Computers, Materials & Continua
DOI:10.32604/cmc.2022.015546
Article

Tech Science Press

OTP-Based Software-Defined Cloud Architecture for Secure Dynamic Routing

Tae Woo Kim[1], Yi Pan[2] and Jong Hyuk Park[1,*]

[1]Department of Computer Science and Engineering, Seoul National University of Science and Technology (Seoultech), Seoul, 01811, Korea
[2]Department of Computer Science, Georgia State University, Atlanta, 30303, USA
[*]Corresponding Author: Jong Hyuk Park. Email: jhpark1@seoultech.ac.kr
Received: 27 November 2020; Accepted: 28 February 2021

Abstract: In the current era, anyone can freely access the Internet thanks to the development of information and communication technology. The cloud is attracting attention due to its ability to meet continuous user demands for resources. Additionally, Cloud is effective for systems with large data flow such as the Internet of Things (IoT) systems and Smart Cities. Nonetheless, the use of traditional networking technology in the cloud causes network traffic overload and network security problems. Therefore, the cloud requires efficient networking technology to solve the existing challenges. In this paper, we propose one-time password-based software-defined cloud architecture for secure dynamic routing to mitigating the above-mention issues. The proposed cloud architecture provides a secure data path through dynamic routing using One-Time Internet Protocol (OTIP) algorithm between each layer. On the network side, we use software-defined technology to provide efficient network management and data security. We introduce a software-defined cloud architecture that applies OTIP algorithms for secure dynamic routing. We conduct a comparative analysis between general IP communication and proposed OTIP communication architecture. It evaluates the performance of OTIP algorithms. Finally, we examine the proposed software-defined cloud architecture, including how to apply OTIP in secure dynamic routing according to the results of the comparative analysis.

Keywords: Secure routing; dynamic routing; one-time password; software-defined network; software-defined perimeter; cloud computing

1 Introduction

With the rapid development of information and communication technology and the activation of the Internet of Everything (IoE), anyone can access the Internet anytime, anywhere. In particular, IoE is rapidly developing with the evolution of the technological environment, personal internet storage, and machine learning based on big data [1,2]. Cloud is a next-generation method of computing that allows users to utilize as many computing resources as necessary through an Internet communication network whenever, wherever [3]. It offers the benefits of excellent

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

connectivity as accessed remotely and superior efficiency by allocating the required computing resources [4]. It is extensively used in a broad range of flexible systems such as smart cities, smart factories, and machine learning services [5,6]. Large-scale clouds use empowered edge that enables the main function of the edge and distributed cloud, which reduces the load on clouds by distributing them [7,8]. Given such wide array of cloud services, technologies such as software-defined cloud and blockchain-based cloud are being studied continuously [9]. Therefore, today's cloud must use faster and more efficient network methods, address network traffic problems, and veer away from existing network construction and operation methods [10,11]. Furthermore, there is a need for an effective cloud security technology so that the cloud can be protected against the many highly advanced and persistent threat attacks targeting the cloud.

Nonetheless, the widespread use of IT technology through the cloud gives rise to several problems. In its report on global networking trends in 2020, Cisco noted that "an increase of network traffic of great complexity and on an exponential scale is inevitable due to the explosion in the use of IoT devices, apps, and related data." In other words, the cloud is vulnerable to traffic problems when using existing networks, and it is a prime target of cyberattacks using vulnerabilities. So, the cloud is the central target of many attackers because it manages a lot of data. According to Checkpoint's 2020 Report on Cybersecurity, over 90% of enterprises were using certain types of cloud services as of 2019, and most of them have been attacked by cloud servers [12]. This is mainly due to cloud misconfiguration and management errors as well as Advanced and Persistent Threats (APTs) and network attacks.

In this paper, we propose an OTP-based software-defined cloud architecture for dynamic routing. For this purpose, we use a Software-Defined Perimeter (SDP) and a Software-Defined Network (SDN) to provide software-defined technological services. Network attacks can be dealt with by applying black cloud-based user identity authentication through the SDP, and network traffic problems can be mitigated by managing the network through the SDN. The OTP-based Internet Protocol (OTIP) algorithm is used for the control path between the controller layer, the SDN layer, and the data path between the user and the SDN layer. This algorithm provides safety against network sniffing, man-in-the-middle attacks, and advanced persistent threat attacks. We introduce the proposed software-defined cloud architecture and the OTIP algorithm for secure dynamic routing and present the results of a comparative analysis with existing IP communication through the OTIP algorithm. Finally, we discuss how software-defined cloud architectures with OTIP technology can be used in large-scale clouds that require secure routing.

2 Related Work

This section describes the core technology of the proposed software-defined cloud architecture and presents the requirements for the safe, efficient use of the cloud architecture. It also describes various relevant studies that have been conducted to meet the requirements of cloud architectures.

2.1 Core Technology

2.1.1 One-Time Password

One-Time Password (OTP) is an authentication technique that applies a single-use password. In this process, users cannot utilize the password again after authentication [13]. In general, passwords are disposable and are generated through proposed OTP algorithms. OTP generation is dependent on the S/Key methods wherein the OTP is generated by hash chain-based time synchronization [14]. The time synchronization method generates the OTP based on a certain time for both the client and the server. This does not require any input, and there are only

a few instances when the client either does not have to communicate or has to communicate. Therefore, the time synchronization OTP is safe against man-in-the-middle attacks and network packet sniffing in the process of client-to-server communication [15]. Nowadays, OTP is often used as part of the two-factor authentication method, and it is also commonly employed for mobile financial authentication, login authentication for Google, Amazon Web Services (AWS), and so on.

2.1.2 Software-Defined Network

Software-Defined Networks (SDN) utilize software-based controllers that are based on programming [16]. Network administrators are managed consistently and efficiently through central control [17]. It is appropriate to support intelligent networks for the proposed architecture work. Additionally, the SDN network programming supports network abstraction through software to decentralize networking devices or control to manage the network. SDN offers service flexibility and simplifies network management through the logical centralization of intelligence and controller. Through such simplification, SDN overcomes hardware and operational costs in large network structures [18].

