Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

A Survey of Load Balancing and Security in Software Defined Networks

[1]Mr.M.Sabarish, [2]Dr.P.Mayilvahanan
[1]*Research Scholar, Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India,sabarish84@gmail.com*
[2]*Professor & Head, Department of Computer Science, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies (VISTAS),Chennai, India, mayil.scs@velsuniv.ac.in*

Abstract: The promise of greater network application creativity and the notion of software-defined networking have gained traction in the networking industry due to reduced network carrier prices (SDN). Developers are eager to unleash a range of new hardware, applications and services that meet SDN requirements, fueled by the enthusiasm of holistic network visibility and the ability to configure network applications. However, in the midst of it all, there is one thing that stands out; one crucial aspect has just recently joined the discussion: network security. This paper surveys protection in SDN, introducing both research and industry advancements in this field. The complexities of protecting the network from persistent attackers are addressed, as is the systemic approach to security design needed for SDN. The efficient routing schemes are necessary to achieve load balancing in SDN, so a comprehensive survey is taken in the existing methods in with the hope of advancing SDN and inspiring new solutions.

Keyword: SDN; Load Balancing; network security; SDN Security.

I. INTRODUCTION

After its inception some ten years ago, SOFTWARE-DEFINED NETWORKING (SDN) has risen to the forefront of the networking agenda. SDN (Software-Defined Networking) is a modern networking architecture in which traffic routing primitives are separated from network control and management. The conventional networking architecture is viewed as static and stagnant as it was designed for one specific form of traffic, namely monotonous text-based content, making it unfit for today's immersive and complex multimedia streams created by increasingly demanding consumers. In addition to interactive trends, the latest Internet of Things (IoT) developed new specialised services with higher levels of accessibility to facilitate the creative use cases. SDN distinguishes the control plane, which includes physical connections and network components, from the data plane, which influences network output. SDN (Software-Defined Networking) is a new network architecture that aims to improve network management and allow networking developments. [1-5].

Load balancing is a valuable tool for the management of network traffic, allocation and increased utilisation of network services. Installation of a number of controllers, including Onix and Hyperflow, solves the bottleneck problem of clustered SDN. Load balancing among multiple controllers, on the other hand, would have an effect on network efficiency [6]. SDN can be used for accelerated infrastructure rollout and virtualization due to its coherent and global control plane view. [number seven]. As the Internet develops rapidly and technological developments take place, SDN is allowing programming and simpler management and quicker growth in the networking industry to revolutionize[8]. Decoupling control and data planes in physical systems like software-dependent networks (SDNs) or virtualization functions in the network (NFVs) makes balancing operations more flexible through multiple infrastructure resources, or to allocate resources to different customers [9]. In comparison to the conventional load balancing approach, Openflow provides another form of load balancing architecture method, the server load balance based on SDN. [10].

The control plane and data plane are merged into a single plane in a traditional network. It becomes more impossible to maintain a network as it increases in complexity. Software Defined Networks can help solve this problem (SDN). SDN (software oriented networking) is a hybrid network architecture that extends the functionality of traditional networks. Control messages are continuously sent and received to and from network switches to allow the network conditions to be tracked and managed via the SDN controller. [11-15].

Dynamic flow control is important in data centres because efficient access to computing and storage resources is critical for end-user Quality of Experience (QoE). Load balancing requires traffic to be distributed uniformly across different routes, allowing the network to handle more data with less time. Workflow in data centres can be modified dynamically using SDN to handle workloads more effectively. SDN simplifies and enhances network management

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

by separating the control and data planes and using complex control mechanisms. Software-defined networking (SDN) is a modern network architecture that expands on the existing network capabilities.[16-19].

SDN has arisen as a modern and promising model for transitioning from current networks to the Future Internet to have programmability and control simplicity. The advancement of information and communication systems is central to the evolution of human culture. SDN centralises network status and is based on the controller that operates in the control plane. The data plane is in charge of data forwarding, while the control plane is in charge of routing decisions. One of the disadvantages of an SDN is that it cannot tolerate extreme temperatures loss in large-scale datacenter networks. While current solutions based on switch migration strategies can address unequal load distribution in multiple controllers, some of these approaches do not take network balancing into account. Since network balance has a direct impact on network efficiency, enhancing balancing is critical for the network. The unified solution employs a dedicated super controller who collects the loading statuses of all other controllers and coordinates traffic delivery. [20-26].

Hybrid SDN networks can be used to reap any of the SDN paradigm's advantages without deploying a complete SDN network. An Internet Service Provider (ISP), for example, SDN-enabled switches, on the other hand, can normally only accept tens of thousands of forwarding entries. While software-defined networking (SDN) offers a viable alternative, In the short term, complete deployment of SDN is currently inaccessible. The hybrid SDN/open shortest path forwarding network (OSPF) will implement SDNs in legacy networks. In the other hand, Hybrid SDN/OSPF faces a number of technological, financial and organisational problems.[27-29].

In today's planet, there are billions of linked objects that can feel, touch, and influence their surroundings. These objects constantly gather data from all over the place, interpret it, and then cause behaviours, allowing a whole new generation of apps and services that are transforming our lives. The Internet of Things (IoT) is a technological phenomenon that has added a new dimension to the field of information technology. Since the Internet of Things (IoT) integrates each computer with network capabilities, a unique protection framework must be devised. As one of the most effective innovations, the Internet of Things has been influential in gaining the interest of a diverse variety of researchers and industries. The massive growth in IoT infrastructure has raised concerns about network protection for IoT devices and the ability for hackers to abuse access and, as a result, disengage the networks on which they depend. [30-41].

As a result of advances in technology and increased skills, the demand for service links will increase, which puts more pressure on the server. The likelihood of overload is also growing. The problem of server cluster traffic congestion is solved using load balancing technologies. Load balancing has been one of the hot spots among the vast number of SDN-related researches because it is an important topic for industrial concerns. The primary goal of load balancing is to disperse traffic in the network in order to prevent congestion, which can result in low network efficiency. [42-45].

SDN provides a logical central control paradigm for the deployment and management of programmable networks by using the principle of data plane and control plane decoupling [1] over a well-defined and understandable controlling protocol such as OpenFlow. Machine-to-Machine (M2M) networks and their service systems have arisen as a critical technology aimed at connecting computers to the Internet in order to deliver advanced cloud applications without the need for human interference. Many applications in the area of networks and the Internet necessitate fast data processing speeds, precision, reliability, and service quality. As a result, several ideas have been suggested to improve the Internet and computer networks with high quality of operation, one of which is software based network-IoT. (SDN-IoT) [46-49].

