Journal of High Speed Networks 29 (2023) 169–181
DOI 10.3233/JHS-230004
IOS Press

Security-aware resource management approaches in software defined networks: Comprehensive analysis, opportunities and challenges

Monire Norouzi [a,b,*], Zeynep Gürkaş-Aydın [a], Sefer Ergen [c] and Mehmet Şerif Bakır [d]

[a] *Department of Computer Engineering, Istanbul University – Cerrahpasa, Istanbul, Turkey*
E-mails: m.norouzisoufiani@ogr.iuc.edu.tr, zeynepg@iuc.edu.tr
[b] *Computer Technology Program, Vocational School, Haliç University, Istanbul, Turkey*
E-mail: monirenorouzi@halic.edu.tr
[c] *Büyükşehir Primary School, Istanbul, Turkey*
E-mail: seferergen@gmail.com
[d] *Baki Gündüz Primary School, Istanbul, Turkey*
E-mail: serifbakir@hotmail.com

Received 21 February 2023
Accepted 26 March 2023

Abstract. Today, with the fast growth of emerging technologies and applying numerous advantages of 5G communications, there is a critical gap between the supporting security of data transmission and resource management of Software Defined Networks (SDN). To provide a secure communication perspective for Internet of Things (IoT) devices and smart applications, network slicing in resource management is currently an important issue and is widely studied for the SDN. Due to the importance of security-aware resource management in several aspects of the SDN, this research aims to represent a new comprehensive review of existing technical classification and deep-detailed categorization of resource management approaches for SDN communications in the IoT environments. Based on each category, a technical taxonomy is presented to show a variety of security-aware platforms that include resource allocation, service composition, task scheduling, and service offloading in the IoT environments. According to the main state-of-the-art discussed comprehensive technical review, some important evaluation factors, main methodologies, advantages, and disadvantages of each case study are elaborated. Finally, some important new research directions and open challenges are presented for future scientific efforts.

Keywords: Internet of Things (IoT), Software Defined Networks (SDN), resource management, security

1. Introduction

Nowadays, the Internet of Things (IoT) and its technologies bear numerous advantages for multiple applications and systems in the future of computer networks. Nevertheless, several IoT aspects like its heterogeneity, ignoring security policies on cheap devices, continuous software updates, and large-scale IoT deployments are subject to various threats and attacks [17]. Many computational systems and applications in the IoT environment are critical

[*] Corresponding author. E-mails: m.norouzisoufiani@ogr.iuc.edu.tr, monirenorouzi@halic.edu.tr.

for us from a safety point of view. Any interruption in their procedure and services may have considerable consequences and make vast security risks from the side of cyber-attacks [5,31]. On the other side, according to the new structures such as big data and the IoT, many bandwidth-starvation applications have appeared, which caused the rapid growth of data center traffic consequently [26]. To manage the large-scale part of traffic effectively, Software Defined Networking (SDN) is presented to the data center [18,21]. In addition, the infrastructure providers can achieve optimal resource management according to SDN's centralized control and global network view. Moreover, the service quality can be ensured by the increased bandwidth and minimum delay presented by IoT communications [38]. An SDN delivers proper support for network slicing and resource management mechanism as it has the functionality feature to perform slice demands and complete data traffic allocation and scheduling [16,29].

SDNs prepare several technical points, such as QoS-aware resource management that are currently focus on existing studies for multiple applications. Some of these technical points are reliable resource provisioning, long-distance collaboration between smart devices, and explanations of optimization problems [27,28].

Focusing and analyzing the security strategies and aspects revealed that these strategies generally include the first level of protection strategies in today's computer systems created from a firewall. Placing at the edge level of the computer network, the firewall tries to purify all the packets that send or receive based on the established security standards and guidelines [6]. Also, this method does not defend against attacks executed by malicious within the network. Thus, additional security systems must be installed at each security level, which creates high purchase and supervision costs [10]. As a solution, security systems and applications which are based on the concepts of SDN and Network Functions Virtualization (NFV) have been suggested to improve and satisfy network security aspects and reduce system operating costs. The SDN platform's control plane is divided from the data plane so the network operator can run flows automatically using a central interface. This procedure can satisfy security policies and standards and improve network security levels considerably. In the NFV platform, it is possible to transfer the load balancers and firewalls into the software which are running on virtual machines. Thus, combining these two SDN and NFV technologies can provide scalable and sufficient security and safety solutions [13,24].

According to the above-mentioned problem statements on resource management of the SDN and IoT communications, there is no detailed and pervasive analytical discussion for comparing existing security-based models and architectures for enhancing security issues against anomaly, intrusion aspects, and attacks. Therefore, a comprehensive review of existing security-aware resource management approaches in the SDN is presented in this paper. While working on this systematic study, the main methods are discovered, earlier challenges are reviewed, state-of-the-art methods are examined, and upcoming research gaps are outlined.

Concisely, this paper contributes to the following:

- Highlighting the existing challenges in the field of security-aware resource management in the SDN;
- Presenting a new technical taxonomy for categorizing existing security-aware resource management approaches in the SDN;
- Providing a comprehensive analysis of the suggested security-aware resource management methods;
- Discussing existing evaluation factors for each case study, open issues, and outlining some potential future directions for forthcoming studies;

The rest of this study is formed as follows: Section 2 describes the research methodology that we used in this study. Section 3 reviews the current studies in the field of security-aware resource management in the SDN. Discussion and analytical comparison of the existing methods are presented in Section 4. In Section 5, open issues and directions for forthcoming studies are presented. Finally, the conclusion is delivered in Section 6.