SDN consists of an infrastructure layer, a control layer, and an application layer. The infrastructure layer is composed of network devices; OpenFlow technology, which is an interface standard between the control layer and the infrastructure layer, is generally used [19]. As a core element of SDN, the control layer has an essential role of software-defined forwarding as a data forwarding function. It is managed by the infrastructure layer with the SDN control software. In addition, network control and management are performed by receiving the network policy of the application layer through the Application Programming Interface (API). The application layer manages the SDN's network policy in an integrated manner [20]. It also performs global management abstraction that can control network elements and reactions according to events (topology change or new flow input, etc.)

2.1.3 Software-Defined Perimeter

Software-Defined Perimeter (SDP) is a virtually separated access control network framework based on user identity and terminal status information [21]. The core concept of the SDP is that identity and status approval is required before the user terminal is allowed to connect [22]. After completing identification, it is a pre-authentication and connection method that lets the user check the list of accessible resources according to the authority. In other words, an authorized user can check who can access it, and this is then provided with an individual and reliable secure connection. Conversely, if devices are not approved, they are "blocked," and the user will not be able to identify the target. The SDP dynamically creates individual segments that can be accessed according to the user's identity. This enables the establishment of highly sophisticated access control policies that ensure the establishment and operation of a consistent access policy in a heterogeneous cloud environment. Consequently, SDP is decreasing the operating costs through simplification of the network configuration. It has been evaluated as a flexible and scalable open architecture for cloud enterprise networks.

The SDP is composed of an SDP controller, an initiating host, and an accepting host [23]. As a key element of the SDP framework, the SDP controller communicates with all the SDP components and acts as a middle manager. It is also a reliable authenticator between the initiating host and the accepting hosts and is responsible for all control messages. Controller can be linked with various methods of authentication, such as certificate issuance, RADIUS, PKI, and OpenID. Meanwhile, the initiating host is an SDP client that processes a connection request for a service or an application. This request is submitted to the SDP controller in order to authenticate

information about the hardware or software in the initiating host. Once authentication is completed using the certificate stored in the SDP controller, the initiating host creates a mutual TLS tunnel that connects to the authorized server or application and accesses the server or application through this process. The accepting host is device that is instructed to accept an SDP controller-approved service or application. SDP is set to reject all packets and requests from all hosts except the services or applications approved by the SDP controller.

2.2 Requirement of Cloud Architecture Secure Dynamic Routing

The requirements of cloud architecture for secure routing is mentioned below which provides secure dynamic routing and stable cloud services. And address the problems such as insecure data paths, a rapid increase in traffic, and cloud security attacks on existing large-scale cloud systems.

Secure routing: The modern cloud performs its specific functions by subdividing the edge layer into specialized edges to manage large-scale clouds effectively. Control channels are used for cloud control through each specialized edge. The attacker targets a specific edge or aims to transmit the necessary data to an attacker. To acquire the authority of the cloud, attackers eavesdrop on packets through a man-in-the-middle attack or an IP spoofing attack. Cyber-attacks that target these clouds can create a threat to the entire cloud. To protect communication channels, the cloud must provide secure routing that establishes and manages secure communication paths.

Privacy: In the cloud, virtualization technology is used to make one single computing resource appear as multiple computing resources. In other words, a user gets allocated one computing resource and uses the same space. Thus, any ensuing privacy infringement can cause a great deal of damage in terms of user data and money. In particular, attention is paid to the management of access rights and to weak control areas. According to CSA, data are most vulnerable to misconfiguration or exploitation of privacy threats. All data accessed over the Internet, so provide the rights to access the data and provide security and privacy. Furthermore, if the logic, security, and verification of the data infrastructure are not completely controlled and managed, the control area becomes weak; this potentially results in problems such as data leak, data non-usability, and data corruption.

Data integrity: The cloud stores data from each client by using each non-overlapping data channel and provides data to the client. In the course of data processing, only authorized users can access, modify, or delete data. To ensure data integrity, it is essential to check whether a user who wants to change data is an authorized user.

Efficiency: The cloud's efficiency should be guaranteed that allows users to use the cloud resources. That way, users can pay in full the lowest cost to them according to the purposes and requirements. The cloud provides its resources according to the user requirements through virtualization technology, so it has an advantage in terms of preventing resource loss compared to the existing computing service. However, the existing system has limited efficiency due to the connection of a wide range of peripheral devices (IoT devices, clients) in a large-scale cloud system. It means that increased traffic wastes resources on unnecessary user access.

Scalability: Nowadays, the cloud does not merely store data but is combined with IoT systems and machine learning technologies. The cloud is to form large-scale cloud networks such as smart cities and smart factories. Therefore, when expanding to a large-scale network, the cloud system must be able to provide the same services as the existing system. It is a crucial requirement in using the cloud. If it does not get, there will be a risk of explosion of network traffic and data breaches from network attacks. So, it will fatally paralyze the network.

