged SDN features within IoT-Fog networks to address security threats specific to the IoT-oriented fog layer. It examined IoT-Fog and SDN-based IoT-Fog networks, highlighting security threats in IoT-Fog environments. Additionally, it discussed the vulnerabilities and attacks prevalent in the fog layer and outlined the most common security defense mechanisms employed in IoT-Fog networks. Reference [13] also examined the benefits of software-defined fog computing networks, taking into account the security and privacy threats inherent to the fog computing network topology and exploring potential solutions to these issues. The authors of [14] considered blockchain technology as a primary solution for securing SDN environments, discussing both its benefits and drawbacks. They examined the practicality of combining the technologies of SDN and Blockchain to ensure the availability, confidentiality, and integrity of network infrastructure. In [15], the authors noted that previous research has examined numerous security aspects of IoT, SDN, and SDN-based IoT systems, alongside their solutions utilizing various technologies, including blockchain. The study concluded that the integration of blockchain with IoT and SDN effectively addresses many security challenges.

2.1 Differences from Existing Surveys

Unlike the aforementioned surveys, our research aims to offer a comprehensive classification of the common security and privacy challenges specific to SDN-enabled IoT systems. This study examines the underlying causes and highlights the most significant methods proposed by researchers and industry experts. Our objective is to evaluate the advanced approaches employed in recent research and determine the specific plane at which each method is most effective in addressing these challenges. Identifying the underlying causes of these security and privacy challenges is also vital, since recognizing and addressing these root causes serves as the foundational step toward implementing effective security solutions. With these distinctions in mind, our study centers on identifying existing gaps to provide a clear direction for future exploration. Table 1 provides a comparison of our work with other surveys in this field.

Table 1: The differences between our work and existing surveys in security of SDN-enabled IoT

Ref.	Target planes	Security	Privacy	Challenges	Causes	Proposed solutions	Future directions	Description	Differences
[6]	All	✓	✓	✓	×	✓	✓	Review of security and privacy challenges in SDN-based IoT systems.	Our work also focuses on the causes of challenges, which is a foundational step toward implementing effective solutions and is not considered in this reference.
[7]	Fog	✓	×	✓	×	✓	×	Survey of SDN applications in IoT-Fog networks.	This reference has focused on the fog layer, whereas our work reviews the challenges and existing security solutions fo r all layers and outlines future directions.

(Continued)

Table 1 (continued)

Ref.	Target planes	Security	Privacy	Chall enges	Causes	Proposed solu-tions	Future direc-tions	Description	Differences
[10]	None	✓	✓	✓	✓	✓	✓	Overview of how SDN and NFV can enhance IoT security.	This reference has examined security methods in SDN and their applications in the IoT. In contrast, our work focuses on reviewing previous studies on SDN-enabled IoT without addressing specific IoT issues.
[11]	None	✓	✓	✓	×	✓	✓	Regular review of SDN-based IoT networks.	This reference has ignored security details while our work focuses on security and privacy challenges.
[12]	Control and data	✓	×	✓	✓	✓	✓	Survey of DDoS attacks and security methods to prevent them in SDN.	Our work is much more comprehensive and this topic is only one part of it.
[13]	Fog	✓	✓	✓	×	✓	×	Review of security and privacy methods in SDN fog computing networks.	As mentioned, our work reviews the challenges and existing security solutions for all layers and outlines future directions.
[14]	None	✓	✓	✓	×	✓	✓	Overview of utilizing blockchain in SDN.	Our work covers all the security and privacy approaches proposed in SDN-enabled IoT systems, including blockchain.
[15]	None	✓	×	✓	×	✓	✓	Survey of how blockchain integration with IoT and SDN can address security challenges.	As mentioned, our work examines all the security methods proposed in SDN-enabled IoT systems.
Our work	All	✓	✓	✓	✓	✓	✓	Comprehensive review of security and privacy challenges, their root causes, proposed solutions, and an outline of future directions.	Not applicable (NA).

3 Classification of Works in the Security and Privacy of SDN-IoT

This section provides a comprehensive review of the current studies in the realm of security and privacy for SDN-enabled IoT systems. The existing literature in this domain is systematically categorized into various sections, encompassing themes such as SDN-based IoT architectures, securing IoT-Fog networks with SDN, the implementation of blockchain, the utilization of machine learning and deep learning, encryption, hashing, and secret sharing techniques, access control, authorization, authentication, and other pertinent topics.

3.1 Securing IoT with SDN Architecture

In [16], the researchers presented a secure architecture for SDN-enabled IoT networks, focusing on safeguarding both metadata and payload. This design incorporates a centralized SDN controller, which serves as a trusted entity for secure routing and efficient management of system performance, effectively countering diverse attacks, including those involving traffic analysis or inference. The secure SDN-enabled IoT framework [17] enhanced security through the SDN control plane, offering services

such as access control, authentication, and lightweight encryption. In [18], an SDN-enabled IoT gateway was crafted to identify and address abnormal behaviors. This gateway, which monitors traffic to and from IoT devices, employs an adaptive mechanism for dynamic traffic pattern analysis, enabling the detection of malicious activities.

Expanding on this in [19], a novel architecture for IoT with SDN was proposed, aiming to establish and secure wired and wireless network infrastructures, encompassing Ad-Hoc networks and diverse network objects. In [20], SDN features like centralized logical control, traffic analysis, and dynamic flow management in remote switches were leveraged for the identification of malicious flows. Addressing security concerns, reference [21] employed NFV to enhance security in SDN-enabled IoT, comprising three main components: physical layer, middle layer, and application layer. Moreover, the SDN-enabled IoT framework with NFV implementation [22] adopted a classic three-layer architecture (service, network, and sensing layers). This underscores the significance of planning a proficient-dispersed operating system using control plane visualization methods. This approach enables the centralized control and visibility of different IoT services to diverse users. To this end, in [23], a system model was introduced to optimize the integration of SDN with IoT networks, along with a strategy to counter man-in-the-middle threats targeting IoT devices.

3.2 Securing IoT-Fog Networks with SDN

Attacks on IoT-Fog systems focus on availability, eavesdropping, and gateway management. Through SDN integration, IoT-Fog can effectively enhance security measures and mitigate conventional cloud-related challenges effectively [7]. Accordingly, a study in [24] proposed an SDN-based fog computing approach for vehicular networks, focusing on core network functions. They also implemented encryption to ensure central security, and secure and reliable communication. A defense framework in [25] utilized SDN to combat IoT-based DDoS attacks in fog-assisted cyber-physical systems. This paper leveraged fog computing, incorporating distributed computational nodes, to decrease response latency. Additionally, reference [26] introduced a multi-objective optimization strategy to balance security and resource efficiency in SDN-based IoT-Fog networks. Lastly, the integration of fog and SDN to meet security needs was elaborated in [27].

3.3 Implementation of Blockchain

In [28], the researchers integrated SDN and blockchain to address safety and privacy concerns within IoT systems enabled by SDN. They devised a routing protocol within the SDN controller specifically tailored for IoT gadgets. In [29], a decentralized entry to manipulate a mechanism based on blockchain for SDN-enabled IoT was proposed. Similarly, reference [30] applied SDN and blockchain innovations to improve the quality of present-day providers in shrewd transportation devices. They devised a fine, blockchain-based, completely secure power alternate gadget for electric-powered cars. In [31], the investigators leveraged the decentralized characteristics of a private blockchain to empower resource-constrained SDN controllers, facilitating the transparent configuration of flow rules for fog nodes and other devices within a fog-enabled IoT network. In addition, they advocated encrypting the data before their inclusion in blocks, thereby enhancing data security against unauthorized access. In [32], blockchain and SDN were utilized to bolster security of IoT through a proactive response, analysis, and traffic monitoring system. This system helps in identifying and mitigating DoS and DDoS attacks.