2. Research methodology

In this section, we examine the research methodology assumed to investigate existing security-aware resource management approaches in the SDN. As shown in Fig. 1, the review process includes four major steps. The first step tries to define the research purposes and questions. Regarding some standards, the appropriate papers are

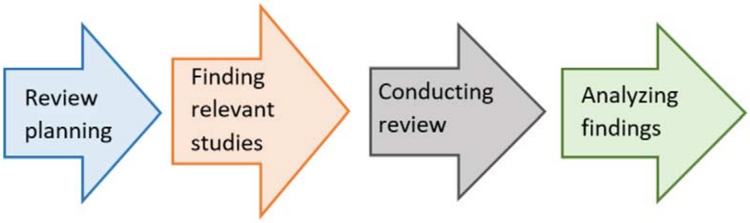

Fig. 1. The research methodology steps.

searched and selected in the second step. In addition, a set of technical keywords are selected to search the engine of scientific databases. We review the selected methods in the third step based on some qualitative metrics. Finally, the last step tries to report the received results, discuss unresolved problems, and offer some potential suggestions for upcoming examinations. Based on this step, some important questions will be defined to discuss on existing technical points of each category in the security-aware resource management approaches in the SDN.

To create a Systematic Literature Review (SLR), fundamental research questions are needed to drive the research methodology. Observing previous studies, it is anticipated that the following research questions will be answered while reviewing the methods.

- **Q1:** What are the significant approaches of security-aware resource management methods in SDN?
- **Q2:** What are the evaluation parameters for analyzing and investigating security-aware resource management methods in SDN?
- **Q3:** Which keywords have been used for evaluating this area?
- **Q4:** What are the most common simulation environments?

We conducted an extensive and detailed search to review the research papers of high repute. The widely used online electronic digital libraries[1] were selected and searched using the following search string.

"Security" AND "Resource Management" OR "Service Management" AND

"Software Defined Networks" OR "SDN"

An automatic search process for published papers between 2012 and 2022 based on the papers' titles was done in October 2022, and 89 studies were found in journals, conferences, and books. Afterward, review papers, working reports, notes, and non-English studies were excluded from the review process to choose the highest-quality papers. In the final step, to select the proper studies for the review that are directly focused on the security-aware resource management methods in SDN, the authors carefully reviewed the full text of the remaining studies. Finally, 20 papers were selected. Moreover, Fig. 2 briefly details the selected studies in the field of security-aware resource management approaches in SDN.

3. Review of security-aware resource management approaches

In this paper, we organized the security-aware management studies into four categories including resource allocation, service composition, task scheduling, and service offloading approaches according to our analyses and examinations. Moreover, the taxonomy of the security-aware management approaches is shown in Fig. 3. In the Service allocation section, we extract the two sub-sections Virtual firewalls and Intrusion Detection Systems (IDS). IDS can monitor a network or systems for malicious activity or policy and a virtual firewall can run entirely within

[1] www.ieeexplore.ieee.org, www.onlinelibrary.wiley.com, www.link.springer.com, www.elsevier.com, www.scholar.google.com, www.scopus.com and www.dl.acm.org.

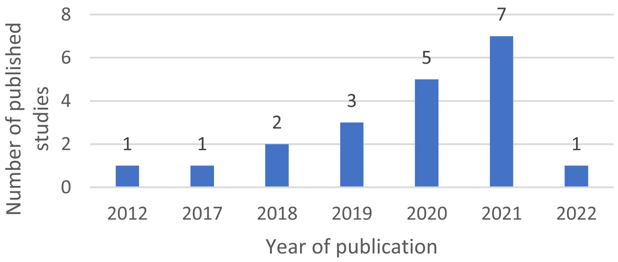

Fig. 2. Published studies in the field of security-aware resource management approaches in SDN.

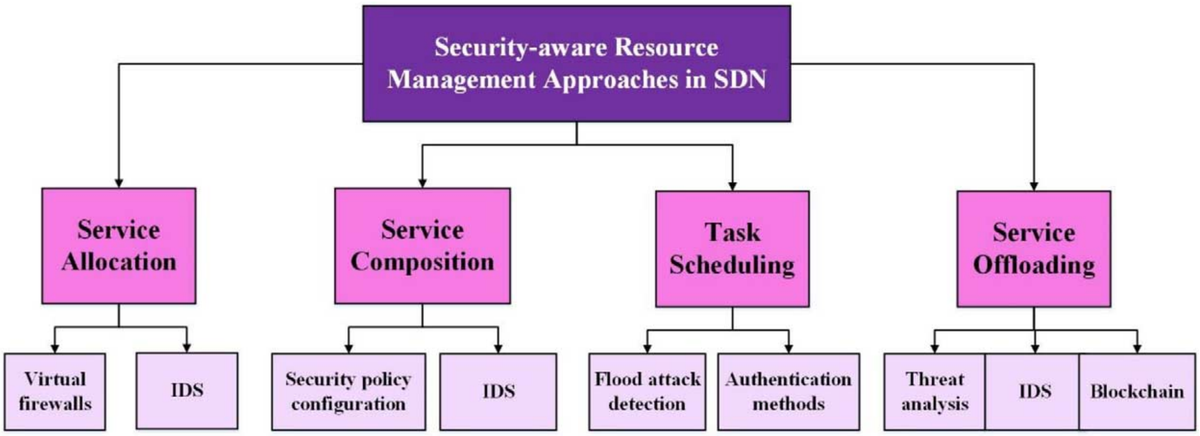

Fig. 3. Taxonomy of the security-aware management approaches.