2.3 Existing Researches

Many existing studies have proposed architecture or a framework for dynamic routing, but this gives rise to various challenges. Singh et al. [24] proposed an NFV-SDP architecture that combines Network Function Virtualization (NFV) and SDP. NFV is a technology that combines virtualization technology with a network and is able to cope with network traffic flexibly. Still, NFV has certain security problems such as hypervisor attacks and Denial of Service (DoS) attacks due to virtualization technology. This problem is addressed through the use of NFV-SDP architecture, which enables the customization of deployment and access control to meet various user needs. The NFV-SDP architecture was tested in a virtual environment. As a result, it was found to be resistant to DoS attacks and is consequently effective in terms of security. Sallam et al. [25] proposed an SDP-SDN integrated architecture that integrates SDN and SDP. Through the widespread adoption of the SDN, network management can be simplified by reducing traffic, Capital Expenditure (CAPEX), and Operation Expenses (OPEX). Nevertheless, the widespread use of SDN poses a problem in terms of security. The architecture can be flexibly deployed so as to adapt to the needs of the general network security perimeter, port canning attacks, and denial of service (DoS) bandwidth attacks. In this respect, the proposed architecture is scalable from the network side through integration of the SDP and the SDN. Moubayed et al. [26] proposed an SDP security model to protect modern networks dynamically. The SDP secure network is a model that first needs to know how to check and authenticate a device's ID before accessing the application infrastructure. Security issues such as proper authentication, access control, data privacy, and data integrity arise in modern networks due to the use of virtualized networking technology. Many studies have been conducted on a security framework capable of dynamically protecting the network. According to the results of a performance evaluation, SDP security networks offer a resilient environment. It despite the longer initial connection set-up time for denial-of-service attacks and port search attacks.

Xie et al. [27] conducted a study on the SDP's initiating host protocol configuration algorithm. They proposed an initiating host protocol algorithm for the software-defined perimeter and studied an efficient SDP for the cloud model. The cloud infrastructure was changed by adding a message queue at the SDP's initiating host. Message queues mainly store control information in a queue in order to resolve the problem of maximum congestion and network congestion. Erdem et al. [28] proposed a One-time Password as a Service (OTPaaS), a cloud-based OTP architecture, for reliable user authentication. OTPaaS establishes an OTP provider in the process of authenticating a cloud service and performs cloud user registration, service provider activation, and authentication. OTPaaS can defend against attacks by outsiders, user disconnection properties, and attacks by OTP validators within the specified environment. El-Booz et al. [29] proposed a cloud storage system that combines time-based one-time password (TOTP) and automatic blocker protocol (ABP). The TOTP for user authentication and ABP are used to protect the system completely. The system consists of the following: 1) An organization manager with full control over the cloud, 2) a third-party auditor (TPA) who can audit the stored data in the cloud at the request of the administrator, and 3) a cloud service provider (CSP) that stores the data. The TOTP authenticates the user. The data communication process is audited by the TPA between the user and the cloud storage. Thus, if a problem occurs, access is blocked through the ABP.

Babiceanu et al. [30] proposed an integrated modeling environment that addresses virtual manufacturing system assurance through cybersecurity and resilience mechanisms for SDN applications. The proposed integrated modeling environment applies SDN to provide a cybersecurity and resilience framework for manufacturing process applications. A resilient-cybersecurity ontology

model and a mechanism are used to maintain the IIoT manufacturing system in a secure state. In addition, the proposed SDN-based manufacturing application is designed to connect to the existing system built to secure the safety and reliability of the Internet network. Nevertheless, the proposed manufacturing application modeling environment is intended to interoperate in an isolated environment and the Internet. The security and privacy aspects were not taken into account in manufacturing the applications, and related vulnerabilities may exist. Cao et al. [31] proposed a new SDN framework (SDQaaS) for QaaS with quantum key distribution as a service (QaaS) function in the SDN controller. The proposed framework suggests extended protocols for QaaS, workflows for intercommunication, routing, and SKR allocation. They verified the proposed approach by constructing an SDQaaS experimental testbed and performing a numerical simulation. The restricting framework provides efficient and flexible QaaS of the QKD network. QaaS can increase the probability of success of Quantum Key Distribution (QKD) service requests by gradually overcoming the requirements.

3 Proposed OTP-Based Software-Defined Cloud Architecture

This section presents the proposed software-defined cloud architecture, which provides OTP-based dynamic routing. The architecture uses a software-defined perimeter (SDP) based on user identity authentication. SDP copes with unauthorized user access and network attacks and complements. The architecture is combined with the software-defined network (SDN) to make it easier to cope with the large traffic. At its core, the OTIP algorithm is used for secure dynamic routing, and it is applied to the control channel between the device layer and the controller layer and the data channel between the SDN layer and the controller layer. This technology can solve the problem of network attacks on communication channels.

3.1 Design Overview

The OTP-based software-defined cloud architecture is composed of the server layer, the SDN layer, the controller layer, and the device layer as shown in Fig. 1. The device layer consists of devices that connect to the cloud. The controller layer is composed of a routing device that serves as an SDP controller. The authentication information and approved device information of each device in the network are stored in the SDP controller. It has an SDP link table where the path of the SDN layer is stored. A device certification table containing information on the approved device layer. The controller layer only allows access by authentication devices among the devices in the device layer. In addition, communication between the device and the SDN layer is carried out by allowing communicating with the SDN layer through the path of the SDN link table. The SDN layer is composed of an SDN-based router that efficiently manages the network. There are SDN link tables where the path of the controller layer is stored, including a server link table for data communication with devices. The SDN layer controls the controller layer by using a control channel that employs the OTIP algorithm, with the controller layer stored in the SDN link table. The path stored in the server link table is also communicated to the device through the data channel using the OTIP algorithm. The server layer is a data server where data are stored, and it provides data according to the request of the SDN layer.

