Design, Implementation and Comparative Analysis of Byod Algorithms for Secured Data Center

P. Soubhagyalakshmi
Research Scholar, Department of C.S.E, VTU-RRC, Belagavi, Karnataka, India, slakshmi.p@gmail.com

Dr. K. Satyanarayan Reddy
Professor, Cambridge Institute of Technology, Bangalore, Karnataka, India, ksatyanreddy@yahoo.com

Abstract

Due to increased organizational mobility, enhanced employee efficiency, and increased worker happiness as an alternative approach to the workplace environment, there is an expanded need for Bring Your Own Device (BYOD) service integration. So far, the BYOD atmosphere enhanced the cyber-attack, which constitutes a significant cyber security concern for most organizations and leads to the segmentation of the business ecosystem. In recent times, a variety of strategies and procedures have been created to minimize cyber-attacks, which address several outstanding problems. However ongoing development is necessary because of new attack strategies and instruments. To support BYOD environments, the majority of the organization has adopted a secure certificate-based authentication solution. In this study, a methodology for increasing safety in SDN-based data centers is given. Using SDN capabilities, network layer security middleware such as Intrusion Prevention System (IPS) is integrated with network layer protection to prevent intruders at the network edge. Quality measurement findings show that the proposed outline offers a compatible self-defending network capable of defending against insider threats and protecting running services while quickening attacker turnaround time.

Key words: *BYOD; Security; SDN; Data centers; malicious access.*

1. INTRODUCTION

Not all benefits associated with setting up BYOD settings exist; businesses must deal with several security-related drawbacks, such as difficulties in managing employee-owned devices [1]. Another drawback is that equipment is continuously on and linked, increasing the risk of malicious assaults along its many networks of communication. The problem is made inferior after we realize that wireless connection networks in smart devices are much more vulnerable to attack than cable networks [2].

Another drawback that organizations face is the lack of enforcement of BYOD policies. Initiatives are a crucial component in the management of safety issues, and every administration necessity to develop a policy that meets its requirements. BYOD requires a significant amount of regulations to regulate and protect corporate information. Corporations didn't reject the BYOD trend, and in a short while, the majority of them will permit workers to customize their mobile devices to negotiate deals. BYOD is a policy that an organization establishes to permit its staff members to take in and use their mobile

devices for work [3]. This implies that this one gadget would contain both personal and professional data for each user. Both inside and outside of the company's environment, employees can obtain the information that belongs to their employer. It may view private entity data while working on devices by this corporate IT policy.

By implementing BYOD, critical infrastructure must be protected from threats. The need for continual abstraction enhancement in this approach arises from the threat landscape's ongoing evolution of new tactics. Security risks are encountered when BYOD traffic is sent over MPLS from several spoke points to the data center's Identification, Authentication, and Accounting system for onboarding. A crucial necessity is just a dependable and secure method of routing legitimate traffic. Additionally, because the proposed architecture is out of band for network traffic, network latency for services is unaltered. The conceptual outline also offers improved security by preventing intruders found by IDS. To replicate the actual datacentre topology, a fat-tree datacentre topology is used. Threats on the networks are used to evaluate system performance. Findings show that, in comparison to related research, the paradigm improves SDN-based data center security and decreases attack response time.

The safe BYOD model and company network security were examined using encryption technology [4]. It also investigated how to control remote site authentication traffic, latency, and DDoS attacks utilizing IPS/IDS. The development of the three-tier multifactor model was a crucial technique before this [5]. Earlier, the blockchain paradigm of multi-factor identification was also examined for identity verification with extra safety precautions. In addition to this, a safe self-service portal paradigm was explored to limit the danger of information leaks and defend against unauthorized users.

Malicious activity identification has been the subject of numerous studies in the past. One of the primary research was conducted on the use of honeypot technology to identify malicious activity and combine deception with the cyber risk management strategy of the FEMA mission with five levels of preparedness [6-7]. To improve the research's overall accuracy and detect occurrences, Smart Threat Stage was used [8]. The overall accuracy was examined to 93.71%, then 90.73%, then 96.16% using the audit trail technique to raise the average accuracy in finding the attack's origin. Evaluation of malware infection risk using a machine learning approach is described as another innovative approach [9].

2. Related works

The paradigm is put to the test in a real-world setting through an experiment. Let's have a look at the real-world case outlined in the following paragraphs [10] to gain a better understanding of the criteria used for framework verification. Dave is employed by an organization that prioritizes its employees' confidentiality and information protection very deeply. Each employee of this company is expected to abide by the BYOD policy that has been established and is being implemented [11]. For allowing employees to start using their mobile devices for work, activation must be completed, including setting up company email and WiFi settings [12]. Before Dave can utilize mobile devices provided by the business or by him for work, he must meet a few conditions. This equipment must be connected to the central controller so that Dave may directly operate them and the company can identify any suspicious actions that violate their policies

[13]. To stop malicious hackers or adversaries from stealing sensitive data, exposing vulnerability, and unauthorized accessing the sensors, the communication channel between the phones and the controller must be protected.