a virtualized environment and provides a monitoring process via a physical network firewall. In the Service composition section, we create two sub-sections according to the reviewed papers: Security policy configuration and IDS. In the Task scheduling section, we divide the reviewed papers into two sub-sections: Flood attack detection approaches and Authentication methods. Moreover, in the Service offloading section, we have three sub-section based on our reviewed papers: Threat analysis, IDS, and Blockchain.

3.1. Security-aware resource allocation approaches

In the SDN platform, the network manager should specify some important initial network security guidelines before assigning or organizing the SDN controllers in the IoT environment. On another side, in the service allocation procedure, the placement of the function should be described in the logical topology. Security policies are an important issue in this procedure and should be examined the detail in its methods [2,5].

In this section, we have eight papers that presented new methods for satisfying the security policies in the service allocation procedure in SDN. We analyze and extract the advantages or weaknesses of these studies in this section. In the first paper, [38] proposed a security-aware and cost-based virtual data center mapping structure to manage the resource allocation issue trying to reduce the general cost and increasing the virtual data center acceptance rate. The advantage of this study is using a virtual data center division method based on the improved label propagation algorithm to separate VMs into various classes to satisfy the resource allocation procedure more efficiently. The simulation results using Python code showed that the proposed structure could reduce the cost of general virtual data center mapping and increase the acceptance rate of the virtual data center and total revenue. Moreover, [5] proposed a new schema for the resource allocation process and design of SDN switches and also manages the security orchestration functions such as detection and mitigation mechanisms. The main purpose of this study is to prepare a model for the SDN switches directions and the network security guidelines in the IoT environment. Moreover, effectiveness and scalability factors are examined and satisfied using Open Network Operating System (ONOS) [3].

In another study, [7] suggested a new SDN-based schema for edge/cloud computing environments to support secure and smart services in IoT environments. Also, a Blockchain case study and reinforcement learning-enabled security is examined in this schema since Blockchain and reinforcement learning are suitable methods for specifying a secure area and smart resource allocation management. Moreover, delay and cost factors are analyzed in this case study. In this study, numerical simulation results confirmed the effectiveness of the proposed deep reinforcement learning-based approach in reducing cost and delay in this scenario. Moreover, [24] analyzed a development way of a traditional network framework to integrate the visions of SDN and NFV and summarized the major advantages of this approach. The advantage of this study is analyzing the several design patterns for the integration, which are based on the SDN/NFV security explanations into enterprise networks. Three possible structure designs were demonstrated and examined for implementation. By examining the advantages and disadvantages of each design, an overview is provided, which is useful as a policy for the development and potential integration of SDN and NFV devices into existing business networks.

In another paper, [37] proposed an active resource allocation method for a virtual data center mapping procedure. An enhanced location-based virtual data center division strategy is executed to decrease bandwidth usage, which separates parts of virtual data center demands into various classes. Then, the parts of virtual data center demands are mapped into the data centers concerning security-based and cost-based orders. In this method, the allocation level delivers the resource allocation procedures and transmits conclusions to the controller section through northbound interfaces. Generally, the advantage of this study is trying to reduce the total cost spent on virtual data center mapping. The PyCharm simulation outcomes demonstrated that the proposed method can decrease bandwidth usage, resource cost, and security cost. In addition, [35] introduced a total reservation technique to execute network security policies and bypass blocked security devices. Moreover, the resource-constrained problem was formulated and solved as an integer linear programming problem to optimize the use of security devices by applying a heuristic algorithm. The main advantage of this study is to present a real-time explanation of allocating restricted security-aware resources to network traffic in a global network topology without the need for understanding traffic designs using SDN as a mechanism to reach this purpose. The simulation using Iperf proved a balance between network throughput and security in this study.

In the other study, [12] proposed a security-aware architecture and implementation framework for Unmanned Aerial Vehicles (UAVs). This study has prepared the unmanned aerial vehicles allocation algorithm and considered various contextual factors for the allocation process, such as the value of operating capacity, battery, and network metrics. The advantage of this study is establishing a security framework to dynamically produce and satisfy security factors in virtual network functions in the UAV field. The tests proved the solution's suitability since it reacts and handles the workload successfully in worst-case scenarios. Finally, [34] proposed a security-based resource-sharing procedure for UAVs to assign bandwidth and security resources in software-defined integrated networks using a game-theoretic method. Moreover, a software-defined cooperative instrument was examined to enable resource utilization for mobile edge computing nodes. Then, a coalitional game model is proposed to complete the Nash-stable coalition design for mobile edge computing nodes. Simulation outcomes indicated that the proposed procedure effectively enhanced resource efficiency levels and decreased the value of average delay.