3.2 One-Time Internet Protocol Algorithm

The One-Time Internet Protocol (OTIP) algorithm is an OTP-based IP change algorithm for secure dynamic routing. It is using for defending network attacks in specific communication channels with periodic changes in control and data channel. OTIP algorithms can change IP information periodically through time information using the OTP. Formula (1) is a mathematical

representation of an OTIP algorithm. Specifically, the OTIP can be used in a set private network by calculating the existing IP XOR operations with the OTP information generated. It is because NOR operations using subnet masks are performed for the proposed methodology.

$$Next\ IP\ Address = Generated\ OTP(4Byte)\ NOR\ SubnetMask\ XOR\ Current\ IP\ Address \quad (1)$$

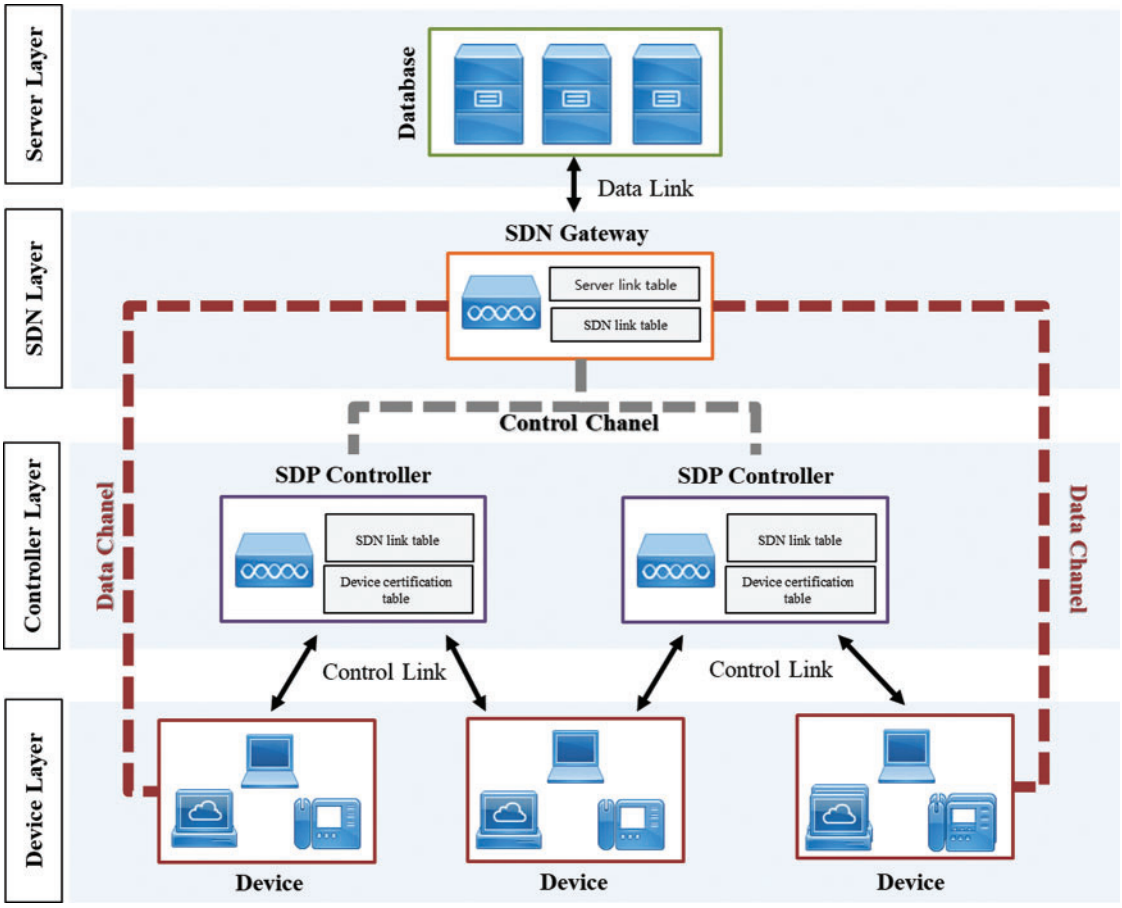

Figure 1: Proposed OTP-based software-defined cloud architecture

For example, assuming that the IP range of the private network is 192.168.0.1 to 192.168.0.127 as shown in Fig. 2, the subnet mask is 255.255.255.128. The devices in a private network should use IP addresses within the IP range, and the subnet mask is 255.255.255.128. The current IP address of a device is assumed to be 192.168.0.5, and the generated OTP, DA52CBA0.

The operation shown in Fig. 3 is calculated to generate the next IP. First, the NOR operation of the generated OTP and the subnet mask in the private network is performed. The network IP address is always 0, and the remaining host IP address is the NOR operation value. This is because the network IP address portion of the calculation result 1 and the current IP is filled with 0. The results of the existing IP address and the XOR operation always fall within the private network of the current IP, as in calculation result 2.

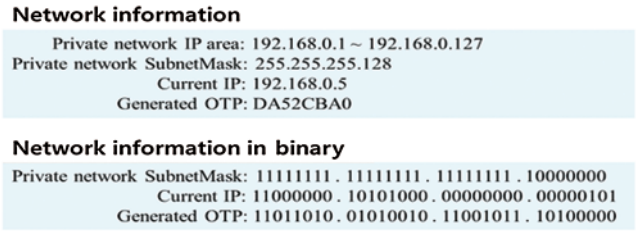

Figure 2: Information of private network

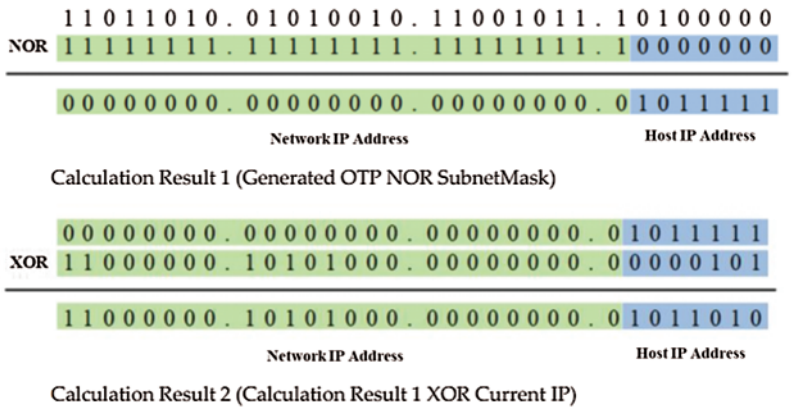

Figure 3: Result of OTTP calculation

The OTIP algorithm consists of four steps, which are as follows: 1) Use the current IP channel, 2) Generate the next IP, 3) Use the next IP channel and open a temporary channel, and 4) Close the temporary channel. These steps are depicted in Fig. 4. Here, the Use current IP channel step is a state wherein an existing IP address and the current IP address are utilized to generate the following IP address. The next IP generation step proceeds at a predetermined time between the two connected nodes making up the communication channel. This step generates the IP addresses within the scope of the private network through operations. The Use of the next IP channel and open the temporary channel step use the newly created IP address rather than the existing IP address. The existing IP channel is also opened as a temporary channel to prevent the loss of packets that are already being transmitted in the process of changing the IP address of the two nodes. Once the changed IP address has stabilized, the temporarily opened channel is deleted through the Close temporary channel step.