In [33], the synergy between blockchain and SDN was explored, with the authors addressing important demanding situations in IoT processing, including strength intake and real-time processing. In [34], the authors introduced a blockchain-primarily enabled architecture that applies a complementary collaboration and decentralized attack statistics switch among more than one SDN domain name. Moreover, reference [35] proposed a blockchain-enabled architecture that facilitates the collaborative and decentralized exchange of attack statistics across multiple SDN domains. In a look at [36], a fusion of blockchain along with SDN was employed to enhance the security level of existing IoT systems. Furthermore, in reference [37], the authors introduced a distributed SDN framework for IoT by integrating blockchain innovation. They presented a method for experimentally validating and updating rule tables, showcasing its effectiveness in terms of scalability, accuracy, and performance overhead. In [38], the authors advocated storing public keys and identities, and agreed with indices present-day IoT gadgets on a blockchain in an SDN-primarily enabled IoT network. Similarly, reference [39] introduced a secure IoT architecture leveraging blockchain technology. The implementation of this methodology is anticipated to improve the security level, performance, and functionality of NFV and SDN.

In [40], the researchers suggested a lightweight and blockchain-enabled security framework tailored for SDN to empower IoT networks in 5G communication. Furthermore, reference [41] presented a layered hierarchical architecture designed to deploy an efficient SDN-IoT framework based on blockchain. Additionally, reference [42] suggested a decision-making method to decide who to trust in IoT networks and how to manage the flow of data in IoT networks more effectively through the integration of blockchain and SDN. Moreover, reference [43] employed a trust list mechanism that outlines the conveyance of trust in the midst of stakeholders in IoT, utilizing blockchains and SDN to control traffic in edge networks of IoT devices without human intervention. In addition, reference [44] tackled defenselessness within the trust relationship between the data and control planes in SDN-controlled IoT networks by proposing an edge computing-based blockchain as a service. The proposed solution offers flow verification using an efficient edge-distributed blockchain solution. Similarly, reference [45] introduced a blockchain-enabled method deployed in SDN setups to accommodate the proliferation of IoT devices. In [46], a novel approach was proposed to make IoT more secure using a combination of blockchain and SDN technology to find and stop attacks. Blockchain was utilized to improve the attack detection model.

Another study [47] delineated a method for routing within an SDN-IoT framework with blockchain innovation in order to enhance the privacy level. In [48], a lightweight blockchain-enabled authentication component was proposed, where the credentials of the sensors were securely embedded in the SDN controller, considering the latest constraints on IoT processing capabilities and energy consumption. Addressing security concerns, reference [49] utilized both proxy re-encryption and blockchain innovations to establish secure communication in SDN-enabled IoT environments. This strategic approach aims to mitigate risks, such as DDoS attacks and data breaches, by avoiding single points of failure. Furthermore, in [50], the authors proposed a new blockchain-enabled authentication approach to make it easier to switch between different cell phone towers in 5G networks without having to repeatedly log in. Eventually, reference [51] investigated a commercial IoT scenario involving numerous SDN controllers and presented a blockchain-enabled consensus algorithm to synchronize and gather network-wide perspectives surrounded by these distinct SDN controllers.

3.4 Utilizing Machine Learning and Deep Learning

In [52], various anomaly detection classification algorithms were compared utilizing the same public dataset. The authors advocated for a new approach based on the Decision Tree algorithm,

emphasizing its potential to decrease packet handling at the edge compared to a single classifier. In [53], the authors proposed an SDN-enabled IoT anomaly identification framework aimed at the early detection of abnormal behaviors and attacks by utilizing Multi-Layer Perceptron, K-Means, and Support Vector Machine. Moreover, reference [54] applied a machine learning method to detect DDoS attacks in an SDN-IoT controller. They added a machine learning tool to the controller and created a test area to pretend cyberattacks. Reference [55] proposed a detection approach utilizing learning algorithms and features from OpenFlow packets to recognize attack traffic in the data and control planes. Similarly, reference [56] introduced an SDN-enabled secure IoT system for the early identification and mitigation of abnormal behaviors and attacks. Machine learning was employed in the SDN controller to observe and learn how IoT devices behave. In [57], researchers presented a method for DDoS attack detection in SDN, focusing on data collection and the analysis of traffic types, particularly emphasizing data entropy.

In [58], the researchers presented a machine learning model coupled with SDN to better predict the extent to which network resources will be used and to improve sensor data delivery. They proposed a centralized SDN to counter network vulnerabilities in the midst of expanded sensors at minimum cost. In [59], an algorithm was presented to enhance secure routing in IoT by employing a system to make decisions about how to connect network components and transfer data based on machine learning and SDN. Furthermore, reference [60] introduced a multilayer classifier for DDoS attack identification by utilizing Support Vector Machine. The study in [61] presented machine learning techniques to detect and categorize low-rate collision flows in SDN-enabled 5G networks. They utilized Decision Tree, K-Means, and Feed Forward Neural Network algorithms for this purpose. Likewise, reference [62] utilized machine learning to detect and defend against DDoS attacks in IoT environments by integrating SDN controllers. An investigation into the impact of DDoS attacks on the controller layer in SDN and its system performance reduction was also conducted in [63].

Building on this understanding, a framework that is SDN-enabled and specifically tailored to implement deep learning procedures was introduced in [64]. The main objective of this framework is to protect the IoT environment from a range of cybersecurity threats, encompassing brute-force attacks, DDoS incidents, bot assaults, malware, and infiltration. Reference [65] introduced an improved Crow-look algorithm utilizing deep learning in an SDN-IoT-type network to reliably detect and classify cyberattacks. In [66], an SDN-based security mechanism was introduced to identify and mitigate DDoS attacks within IoT networks. This method involves utilizing a trained Multi-Layer Perceptron for attack detection, followed by the classification of detected attacks. Furthermore, reference [67] employed advanced deep learning strategies, such as Long Short-Term Memory (LSTM), to detect and mitigate the impact of DDoS attacks on SDN controllers, showcasing a commitment to robust security measures in the face of evolving cyber threats. Similarly, reference [68] introduced an architecture based on LSTM for efficient multiclass classification within SDN-enabled intrusion detection systems in IoT networks. The significance of privacy preservation was underscored in [69], where deep learning methodologies were employed to handle sensitive information more robustly. The authors of [70] introduced a deep reinforcement learning system for monitoring traffic in the SDN-IoT. The aim is to enhance the learning performance at edge nodes and enable detailed traffic analysis, including intrusion detection systems.

The efficiency of communication between controllers and switches in SDN-based networks was significantly enhanced in [71]. This enhancement contributes to elevating the system performance and user usability. Navigating the challenges of resource-constrained IoT scenarios, reference [72] employed deep learning techniques explicitly designed to identify threats while being mindful of the limitations imposed by resource constraints. In a medical IoT domain based on SDN, reference [73]

implemented a deep learning approach to effectively identify and mitigate malware, contributing to the overall system's safety. Additionally, reference [74] utilized a deep learning classification method, specifically targeting anomaly identification in an IoT setting, taking into consideration the limitations associated with available resources. Reference [75] proposed a secure framework for SDN-based IoT, incorporating a system that uses Restricted Boltzmann Machines to detect intrusions. Finally, reference [76] presented a sophisticated intrusion prevention framework grounded in deep learning principles. This system is strategically designed to counteract DDoS attacks, brute-force attacks, and the incursion of malicious packets within an SDN environment.

3.5 Encryption, Hashing, and Secret Sharing Techniques

In [77], the authors analyzed various encryption algorithms, highlighting why existing algorithms are unsuitable for direct application in software-defined industrial IoT edge networks. Subsequently, they introduced a novel encryption algorithm tailored to this context. Meanwhile, reference [78] proposed a simplified handshake protocol aimed at reducing the computational burden on IoT devices in device-to-device communications based upon SDN. This protocol involves a controller making a secret key on its own, which is then encrypted and distributed to the both communicating IoT devices. Additionally, reference [79] presented an attribute-based encryption scheme designed to ensure secure data communication within an SDN industrial IoT communication model. Moreover, reference [80] proposed a novel approach to streamline the transport layer security handshake protocol based on SDN. Their method involves a controller that dynamically generates the premaster secret and distributes it to the IoT devices through an encrypted channel.

In [81], a secure multipath routing scheme focused on energy efficiency was suggested, incorporating a secret sharing scheme to bolster security while ensuring energy efficiency. Reference [82] presented a method for securing data transmission among IoT devices in smart cities. This approach combines a secret-sharing mechanism with SDN techniques to securely transport IoT data. Additionally, reference [83] introduced a secret-sharing-based distributed cloud system aimed at privacy protection within IoT environments. Moreover, reference [84] proposed a secure service path validation method that employs Batch Hashing and Tag Verification to improve the security of SDN-IoT systems. Likewise, reference [85] suggested a hash-based dispersed capacity methodology for Flow Tables within SDN-IoT Systems.