3.2. *Security-aware service composition approaches*

A service composition is a famous technique for executing value-added services by merging other essential services in multiple application scenes such as smart building and QoS provisioning. For service composition in advanced metering infrastructure, it may require integrating several real-world services, which should try to satisfy the security directions [8,25]. We need some strategies to satisfy the security rules and also, the network security procedures should be developed at the level of infrastructures in a distributed way dynamically. But generally, energy usage and network capability factors are two limitations in the process of establishing the security politics for dispersive infrastructures, which should be taken into consideration [22].

In this section, we have three papers that presented new methods for satisfying the security policies in the service composition procedure in SDN. Here, we analyze and examine the advantages or disadvantages of these studies. As the first study in this section, [19] presented a new combined network security-based method for SDN. The main idea of this method is based on coarse-grained flow monitoring algorithms on the data plane for quick abnormality discovering and forecast of the DDoS attacks. The other advantage of this study is detecting attacks in real-time with high accuracy and summarizing different Intrusion Detection Systems (IDS) using machine learning and deep learning techniques. Mininet simulation results confirmed the success of this method. Moreover, [22] proposed a distributed service composition and security-aware strategy for smart grid metering for wireless sensor networks based on SDN. This strategy keeps fine-grained safeguards for distributed data safety by applying a dynamic security policy design. The resource-constrained strategy is developed by using an Energy Matrix. The advantage of this study is realizing an SDN security structure for WSN-based smart metering in a smart grid. The analysis showed that communication latency and network congestion were decreased remarkably for time-critical applications.

Finally, [23] proposed a new and dynamic service composition method of security service oriented based on SDN/NFV Networks. The main goal of this study is to apply a novel heuristic algorithm to deliver the best solution. Matlab simulation outcomes showed that the proposed heuristic algorithm achieved optimal results in terms of network resource utilization, cost, execution time, latency, and bandwidth.

3.3. *Security-aware resource scheduling approaches*

With the continued growth of SDN, SDN technology can provide a proper management interface and operational environment for the network. Simultaneously, network security-aware methods are used to safely use centralized resource scheduling strategies based on network security standards and cooperative integration of network security policies [39]. Some studies focus on the security-aware resource scheduling approaches in SDN.

Here, we have three papers that presented new methods for satisfying the security policies in the resource scheduling procedure in SDN. In this section, we analyze the goals and weaknesses of these studies. In the first study, [14] suggested a security-based task scheduler framework in IoT and fog environments. This method used a fuzzy-based meta-heuristic algorithm to collect the optimal computing resources and satisfy security safeguards to discover a suitable solution. Considering the security problems of allocating IoT end-client tasks to fog devices in the SDN network is the main goal of this paper. The iFogSim simulation outcomes based on IoT scenarios demonstrated that the proposed method improved the average response time and network utilization factors by changing attack rates. Moreover, [28] presented a traffic-aware scheduling method for resource assignment in SDN-enabled 5G networks. In this study, the virtual authority is created and authenticated to the 5G access points for achieving secure transmission and it can decrease the transmission overhead. Moreover, dynamic flow offloading is implemented to match the underloaded controls to evade packet dropping. Also, DDoS attackers are extracted from the network via packet category. The main advantage of this paper is improving the QoS in an SDN/NFV network and service level agreement condition for recommendations from an appliance or client. Eventually, the implementation results of the system were acceptable in terms of throughput, latency, response time, and packet transmission ratio.

Finally, [39] proposed a security-based software-defined IoT network architecture to improve the security elements. The main goal of this paper is to merge SDN with the IoT, rewrite the SDN network, and add security features to enhance the security of the smart society significantly. The simulation results showed the ability of the proposed architecture; the number of successful transactions improved when the users' number increased in a smart society.

3.4. *Security-aware resource offloading approaches*

In the SDN platform, some smart controllers make conditional determinations for ask or resource scheduling in fog computing for dependable and secured task processing intelligently based on the dynamic data gathered from the network. In other words, when having computationally intensive tasks to offload, the edge instruments assign service recommendations to the controller to assign optimal fog nodes for task processing. As we know, task offloading is used for mobile nodes to reduce the total cost of energy usage and delay factors typically [30].

Some studies focus on the security-aware Resource offloading approaches in SDN. Here, we have six papers that presented new methods for satisfying the security policies in the resource scheduling procedure in SDN. In this section, we analyze the advantages and disadvantages of these papers. In this first paper in this section, [11] presented a security-aware method in the SDN platform to support mobile application resource offloading. The authors studied the overhead of transport-layer encryption and classified the dangers associated with business data. Upon these statements, the authors developed a simple, graphic procedure language that catches the privacy restrictions of applications/devices and the trust statuses of resources. The advantage of this study is presenting a way to adapt trust and privacy respect in offloading without resorting to complicated trust strategies. Moreover, how to scale offloading to numerous mobile appliances and compute resources is discussed in this study. Finally, a decision process for applying encryption and network-level policy enforcement mechanisms is examined in this study. Execution time, latency, and energy usage factors have been measured, too.

Moreover, [33] presented a self-adaptive smart resource management strategy for positively effective communication, analysis, and agreement in improved hybrid cloud/edge Blockchain. The main goal of this study is to develop a combined optimization issue to reduce the communication, calculation, and agreement latency factor while ensuring that specific communication rates and secure offloading are satisfied. Simulation results revealed that the proposed method reduced the whole latency for offloading and resource allocation as long as guarantee the data security of the general system.