Based on other data, such as accessibility to third-party app stores that are known to harbor malware, the system also develops security intelligence [14]. The administrator can learn more and take the necessary mitigation actions. For instance, the administrator can block network access by blacklisting a device based on its MAC address when it accesses potentially hazardous app stores. In a broader sense, we give the administrator a device reputation score that is based on all of the observations made about a specific device [15]. We can identify when machines engage enterprise resources and services by examining the NetFlow logs. We can explicitly state when mobile devices are viewing sensitive enterprise assets with the right annotations. Administrators can recognize when dangerous devices access critical resources due to this and the device reputation ratings [16]. With this knowledge, such devices can be targeted for remediation.

Enterprises can analyze the mobile landscape using the passive monitoring strategy without requiring the deployment of agents or imposing any other kind of control or restriction on the device. This gives users of mobile devices the greatest amount of flexibility while also preserving network security and usage control [17]. The aggregate device assessment that we provide can be utilized to influence remediation actions on potentially dangerous devices by being connected with external susceptibility and risk sources. Of course, for this method to properly analyze the apps operating on the devices, exposure to network traffic, such as HTTP headers, is necessary [18]. When the information is secured, it will be more challenging but not impossible to precisely define the network data and device behavior.

There are numerous techniques for keeping an eye on software activities on mobile devices, which can be classified as passive or active, on-device, or on the network. We discuss research about all of these choices in this section [19]. MDM, which combines functionality offered by the mobile device platform and vendor software that offers enterprise-grade device management, is one of the most widely utilized technologies in the area of mobile computing [20]. Software deployment administration and device password policies are just two examples of versatility. While the collection of installed apps may be analyzed, these technologies normally do not monitor specific network traffic [21]. Many businesses do not want to exert this degree of surveillance on visitors' devices or the devices of persons who are only viewing their company.

Future virtual data center security mechanisms are expected to follow SDN-based security methodologies. Several studies on safety utilizing SDN will be addressed in this part. By checking packets accessing the network, the DAMASK design prevents DDOS assaults in cloud and SDN architecture [22, 23]. Using the Open Flow protocol, blocking actions are transmitted to switches or routers [24]. Given that it only relates to one particular type of IPS, this kind of interaction does not offer scalability. The controller has yet another version of an IPS unit that analyses Snort logs and produces the blocking response [25]. This approach is not scalable because logs rely on Snort parsing. The component within the controller must be configured to install another IPS. It can readily interface with various controllers, and installing a security program

outside an SDN controller allows for architecture flexibility.

Various BYOD strategies can be used, including offering employees controlled enterprise devices, including employee-owned procedures in the enterprise device pool, and exchanging employee-owned devices with enterprise devices. The main goal of BYOD is to offer practical solutions so that customers can benefit from IT services outside of the limitations of company-owned equipment and working hours. Hence, it should be possible to access everything needed to do work-related activities from any device, at any time, and from any location via a connection to the Internet or a WLAN at the workplace [26].

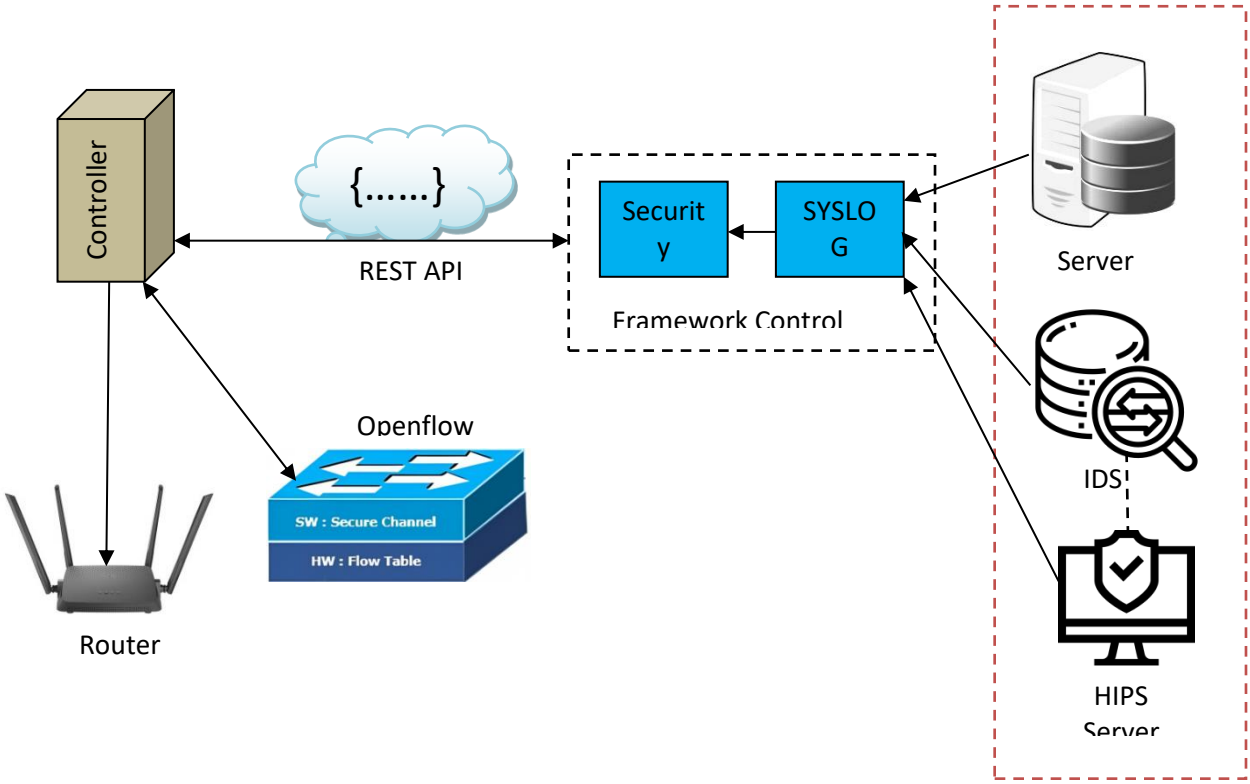
Here is your own device (HYOD) is as follows: Plans are supplied by the administration in this idea. The firm has full control over the gadget. From setup to customization and device settings, the business will provide full assistance for the appliance. Choose your own device (CYOD): In this kind of approach, the business provides a variety of devices from which each worker can select the one they want to utilize. The rules are less stringent than they were when using equipment, and the consumer has the power to acquire particular software and programs. CYOD is a technique that limits the number of devices an employee may utilize to obtain company information while adopting the foundations of "consumerization."In comparison to BYOD, the company is responsible for all aspects of the acquisition and equipment servicing, not the customer [27].