3.6 Access Control, Authorization, and Authentication

In response to the challenges in establishing reliable connections among high-speed IoT devices, reference [86] presented a novel privacy-preserving approach for IoT networks. This scheme utilizes mutual authentication across the certificate authorities. Drawing on the core attributes of SDN, reference [87] developed a simple process to authenticate IoT devices and secure network flows. In [88], a secure multifactor authentication protocol was proposed for healthcare services utilizing cloud-based SDN. Furthermore, reference [89] devised a dedicated SDN-based smart home communication scheme to ensure privacy. This scheme focuses on providing authentication for users and smart devices as well as privacy for data and user queries through lightweight authentication and searchable query protocols. Another study [90] offered an innovative and efficient handover authentication scheme based on SDN for utilizing versatile gadgets in computing within cyber-physical frameworks. Furthermore, reference [91] presented a secure authentication framework for SDN-IoT networks utilizing Bliss-B and Keccak-256 algorithms, whereas reference [92] proposed a secure access control scheme for SDN-based industrial IoT. Reference [93] also introduced a security architecture aimed

at defining and enforcing security profiles within SDN-based IoT systems by employing an attribute-based access control approach. Similarly, reference [94] presented an access control mechanism based on SDN for collaborative networks between cloud and edge computing environments. Moreover, reference [95] suggested a role-based access control system enabled by SDN, coupled with a trust-based model to enhance virtual machine security within cloud environments.

3.7 Attacks and Other Security Challenges in SDN-IoT

An investigation into privacy protection within smart grids integrated with software-defined networks was detailed in [96]. This framework incorporates dual privacy measures and formulates a distributed privacy-optimization algorithm to minimize network costs. Similarly, reference [97] proposed an approach involving IP analysis and anomaly behaviors to detect DDoS attacks. In [98], the authors employed a method using OpenFlow to detect and prevent DDoS attacks by targeting malicious packets at switches before reaching the control panel. Additionally, reference [99] introduced an approach to mitigate DDoS threats through SDN, enabling the prediction of attack traffic drops and effective traffic mitigation measures. Damage mitigation and defense strategies against DDoS attacks were reviewed in [100], proposing a cost-effective approach to reduce controller burdens. Meanwhile, reference [101] suggested hybrid preventive defense methods that combine moving target defense tactics with cyber deception strategies to mislead potential attackers. The authors of [102] investigated the energy efficiency of anomaly detection by introducing dynamic strategy selection and a lightweight detection module.

In [103], researchers proposed a security solution to preemptively identify attacker-end hosts before the submission of flow requests to the SDN controller. The examination of DDoS attacks targeting the control plane was detailed in [104], with 5G as a benchmark for experiments. Another study [105], analyzed a Multi-Hop New Link attack and its prevention within a hybrid SDN environment. Exploration of abnormal behavior detection across various IoT programs, examining the relationship and impact of distributed rules within SDNs, was discussed in [106]. Reference [107] focused on traffic management in IoT environments, and predicted and monitored malicious traffic at IoT gateways. Furthermore, abnormality detection in diverse IoT applications, such as smart homes and healthcare, was addressed in [108], and the identification and mitigation of attack effects using SDN. In a related vein, reference [109] presented a roadmap for enhancing smart home security through SDN, and an extension of this approach to smart health applications, emphasizing edge processing, was detailed in [110]. A novel framework centered on certificate trust to mitigate Crossfire attacks through the utilization of SDN for IoT was introduced in [111].

4 Discussion

The principal objective of this paper is to present comprehensive knowledge derived from the literature within the research field in an organized manner. Additionally, the paper serves the dual purpose of identifying extant research gaps and subsequently recognizing potential avenues for future researches. To achieve this, the methodology employed incorporates Analytical Questions (AQs).

This paper elucidates the following AQs, providing clear and concise answers to each:

AQ1: What are the predominant challenges facing the planes in SDN-enabled IoT that have been addressed in the literature?

AQ2: What are the principal causes of challenges mentioned in the literature?

AQ3: Which security and privacy methods have been implemented to overcome the challenges in SDN-enabled IoT applications?

AQ4: What are the identified research gaps and open questions that pave the way for future research directions?

This paper centers on data collection from selected studies, aligning with predefined AQs. Following a comprehensive analysis of the chosen papers, the classification results, based on the extracted data, provide answers to all the AQs. The summary of findings is depicted in Table 2.

Table 2: Summary of the security and privacy challenges and proposed solutions in SDN-enabled IoT

Ref.	Target planes	Challenges	Causes	Proposed solutions
[16]	Data	Meta-data	Meta-data attack occurs due to traffic analysis or inference from data sent directly on a public channel.	Encrypting both payload and meta-data and employing the SDN controller as a dependable middle person to guarantee secure routing.
[18]	Control and data	DDoS	Resources are inaccessible due to malicious traffic.	Identifying abnormal behaviors and addressing them through measures such as blocking, forwarding, and implementing Quality of Service protocols.
[19]	Control	DoS	Using just one controller can result in a DoS.	Security policies are enforced and monitored through the use of multiple security controllers.
[21]	Control	Communication hijacking and intrusion	Weak authentication is the cause of the attack.	Putting software-defined storage and security into a control model that is software-based.
[26]	Control and data	DDoS	To interfere with the operation of computational nodes, a malicious node generates numerous half-open TCP connections.	Managing resources with the help of the combination of a multi-objective particle swarm optimization and fuzzy logic methods.
[27]	All	DoS and DDoS	The exponential growth of connected devices in IoT contributes to the escalation of attacks.	Integration of fog and SDN in IoT to fulfill security requirements.
[28]	Control	Network manipulating and policy enforcement	Hidden influences are imposed on users through the data interface by targeting and exploiting decision-making vulnerabilities.	SDN controllers and IoT gadgets are communicating using both private and public blockchains, along with an efficient authentication mechanism.
[31]	Application	App manipulation, accountability, and information leakage	The absence of authentication, and integration in SDN standards causes this to occur.	Taking advantage of the decentralized nature of a private blockchain and encrypting data before including it in blocks.
[32]	Application and control	DoS and DDoS	Malicious traffic, flow timeouts, and flow rules lead to these attacks.	Proactive traffic monitoring, analysis, and response systems are used to bolster security.
[35]	Control	DDoS	IoT networks can become part of a botnet without proper prevention.	Collaborative and decentralized exchange of attack statistics across multiple SDN domains is made possible by a blockchain-enabled architecture with distributed botnet detection.
[36]	Control and data	Flow rule conflicts	A malicious program changes the rules for how data is sent over the internet so that it can change the IP address of the data packets.	A novel method is being suggested to update the flow rule table, leveraging blockchain technology to securely authenticate the flow rule and validate a replica of the flow rule table.

(Continued)

Table 2 (continued)