Ant Colony Optimization (ACO) is a modern heuristic algorithm for distributed computing, constructive information feedback and heuristic study, widely employed in a wide range of fields including NoC device load balancing, bin packing, job shop shop scheduling, routing problems, etc. Inefficient and stagnant are also traditional load balancing algorithms. Therefore, SDN needs a new algorithm for load balancing. This article provides a Joint Load Load Balancing (JLB) Algorithm, which not only balance the loading of the server, but also the loading of the data link. A load-balancing algorithm (DSLB) and a hybrid routing algorithm are used in the jlb algorithm (HRA).In order to construct HRA algorithm, the Shortest Path Algorithm and the Ant Colony System (ACS) algorithm have been merged. [50-55].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

II. LITERATURE SURVEY

SDN security is discussed, with research and industry advances in this area provided. Network virtualization (NV) uses containers to isolate functions while sharing hardware infrastructure, resulting in lower costs, improved network service deployment, and network performance. After providing the reader with a perspective on such emerging stateful SDN data plane ideas, we turn our attention to the security consequences of data plane programmability. [1-5].

They parameterize server capacity and use stochastic latency as the metric to aid load balancing inference. They also suggest a flow table that is complex modelling algorithm based on the combination of "single flow table" and "group flow table." The proposed SDN-based algorithm improves processing speed, predicts the loaded VM in high-load situations, and optimises resource usage. SMCLBRT is a response time-based loadbalancing technique for multiple SDN controllers that consider the changing characteristics of real-time reaction times vs. controller loads.SHLB also eliminates transfer migrations between controllers and significantly increases network efficiency. [6-10].

Qiaozhi Xu et al. [6] To reduce the effects of switch migrations on network output and to manage control plane load more effectively, SHLB has been introduced, a paradigm for the modular and hierarchical load balancing for a distributed SDN control plane. As seen in figure 1, SHLB inserts an intermediate plane between the control and data planes. The control plane consists of several controllers, who receive and process mid-plane message until the results are returned to the medium-plane; the mid-plane receives packet-in messages from the data plane before returning the results of the controller to the data plane.

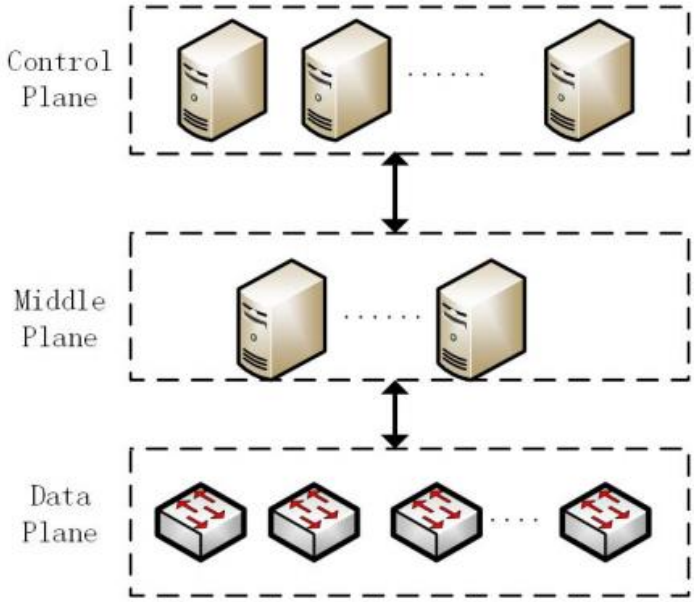

Figure1. Architecture of the SHLB.

S.WilsonPrakash and colleagues [7] The server virtualization is built using Libvirt, a common open source virtual machine management application programming interface that supports a wider variety of hypervisors and virtualization. Libvirt includes OpenStack, the most used open source cloud platform, as a default driver. On hypervisors, it can start, stop, and migrate virtual machines. The live migration is carried out at each migration by copying the whole disc.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

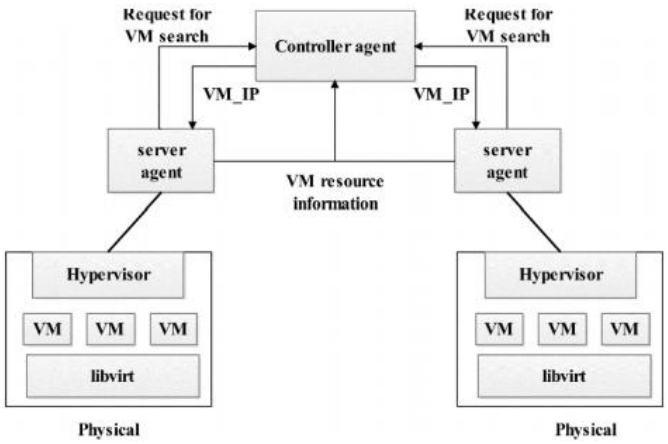

Figure2. DA-LB Architecture

The server agent in the DA-LB architecture seen in Figure 2 receives a user request and assigns a VM based on the desired configuration. The server agent sends a relocation request to the administrator when a virtual machine gets overburdened. The controller then uses a Back Propagation Artificial Neural Network algorithm to choose the best VM for the job. BP-ANN takes into account CPU use, memory utilisation, and response time. The output neuron assigns the VM and configures the IP address for the VM migration after processing the order.

Jie Cui and his associates[8]. They proposed SMCLBRT to balance multiple controls overloaded in the distributed SDN control aircraft, which uses reaction time to make fine-grained decisions on overloaded controllers. In the SDN control plane, load balancing, like other transfer migration systems, is divided into three stages:the calculation of controller load imbalance; the collection of overwhelmed controllers, main load switches, and immigration controllers for migration plans; as well as the execution of migration strategies to change the loads of overwhelmed controllers.

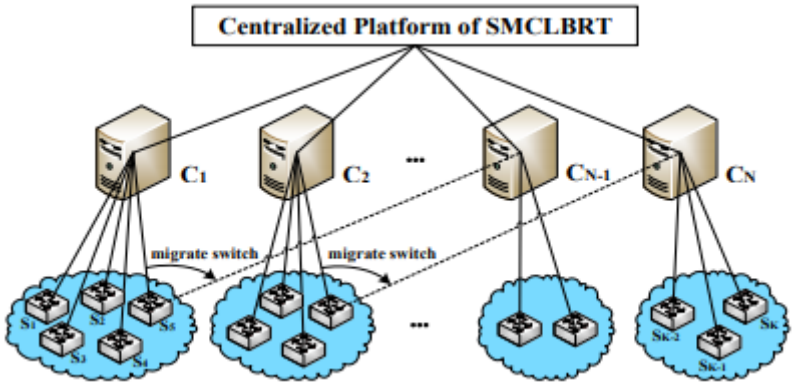

Figure3. System model of SMCLBRT.