BYOD: It refers to the process when an employee purchases their gadget or receives financial support from their employer to do so. Here, the organization has less authority over the gadget and the policies are lower. Only if the customer complies with the organization's policies can they carry out whatever they want and download as many programs as they desire. On Your Own Device (OYOD) any gadget that the organization does not support may be brought by the end user. The user must manage the gadget. It is not necessary to adhere to any policies.

3. Proposed Framework

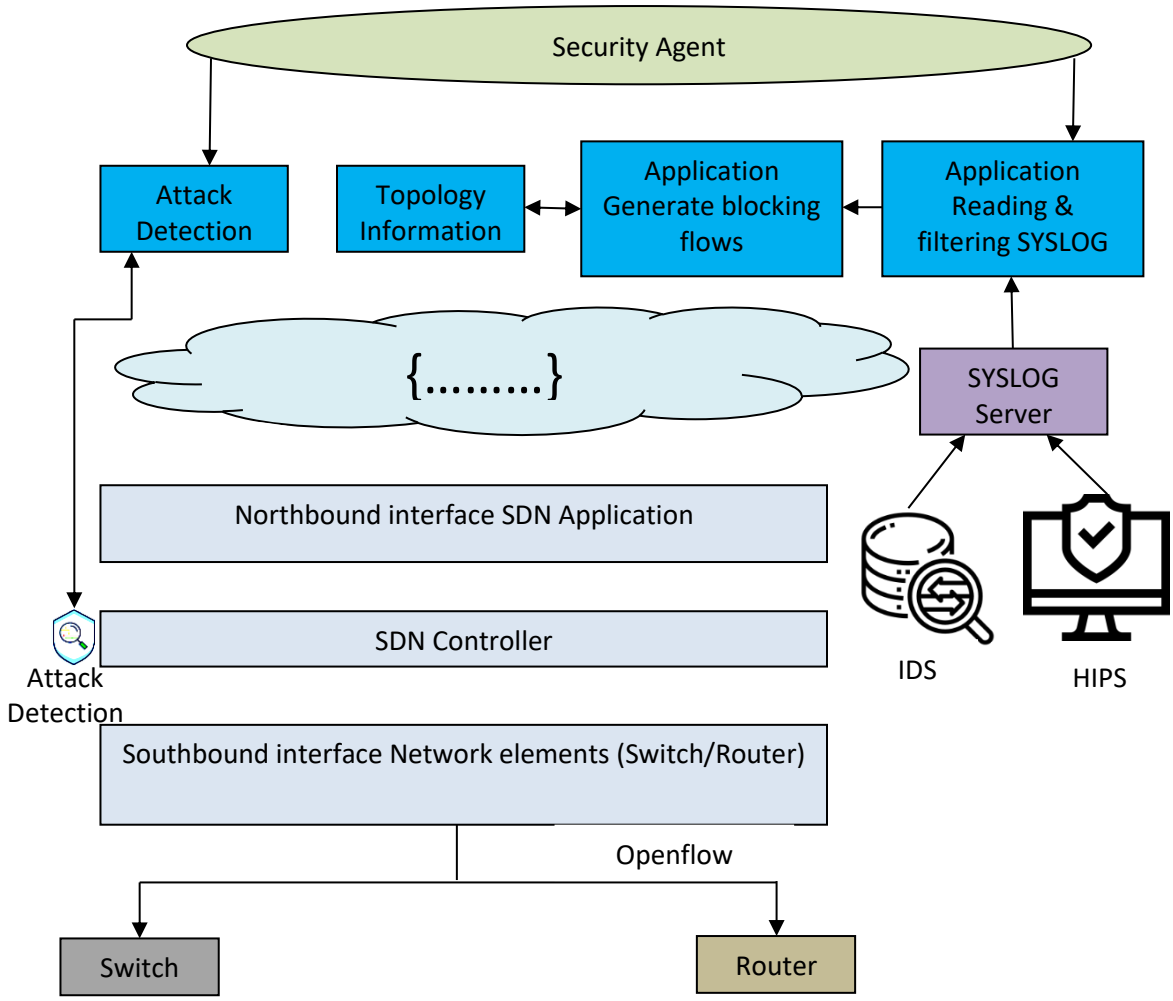
This research includes a methodology to improve data centers using SDN security. The framework provides SDN to build network architecture for a data center that is focused on applications. Using a Syslog service, the framework connects with security solutions. Any security device that enables remote Syslog can be integrated with the proposed approach. Using its northbound connection; the architecture is integrated with the SDN controller. The conceptual structure for the system is shown in Figure 1. Security logs are sent to the Syslog server from various security middleboxes. The security agent unit and Syslog server are parts of the architecture control unit. The Syslog server and SDN controller are integrated with this control unit. The security representative is separate from the SDN controller to offer flexibility.