In another study, [1] presented a new structure for load-balancing and secure communication problems in SDN/fog-based Internet of Vehicles (IoV) networks. In the proposed structure, all tasks are distributed efficiently using reinforcement learning methods. Moreover, this structure delivered secure communication using Blockchain technology. The main goal of this study is to propose a way to employ the available resources while ignoring network congestion and reducing latency in the IoV network. The simulation results of sumo showed that the proposed structure can avoid congestion in the network and decrease latency while operating the resources efficiently. Moreover, [36] developed an SDN-based schema to manage the uncertainty of edge nodes and networks for IoV during the service offloading. The main advantage of this article is applying a data-clustering algorithm to determine appropriate resources to be offloaded to the edge node to optimize offloading time, reduce energy consumption, and maintain load balance. The simulation results proved the proposed method's ability to optimize offloading time and reduce energy consumption. In another paper, [20] proposed a security monitoring approach according to the customized stack-flow method in the SDN. The main advantage of this paper is adding a security layer in the data plane to the traditional SDN prototype to manage security and scalability problems. Under simulation of real-life botnet attacks, the proposed framework reached a much faster response time to mitigate the attack nearer to the origin.

Finally, [30] presented a new centralized task offloading architecture for loT healthcare applications. Moreover, a task-offloading procedure with minimum latency, secured, and dedicated decision-making algorithm is proposed to define the ideal fog nodes to assign as a task-offloading method. MATLAB simulation and numerical results showed that the system performances such as other quality of service factors are greatly enhanced.

4. Discussion and analytical comparison

According to Table 1, some necessary technical factors such as the main idea, evaluation parameters, simulation environment, advantages, and weaknesses are reviewed in this section.

According to the questions in Section 2, we analyze and answer to discuss them as follows:

- **Q1:** What are the significant approaches of security-aware resource management methods in SDN and how many papers are published on each approach?

Table 1

Necessary technical factors

Ref.	Main idea	Evaluation parameters	Advantage	Weakness
[38]	A new security-aware and resource allocation-based schema in SDN data center networks.	Cost, acceptance rate, total revenue.	– Decreasing the overall virtual data center mapping cost. – Increasing the virtual data center acceptance rate and the total revenue.	There are no test results for the proposed methods in real data center environments.
[5]	A security-based method for resource allocation process in SDN-aware IoT networks.	Scalability	Formal model for SDN switch configuration.	The variety of the IoT end-points linked to an SDN-aware IoT network is not considered.
[7]	An SDN-enabled architecture to support secure and intelligent services in IoT.	Cost and delay.	A Blockchain and reinforcement learning case study to get secure and intelligent computing offloading.	Privacy safeguard is essential to enhance mobile users' quality of experience.
[24]	An SDN/NFV-based method for resource allocation and security policy implementations.	–	Analyzing the different designs for the integration of SDN/NFV-based security explanations.	The other security considerations that are introduced by the new SDN features did not consider.
[37]	A new resource allocation method in optical data center networks.	Cost, bandwidth and utilization.	Reduce the overall cost spent on virtual data center mapping.	The elasticity, category, and granularity of optical network resources should be considered.
[35]	A security-aware resource allocation in real time using SDN.	Bandwidth, utilization, time and throughput.	Establishing a security framework to dynamically orchestrate security virtual network functions in UAVs.	It was supposed that the links consistently have enough bandwidth. There is no plan for other situations.
[12]	An SDN-based and security management framework for unmanned aerial vehicles.	Cost and bandwidth.	Finding the most suitable method to perform the tasks and allocate the virtualized network functions without human intervention.	There is no discussion about a collaboration among unmanned aerial vehicles and the migration of virtual network functions between them.
[34]	A security-based resource allocation method for unmanned aerial vehicles.	Cost, bandwidth and delay.	Improving resource efficiency and decreasing average delay.	The collaboration between UAVs in data transmission and resource sharing should be examined.
[19]	A multi-plane security-aware framework for SDN.	Cost, response time and accuracy.	Detecting attacks in real-time with high accuracy.	This study should be developed with an online network security and intrusion detection system and perspective.
[22]	A security-aware service composition structure for WSNs-based smart metering in smart grid.	Cost, energy usage and latency.	Being the first to realize a software-defined security structure for WSN-based smart metering in a smart grid.	This study should be developed considering the other security considerations.
[23]	A dynamic service composition method of Security Service Chaining Oriented based on SDN Networks.	Resource utilization, cost, time, latency and bandwidth.	Applying a novel heuristic algorithm to deliver the best solution.	This method should be adjusted to the dynamic structure of security service chaining to fulfill the other security conditions.