Ref.	Target planes	Challenges	Causes	Proposed solutions
[37]	All	Privacy	Managing user privacy while simultaneously preventing various attacks at different planes within the SDN architecture poses significant challenges for the administrator.	Applying a distributed SDN architecture for IoT by integrating blockchain for updating and validating rule tables.
[38]	Application and control	DDoS	A major reason is the separation of the planes.	Storing the identities and public keys and recording the indicators of the current IoT devices on a blockchain.
[42]	Application and control	Internet-scale and DDoS	Failure to confirm the authenticity of IoT services, and bankruptcy to prevent unwanted traffic from devices leads to this attack.	Defining a trust distribution through the use of a trust list mechanism in blockchain.
[46]	Control and data	Flow rule conflicts	SDN logical centralization of controllers and global network overview increased the network communication security challenges.	A decentralized security architecture is utilized for dynamic updates to attack detection.
[47]	Control and data	Network manipulating	Serious concerns may arise due to malicious or unintentional interference with IoT data.	The incorporation of SDN security architecture and blockchain led to a new secure routing protocol with the cluster structure.
[48]	Application and control	Impersonation and spoofing	Perpetrators can execute these attacks using brute-force tactics owing to the limited number of credentials available.	Sensor credentials are stored within the SDN controller thanks to the introduction of a blockchain-based authentication mechanism that takes into account resource limitations.
[50]	All	Privacy	Inefficient authentication handover procedures could heighten the likelihood of encountering user privacy challenges.	Applying a blockchain-based authentication handover method, aiming to eliminate unnecessary reauthentication during repeated handovers between heterogeneous cells in 5G networks.
[52]	Control and data	Synthetic attack traffic	Due to the frequent absence of visibility and standardized management systems for updates, end devices become vulnerable when connected to the Internet.	Employing a Decision Tree-based machine learning approach to identify irregularities in the traffic of an IoT network interconnected via an SDN.
[55]	Control and data	DDoS	Detecting low-traffic DDoS attacks in SDN-IoT poses a greater challenge due to the distinct behaviors compared to traditional networks.	A detection approach utilizing learning algorithms and features from OpenFlow packets is presented to identify attack traffic.
[60]	Control	DDOS	The proliferation of diverse entities within the SDN escalates the threat of DDoS attacks, posing a significant danger to IoT systems.	Utilizing support vector machine as a multi-layer classifier for DDoS attack detection.
[61]	Control and data	Flow rule conflicts	When the flow table becomes overloaded and experiences abuse, a low-rate flow table is activated, leading to the installation of collision flow rules and the excessive consumption of existing flow table capacity.	Using Feed Forward Neural Network, K-Means, and Decision Tree algorithms to detect and categorize low-rate collision flows.
[64]	All	Benign, bot, DDoS, brute-force, and infiltration	The extensive connectivity and the diverse array of devices within SDN-IoT networks render them susceptible to various cyberattacks, leading to potential data breaches.	Devising a customized SDN solution empowered with deep learning techniques to safeguard the IoT ecosystem against various cybersecurity threats.

(Continued)

Table 2 (continued)

Ref.	Target planes	Challenges	Causes	Proposed solutions
[67]	All	DDoS	The centralized controller in SDN serves as a single point of attack.	Employing deep learning methodologies to identify and mitigate the effects of DDoS attacks within an SDN controller.
[69]	All	Privacy	Network operators are hesitant to reveal intricate resource availability and network topology specifics, thus elevating the necessity for preserving privacy in service function chaining within a multi-domain scenario.	Utilizing a deep learning method in the authentication procedure to enhance privacy levels.
[72]	All	DDoS	The attacker takes into account resource limitations and gains control over an entire network by inundating it with a substantial volume of malicious traffic.	Using deep learning techniques to identify threats while being mindful of the limitations imposed by resource constraints.
[74]	All	DoS, brute-force, and botnet	The large number of users, along with the huge influx of data and the heterogeneity of devices, make detecting anomalies and attacks a difficult task.	A deep learning approach is utilized for anomaly detection.
[76]	All	DDoS, brute-force, and malicious packets	The OpenFlow SDN switch route the attacking traffic towards the victim hosts based on the preconfigured flow table.	A sophisticated intrusion detection grounded in deep learning principles is proposed to prevent the attacks.
[79]	Data	Meta-data	Lack of an effective design required for secure data communication to fulfill the scalable and flexible demands of generated data.	Applying an attribute-based encryption scheme designed to ensure secure data communication.
[81]	Data	Network manipulation, flow rule conflicts, and configuration errors	Insufficient security measures are in place while aiming to ensure energy efficiency.	Devising a secure multipath routing approach that incorporates a secret sharing scheme to bolster security while ensuring energy efficiency.
[83]	All	Privacy	The rapid growth of smart cities leads to a substantial increase in data volume, resulting in various challenges in cloud infrastructure, including privacy concerns.	Employing a secret sharing-based distributed cloud system aimed at privacy protection.
[86]	All	Privacy	The exponential growth of network devices is stretching the capabilities of access layers and introducing privacy concerns.	Using an SDN-based privacy scheme that leverages mutual authentication across certificate authorities.
[88]	Application	DoS, Man in the Middle, replay, and phishing	Centralizing data increases its susceptibility to attacks.	A secure multi-factor authentication protocol is proposed for healthcare services utilizing cloud-based SDN.
[89]	All	Privacy	The transmission of plain text data along with the absence of authentication enables attackers to access user profiles, understand user behavior, and potentially inject malware into devices.	Focusing on providing authentication for users and smart devices, as well as privacy for data and user queries, through lightweight authentication and searchable query protocols.
[90]	Application	Man in the Middle and replay	For applications in mobile edge computing in cyber-physical systems, traditional authentication schemes, known for their low performance, are no longer suitable.	Utilizing an innovative and efficient handover authentication scheme based on SDN.

(Continued)

Table 2 (continued)

Ref.	Target planes	Challenges	Causes	Proposed solutions
[92]	Control	Man in the Middle and forgery	In an SDN-IoT environment, communication between entities is susceptible to numerous threats, largely due to insecure wireless channels.	Devising a secure user access control mechanism for SDN-enabled industrial IoT.
[95]	Control	Unauthorized access and data theft	Cloud environments are susceptible to attacks from both external sources and internal users.	Employing a role-based access control system enabled by SDN, coupled with a trust-based model.
[100]	Control	DDoS	Mitigating DDoS attacks using firewalls is challenging due to the attackers establishing multiple connections to the victim from various IP addresses.	Applying a cost-effective approach to reduce controller burdens.
[103]	Control	Malicious packets	Lack of a suitable solution to deal with the attacks of malicious end hosts in the SDN environment.	Using a security architecture to preemptively identify attacker-end hosts before submission of flow requests to the SDN controller.
[107]	Control	Malicious packets and malicious traffic injection	Compromised IoT devices inundate the application servers, resulting in widespread service disruption.	Focusing on traffic management in IoT environments, and predicting and monitoring malicious traffic at SDN-enabled IoT gateways.

4.1 AQ1: What Are the Predominant Challenges Facing the Planes in SDN-Enabled IoT That Have Been Addressed in the Literature?

A comprehensive review of the literature shows that at the application plane, notable security threats include accountability issues, application manipulation, information leakage, impersonation, and communication hijacking. Concerning the control plane, significant security challenges involve conflicts of flow rules, policy enforcement, network manipulation, and unauthorized access. In the data plane, common security challenges include network manipulation, conflicts in flow rules, configuration errors, and metadata attacks. Additionally, privacy concerns, malicious packets, and DoS and DDoS attacks are recognized as challenges spanning all planes of the SDN-enabled IoT system. Fig. 2 illustrates common security challenges in different planes of SDN-enabled IoT systems.

4.2 AQ2: What Are the Principal Causes of Challenges Mentioned in the Literature?

It can be seen that the primary causes of security challenges in SDN-enabled IoT systems include the proliferation of data and devices, vulnerabilities in controllers—especially pronounced in instances where a single controller is relied upon—the segregation of planes, malicious traffic and packets, traffic analysis or inference, inadequate authentication mechanisms, data integrity issues, legal constraints, compatibility challenges with flow rules, scalability limitations, insecure wireless communication channels, and configuration discrepancies. This paper undertakes an analysis of security and privacy threats and their root causes, culminating in a summary of findings depicted in Table 2, illustrating their ramifications across SDN planes.

4.3 AQ3: Which Security and Privacy Methods Have Been Implemented to Overcome the Challenges in SDN-Enabled IoT Applications?

Recent advancements include exploring blockchain technology for recording transactions to enhance security and privacy, as well as utilizing machine learning and deep learning techniques to detect and mitigate the impacts of DoS and DDoS attacks. The categorization of the collected papers clearly states that encryption and hashing techniques are currently prevalent in the data plane,

while access control and certificate authorization are predominantly considered in the control plane. Authentication methods are commonly employed within the application plane.