Figure 1: Proposed Framework logical diagram



All network security systems have signatures available for selection by administrators. When a signature is activated, the security agent component sends a route to the controllers to be restricted as close as feasible to the source connection. The security agent unit receives the assailant's topological information from the controller and filters and analyses the acquired security logs. The design units of the structure are shown in Figure 2 [28]. The primary component is the security agent. For network management, a management web interface is established in this component. The administrator installs trends to be identified for APT identification or signatures to be discarded through the web interface. The task of gathering topology information for intruders falls to the Topology Information Unit. To obtain topology data, this device interacts with the SDN controller using a REST API connection. This device's output is the switch port of the intruder that will be disabled.

Figure 2: Proposed framework design units



The blocking unit uses the interference demand to create streams that will be delivered to the SDN controller through REST API to block attackers. Furthermore, a program has been generated on the floodlight controller to recognize affected PCs from APT or zero-day assaults. This receiver takes patterns from the security agent and scans the network traffic for certain patterns. Supervisors can customize these patterns via a web interface. To scan network traffic for threats, this unit can be integrated with other cutting-edge attack detection systems. To avoid them from being denied by erroneous positives, the administrator maintains a list of trustworthy IP addresses. The following is a summary of the architecture process flow:

1-Ossec IDS or Snort IDS recognizes intrusions on the victim machine and transmits Syslog to the built-in or Kiwi Syslog servers.

2- The security agent unit examines the Syslog server for outbreak patterns and alerts the topology unit if it detects one.

3. The blocking unit receives information about attacker ports from the topology unit via a REST API query to the controller.

4. Blocking unit transmits topology data to the controller to set up a flow and block the intruder.

5. If a particular set is found in a host's traffic, the system will send a signal to the controller to restrict the access points that are the origin of the fraudulent pattern.

3.1 Detection BYOD Malicious Traffic

The primary strategy used throughout this study period has been recognition. In the BYOD setting, a certificate-based strategy was thought to be the safest way to offer access control. However, a vulnerability in this approach that exposed significant cyber security risk was found [29]. The architectural approach of this system is supported by an algorithm that presents a detailed method to identify BYOD traffic that has been accessed without authorization.

Begin

Inputs: Variables V1, V2 and V3

Incorporate User Database (UD) with Identity Awareness (IA)

Interpret date from UD based on run time

Allocate values

V1 = Issue date of Secure PKI

V2 = Expiry date of Secure PKI

V3 = Deactivation date BYOD user ID from UD

N1 = V2 - V3

Equate the values

if (V3 = Void && V2<V3) then

Let Forensic access and Sandboxing

else

Goto Step 7 for existence analysis

end if

if V2> V3 then

Identify and observant as "Malicious"

Goto Module "PROTECT"