They introduced a new load balancing system to resolve the problem of dynamic controller delivery (DCPP) of SDN based on switch migration. Six features of SDN improved transmission efficiency: bandwidth ratio, hop count, latency, packet overhead, trust, and packet loss. In cases where the server-side infrastructure becomes overloaded, the suggested solution outperforms non-SDN methods as compared to a conventional load balancing scheme. The key contribution of this research is the SDN centralised control environment load balancing architecture which can be used anywhere within a network. The proposed model employs Monte Carlo simulation to produce future predictions of the load balancing technique's behaviour. The obtained findings were analysed using Value at Risk (VaR) and statistics to obtain a full picture of the load balancing action. [11-15].

They suggest a hierarchical control plane-based dynamic and adaptive load handling method for distributed controllers in SDN. Hadar Sufiev proposed a new multi-controller SDN architecture. They suggested a dynamic load-balancing system that adjusts rules in the SDN flow table to minimise response time. The binary tree in our

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

scheme can be adjusted based on the demand on each server. They suggested a dynamic load management algorithm based on SDN for maximising connection usage in DCNs when taking flow priority into account. [16-19].
Wen-Hwa Liao and colleagues [19] The controller in the SDN network framework is used to dynamically update the flow chart. When a server's capability is exceeded, the SDN controller gathers and saves the state and adjusts the load balancing structure by changing the flow table automatically. First, the system handles the SDN network's servers and generates a flow table using wildcard rules. The flow table is used for the load balancer switch to balance the network workflow and decide when a goal server is available. The load balancer switch sends a user request to the server as usual if the server can handle it. The load balancer transfer notifies the dispatcher whether the server is at full, and the dispatcher changes the flow table so that the server can process the request, as seen in Fig. 4.

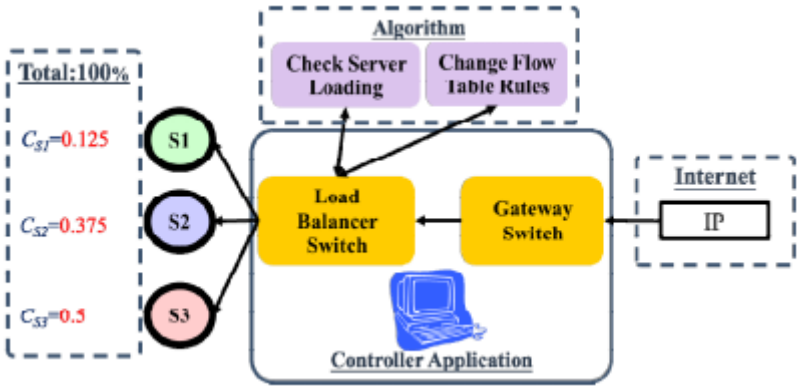

Figure4. Structure of dynamic load balancing in SDN.

They proposed a load balancing mechanism based on a load telling method for many distributed controllers. They suggested a load adjustment system for each controller to achieve load balancing among controllers. On SDN controllers with multicore architecture, a hierarchical system of load balancing routing is proposed. They suggested a load handling system for multiple controllers dependent on switch groups.Three architectures are suggested, all of which are intended to be compatible with all current OpenFlow, OpenStack, and OpenDaylight platforms. Throughput and reaction time were used to assess performance. They start by calculating the total cost of the flow order, which includes switch weights, switch-to-controller routing costs, and inter-controller routing costs. [20-26].

The design of our proposed distributed judgement, as proposed by Jinke Yu et al. [20], is depicted in Fig. 5. The controller-to-switch relationship in this architecture is many-to-many, which is provided by OpenFlow 1.3 or higher. JGroups are used for control plane connectivity and teamwork. In this architecture, our suggested load balancing method is implemented as a load balancing module in each SDN controller.

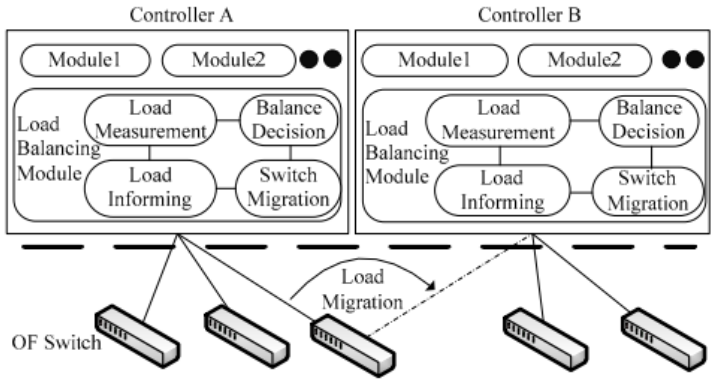

Figure5.The architecture of the proposed distributed decision.

Wael Hosny's formal name is Wael Hosny. Fouad Aly et al. [22] Propose the model for Controller Adaptive Load Balancing Technique (CALB), discussed. In a multi-controller SDN paradigm, CALB attempts to balance load over

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

multiple controllers. CALB takes into account the delay between the switches and their slave controllers to reduce the reactions duration. CALB assumes that the main controller is linked to n slave controllers. A master controller is connected to two slave controllers in Figure 6.

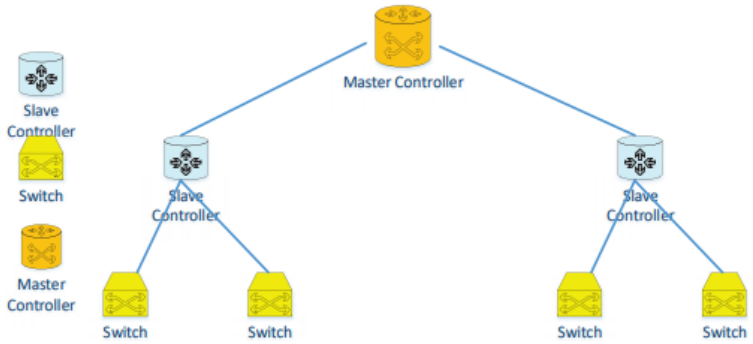

Figure6. Two slave controllers connected to a Master controller.