The OTIP algorithm can change the IP channel for communication regularly without prior consultation between the two communication nodes by employing the time-synchronization OTP. Thus, OTIP can effectively defend against MITM attacks and ARP spoofing attacks. As another advantage of OTIP, it is difficult to analyze packets through network sniffing as all the communication channels change periodically. In terms of packet communication, packet loss during IP changes over temporary channels is addressed, providing the same degree of reliability as the traditional IP method.

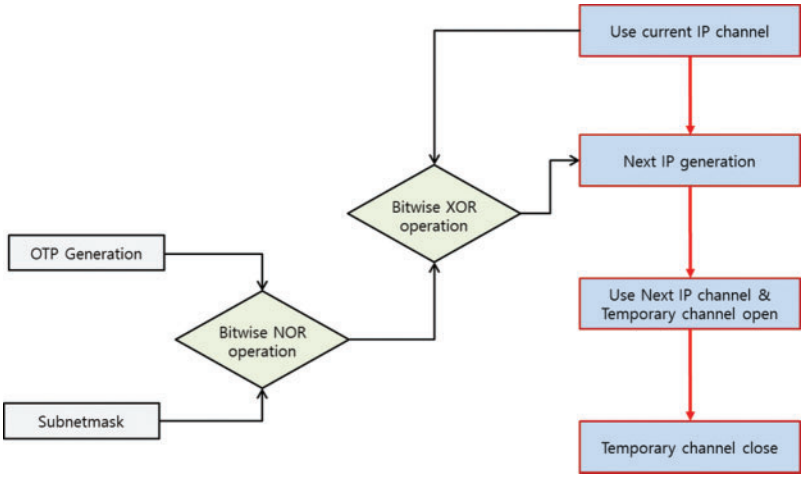

Figure 4: Flow chart of one-time Internet protocol

3.3 Methodological Flow of the Proposed Architecture

The proposed cloud architecture uses OTIP algorithms in controller-to-SDN and device-to-SDN communications. The operational process of the cloud works is shown in Fig. 5.

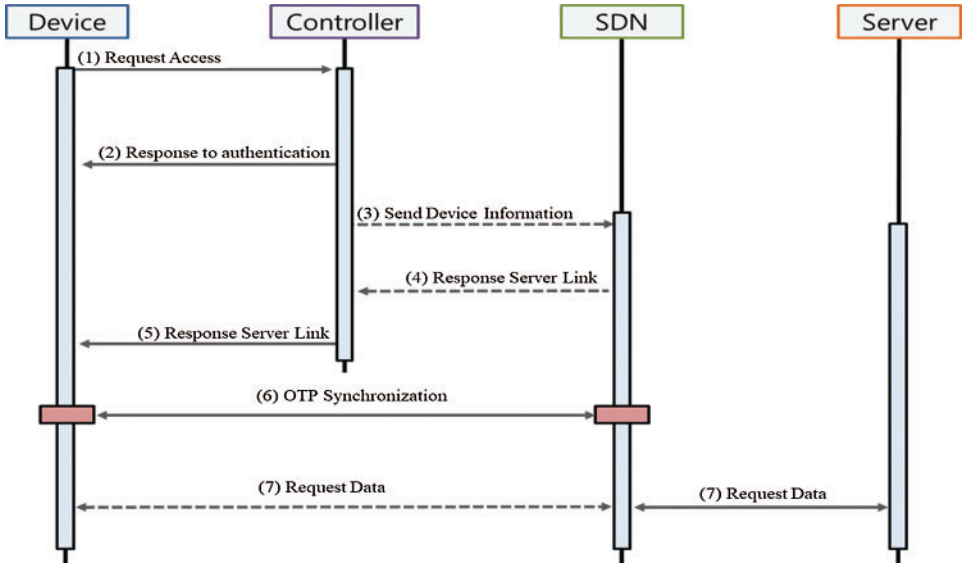

Figure 5: Flow chart of the proposed cloud architecture

First, the user requests the controller to authenticate the authenticated device to access the cloud. Only operations with approved devices are accepted, and unapproved devices will be blocked. The controller delivers the certification result to the device through the response to the authentication action. If the authentication results fail more than a certain number of times, the status of the device certification table is locked; further attempts to authenticate are prevented as well. The controller checks the path of the SDN that the device can access through the SDN link table. The controller offers the information of the certified device. The path information of

devices is provided through response server link operation. The communication channel between the controller and the SDN is continuously synchronized and maintained through the OTIP algorithm. The device and the SDN then generate data channels that do not pass through the controller and which are continuously synchronized through the OTIP algorithm. The device proceeds to send and receive data on the cloud to the SDN through this data channel. SDN provides processing and data on device requests if there are no security policy issues.

4 Analysis

This section presents the results of analyzing the performance proposed architecture. The analysis consists of three subsections: Experiment setup, security analysis, and performance analysis. The security analysis targeted the proposed architecture based on three types of attacks: Network sniffing, man-in-the-middle attacks, and denial of service attacks.