else

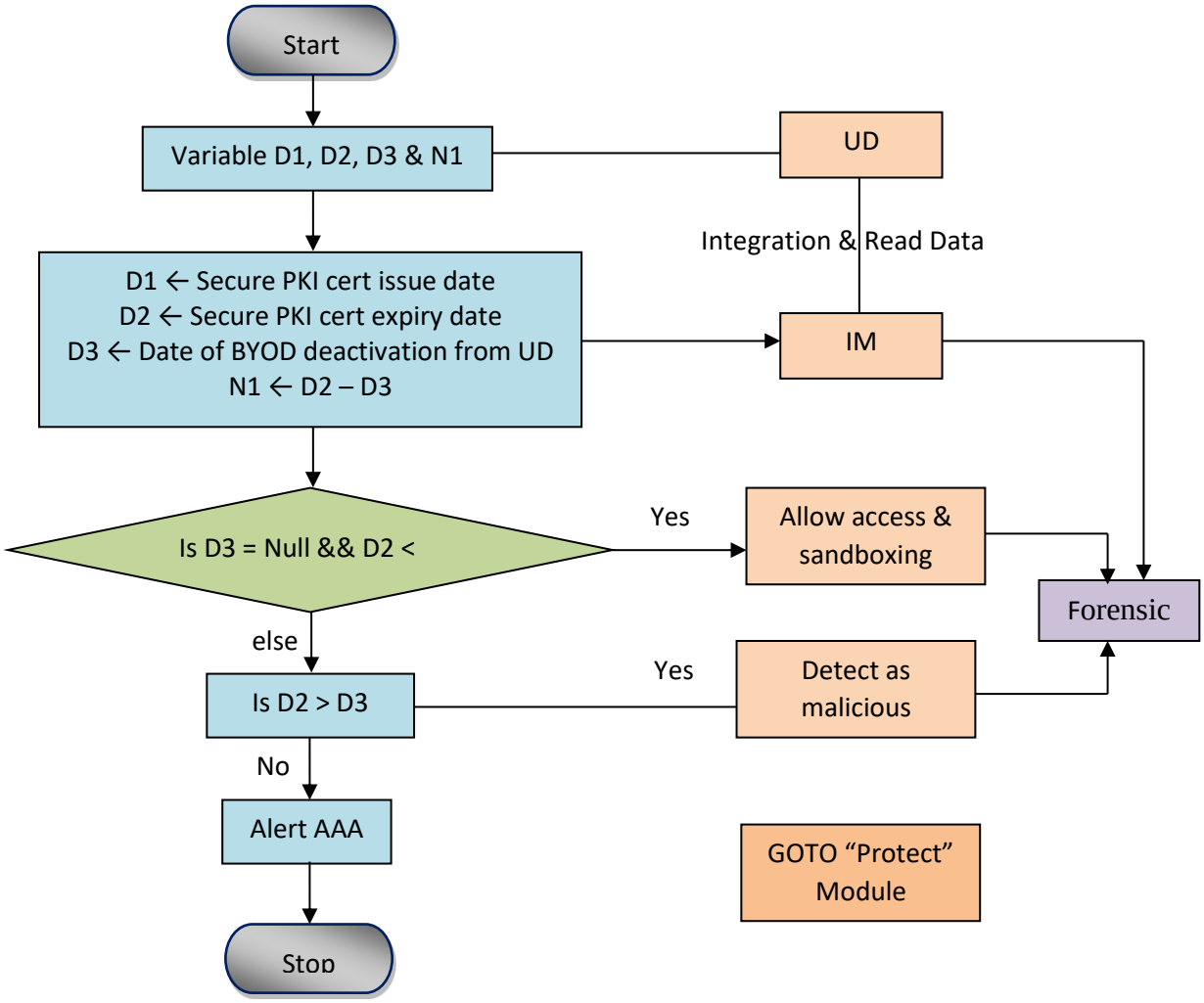
Active to AAA

end if

end

A workflow is also created based on the method to illustrate the detection model, as shown in Figure 3.

Figure 3: Malicious traffic detection model of BYOD



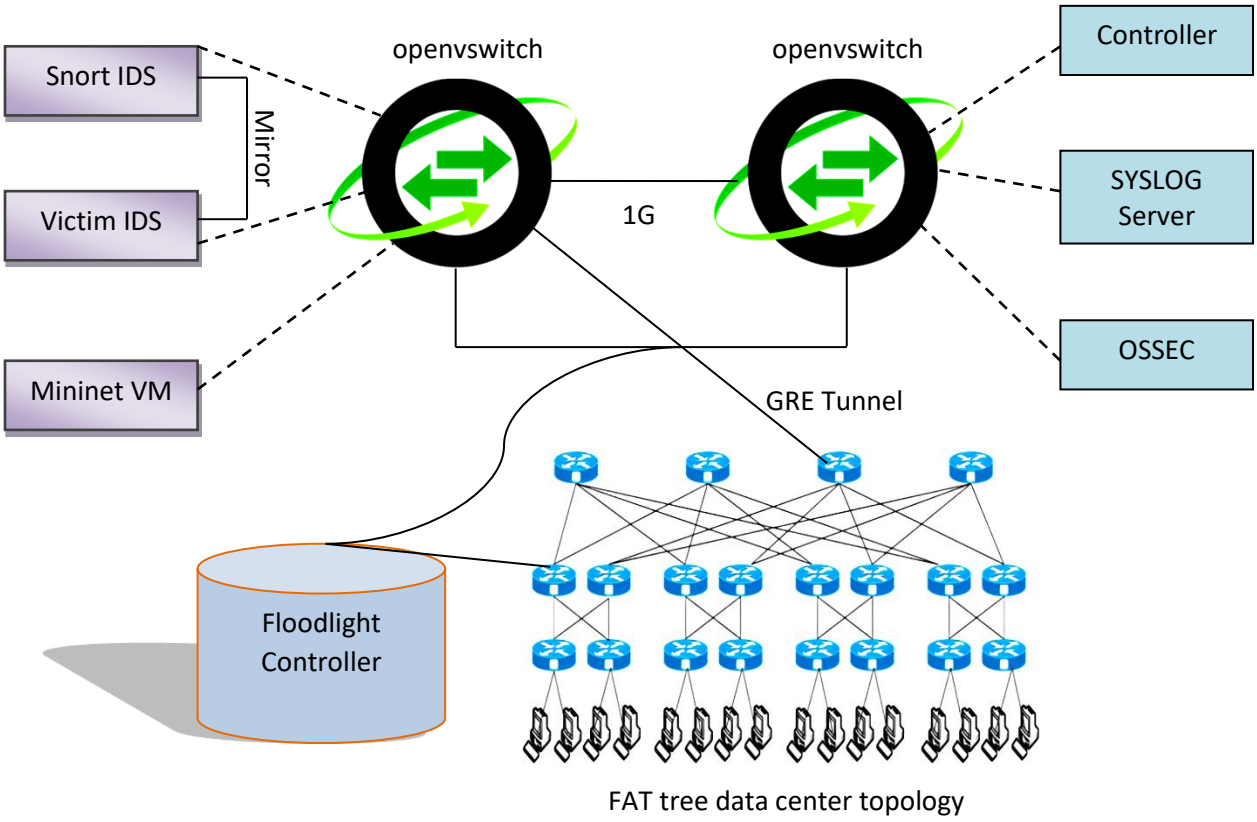
Since 2009, this technology has greatly advanced, leading to the development of numerous implementation strategies that combine the technology with traditional network infrastructure that has been established while allowing the coexistence of the two networks. The outcome chapter demonstrates one of the causes of an increase in insider intruders since intrusions are also expanding quickly and ethical hacking is a serious issue as 62% of attacks come from insiders. According to the PWC Global Crisis Latest survey, 26% of the significant problem for cybercrime is also a sign of this. Information security business models transition from conventional to online, and this is a crucial point to remember when making decisions.BYOD usage is required for enterprises in the digital business ecosystem, where cyber security is becoming a key factor to take into account. This research includes approaches for critical infrastructure security and the construction of a BYOD architecture using a secured certificate-based methodology.