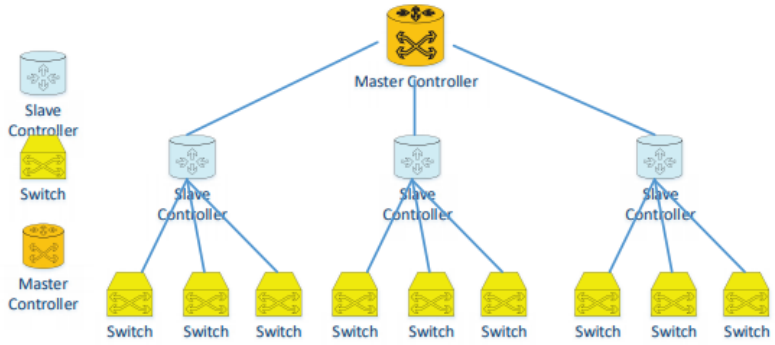

Figure7. Three slave controllers connected to a Master controller.

A CALB with a master controller and three slave controllers is shown in Figure 7. A set of switches connects each slave controller.

They use this taxonomy to do a thorough analysis of existing hybrid SDN network research, Finding holes and defects in the existing information body. We draw recommendations for more research on hybrid SDN networks on the basis of recent research findings, as well as detected holes and weaknesses. They began by applying the latest technology to optimise energy efficient routing and load balance globally. You have a classic hybrid load management system, BLEND. It encourages network component collaboration and takes advantage of both a global perspective and fast end-host action. [27-29].

They provide an overview of common SDN security issues when linked to IoT clouds, as well as an explanation of the Blockchain model's design concepts, and argue for the factors that make Blockchain a major security driver for solutions involving SDN and IoT. Centered on SDN standards, a distributed approach for accelerating data management and managing the load between IoT devices is proposed. They will discuss the security issues in SDN as well as a stable architecture for IoT in an SDN-based network. Their paper aims to provide an outline of SDN as well as a detailed discussion of SDN-based IoT implementation styles, such as centralised and decentralised.They will propose a proposal for IoT security focused on SDN and Cloud integration. [30-35].

Yanbing Liu et al. [38] Middlebox-Guard, Built an SDN-based data transfer protection model (MG). Reduce the difficulty of the network by balancing the data flow correctly in order to make sure the network operates securely. Firstly, according to different security policies, data flow abstractions and heuristic algorithms are used to locate middle boxes linked to the given protected policies in the most suitable places. In M-G, a pruning algorithm is proposed to overcome the limitations of transference volume in an offline integer linear programme (ILP) and to prevent the use of any midbox. An online linear programme (LP) formulation for the balancing of loads is also developed. In conclusion, secure protocols are recommended to deal with different risks. Via dataflow control protocols that are generated by combining tunnels and tags, network routing is scalable. Experimental results show that this model can improve protection performance and manage data stream in an SDN IoT environment efficiently.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

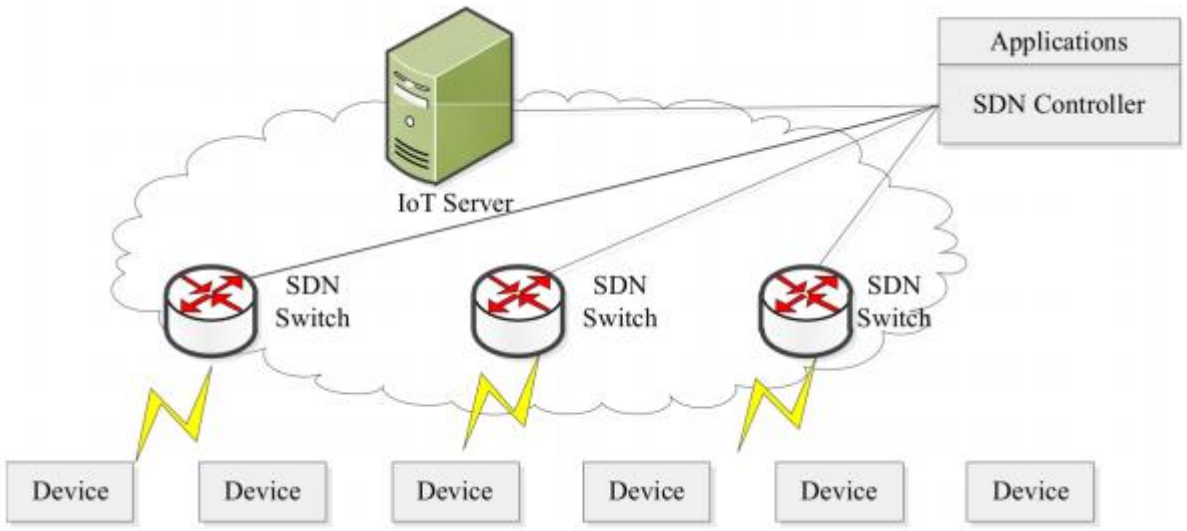

Figure8. SDN-based IoT architecture.

Kallol Krishna Karmakar et al. [39] proposed a security architecture for IoT networks that takes advantage of the fundamental capabilities of Software Defined Networks (SDN). Authorization is accomplished by the use of a complex policy-driven approach. Such an advanced security solution entails IoT system protection and allows approved flows to secure IoT networks from malicious IoT devices and attacks. In their report, they provide an outline of the security and performance of the suggested security protocols and their implementations.

Muhammad Arief Nugroho et al. [43] On web servers operating on SDN networks, The testing of the load balancing algorithms Least Connection and IP Hash was suggested. Some algorithms lack a service attachment feature, which does not occur on a web server with linked functions such as login session function. As a consequence, a possible function algorithm was developed. The Hash and Least Connection IP algorithms are two examples of algorithms that may be useful in this web server's case. Last Connection and IP Hash algorithms have strengthened and checked the utility for charging. This validation test would test all algorithms against a series of essential Web Server parameters. The criteria concerned are response time, processing and the utilisation of resources. In terms of response time the IP Hash algors outperform the LDC algorithm by 17 percent, throughput by 10%, and memory use by 8%, according to the results of the parameter checks.