4.1 Experiment Setup

This subsection provides a comparative analysis of the existing IPs and the OTIP algorithms used for secure dynamic routing in the proposed software-defined cloud architecture. The analysis process is carried out the "Network simulator 3" tool in the Ubuntu 20.04 LTS environment. The OTIP algorithm changes the IP address every 30 s as the minimum OTP change time of the time-based one-time password. As part of the security analysis, simulations are carried out against network sniffing, man-in-the-middle attacks, and denial of service attacks. The attack is rerun at intervals of 20, 50, and 80 s for accurate comparative analysis.

4.2 Security Analysis

This subsection presents an analysis of the security based on various types of attacks such as network sniffing, man-in-the-middle attacks, and denial of service attacks.

- **Network sniffing:** Network sniffing is a type of attack wherein the attacker eavesdrops on packets sent to the network. The attacker gets essential information from the system to be attacked by sniffing. Fig. 6 shows the results of a network simulation of sniffing conducted on the OTIP and the existing IP. In the simulation, sniffing was carried out at the 20-s section of communication between the cloud and the client. While packets were continuously sniffed for existing IPs, the OTIPs changed the IP address every 30 s to prevent continuous sniffing. In actual network sniffing, the attacker uses the promiscuous mode for the network monitoring of the packets. Continuous sniffing specifies the target's communication packet and collects information based on the IP address. In the case of the OTIP, it was difficult for an attacker to get a particular communication packet because the IP address was changed continuously. Even if the communication packet was specified, it is difficult for an attacker to collect information through the communication packet.

- **Man-in-the-middle (MITM) attack:** MITM attacks are attacks wherein an attacker approaches and relays data in the middle of the network communication process. The attacker snoops or manipulates all communications to intercept sensitive data or to change the data to the attacker's advantage [32]. Fig. 7 shows the results of a network simulation wherein an MITM attack was launched against the OTIP and the existing IPs. MITM attacks have succeeded by launching attacks on the OTIP and the IP at 20-s intervals. For existing IPs, a successful attack can allow an attacker to tap packets continuously [33]. In OTIP, the IP address changes every 30 s. So, the attack can be confirmed after 30 s. Subsequently, the MITM attack was successful again at 50 and 80 s. Since the IP address changes every 30 s, however, the attacks fail.

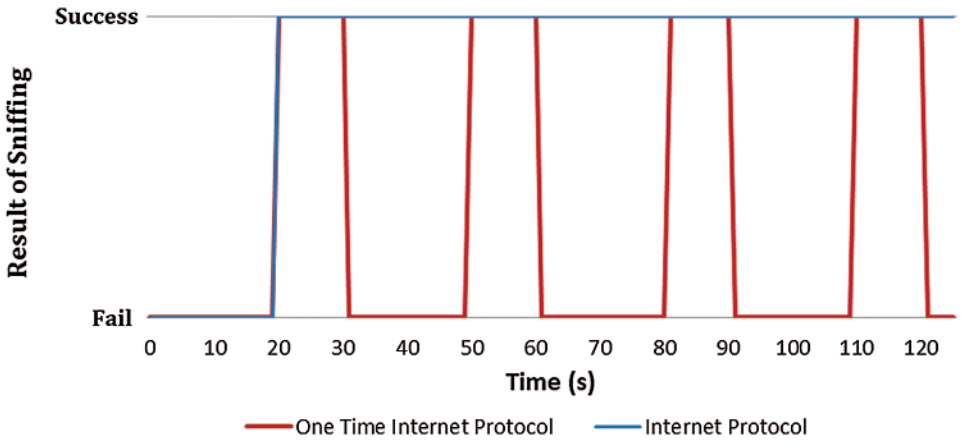

Figure 6: Network sniffing results

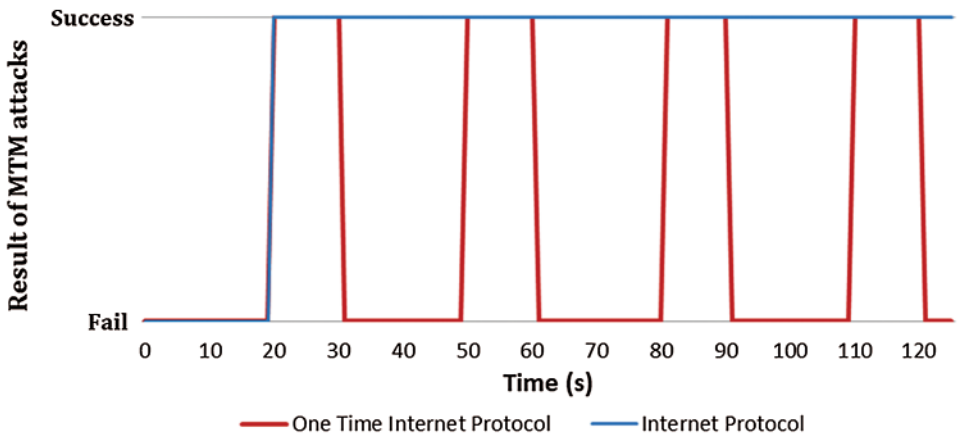

Figure 7: Man-in-the-middle attack results

• **Denial of service (DoS) attack:** The DoS attack is an attack wherein an attacker generates traffic by transmitting a large packet to the target. It will cause the server to be paralyzed, making it impossible to gain ordinary service access [34,35]. Fig. 8 shows the results of a network simulation wherein a DoS attack was launched against the OTIP and the existing IPs. In the simulation, 100 normal packets were sent and received in the course of communication between the cloud system and the client. In the next 20 s, an attacker sent a large number of dummy packets to the cloud system to launch a DoS attack. As a result, in systems with existing IPs, large dummy packets paralyze the service, making it impossible to transmit and receive normal packets. For the OTIP, however, the IP address can be changed every 30 s to ensure that normal packet transmission and reception of cloud systems and users progress at 30-s intervals. As a result of a further DoS attack on the OTIP at 50 and 80-s intervals, the IP address was observed to have changed every 30 s to recover the system.