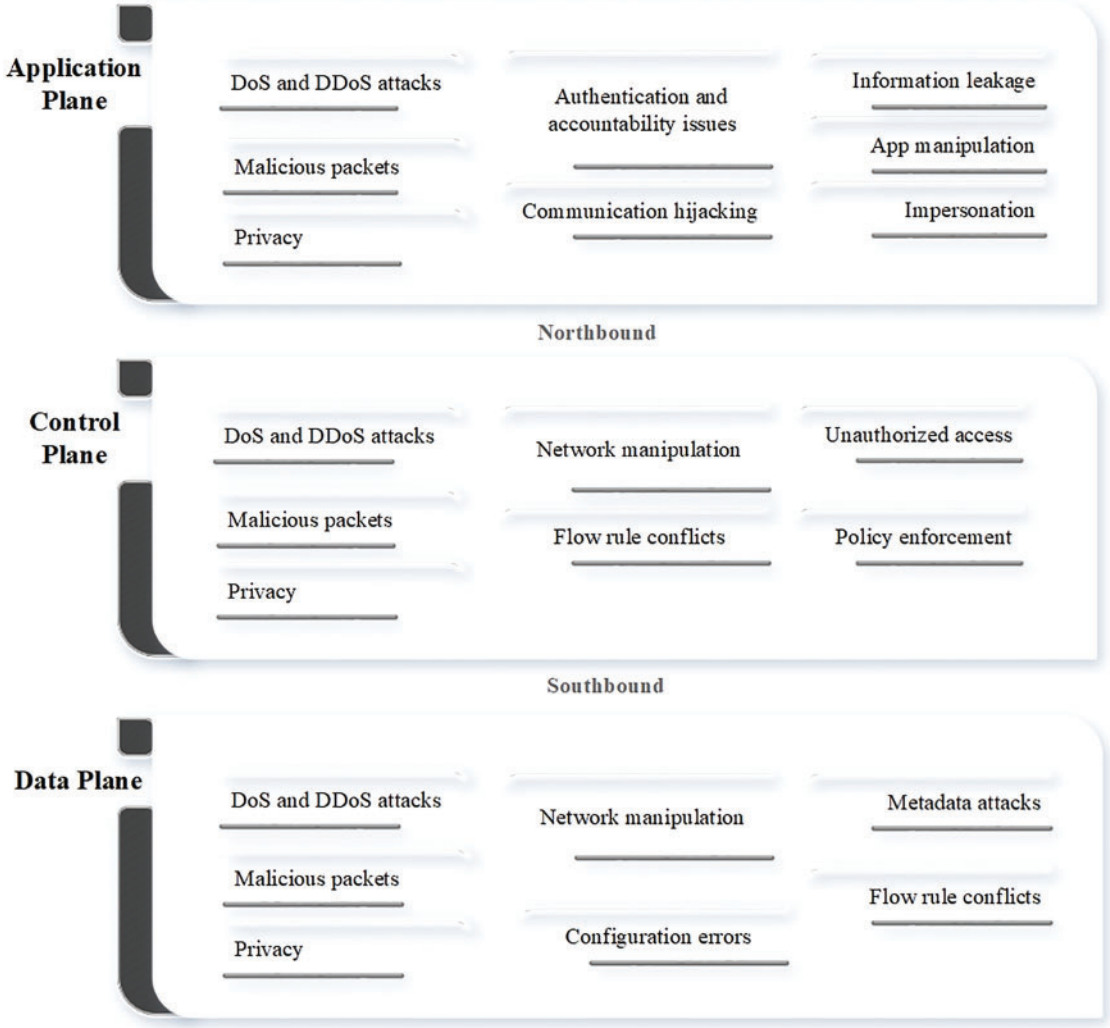

Figure 2: Security challenges in SDN-enabled IoT systems

4.4 AQ4: What Are the Identified Research Gaps and Open Questions That Pave the Way for Future Research Directions?

To achieve an acceptable level of security and privacy in SDN-enabled IoT systems, it is crucial to address challenges across all three layers simultaneously. This involves creating unified protocols and standards to ensure consistent security measures across all layers, thereby preventing exploitable gaps. Additionally, it requires investigating advanced threat detection systems capable of real-time monitoring and analysis of data across all layers. Developing automated tools and frameworks for the deployment, management, and updating of security policies and measures can also be beneficial. Automation can rapidly address new threats, reduce the manual effort required for security management, and ensure consistent application of security measures.

Although security has received considerable attention, privacy protection needs more focus from researchers. Techniques such as differential privacy and homomorphic encryption can help protect data privacy while still allowing for necessary data analysis and processing. Integrating blockchain components, known for their distributed nature, with the centralized nature of SDN in IoT networks to uphold security and privacy requires more coordination and adaptation. Given the importance of machine learning and deep learning methods in identifying malicious packets, DoS, and DDoS attacks, there is a need for low-overhead solutions for processing these methods. Enhancing lightweight encryption and energy-efficient security protocols can bolster security in these systems without significantly draining device resources. Therefore, it is essential to explore resource-efficient security mechanisms tailored to the constraints of IoT devices, such as limited processing power and battery life.

Nowadays, SDN-IoT has become more flexible with the integration of fog computing. Researchers need to also focus on several key areas within this combined field. Firstly, optimizing resource management and allocation in fog computing environments can enhance data processing efficiency. Additionally, scalable solutions must be explored to support the increasing number of IoT devices, ensuring seamless connectivity and interoperability. Furthermore, developing energy-efficient secure algorithms and protocols is essential to minimize the power consumption of IoT devices and Fog nodes.

Securing IoT networks through the development of novel SDN architectures can be useful. Additionally, implementing new methods like secret sharing and data minimization can substantially alleviate privacy concerns. As data generation proliferates with the expansion of IoT networks, adopting data minimization approaches becomes imperative. Minimizing the amount of data collected, stored, and shared by smart devices simplifies the protection of users' personal information. Processing collected data with data minimization models not only enhances data privacy but also facilitates efficient data storage, easier data management, and heightened awareness of data accuracy.

Furthermore, processing speed and latency pose significant challenges in SDN-enabled IoT systems, and extensive research is urgently needed to address security and privacy challenges, while ensuring service availability and support for high mobility. For real-time applications in the SDN-IoT, such as video streaming, which requires fast response and processing times, researchers should also consider service availability in the network architecture. In addition, most IoT devices, including smartphones, drones, and cars, are constantly moving, connecting, and disconnecting to and from the network, leading to numerous security issues. Consequently, specialized secure algorithms and protocols must be developed to address these challenges effectively.

5 Conclusion

The critical nature of security and privacy challenges in IoT systems with SDN, compounded by real-time applications and resource limitations, prompted an investigation and analysis in this study. To reach a comprehensive discussion, the most important existing studies were categorized based on the types of challenges, causes, proposed solutions, and target layers. Specifically, the literature analysis revealed that at the application plane, major security threats include accountability issues, application manipulation, information leakage, impersonation, and communication hijacking. The control plane faces challenges, such as conflicts in flow rules, policy enforcement, network manipulation, and unauthorized access. Data planes encounter issues such as network manipulation, flow rule conflicts, configuration errors, and metadata attacks. Additionally, privacy concerns, malicious packets, and DoS and DDoS attacks affect all the planes of the system. Therefore, this paper also summarized the existing security solutions proposed by researchers for each plane and categorized these methods based

on the plane for which they are most commonly used. Finally, this paper provided suggestions for future research to mitigate security attacks with the aim of providing more reliable and robust security solutions for SDN-enabled IoT systems. This thorough review is expected to benefit researchers and policymakers by developing effective security strategies.

Acknowledgement: The anonymous reviewers of Computers, Materials & Continua journal are highly acknowledged for their valuable comments, which enhanced the quality of this paper.

Funding Statement: This work was supported by National Natural Science Foundation of China (Grant No. 62341208), Natural Science Foundation of Zhejiang Province (Grant Nos. LY23F020006 and LR23F020001). Moreover, it has been supported by Islamic Azad University with the Grant No. 133713281361.

Author Contributions: Ahmad Rahdari was responsible for the ideation, research, development, and writing of the initial draft. Ahmad Jalili reviewed the manuscript and provided comments to enhance the first version. Mehdi Gheisari and Panjun Sun, as the corresponding authors, conceptualized and coordinated the study. Zongda Wu and Zhaoxi Fang were the supervisors of this project. Hamid Tahaei supported us in revision and comments. Alisa A. Vorobeva, Ilya Popov and Viktoriia M. Korzhuk were responsible for analysis. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: This paper did not utilize or generate any datasets.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Safaei Yaraziz, A. Jalili, M. Gheisari, and Y. Liu, "Recent trends towards privacy-preservation in Internet of Things, its challenges and future directions," *IET Circuits, Devices & Syst.*, vol. 17, no. 2, pp. 53–61, 2023. doi: 10.1049/cds2.12138.