Table 1

(Continued)

Ref.	Main idea	Evaluation parameters	Advantage	Weakness
[14]	A security-aware resource scheduling method for SDN-based IoT networks.	CPU and RAM usage, response time and network utilization.	Considering the security problems of actually allocating IoT end-user tasks to fog appliances in the SDN structure.	This method should be tested using various optimization strategies such as genetic algorithms against the other kinds of attacks in IoT–fog networks.
[28]	A traffic-aware scheduling method for resource allocation in SDN/NFV 5G Networks.	Bandwidth, time, throughput and latency.	Improving the QoS in an SDN/NFV-enabled 5G network based on service and service level agreement conditions for recommendations coming from an appliance or client.	It is better to test this method against other kinds of attacks in SDN/NFV-Enabled 5G Networks.
[39]	A security-aware SDN architecture for resource allocation in IoT.	Cost.	Merging SDN with the IoT and adding security features to enhance the security of the smart society.	The other QoS factors should be evaluated by this architecture.
[11]	A security-aware method in SDN platform to support mobile application resource offloading.	Execution time, latency and energy usage.	Presenting a way to adapt trust and privacy respect in offloading without resorting to complicated trust strategies.	The obtained results should be compared to the other methods.
[33]	A resource offloading management method in cyber–physical systems.	Cost and latency.	Reducing the total latency for offloading and resource allocation process while ensuring the data security of the general system.	The obtained results should be compared to the other methods.
[1]	A security-aware communication method for IoV in fog environment using SDN and Blockchain.	Cost and latency.	Employing the available resources while ignoring network congestion and reducing latency in the IoV network.	It is better to examine the integration of hierarchical SDN control with fog-based computing and IoT.
[36]	A security-aware resource offloading method for IoV in SDN-based mobile edge computing.	Time, energy usage and latency.	Applying a data clustering algorithm to the resource allocation process to optimize offloading time and reduce energy consumption.	The proposed method should be implemented in real life and considering real details of the IoV environment.
[20]	A flexible security-aware monitoring and defense framework based on the SDN stack.	Time, throughput and latency.	Adding a security layer in the data plane to the traditional SDN prototype to manage security and scalability problems.	This framework should be tested for emerging 5G and Industry 4.0 networks.
[30]	A security-aware and SDN-based task offloading strategy for healthcare loT in fog environment.	Time, cost, throughput, reliability and latency.	A hierarchy network framework with centralized control and distributed computing with a down latency and secure decision-making algorithm for smart healthcare loT applications.	The obtained results should be compared to the other methods.

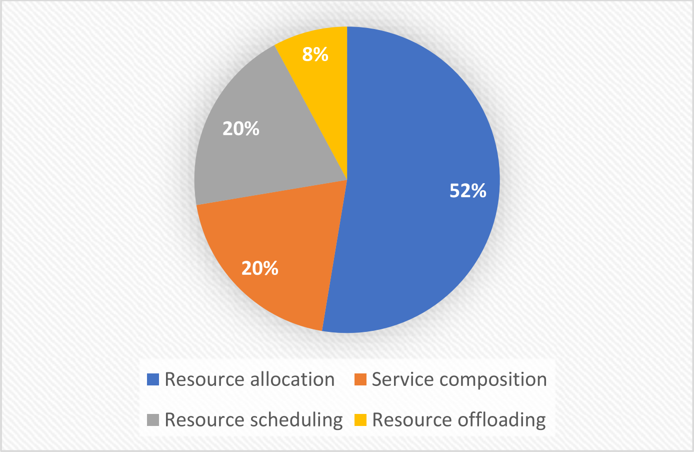

Fig. 4. Security-aware resource management approaches and the published papers of each approach.

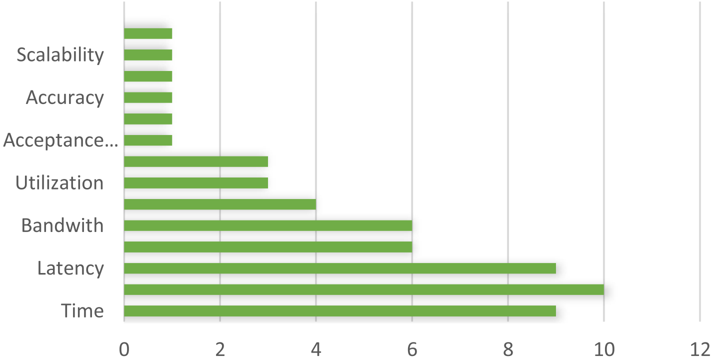

Fig. 5. Evaluation parameters for analyzing security-aware resource management.

According to Fig. 4 and analysis of 20 papers related to security-aware resource management approaches in SDN, we classified the security-aware management studies into four categories including resource allocation, service composition, task scheduling, and service offloading approaches.

- **Q2:** What are the evaluation parameters for analyzing and investigating security-aware resource management methods in SDN?

According to Fig. 5, cost, time and latency are the most used evaluation parameters in the examined papers. The other evaluation parameters are delay, bandwidth, throughput, and energy usage.

- **Q3:** Which keywords have been used for evaluating this area?

As shown in Fig. 6, the keywords for analyzing security-aware resource management in these studies are resource management, SDN, security, service offloading, task scheduling, service composition, and resource allocation.

- **Q4:** What are the most common simulation environments?

According to Fig. 7, Matlab and Python language is the most used environment in these papers. Pycharm, Mininet, iFogSim, and Java language are the other simulation environments.

Fig. 6. Keywords for analyzing security-aware resource management.