4. Implementation and performance evaluation

Parts of the conceptual proof and interconnection of the experimental set - up are shown in Figure 4. Software called Mininet

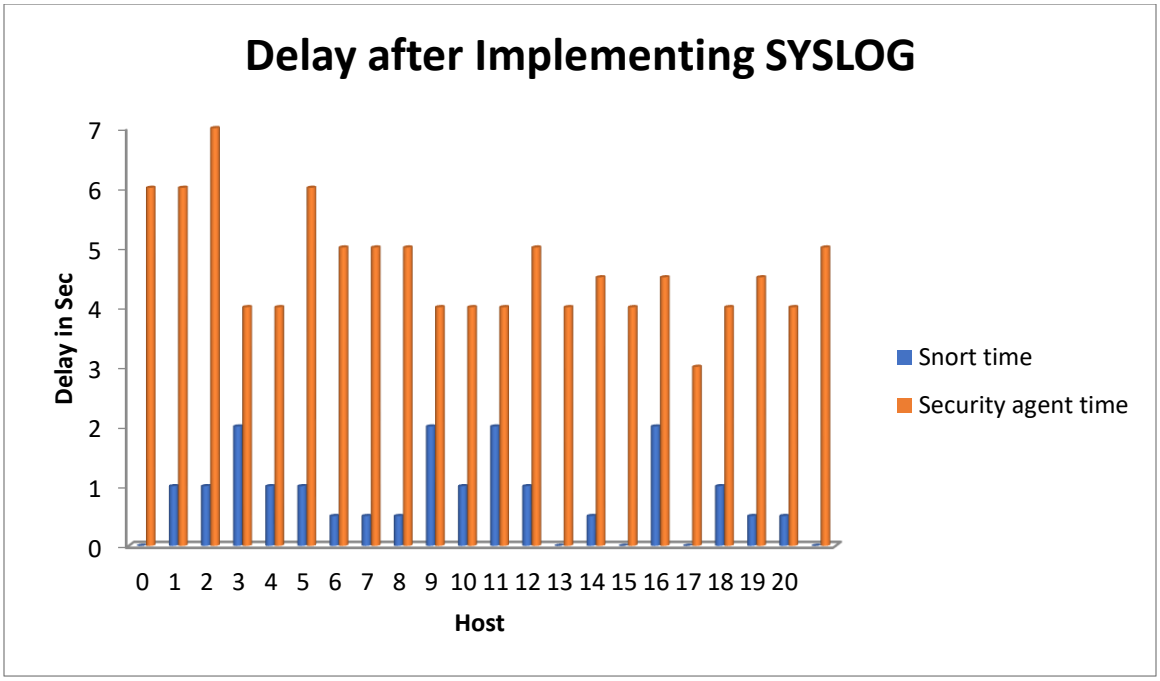
Emulation is used to simulate network topologies. As a standard data center topology, fat-tree data center topology is used. Twenty switches make the topology, and the number of hosts was altered while maintaining the topology. The GRE tunnel with the XenServer switch connects the mininet network to the physical topology. The modular design of the Floodlight controller makes it easy to extend and improve the controller. Since it allows openvswitch to link virtual machines, the Citrix XenServer hypervisor was used.