4.3 Performance Analysis

Fig. 9 presents the results of a network simulation of the OTIP and the existing IP. In the simulation, 500 ping-pong packets were sent and received per second. To verify the smooth

transmission and reception of packets in the OTIP network, the IP address was changed every 30 s using the OTIP algorithm. In the case of existing IPs, it can be seen that the packets were sent and received reliably. For the OTIP, a temporary decrease in the number of packets throughout can be seen in the 30-s interval at which the IP address changes. In this process, however, packet delays rather than packet loss occur, and subsequent sections also handle packets that have not been processed. In other words, the process of changing the IP of OTIP has a temporary delay. Still, it can be seen that the packet is processed without any packet loss.

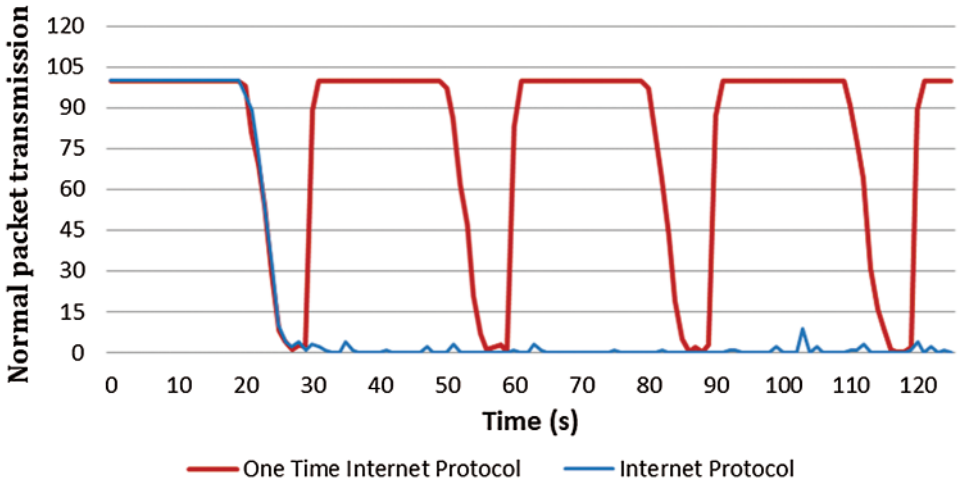

Figure 8: Denial of service attack results

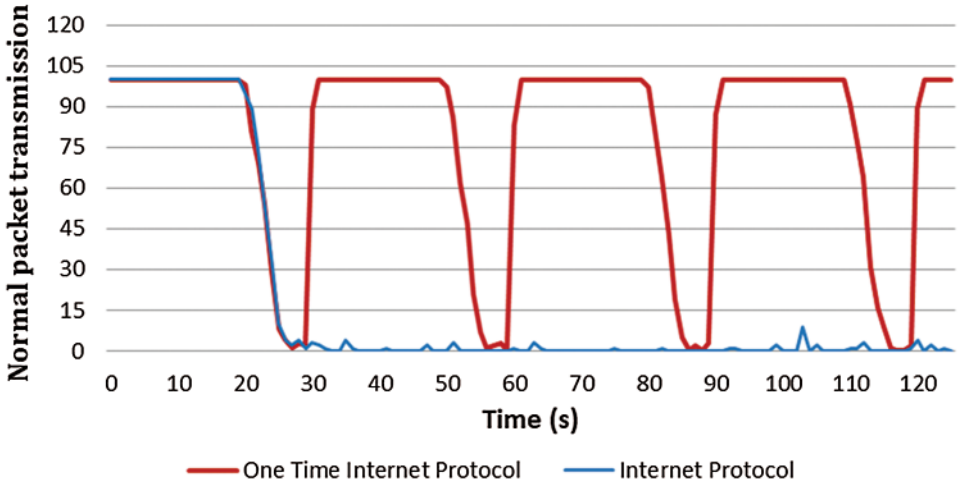

Figure 9: Packet throughput results

5 Conclusion

The proposed OTP-based software-defined cloud architecture uses software-defined perimeter techniques designed based on user identity. It prevents unauthorized devices from attempting to access the cloud so that only pre-authenticated devices can access it. Therefore, our proposal

shows an effective reduction of resource loss in the cloud by proactively blocking unnecessary accesses. We used software-defined network technology to control and manage network behavior on software-based controllers. This allows flexibility in responding to large-scale traffic and increases scalability. We deployed secure dynamic routing, which changes automatically to specific intervals using the OTP-based OTIP algorithm in terms of communication channels. The proposed secure dynamic routing is safe against various types of network attacks, including network sniping, MITM attacks, and DoS attacks. Also, the architecture supports the continuous upgrading of information, making repetitive attacks impossible. Thus, stability is provided against intelligent threat attacks. As a result of the performance evaluation, efficiency and stability of OTIP are similar to existing IP methods. In conclusion, the proposed software-defined cloud architecture is safe from ever-evolving cyber-attacks. Furthermore, cloud architectures are forecast to have effective advantages in terms of scalability and efficiency. Proposed architecture offers the benefit today's real-world scenarios such as smart cities.

Funding Statement: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2019R1A2B5B01070416) and also supported by the Advanced Research Project funded by the SeoulTech (Seoul National University of Science and Technology).

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

References

[1] S. Singh, Y. S. Jeong and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, no. 7, pp. 200–222, 2016.

[2] S. K. Singh, S. Rathore and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence," *Future Generation Computer Systems*, vol. 110, no. 2, pp. 721–743, 2019.

[3] Y. Liu, S. Xiao, H. Wang and X. A. Wang, "New provable data transfer from provable data possession and deletion for secure cloud storage," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, pp. 1550147719842493, 2019.

[4] Y. Lee, S. Rathore, J. H. Park and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-Centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–14, 2020.

[5] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. E. Azzaoui *et al.,* "A Comprehensive survey on core technologies and services for 5g security: Taxonomies, issues, and solutions," *Human-Centric Computing and Information Sciences*, vol. 11, no. 3, pp. 22, 2021.