[2] M. A. Al-Shareeda, A. A. Alsadhan, H. H. Qasim, and S. Manickam, "Software defined networking for internet of things: Review, techniques, challenges, and future directions," *Bull. Electr. Eng. Inform.*, vol. 13, no. 1, pp. 638–647, 2024. doi: 10.11591/eei.v13i1.6386.

[3] M. Hussain, N. Shah, R. Amin, S. S. Alshamrani, A. Alotaibi and S. M. Raza, "Software-defined networking: Categories, analysis, and future directions," *Sensors*, vol. 22, no. 15, pp. 5551, 2022. doi: 10.3390/s22155551.

[4] "SDN/OpenFlow|Flowgrammable," Accessed: Mar. 27, 2018. [Online]. Available: https://flowgrammable.org/sdn/

[5] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy internet of things: A survey on trust management applications and schemes," *Comput. Commun.*, vol. 160, no. 15, pp. 475–493, 2020. doi: 10.1016/j.comcom.2020.06.030.

[6] H. Ahmadvand, C. Lal, H. Hemmati, M. Sookhak, and M. Conti, "Privacy-preserving and security in SDN-based IoT: A survey," *IEEE Access*, vol. 11, pp. 44772–44786, 2023. doi: 10.1109/ACCESS.2023.3267764.

[7] S. Javanmardi, M. Shojafar, R. Mohammadi, M. Alazab, and A. M. Caruso, "An SDN perspective IoT-Fog security: A survey," *Comput. Netw.*, vol. 229, no. 4, pp. 109732, 2023. doi: 10.1016/j.comnet.2023.109732.

[8] M. S. Farooq, S. Riaz, and A. Alvi, "Security and privacy issues in software-defined networking (SDN): A systematic literature review," *Electronics*, vol. 12, no. 14, pp. 3077, 2023.

[9] O. Yurekten and M. Demirci, "SDN-based cyber defense: A survey," *Future Gen. Comput. Syst.*, vol. 115, pp. 126–149, 2021.
[10] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 812–837, 2019. doi: 10.1109/COMST.2018.2862350.
[11] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for internet of things: A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1994–2008, 2017. doi: 10.1109/JIOT.2017.2746186.
[12] M. P. Singh and A. Bhandari, "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Comput. Commun.*, vol. 154, no. 2, pp. 509–527, 2020. doi: 10.1016/j.comcom.2020.02.085.
[13] A. Alamer, "Security and privacy-awareness in a software-defined fog computing network for the Internet of Things," *Opt. Switching Netw.*, vol. 41, no. 3, pp. 100616, 2021. doi: 10.1016/j.osn.2021.100616.
[14] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020. doi: 10.1109/ACCESS.2020.2964751.
[15] N. Indrason and G. Saha, "Exploring blockchain-driven security in SDN-based IoT networks," *J. Netw. Comput. Appl.*, vol. 224, no. 4, pp. 103838, 2024. doi: 10.1016/j.jnca.2024.103838.
[16] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the internet of things," in *Proc. IEEE 12th Int. Conf. Mobile Ad Hoc Sens. Syst. (MASS)*, Dallas, TX, USA, 2015.
[17] S. Choi and J. Kwak, "Enhanced SDIoT security framework models," *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 5, pp. 4807804, 2016. doi: 10.1155/2016/4807804.
[18] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for IoT devices using an SDN gateway," in *IEEE 4th Int. Conf. Future Int. Things and Cloud (FiCloud)*, Vienna, Austria, 2016.
[19] O. Flauzac, C. González, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," in *IEEE 29th Int. Conf. Ad. Inform. Netw. Appl. Workshops*, Gwangiu, Republic of Korea, 2015.
[20] M. E. Ahmed and H. Kim, "DDoS attack mitigation in Internet of Things using software defined networking," in *IEEE Third Int. Conf. Big Data Comput. Serv. Appl. (BigDataService)*, 2017.
[21] Y. Jararweh, A. Mahmoud, A. Darabseh, E. Benkhelifa, M. Vouk and A. Rindos, "SDIoT: A software defined based internet of things framework," *J. Ambient Intell. Humaniz. Comput.*, vol. 6, no. 4, pp. 453–461, 2015. doi: 10.1007/s12652-015-0290-y.
[22] J. Li, E. Altman, and C. Touati, "A general SDN-based IoT framework with NVF implementation," *ZTE Communications*, vol. 13, no. 3, pp. 42–45, 2015.
[23] A. A. Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving Internet of Things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, pp. 8, 2020. doi: 10.3390/computers9010008.
[24] M. Arif, G. Wang, V. E. Balas, O. Geman, A. Castiglione and J. Chen, "SDN based communications privacy-preserving architecture for VANETs using fog computing," *Veh. Commun.*, vol. 26, no. 3, pp. 100265, 2020. doi: 10.1016/j.vehcom.2020.100265.
[25] M. Snehi, A. Bhandari, and J. Verma, "Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems," *Comput. & Secur.*, vol. 139, no. 3, pp. 103702, 2024. doi: 10.1016/j.cose.2024.103702.
[26] S. Javanmardi, M. Shojafar, R. Mohammadi, A. Nazari, V. Persico and A. Pescapè, "FUPE: A security driven task scheduling approach for SDN-based IoT-fog networks," *J. Inf. Secur. Appl.*, vol. 60, no. 4, pp. 102853, 2021. doi: 10.1016/j.jisa.2021.102853.
[27] S. Prabavathy and V. Supriya, "SDN based cognitive security system for large-scale Internet of Things using fog computing," in *Int. Conf. Emerg. Tech. Comput. Intell. (ICETCI)*, Hyderabad, India, 2021.
[28] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, K. K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 625–638, 2020. doi: 10.1109/TSC.2020.2966970.

[29] W. Ren, Y. Sun, H. Luo, and M. Guizani, "SILedger: A blockchain and ABE-based access control for applications in SDN-IoT networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 4, pp. 4406–4419, 2021. doi: 10.1109/TNSM.2021.3093002.

[30] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar and K. K. R. Choo, "BEST: Blockchain-based secure energy trading in SDNenabled intelligent transportation system," *Comput. & Secur.*, vol. 88, no. 1, pp. 288–299, 2019. doi: 10.1016/j.cose.2019.05.006.

[31] S. Misra, P. K. Deb, N. Pathak, and A. Mukherjee, "Blockchain-enabled SDN for securing fog-based resource-constrained IoT," in *IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Toronto, Canada, 2020.

[32] M. Ibrahim *et al.*, "SDN based DDos mitigating approach using traffic entropy for IoT network," *Comput. Mater. Contin.*, vol. 70, no. 3, pp. 5651–5665, 2022. doi: 10.32604/cmc.2022.017772.

[33] M. J. Islam *et al.*, "Blockchain-SDN based energy-aware and distributed secure architecture for IoT in smart cities," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3850–3864, 2021. doi: 10.1109/JIOT.2021.3100797.

[34] A. Z. El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An intra- and inter-domain ddos mitigation scheme based on blockchain using SDN and smart contract," *IEEE Access*, vol. 7, pp. 98893–98907, 2019. doi: 10.1109/ACCESS.2019.2930715.

[35] Q. Shafi and A. Basit, "DDoS botnet prevention using blockchain in software defined Internet of Things," in *16th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, 2019.

[36] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, 2017. doi: 10.1109/MCOM.2017.1700041.

[37] R. Shashidhara, N. Ahuja, M. Lajuvanthi, S. Akhila, A. K. Das and J. J. P. C. Rodrigues, "SDN-chain: Privacy-preserving protocol for software defined networks using blockchain," *Secur. Priv.*, vol. 4, no. 6, pp. 102647, 2021. doi: 10.1002/spy2.178.

[38] S. Hameed *et al.*, "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology," *IEEE Sens. J.*, vol. 21, no. 6, pp. 8716–8733, 2021. doi: 10.1109/JSEN.2021.3052009.

[39] A. Hakiri and B. Dezfouli, "Towards a blockchain-SDN architecture for secure and trustworthy 5G massive iot networks," in *Proc. 2021 ACM Int. Work. Softw. Defined Netw. & Netw. Fun. Virtual. Secur.*, New York, NY, USA, 2021.