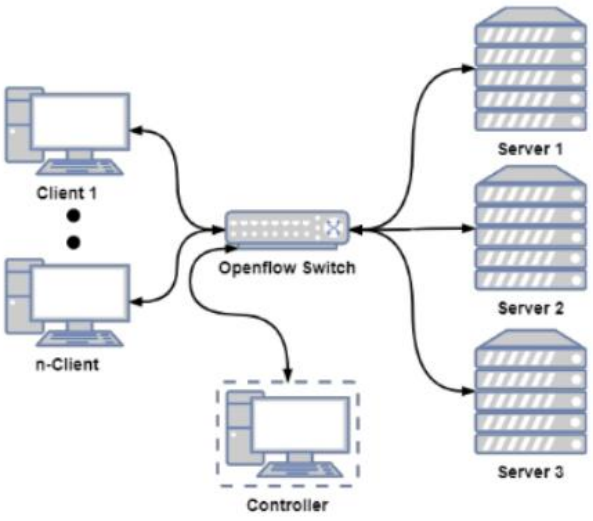

Figure 9. System Architecture.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

figure 9 used to implement the system.
The machine is made up of many devices, which are as follows:

- User: a computer or client that connects to the database server.
- Openflow switch: a network policy process against the network and assists in packet forwarding.
- Cloud Server: a computer that offers web resources or software..

Hailong Zhang et al. [45] used the new SDN network architecture to incorporate two load balancing algorithms. A static scheduling algorithm and a dynamic scheduling algorithm are also available. In terms of efficiency, our experiments show that the dynamic algorithm outperforms the static algorithm.

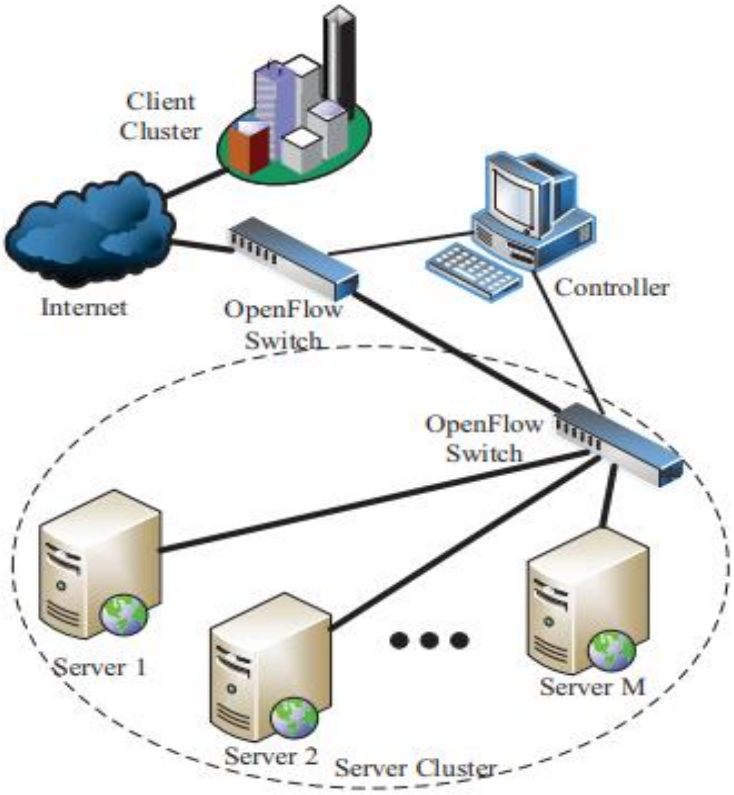

Figure 10. Structure diagram of OpenFlow load balancing.

The fundamental concept behind the OpenFlow load balancing philosophy is to replace expensive and statically specified hardware components in clusters with an OpenFlow controller that executes load balancing strategies using the local network infrastructure. Figure 10 shows the OpenFlow load balancing structure diagram. Using an OpenFlow flow table, the controller can handle data transmission.

Yu-Jia Chen et al. [49] suggested a traffic-aware load balancing scheme for machine-to-machine (M2M) networks focused on software-defined networking (SDN). To relieve the high demand load caused by bursty traffic, M2M networks need load balancing strategies. The proposed load-balance system would fulfil various service quality (QoS) specifications by traffic detection and reprocessing by leveraging the capacity of SDN to track and manage the network. Experiments show the expected operation response time to a non-SDN load balancing unit will be reduced by up to 50%.

Jingmei Li et al. [55] proposed a Software Defined Network-based Joint Load Balancing Algorithm. Not just data link load balance, but server load balance is taken into consideration in this paper's algorithm. The Ant Colony System is coupled with the Shortest Path Algorithm in the Hybrid Routing Algorithm. In this document, the Joint Load Balancing Algorithm proposed as a load balancing module is implemented and simulated by Mininet on the OpenDayLight controller. The findings of the tests demonstrate the efficiency of the algorithm. The algorithm

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

proposed in this paper exceeds the shortest path survey and random algorithms with regard to network efficiency, better network performance and lower latency.

Table I. Comparison of Average accuracy, Precision, Recall, F1-score

	Average accuracy	Precision	Recall	F1-score
J48	81.05	79	72	72
Navie Bayes	76.56	82	73	72
NB Tree	82.02	83	75	75
Random Forest	80.67	83	76	74
Random Tree	81.59	84	78	76
Multi-layer Perceptron	77.41	86	77	78
Support Vector Machine (SVM)	69.52	84	79	77
DNN	75.75	87	75	79