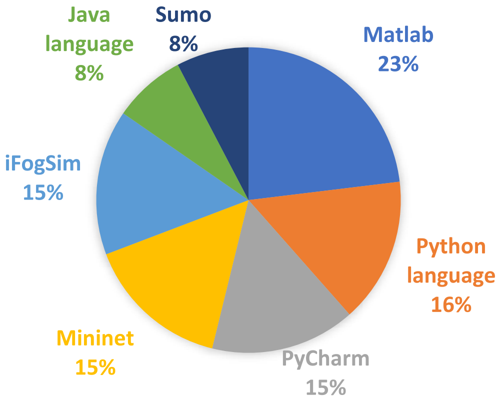

Fig. 7. The most common simulation environments used in security-aware resource management.

5. Open issues and challenges

This section presents a set of open issues and main challenges of security-aware methodologies based on new aspects and evaluation factors of resource management in the SDN and IoT environments. The following research challenges can be evaluated using new optimized meta-heuristic algorithms or machine learning methods.

- According to the increased execution time of processing critical information in the SDN which is collected by the IoT, a new security-aware architecture to improve the QoS factors can be suggested [9]. If we have some critical information that cannot be evaluated on run-time, privacy conditions should be checked for critical information of the open-flow model.
- Blockchain technology can be used to protect the privacy and security of SDN architectures. Smart devices can collaborate with important features such as a high two-phase authentication system [4], private-based Blockchain, and public Blockchain method to enhance the security of data transactions.
- One of the main problems in the SDN system is finding a safe way for data sharing with supporting privacy and bounded accessibility in various levels of persons [15]. Therefore, some strategies for applying machine learning methods on big data without sharing data are used like Federated Learning. Federated Learning techniques can apply and examine to satisfy security strict in SDN systems.
- Formal methods techniques can be applied to the SDN in different strategies and also used to significantly decreased main errors and have new methods for open flow methods to receive IoT services [32]. In formal

methods, authors can apply model checking to prove the correctness of the behavioral model of the SDN system with some critical rules.

6. Conclusion

This research presented a comprehensive technical analysis for secure-aware resource management strategies in the SDN. Also, the existing challenges in the SDN field of security-aware resource management have been discussed. According to the presented taxonomy, we suggested existing security-aware resource management methods in four categories: resource allocation, service composition, task scheduling, and service offloading. On the other side, further examining these methods' major advantages and disadvantages were elaborated. Finally, some open issues and outlining potential future directions for forthcoming studies in resource management strategies have been illustrated. Based on the above-mentioned sub-categories, optimizing security issues in resource allocation methods has more evaluation and discussion in the SDN. Also, concerning evaluation results, time and latency are two main factors that many case studies have evaluated them using machine learning and evolutionary algorithms. According to technical analysis, MATLAB was established for the evaluation of the existing case studies with the highest usage in resource management strategies. For future work, other case studies can be examined and discussed based on other evaluation factors.

Conflict of interest

None to report.

References

[1] J. Alotaibi and L. Alazzawi, Safiov: A secure and fast communication in fog-based Internet-of-vehicles using sdn and blockchain, in: *2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, IEEE, 2021.

[2] C. Basile et al., Adding support for automatic enforcement of security policies in NFV networks, *IEEE/ACM Transactions on Networking* **27**(2) (2019), 707–720. doi:10.1109/TNET.2019.2895278.

[3] P. Berde et al., *ONOS: Towards an Open, Distributed SDN OS. in Proceedings of the Third Workshop on Hot Topics in Software Defined Networking*, 2014.

[4] M. Bhuyan et al., *A Survey on Blockchain, SDN and NFV for the Smart-Home Security*, Internet of Things, 2022, p. 100588.

[5] D. Bringhenti et al., Automatic, verifiable and optimized policy-based security enforcement for SDN-aware IoT networks. *Computer Networks* **213** (2022), 109123.

[6] M. Casado et al., Ethane: Taking control of the enterprise, *ACM SIGCOMM computer communication review* **37**(4) (2007), 1–12. doi:10.1145/1282427.1282382.

[7] M. Dai et al., A software-defined-networking-enabled approach for edge-cloud computing in the Internet of things, *IEEE Network* **35**(5) (2021), 66–73. doi:10.1109/MNET.101.2100052.

[8] G. Dán et al., Cloud computing for the power grid: From service composition to assured clouds, in: *5th USENIX Workshop on Hot Topics in Cloud Computing*, HotCloud, Vol. 13, 2013.

[9] X. Deng et al., PAS: Privacy-preserving authentication scheme based on SDN for VANETs, *Applied Sciences* **12**(9) (2022), 4791. doi:10.3390/app12094791.

[10] ETSI, G. 002, *Network Functions Virtualisation (NFV); Architectural Framework*. Group Specification, 2014.

[11] A. Gember, C. Dragga and A. Akella, ECOS: Leveraging software-defined networks to support mobile application offloading, in: *2012 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, IEEE, 2012.

[12] A. Hermosilla et al., Security orchestration and enforcement in NFV/SDN-aware UAV deployments, *IEEE access* **8** (2020), 131779–131795. doi:10.1109/ACCESS.2020.3010209.

[13] M. Jarschel et al., Interfaces, attributes, and use cases: A compass for SDN, *IEEE Communications Magazine* **52**(6) (2014), 210–217. doi:10.1109/MCOM.2014.6829966.