[6] G. S. Mahmood, D. J. Huang and B. A. Jaleel, "A secure cloud computing system by using encryption and access control model," *Journal of Information Processing Systems*, vol. 15, no. 3, pp. 538–549, 2019.

[7] Y. Dai, D. Xu, S. Maharjan, G. Qiao and Y. Zhang, "Artificial intelligence empowered edge computing and caching for internet of vehicles," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 12–18, 2019.

[8] S. K. Singh, Y. S. Jeong and J. H. Park, "A deep learning-based iot-oriented infrastructure for secure smart city," *Sustainable Cities and Society*, vol. 60, no. 1, pp. 102252, 2020.

[9] K. Bhushan and B. B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 5, pp. 1985–1997, 2019.

[10] C. L. Chen, P. T. Huang, Y. Y. Deng, H. C. Chen and Y. C. Wang, "A secure electronic medical record authorization system for smart device application in cloud computing environments," *Human-Centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–31, 2020.

[11] J. Cha, S. K. Singh, Y. Pan and J. H. Park, "Blockchain-based cyber threat intelligence system architecture for sustainable computing," *Sustainability*, vol. 12, no. 16, pp. 6401, 2020.

[12] Check Point Research, "Attacks against cloud environments," in *2020 Cyber Security Report*. Tel Aviv, Israel: Check Point Software Technologies, 2020. [Online]. Available: https://pages.checkpoint.com/cyber-security-report-2020.html.

[13] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen *et al.,* "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, pp. 1, 2018.

[14] C. S. Park, "One-time password based on hash chain without shared secret and re-registration," *Computers & Security*, vol. 75, no. 2, pp. 138–146, 2018.

[15] I. Permana, M. Hardjianto and K. A. Baihaqi, "Securing the website login system with the SHA256 generating method and time-based one-time password (TOTP)," *SYSTEMATICS*, vol. 2, no. 2, pp. 65–71, 2020.

[16] Y. Jararweh, M. Al-Ayyoub, E. Benkhelifa, M. Vouk and A. Rindos, "Software defined cloud: Survey, system and evaluation," *Future Generation Computer Systems*, vol. 58, no. 1, pp. 56–74, 2016.

[17] M. Conti, P. Kaliyar and C. Lal, "CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm, concurrency and computation," *Practice and Experience*, vol. 31, no. 8, pp. e4978, 2019.

[18] N. Ha and N. Kim, "Efficient flow table management scheme in SDN-based cloud computing networks," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 228–238, 2018.

[19] Z. Yao and Z. Yan, "A trust management framework for software-defined network applications, concurrency and computation," *Practice and Experience*, vol. 32, no. 16, pp. e4518, 2020.

[20] F. A. Zaman, A. Jarray and A. Karmouch, "Software defined network-based edge cloud resource allocation framework," *IEEE Access*, vol. 7, pp. 10672–10690, 2019.

[21] E. L. R. Lucion and R. C. Nunes, "Software defined perimeter: Improvements in the security of single packet authorization and user authentication," in *2018 XLIV Latin American Computer Conf.*, São Paulo, Brazil, pp. 708–717, 2018.

[22] L. A. Tawalbeh, Y. Haddad, O. Khamis, E. Benkhelifa, Y. Jararweh *et al.,* "Efficient and secure software-defined mobile cloud computing infrastructure," *International Journal of High Performance Computing and Networking*, vol. 9, no. 4, pp. 328–341, 2016.

[23] A. Refaey, A. Sallam and A. Shami, "On IoT applications: A proposed SDP framework for MQTT," *Electronics Letters*, vol. 55, no. 22, pp. 1201–1203, 2019.

[24] J. Singh, A. Refaey and A. Shami, "Multilevel security framework for NFV based on software defined perimeter (SDP)," *IEEE Network*, vol. 34, no. 5, pp. 114–119, 2020.

[25] A. Sallam, A. Refaey and A. Shami, "On the security of SDN: A completed secure and scalable framework using the software-defined perimeter," *IEEE Access*, vol. 7, pp. 146577–146587, 2019.

[26] A. Moubayed, A. Refaey and A. Shami, "Software-defined perimeter (SDP): State of the art secure solution for modern networks," *IEEE Network*, vol. 33, no. 5, pp. 226–223, 2019.

[27] X. Xie, G. Gan and Y. Chen, "Research on SDP software defined perimeter initiating host protocol configuration algorithm," *IOP Conference Series: Earth and Environmental Science*, vol. 428, no. 1, pp. 012054, 2020.

[28] E. Erdem and M. T. Sandıkkaya, "OTPaaS—One time password as a service," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 743–756, 2018.

[29] S. A. El-Booz, G. Attiya and N. El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol," *EURASIP Journal on Information Security*, vol. 2016, no. 1, pp. 1–13, 2016.

[30] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," *Computers in Industry*, vol. 104, no. 1, pp. 47–58, 2019.

[31] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma *et al.,* "SDQaaS: Software defined networking for quantum key distribution as a service," *Optics express*, vol. 27, no. 5, pp. 6892–6909, 2019.

[32] J. C. S. Sicato, S. K. Singh, S. Rathore and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020.

[33] X. Jiang, M. Liu, C. Yang, Y. Liu and R. Wang, "A blockchain-based authentication protocol for WLAN mesh security access," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 45–59, 2019.

[34] A. E. Azzaoui, S. K. Singh, Y. Pan and J. H. Park, "Block5GIntell: Blockchain for ai-enabled 5G networks," *IEEE Access*, vol. 8, pp. 145918–145935, 2020.

[35] C. Li, P. Wang, C. Sun, K. Zhou and P. Huang, "WiBPA: An efficient data integrity auditing scheme without bilinear pairings," *Computers, Materials & Continua*, vol. 58, no. 2, pp. 319–333, 2019.