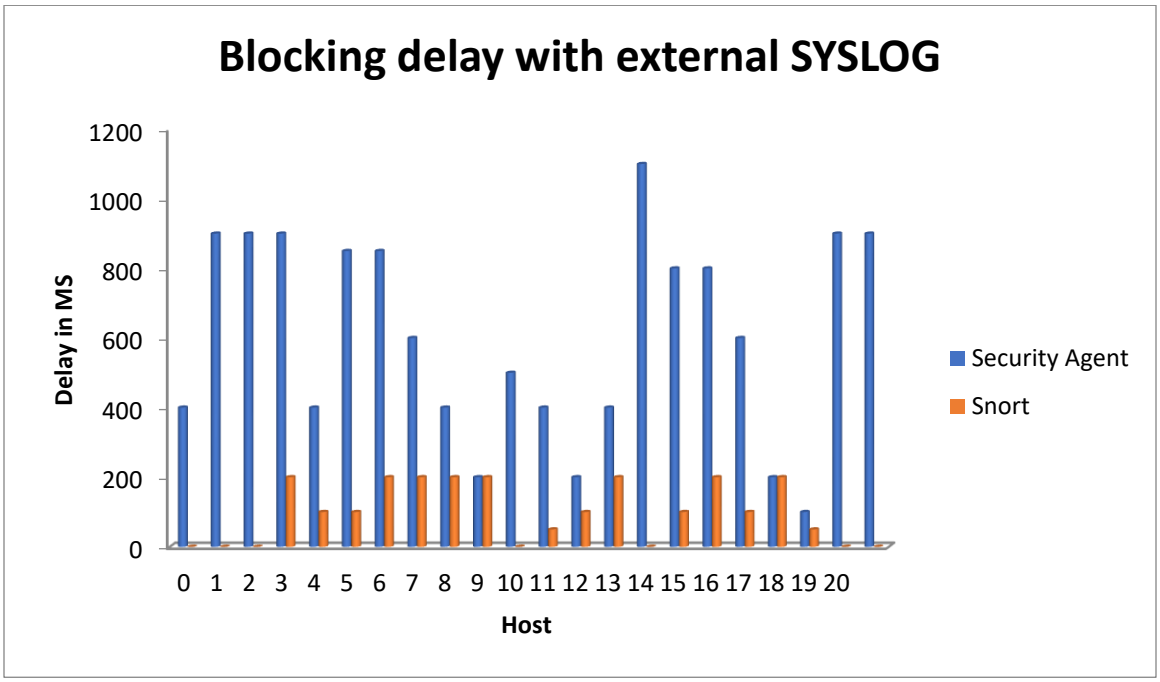
Figure 4 Experimental setup



There were several attempts tried. The proposed design demonstrates the system's capacity to identify the aforementioned assaults and stop attackers at the network edge. It can utilize an internal Syslog server or use the Kiwi Syslog server as an alternative to Syslog servers. It is determined that the delay in receiving occurrences*/ from the outside syslog file results in a rise in blocking delay. Using a Syslog server that was installed locally minimized delay. Snort's syslog signals are filtered before being sent to the log file. Blocking delays are shown in Figure 5 (a & b) for both the implementation of a syslog server and the use of a kiwi syslog server. The performance improvement when using an individual syslog server is apparent.

Figure 5: (a) internal and (b) kiwi syslog server





Strategies for creating a cyber-secure ecosystem have been taken into consideration when it comes to BYOD safety, and these studies show an extra method. An innovative strategy is proposed that contributes to improving the BYOD infrastructure's security layer. First, a weakness in the protected certificate-based BYOD approach is detected. The algorithm is created to identify harmful activity and illegal access to vital infrastructure, and the detection method has been developed. An improved degree of

Security mechanism algorithm is constructed for detection. After a cyber-attack, one of the biggest challenges is threat hunting to identify the attack's origin so that digital information may be gathered, analyzed, and provided for the creation of a cyber-forensic ecosystem.

4.1 Comparison

The conceptual approach can expand the reach of security devices, improve data center protection, and recognize a wide range of intrusions. By connecting with various security appliances, versatility is offered. High throughput is one of the criteria for data center layout. Intruders are dropped by the proposed scheme without being scheduled. The disadvantage of this method is that it cannot identify assaults that occur in a single packet. The primary function of the network layer is to deliver traffic without delay. We put crucial resources behind an IPS to protect them from atomic attacks, but in that instance, the asset's permitted bandwidth will be constrained by the IPS data. Today's systems need to recognize APT through traffic pattern detection since APT poses a serious threat. Security solution was incorporated in the controller as a component by related research. More flexibility and controller-type independence are provided by placing the security solution outside the controller. Furthermore, it's critical to have the capacity to resist internal intruders since new challenges in ensuring secure data center designs are introduced by techniques like BYOD.