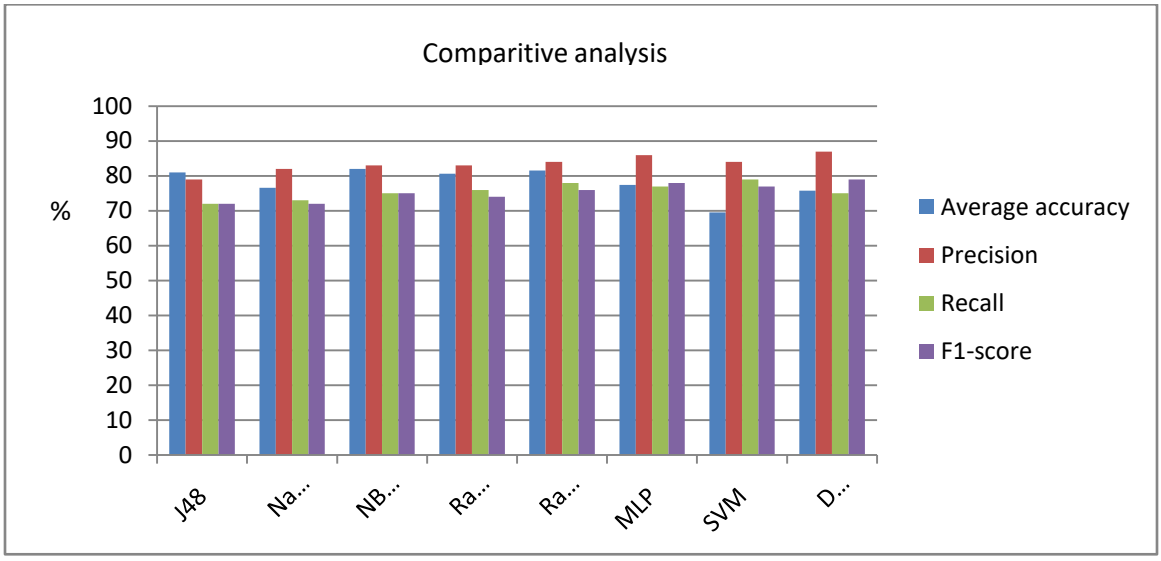

Figure1. Comparison of Average accuracy, Precision, Recall, F1-score

Table II. Comparison of different analysis in various paper

s.no	year	Author	Title	Analysis
1	2018	Yu	Fault management in software-defined networking: A survey	SDN reliability, SDN faults, fault classification, system monitoring, fault diagnosis, fault recovery and repair, fault tolerance.
2	2015	Scott-Hayward	A survey of security in software defined networks.	SDN, network security, OpenFlow, secure SDN architecture.
3	2016	Sheetal Chaudhari	SDN Network Virtualization Survey	Hypervisor, network virtualization, vSDN, hSDN, OpenFlow (OF) , HyperFlex, FlowVisor, VeRTIGO.
4	2017	Tooska Dargahi	A Survey on the Security of Stateful SDN Data Planes	Stateful SDN Data Planes, Data Plane Programmability, SDN Security, Vulnerability

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

				Assessment, OpenFlow, OpenState, P4
5	2017	Bannour	Distributed SDN control: Survey, taxonomy, and challenges.	Distributed Control, Network Management, Quality of Experience (QoE), Adaptive and Automatic control approaches, Programmable Networks.
6	2018	Sayali Patil	Load Balancing Approach for Finding Best Path in SDN	(Dynamic Source Routing, Ad hoc On Demand Distance vector
7	2018	M.C. Nkosi	Multi-path Load Balancing for SDN Data Plane	OpenFlow, Data Plane, Controller, Load balancing
8	2019	Sejun Kim	Load Balancing for Distributed SDN with Harmony Search	DCPP (dynamic controller provisioning problem), switch migration, harmony search, SDN, K-means clustering
9	2019	Aymen Hasan Alawadi	Risk Analysis of Blocked Rate Predictions for SDN Load Balancing Using Monte Carlo Simulation	Risk analysis, Value-at-Risk, Simulation, Measurements techniques
10	2018	Qiaozhi Xu	A Scalable and Hierarchical Load Balancing Model for Control Plane of SDN	Distributed SDN, Load balancing, Load management, Network balancing, Control plane
11	2019	Tiago Oliveira	QoE-based Load Balancing of OTT Video Content	OTT, SDN, QoE, Load Balancing
12	2018	Jie Cui	A Load-balancing Mechanism for Distributed SDN Control Plane Using Response Time	load-balancing, multiple controllers, response time, switch migration
13	2015	Mao Qilin	A Load Balancing Method Based on SDN	Load Balancing; SDN, OpenFlow; Group Flow Table
14	2016	Hao Wang	Load Balancing - Towards Balanced Delay Guarantees in NFV/SDN	of load balancing, service latency, stochastic delay bound
15	2019	S.WilsonPrakash	Artificial Neural Network Based Load Balancing On Software Defined Networking	Load balancing, C SDN, enter, Hypervisor, Artificial Neural Network
16	2016	Hadar Sufiev	A Dynamic Load Balancing Architecture for SDN	Load balancing; Scalability; Software-defined networking.
17	2018	Wenjing Lan	A Dynamic Load Balancing Mechanism for Distributed Controllers in SoftwareDefined Networking	OpenFlow; Load Balancing; Distributed Controller
18	2016	Wen-Hwa Liao	Dynamic Load-Balancing Mechanism for Software-Defined Networking	load balancing; OpenFlow
19	2017	Umme Zakia	Dynamic Load Balancing in SDN-Based Data Center Networks	Data center networks; dynamic load balancing algorithm; software defined networking;
20	2018	Kai-Yu Wang	An Efficient Load Adjustment for Balancing Multiple Controllers in Reliable SDN Systems	OpenFlow, SDN, Multiple controllers, Load balance
21	2019	Wael Hosny Fouad Aly	Controller Adaptive Load Balancing for SDN Networks	Fault tolerance, OpenFlow, load balancing, switch

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

				migration
22	2015	Dharmendra Chourishi	Role-Based Multiple Controllers for Load Balancing and Security in SDN	controller, security, load balancing
23	2016	Jinke Yu	A Load Balancing Mechanism for multiple SDN Controllers based on Load Informing Strategy	Future Internet; Load balancing; Load informing;
24	2018	Oleksandr Lemeshko	Hierarchical Method of Load Balancing Routing on SDN Controllers with Multicore Architecture	SDN controller; multicore arcitecture; load balansing routing; hierarchical method; coordination; flow;
25	2018	Peiying Tao	The Controller Placement of Software-Defined Networks Based on Minimum Delay and Load Balancing	load-balance; controller placement; delay
26	2017	Yaning Zhou	Load Balancing for Multiple Controllers in SDN Based on Switches Group	Load balancing; Network balancing; Time efficiency; Switches group
27	2020	RICHARD ETENGU	AI-Assisted Framework for Green-Routing and Load Balancing in Hybrid Software-Defined Networking: Proposal, Challenges and Future Perspective	Hybrid SDN/OSPF, traffic engineering, energy-aware routing, quality of service, scalable, machine learning, artificial intelligence, and deep reinforcement learning
28	2019	Lu Liu	An SDN-based Hybrid Strategy for Load Balancing in Data Center Networks	Data Center Networks, SDN, Load Balancing
29	2018	Rashid Amin	Hybrid SDN Networks: A Survey of Existing Approaches	Hybrid SDN network, Network management, Software Defined Networking (SDN), SDN controller, Traffic engineering.
30	2015	Kshira Sagar Sahoo	A secured SDN framework for IoT	IoT, Ad-hoc network