[40] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Bloc-Sec: Blockchain-based lightweight security architecture for 5G/B5G enabled SDN/NFV cloud of IoT," in *IEEE 20th Int. Conf. Commun. Technol. (ICCT)*, Nanning, China, 2020.

[41] A. Rahman *et al.*, "SmartBlock-SDN: An optimized blockchain-SDN framework for resource management in IoT," *IEEE Access*, vol. 9, pp. 28361–28376, 2021. doi: 10.1109/ACCESS.2021.3058244.

[42] K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," in *IEEE 4th World Forum Internet of Things (WF-IoT)*, Singapore, 2018.

[43] J. Hu, M. Reed, N. Thomos, M. K. AI-Naday, and K. Yang, "Securing SDN-controlled IoT networks through edge blockchain," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2102–2115, 2020. doi: 10.1109/JIOT.2020.3017354.

[44] S. Faizullah, M. A. Khan, A. Alzahrani, and I. Khan, "Permissioned blockchain-based security for SDN in IoT cloud networks," in *Int. Conf. Adv. Emerg. Comput. Technol. (AECT)*, Al Madinah Al Munawwarah, Saudi Arabi, 2020.

[45] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchainbased decentralized security architecture for IoT network," *J. Netw. Comput. Appl.*, vol. 143, no. 4, pp. 167–177, 2019. doi: 10.1016/j.jnca.2019.06.019.

[46] S. Boukria, M. Guerroumi, and I. Romdhani, "BCFR: Blockchain-based controller against false flow rule injection in SDN," in *2019 IEEE Symp. Comput. Commun. (ISCC)*, Barcelona, Spain, 2019.

[47] S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Comput. Commun.*, vol. 181, no. 6, pp. 274–283, 2022. doi: 10.1016/j.comcom.2021.09.029.

[48] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739–139754, 2021. doi: 10.1109/ACCESS.2021.3118948.

[49] Y. Gao, Y. Chen, H. Lin, and J. J. Rodrigues, "Blockchain based secure IoT data sharing framework for SDN-enabled smart communities," in *IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, 2020.

[50] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1120–1132, 2019.

[51] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu and C. Zhao, "Blockchainbased software-defined industrial internet of things: A dueling deep qlearning approach," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4627–4639, 2018. doi: 10.1109/JIOT.2018.2871394.

[52] P. Amangele, M. J. Reed, M. Al-Naday, N. Thomos, and M. Nowak, "Hierarchical machine learning for IoT anomaly detection in SDN," in *Int. Conf. Inform. Technol. (InfoTech)*, Varna, Bulgaria, 2019.

[53] J. Ashraf, N. Moustafa, A. D. Bukhshi, and A. Javed, "Intrusion detection system for SDN-enabled IoT networks using machine learning techniques," in *IEEE 25th Int. Enterprise Distribut. Object Comput. Workshop (EDOCW)*, Gold Coast, Australia, 2021.

[54] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Eng. Appl. Artif. Intell.*, vol. 123, no. 1, pp. 106432, 2023. doi: 10.1016/j.engappai.2023.106432.

[55] H. Cheng, J. Liu, T. Xu, B. Ren, J. Mao and W. Zhang, "Machine learning based low-rate DDoS attack detection for SDN enabled IoT networks," *Int. J. Sens. Netw.*, vol. 34, no. 1, pp. 56–69, 2020. doi: 10.1504/IJSNET.2020.109720.

[56] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," in *27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Melbourne, Australia, 2017.

[57] A. B. Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *J. Supercomput.*, vol. 77, no. 3, pp. 2383–2415, 2021. doi: 10.1007/s11227-020-03323-w.

[58] K. Haseeb, I. Ahmad, I. I. Awan, J. Lloret, and I. Bosch, "A machine learning SDN-enabled big data model for IoMT systems," *Electronics*, vol. 10, no. 18, pp. 2228, 2021. doi: 10.3390/electronics10182228.

[59] K. Rui, H. Pan, and S. Shu, "Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques," *Sci. Rep.*, vol. 13, no. 1, pp. 3459, 2023. doi: 10.1038/s41598-023-44764-6.

[60] K. S. Sahoo *et al.*, "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020. doi: 10.1109/ACCESS.2020.3009733.

[61] A. Aqdus, R. Amin, S. Ramzan, S. S. Alshamrani, A. Alshehri and E. S. M. El-Kenawy, "Detection collision flows in SDN based 5G using machine learning algorithms," *Comput. Mater. Contin.*, vol. 75, no. 1, pp. 1413–1435, 2023. doi: 10.32604/cmc.2023.031719.

[62] K. M. S. Azad, N. Hossain, M. J. Islam, A. Rahman, and S. Kabir, "Preventive determination and avoidance of ddos attack with sdn over the iot networks," in *Int. Conf. Automat., Control and Mechatron. Industry 4.0 (ACMI)*, Rajshahi, Bangladesh, 2021.

[63] R. Swami, M. Dave, and V. Ranga, "DDoS attacks and defense mechanisms using machine learning techniques for SDN," in *Research Anthology on Combating Denial-of-Service Attacks*. PA, USA: IGI Global, 2021. pp. 248–264.

[64] D. Javeed, T. Gao, M. T. Khan, and I. Ahmad, "A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT)," *Sensors*, vol. 21, no. 14, pp. 4884, 2021. doi: 10.3390/s21144884.

[65] A. Motwakel *et al.*, "Enhanced crow search with deep learning-based cyberattack detection in SDN-IoT environment," *Intell. Automat. & Soft Comput.*, vol. 36, no. 3, pp. 3157–3173, 2023. doi: 10.32604/iasc.2023.034908.

[66] A. Wani and S. Revathi, "DDoS detection and alleviation in IoT using SDN (SDIoT-DDoS-DA)," *J. Instit Eng. (India): Series B*, vol. 101, no. 2, pp. 117–128, 2020. doi: 10.1007/s40031-020-00442-z.

[67] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A. B. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," *Technologies*, vol. 9, no. 1, pp. 14, 2021. doi: 10.3390/technologies9010014.

[68] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," *Information*, vol. 14, no. 1, pp. 41, 2023. doi: 10.3390/info14010041.

[69] K. D. Joshi and K. Kataoka, "pSMART: A lightweight, privacy-aware service function chain orchestration in multi-domain NFV/SDN," *Comput. Netw.*, vol. 178, no. 2, pp. 107295, 2020. doi: 10.1016/j.comnet.2020.107295.

[70] T. G. Nguyen, T. V. Phan, D. T. Hoang, T. N. Nguyen, and C. So-In, "Federated deep reinforcement learning for traffic monitoring in SDN-based IoT networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 4, pp. 1048–1065, 2021. doi: 10.1109/TCCN.2021.3102971.

[71] Q. Zhou, J. Yu, and D. Li, "A dynamic and lightweight framework to secure source addresses in the SDN-based networks," *Comput. Netw.*, vol. 193, pp. 108075, 2021. doi: 10.1016/j.comnet.2021.108075.

[72] D. Javeed, T. Gao, and M. T. Khan, "SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT," *Electronics*, vol. 10, no. 8, pp. 918, 2021. doi: 10.3390/electronics10080918.

[73] S. Khan and A. Akhunzada, "A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 170, no. 11, pp. 209–216, 2021. doi: 10.1016/j.comcom.2021.01.013.

[74] A. Wani and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," *CAAI Trans. Intell. Technol.*, vol. 6, no. 3, pp. 281–290, 2021. doi: 10.1049/cit2.12003.

[75] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: Towards secure IoT architecture," *Int. of Things*, vol. 3, no. 8, pp. 82–89, 2018. doi: 10.1016/j.iot.2018.09.003.

[76] T. H. Lee, L. H. Chang, and C. W. Syu, "Deep learning enabled intrusion detection and prevention system over SDN networks," in *IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Dublin, Ireland, 2020.

[77] D. Ma and Y. Shi, "A lightweight encryption algorithm for edge networks in software-defined industrial internet of things," in *IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, 2019.

[78] Y. Ma, L. Yan, X. Huang, M. Ma, and D. Li, "DTLShps: SDN-based DTLS handshake protocol simplification for IoT," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3349–3362, 2020. doi: 10.1109/JIOT.2020.2967464.