[14] S. Javanmardi et al., FUPE: A security driven task scheduling approach for SDN-based IoT–Fog networks, *Journal of Information Security and Applications* **60** (2021), 102853. doi:10.1016/j.jisa.2021.102853.

[15] M. Khalid et al., Towards SDN-based smart contract solution for IoT access control, *Computer Communications* **198** (2023), 1–31. doi:10.1016/j.comcom.2022.11.007.

[16] Y. Kim, S. Kim and H. Lim, Reinforcement learning based resource management for network slicing, *Applied Sciences* **9**(11) (2019), 2361. doi:10.3390/app9112361.

[17] C. Kolias et al., *DDoS in the IoT: Mirai and Other Botnets*, Vol. 50, Computer, 2017, pp. 80–84.

[18] D. Kreutz et al., Software-defined networking: A comprehensive survey, in: *Proceedings of the IEEE*, Vol. 103, 2014, pp. 14–76.

[19] P. Krishnan, S. Duttagupta and K. Achuthan, VARMAN: Multi-plane security framework for software defined networks, *Computer Communications* **148** (2019), 215–239. doi:10.1016/j.comcom.2019.09.014.

[20] P. Krishnan, S. Duttagupta and K. Achuthan, SDN/NFV security framework for fog-to-things computing infrastructure, *Software: Practice and Experience* **50**(5) (2020), 757–800.

[21] A. Kumar et al., A secure drone-to-drone communication and software defined drone network-enabled traffic monitoring system, *Simulation Modelling Practice and Theory* **120** (2022), 102621. doi:10.1016/j.simpat.2022.102621.

[22] G. Li et al., Security-aware distributed service composition for wireless sensor networks based smart metering in smart grid using software defined networks, in: *International Wireless Internet Conference*, Springer, 2016.

[23] Y. Liu et al., A dynamic composition mechanism of security service chaining oriented to SDN/NFV-enabled networks, *IEEE Access.* **6** (2018), 53918–53929. doi:10.1109/ACCESS.2018.2870601.

[24] C. Lorenz et al., An SDN/NFV-enabled enterprise network architecture offering fine-grained security policy enforcement, *IEEE communications magazine* **55**(3) (2017), 217–223. doi:10.1109/MCOM.2017.1600414CM.

[25] F. Paganelli, M. Ulema and B. Martini, Context-aware service composition and delivery in NGSONs over SDN, *IEEE Communications Magazine* **52**(8) (2014), 97–105. doi:10.1109/MCOM.2014.6871676.

[26] S. Peng et al., Multi-tenant software-defined hybrid optical switched data centre, *Journal of Lightwave Technology* **33**(15) (2015), 3224–3233. doi:10.1109/JLT.2015.2438398.

[27] A.J. Ramadhan, Implementation of 5G FBMC PHYDYAS prototype filter, *International Journal of Applied Engineering Research* **12**(23) (2017), 13476–13481.

[28] A.J. Ramadhan, T-s3ra: Traffic-aware scheduling for secure slicing and resource allocation in sdn/nfv enabled 5 g networks, 2021, arXiv preprint arXiv:2107.05056.

[29] M.R. Raza et al., Reinforcement learning for slicing in a 5G flexible RAN, *Journal of Lightwave Technology* **37**(20) (2019), 5161–5169. doi:10.1109/JLT.2019.2924345.

[30] J. Ren et al., Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT, *Tsinghua Science and Technology* **27**(4) (2021), 760–776. doi:10.26599/TST.2021.9010046.

[31] K. Sha et al., On security challenges and open issues in Internet of Things, *Future generation computer systems* **83** (2018), 326–337. doi:10.1016/j.future.2018.01.059.

[32] A. Souri et al., A systematic literature review on formal verification of software-defined networks, *Transactions on Emerging Telecommunications Technologies* **31**(2) (2020), e3788. doi:10.1002/ett.3788.

[33] D. Wang et al., Resource management for secure computation offloading in softwarized cyber–physical systems, *IEEE Internet of Things Journal* **8**(11) (2021), 9294–9304. doi:10.1109/JIOT.2021.3057594.

[34] Y. Wang et al., Security-aware resource sharing in software defined air-ground integrated networks: A game approach, in: *GLOBECOM 2020–2020 IEEE Global Communications Conference*, IEEE, 2020.

[35] H. Wu et al., Security inspection resource allocation in real time using SDN, *Security and Privacy* **4**(6) (2021), e174. doi:10.1002/spy2.174.

[36] X. Xu et al., Secure service offloading for Internet of vehicles in SDN-enabled mobile edge computing, *IEEE Transactions on Intelligent Transportation Systems* **22**(6) (2020), 3720–3729. doi:10.1109/TITS.2020.3034197.

[37] B. Yi et al., Cost and security-aware resource allocation in optical data center networks, *IEEE Communications Letters* **23**(11) (2019), 2031–2035. doi:10.1109/LCOMM.2019.2933210.

[38] B. Yi et al., Novel resource allocation mechanism for SDN-based data center networks, *Journal of Network and Computer Applications* **155** (2020), 102554. doi:10.1016/j.jnca.2020.102554.

[39] X. Zuo et al., A security-aware software-defined IoT network architecture, in: *2020 IEEE Computing, Communications and IoT Applications (ComComAp)*, IEEE, 2020.