III. CONCLUSION

This paper is just a subset of SDN-features, which restricts it compared to the full SDN-flow. The proof was debated on both sides of the safety coin of the SDN: that using the characteristics of the SDN architecture, it is possible to enhance network security, and that the SDN architecture raises security problems. The result is that the work on network security upgrades through SDN has progressed. The publicly viable frameworks attest to this. However, research alternatives to some of the security problems proposed by SDN have been provided, such as how to minimise the possible harm from a malicious/compromised programme. The increasing protection interest of industry-sponsored standardisation and consulting organisations is encouraging work on these topics. A collection of topics for future study has been established after an analysis of the security literature in SDN. A common thread running through these discussions is the projection of future security vulnerabilities and the use of automated responses to respond quickly to network threats. As proven mitigation mechanisms of current network deployments are applied, established SDN protection problems resolved and SDN's dynamic, programmable and clear characteristics further exploited as software-defined networks may be more efficient than traditional networks. There is also a lot of work to be done before this vision becomes a reality.

References

[1]. Yu, Y., Li, X., Leng, X., Song, L., Bu, K., Chen, Y., ... & Xiao, X. (2018). Fault management in software-defined networking: A survey. IEEE Communications Surveys & Tutorials, 21(1), 349-392.
[2]. Scott-Hayward, S., Natarajan, S., & Sezer, S. (2015). A survey of security in software defined networks. IEEE Communications Surveys & Tutorials, 18(1), 623-654.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

[3]. Chaudhari, S., Mani, R. S., & Raundale, P. (2016, March). SDN network virtualization survey. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 650-655). IEEE.
[4]. Dargahi, T., Caponi, A., Ambrosin, M., Bianchi, G., & Conti, M. (2017). A survey on the security of stateful SDN data planes. IEEE Communications Surveys & Tutorials, 19(3), 1701-1725.
[5]. Bannour, F., Souihi, S., & Mellouk, A. (2017). Distributed SDN control: Survey, taxonomy, and challenges. IEEE Communications Surveys & Tutorials, 20(1), 333-354.
[6]. Patil, S. (2018, July). Load balancing approach for finding best path in sdn. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 612-616). IEEE.
[7]. Nkosi, M. C., Lysko, A. A., & Dlamini, S. (2018, December). Multi-path load balancing for SDN data plane. In 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC) (pp. 1-6). IEEE.
[8]. Kim, S., Ebay, S. K., Lee, B., Kim, K., & Youn, H. Y. (2019, January). Load balancing for distributed SDN with harmony search. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-2). IEEE.
[9]. Alawadi, A. H., & Molnár, S. (2019, June). Risk Analysis of Blocked Rate Predictions for SDN Load Balancing Using Monte Carlo Simulation. In 2019 IEEE Symposium on Computers and Communications (ISCC) (pp. 1028-1033). IEEE.
[10]. Xu, Q., Li, L., Liu, J., & Zhang, J. (2018, August). A scalable and hierarchical load balancing model for control plane of SDN. In 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD) (pp. 6-11). IEEE.
[11]. Oliveira, T., & Sargento, S. (2019, June). QoE-based Load Balancing of OTT Video Content in SDN Networks. In 2019 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-6). IEEE.
[12]. Cui, J., Lu, Q., Zhong, H., Tian, M., & Liu, L. (2018). A load-balancing mechanism for distributed SDN control plane using response time. IEEE transactions on network and service management, 15(4), 1197-1206.
[13]. Qilin, M., & Weikang, S. (2015, June). A load balancing method based on SDN. In 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation (pp. 18-21). IEEE.
[14]. Wang, H., & Schmitt, J. (2016, November). Load balancing-towards balanced delay guarantees in NFV/SDN. In 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 240-245). IEEE.
[15]. WilsonPrakash, S., & Deepalakshmi, P. (2019, April). Artificial Neural Network Based Load Balancing On Software Defined Networking. In 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS) (pp. 1-4). IEEE.
[16]. Sufiev, H., & Haddad, Y. (2016, November). A dynamic load balancing architecture for SDN. In 2016 IEEE International Conference on the Science of Electrical Engineering (ICSEE) (pp. 1-3). IEEE.
[17]. Lan, W., Li, F., Liu, X., & Qiu, Y. (2018, February). A dynamic load balancing mechanism for distributed controllers in software-defined networking. In 2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA) (pp. 259-262). IEEE.
[18]. Liao, W. H., Kuai, S. C., & Lu, C. H. (2016, July). Dynamic load-balancing mechanism for software-defined networking. In 2016 International Conference on Networking and Network Applications (NaNA) (pp. 336-341). IEEE.
[19]. Zakia, U., & Yedder, H. B. (2017, October). Dynamic load balancing in SDN-based data center networks. In 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 242-247). IEEE.
[20]. Wang, K. Y., Kao, S. J., & Kao, M. T. (2018, April). An efficient load adjustment for balancing multiple controllers in reliable SDN systems. In 2018 IEEE international conference on applied system invention (ICASI) (pp. 593-596). IEEE.
[21]. Aly, W. H. F. (2019, July). Controller adaptive load balancing for sdn networks. In 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 514-519). IEEE.
[22]. Chourishi, D., Miri, A., Milić, M., & Ismaeel, S. (2015, May). Role-based multiple controllers for load balancing and security in SDN. In 2015 IEEE Canada International Humanitarian Technology Conference (IHTC2015) (pp. 1-4). IEEE.
[23]. Yu, J., Wang, Y., Pei, K., Zhang, S., & Li, J. (2016, October). A load balancing mechanism for multiple SDN controllers based on load informing strategy. In 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS) (pp. 1-4). IEEE.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