[79] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment," *IEEE Trans. Ind. Inform.*, vol. 14, no. 6, pp. 2629–2640, 2018. doi: 10.1109/TII.2018.2789442.

[80] L. Yan, M. Ma, and Y. Ma, "TLShps: SDN-based TLS handshake protocol simplification for IoT," in *Security, Privacy, and Anonymity in Comput., Commun., Storage: 12th Int. Conf.*, Atlanta, GA, USA, 2019.

[81] W. Fang, C. Zhu, F. R. Yu, K. Wang, and W. Zhang, "Towards energy-efficient and secure data transmission in AI-enabled software defined industrial networks," *IEEE Trans. Ind. Inform.*, vol. 18, no. 6, pp. 4265–4274, 2021. doi: 10.1109/TII.2021.3122370.

[82] B. Yuan *et al.*, "Secure data transportation with software-defined networking and *k-n* secret sharing for high-confidence IoT services," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7967–7981, 2020. doi: 10.1109/JIOT.2020.2993587.

[83] T. W. Kim, A. E. Azzaoui, B. Koh, J. Kim, and J. H. Park, "A secret sharing-based distributed cloud system for privacy protection," *Hum.-Centric Comput. Inf. Sci.*, vol. 12, pp. 20–36, 2022.

[84] S. Pradeep *et al.*, "Developing an SDN security model (EnsureS) based on lightweight service path validation with batch hashing and tag verification," *Sci. Rep.*, vol. 13, no. 1, pp. 799, 2023. doi: 10.1038/s41598-023-44701-7.

[85] W. Ren, Y. Sun, T. Y. Wu, and M. S. Obaidat, "A hash-based distributed storage strategy of flowtables in SDN-IoT networks," in *IEEE Global Commun. Conf.*, Singapore, 2017.

[86] I. Appiah, X. Jiang, E. K. Boahen, and E. Owusu, "A 5G perspective of an SDN-based privacy-preserving scheme for IoT networks," *Int. J. Commun., Netw. Syst. Sci.*, vol. 16, no. 8, pp. 169–190, 2023. doi: 10.4236/ijcns.2023.168012.

[87] N. Hossain, M. Z. Hossain, and M. A. Hossain, "An ontological security framework to secure the SDN based IoT networks," *American J. Agri. Sci., Eng., Technol.*, vol. 5, no. 1, pp. 4–18, 2021. doi: 10.54536/ajaset.v5i1.55.

[88] S. Midha, S. Verma, M. Mittal, N. Z. Jhanjhi, M. Masud and M. A. AlZain, "A secure multi-factor authentication protocol for healthcare services using cloud-based SDN," *Comput. Mater. Contin.*, vol. 74, no. 2, pp. 3711–3726, 2023. doi: 10.32604/cmc.2023.027992.

[89] W. Iqbal, H. Abbas, B. Rauf, Y. A. Bangash, M. F. Amjad and A. Hemani, "PCSS: Privacy preserving communication scheme for SDN enabled smart homes," *IEEE Sens. J.*, vol. 22, no. 18, pp. 17677–17690, 2021. doi: 10.1109/JSEN.2021.3087779.

[90] C. Wang, Y. Zhang, X. Chen, K. Liang, and Z. Wang, "SDN-based handover authentication scheme for mobile edge computing in cyber-physical systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8692–8701, 2019. doi: 10.1109/JIOT.2019.2922979.

[91] D. S. Sahana and S. H. Brahmananda, "Secure authentication framework for SDN-IoT network using Keccak-256 and Bliss-B algorithms," *Int. J. Inf. Tecnol.*, vol. 15, no. 1, pp. 335–344, 2023. doi: 10.1007/s41870-022-01074-w.

[92] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq and H. Song, "SUSIC: A secure user access control mechanism for SDN-enabled IIoT and cyber physical systems," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16504–16515, 2023. doi: 10.1109/JIOT.2023.3268474.

[93] S. N. Matheu *et al.*, "Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems," *Sensors*, vol. 20, no. 7, pp. 1882, 2020. doi: 10.3390/s20071882.

[94] B. Jiang, Q. He, Z. Zhai, and H. Su, "Anomaly detection and access control for cloud-edge collaboration networks," *Intell. Automat. & Soft Comput.*, vol. 37, no. 2, pp. 2335–2353, 2023. doi: 10.32604/iasc.2023.039989.

[95] H. M. Anitha, P. Jayarekha, A. Sivaraman, A. Mehta, and V. Nalina, "SDN enabled role based shared secret scheme for virtual machine security in cloud environment," *Cyber Secur. Appl.*, vol. 2, no. 9, pp. 100043, 2024. doi: 10.1016/j.csa.2024.100043.

[96] V. Sivaraman and B. Sikdar, "A game-theoretic approach for enhancing data privacy in sdn-based smart grids," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10583–10595, 2020. doi: 10.1109/JIOT.2020.3048357.

[97] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença Jr, "Adversarial deep learning approach detection and defense against DDoS attacks in SDN environments," *Future Gener. Comput. Syst.*, vol. 125, no. 1, pp. 156–167, 2021. doi: 10.1016/j.future.2021.06.047.

[98] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach," *Sensors*, vol. 20, no. 3, pp. 816, 2020. doi: 10.3390/s20030816.

[99] M. Revathi, V. V. Ramalingam, and B. Amutha, "A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework," *Wirel. Pers. Commun.*, vol. 127, no. 3, pp. 2417–2441, 2022. doi: 10.1007/s11277-021-09071-1.

[100] Y. C. Wang and Y. C. Wang, "Efficient and low-cost defense against distributed denial-of-service attacks in SDN-based networks," *Int. J. Commun. Syst.*, vol. 33, no. 14, pp. 375, 2020. doi: 10.1002/dac.4461.

[101] Y. Zhou, G. Cheng, and S. Yu, "An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 5366–5380, 2021. doi: 10.1109/TIFS.2021.3127009.

[102] B. Wang, Y. Sun, and X. Xu, "A scalable and energy-efficient anomaly detection scheme in wireless SDN-based mMTC networks for IoT," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1388–1405, 2020. doi: 10.1109/JIOT.2020.3011521.

[103] V. Varadharajan and U. Tupakula, "Counteracting attacks from malicious end hosts in software defined networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 160–174, 2019. doi: 10.1109/TNSM.2019.2931294.

[104] R. S. Silva *et al.*, "REPEL: A strategic approach for defending 5G control plane from DDoS signalling attacks," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 3231–3243, 2020. doi: 10.1109/TNSM.2020.3035342.

[105] P. Shrivastava and K. Kataoka, "Topology poisoning attacks and prevention in hybrid software-defined networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 1, pp. 510–523, 2021. doi: 10.1109/TNSM.2021.3109099.

[106] R. Kiani and A. Bohlooli, "Distributed rule anomaly detection in SDN-based IoT," in *5th Int. Conf. Internet of Things and Appl. (IoT)*, Isfahan, Iran, 2021.

[107] P. Thorat, N. K. Dubey, K. Khetan, and R. Challa, "SDN-based predictive alarm manager for security attacks detection at the IoT gateways," in *IEEE 18th Annual Consumer Commun. & Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2021.

[108] C. H. Lee, J. S. Park, and J. G. Shon, "An SDN-based distributed identifier locator separation scheme for IoT networks," in *Advances in Computer Science and Ubiquitous Computing*, 2021, pp. 349–355.

[109] T. Altaf and R. Braun, "A roadmap to smart homes security aided SDN and ML," in *5th Conf. Cloud and Internet of Things (CIoT)*, Marrakech, Morocco, 2022.

[110] H. Babbar, S. Rani, and S. A. AlQahtani, "Intelligent edge load migration in SDN-IIoT for smart healthcare," *IEEE Trans. Ind. Inform.*, vol. 18, no. 11, pp. 8058–8064, 2022. doi: 10.1109/TII.2022.3172489.

[111] L. Yan, D. Li, X. Huang, Y. Ma, and K. Xie, "Certrust: An SDN-based framework for the trust of certificates against Crossfire attacks in IoT scenarios," *Comput. Model. Eng. Sci.*, vol. 134, no. 3, pp. 2137–2162, 2023. doi: 10.32604/cmes.2022.022462.