[24]. Lemeshko, O., Nevzorova, O., Rossikhin, V., & Hailan, A. M. (2018, October). Hierarchical Method of Load Balancing Routing on SDN Controllers with Multicore Architecture. In 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) (pp. 457-460). IEEE.
[25]. Tao, P., Ying, C., Sun, Z., Tan, S., Wang, P., & Sun, Z. (2018, August). The controller placement of software-defined networks based on minimum delay and load balancing. In 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 310-313). IEEE.
[26]. Zhou, Y., Wang, Y., Yu, J., Ba, J., & Zhang, S. (2017, September). Load balancing for multiple controllers in SDN based on switches group. In 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS) (pp. 227-230). IEEE.
[27]. Etengu, R., Tan, S. C., Kwang, L. C., Abbou, F. M., & Chuah, T. C. (2020). AI-Assisted Framework for Green-Routing and Load Balancing in Hybrid Software-Defined Networking: Proposal, Challenges and Future Perspective. IEEE Access, 8, 166384-166441.
[28]. Liu, L., Jiang, Y., Shen, G., Li, Q., Lin, D., Li, L., & Wang, Y. (2019, June). An SDN-based hybrid strategy for load balancing in data center networks. In 2019 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-6). IEEE.
[29]. Amin, R., Reisslein, M., & Shah, N. (2018). Hybrid SDN networks: A survey of existing approaches. IEEE Communications Surveys & Tutorials, 20(4), 3259-3306.
[30]. Sahoo, K. S., Sahoo, B., & Panda, A. (2015, December). A secured SDN framework for IoT. In 2015 International Conference on Man and Machine Interfacing (MAMI) (pp. 1-4). IEEE.
[31]. Djouani, R., Djouani, K., Boutekkouk, F., & Sahbi, R. (2018, October). A Security Proposal for IoT integrated with SDN and Cloud. In 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1-5). IEEE.
[32]. Sambandam, N., Hussein, M., Siddiqi, N., & Lung, C. H. (2018, December). Network security for iot using sdn: Timely ddos detection. In 2018 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-2). IEEE.
[33]. Karmakar, K. K., Varadharajan, V., Nepal, S., & Tupakula, U. (2020). SDN enabled secure IoT architecture. IEEE Internet of Things Journal.
[34]. Aggarwal, C., & Srivastava, K. (2016, October). Securing IoT devices using SDN and edge computing. In 2016 2nd International Conference on Next Generation Computing Technologies (NGCT) (pp. 877-882). IEEE.
[35]. Eghbali, Z., Lighvan, M. Z., & Beheshti, A. (2019, July). An Efficient Distributed Approach for Load Balancing in IoT Based on SDN Principles. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
[36]. Tselios, C., Politis, I., & Kotsopoulos, S. (2017, November). Enhancing SDN security for IoT-related deployments through blockchain. In 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 303-308). IEEE.
[37]. Wang, S., Gomez, K. M., Sithamparanathan, K., & Zanna, P. (2019, December). Software Defined Network Security Framework for IoT based Smart Home and City Applications. In 2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS) (pp. 1-8). IEEE.
[38]. Hasan, T., Adnan, A., Giannetsos, T., & Malik, J. (2020, June). Orchestrating SDN Control Plane towards Enhanced IoT Security. In 2020 6th IEEE Conference on Network Softwarization (NetSoft) (pp. 457-464). IEEE.
[39]. Zheng, S. (2019, May). Research on SDN-based IoT security architecture model. In 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) (pp. 575-579). IEEE.
[40]. Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. IEEE Internet of Things Journal, 7(10), 10250-10276.
[41]. Liu, Y., Kuang, Y., Xiao, Y., & Xu, G. (2017). SDN-based data transfer security for Internet of Things. IEEE Internet of Things Journal, 5(1), 257-268.
[42]. Lin, T. L., Kuo, C. H., Chang, H. Y., Chang, W. K., & Lin, Y. Y. (2016, July). A parameterized wildcard method based on SDN for server load balancing. In 2016 International Conference on Networking and Network Applications (NaNA) (pp. 383-386). IEEE.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2978 - 2991
Received 25 April 2021; Accepted 08 May 2021.

[43]. Suwandika, I. P. A., Nugroho, M. A., & Abdurahman, M. (2018, May). Increasing SDN Network Performance Using Load Balancing Scheme on Web Server. In 2018 6th International Conference on Information and Communication Technology (ICoICT) (pp. 459-463). IEEE.
[44]. Raghul, S., Subashri, T., & Vimal, K. R. (2017, March). Literature survey on traffic-based server load balancing using SDN and open flow. In 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN) (pp. 1-6). IEEE.
[45]. Zhang, H., & Guo, X. (2014, November). SDN-based load balancing strategy for server cluster. In 2014 IEEE 3rd International Conference on Cloud Computing and Intelligence Systems (pp. 662-667). IEEE.
[46]. Ejaz, S., Iqbal, Z., Shah, P. A., Bukhari, B. H., Ali, A., & Aadil, F. (2019). Traffic load balancing using software defined networking (SDN) controller as virtualized network function. IEEE Access, 7, 46646-46658.
[47]. Chen, Y. J., Shen, Y. H., & Wang, L. C. (2014, December). Traffic-aware load balancing for M2M networks using SDN. In 2014 IEEE 6th International Conference on Cloud Computing Technology and Science (pp. 668-671). IEEE.
[48]. Chen, Y. J., Wang, L. C., Chen, M. C., Huang, P. M., & Chung, P. J. (2018). SDN-enabled traffic-aware load balancing for M2M networks. IEEE Internet of Things Journal, 5(3), 1797-1806.
[49]. Al-Jamali, N. A. S., & Al-Raweshidy, H. S. (2020). Intelligent Traffic Management and Load Balance Based on Spike ISDN-IoT. IEEE Systems Journal.
[50]. Huong, T. T., Khoa, N. D. D., Dung, N. X., & Thanh, N. H. (2019, October). A global multipath load-balanced routing algorithm based on Reinforcement Learning in SDN. In 2019 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1336-1341). IEEE.
[51]. Tkachova, O., Yahya, A. R., & Muhi-Aldeen, H. M. (2016, October). A network load balancing algorithm for overlay-based sdn solutions. In 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T) (pp. 139-141). IEEE.
[52]. Singhal, C., & Rahul, K. (2019, November). LB-UAVnet: Load Balancing Algorithm for UAV Based Network using SDN. In 2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC) (pp. 1-5). IEEE.
[53]. Wang, C., Zhang, G., Xu, H., & Chen, H. (2016, November). An ACO-based link load-balancing algorithm in SDN. In 2016 7th International Conference on Cloud Computing and Big Data (CCBD) (pp. 214-218). IEEE.
[54]. Li, J., Yang, L., Wang, J., & Yang, S. (2018, December). Research on SDN Load Balancing based on Ant Colony Optimization Algorithm. In 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC) (pp. 979-982). IEEE.
[55]. Giri, N., Kukreja, V., Panchi, D., Sajnani, J., & Seedani, H. (2018, August). Performance Evaluation of Load Balancing Algorithms for SDN. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-4). IEEE.