Table 1: Comparison of the existing system with proposed

	[11]	[14]	[16]	Proposed
IPS (delay)	√	√	X	X
Web attacks Protection	X	X	X	√
Encrypted attacks protection	X	X	X	√
multiple IDS scaling	X	X	X	√
Vulnerabilities in DOS attacks services	X	X	X	√

The conceptual methodology and similar work are compared in Table 1. The proposed architecture offers simple interaction with security solutions and can identify more threats. Voice and video apps with low latency are unaffected because their designs do not consider congestion. It is possible to integrate with various security appliances. The architecture can also defend itself from assaults disguised as data encryption. The architecture can also prevent DOS assaults that make use of services' flaws. Some models attempt to directly interact with security products, which is one of the major contrasts. On the other hand, the proposed approach is independent of security appliances and interacts with them via a Syslog server. To integrate with the controller of SDN, a northbound intersection application was developed. Table 2 lists the various BYOD security models' levels of coverage for each attribute. Table 2 shows that the BYOD models are concentrated on technology issues, however no model exists that enables the management of safety in the circumstances where the worker has complete authority over the mobile method.

Table 2: Security Models of BYOD system

Models	Features									
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**
Virtualization of the system	Yes	No	No	Yes	Yes	Yes	Yes	No	No	Yes
Container Device application	Yes	No	No	Yes	No	Yes	Yes	Yes	No	Yes
T-dominance	Yes	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes
BYOD (Cisco)	Yes	No	No	Yes	Yes	Yes	Yes	No	No	Yes
BYOD Model (Brain)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
BYOD Model (BRADFORD)	Yes	No	Yes	Yes	No	No	No	Yes	No	Yes

5. Conclusions

This paper presented a paradigm to improve security in SDN-based data centres. As a result, the system is evolving into a self-defending network that can adapt its resources to meet the needs of certain applications and expand safety to the network edge. The architecture depends on the introduction of a control unit made up of an internal syslog server and a security agent. A variety of security devices produce safety records. These logs are examined by the security agent to stop intruders assisted by the SDN controller. An experiment that used a combination of an emulation and simulation environment was created and put into effect. Investigations with evaluations showed that the proposed approach is feasible. Increased traffic analysis of cloud environments with BYOD infrastructure is the primary objective of subsequent studies in this field. The establishment of a cyber-secure cloud environment is a subject that requires more study.

REFERENCES

[1] Soubhagyalakshmi, P., & Reddy, K. S. (2023). An efficient security analysis of bring your own device. IAES International Journal of Artificial Intelligence, 12(2), 696.

[2] Bahaddad, A. A., Almarhabi, K. A., &Alghamdi, A. M. (2022). Factors Affecting Information Security and the Implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA). Applied Sciences, 12(24), 12707.

[3] Demanuele, C., Lokker, C., Jhaveri, K., Georgiev, P., Sezgin, E., Geoghegan, C., ...& McCarthy, M. (2022). Considerations for Conducting Bring Your Own "Device"(BYOD) Clinical Studies. Digital Biomarkers, 6(2), 47-60.

[4] Alothman, R. B., Saada, I. I., & Al-Brge, B. S. B. (2022).A Performance-Based Comparative Encryption and Decryption Technique for Image and Video for Mobile Computing. Journal of Cases on Information Technology (JCIT), 24(2), 1-18.

[5] Almarhabi, K., Bahaddad, A., &Alghamdi, A. M. (2023). Security management of

BYOD and cloud environment in Saudi Arabia. Alexandria Engineering Journal, 63, 103-114.

[6] Abdulkarim, S., Muhammed, A. I., & Ahmad, S. K. (2022). BYOD, The Advancement of Enterprise and Mobile Civilization: Challenges and Prevalence. J Med-Clin Res & Rev, 6(7), 1-7.

[7] Lad, S. (2022). Application and Data Security Patterns. In Azure Security For Critical Workloads: Implementing Modern Security Controls for Authentication, Authorization and Auditing (pp. 111-133). Berkeley, CA: Apress.

[8] Kulkarni, M., Deshpande, P., Nalbalwar, S., &Nandgaonkar, A. (2022). Cloud computing based workload prediction using cluster machine learning approach. In Applied Computational Technologies: Proceedings of ICCET 2022 (pp. 591-601). Singapore: Springer Nature Singapore.

[9] Wardhani, R. S., Kant, K., Sreeram, A., Gupta, M., Erwandy, E., & Bora, P. K. (2022, September). Impact of Machine Learning on the Productivity of Employees in Workplace.In 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 930-934).IEEE.

[10] Ali, M. D., &Kaur, D. (2020). Byod cyber forensic eco-system. International Journal of Advanced Research in Engineering and Technology (IJARET), 11(9).

[11] Ali, M. I., &Kaur, S. (2021, February). BYOD cyber threat detection and protection model.In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 211-218).IEEE.

[12] Hernández, O. S., Borrego, R. H., &Brito, H. R. G. (2021). Metodologíaparaevaluar el nivel de seguridad de lasaplicacionesmóvilessobreplataforma Android en ETECSA. SerieCientífica de la Universidad de lasCienciasInformáticas, 14(8), 1-16.

[13] Ali, M. I., &Kaur, S. (2021). Next-generation digital forensic readiness BYOD framework. Security and Communication Networks, 2021, 1-19.

[14] Lee, S. J., & Kim, G. B. (2021). K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea. IEEE Access, 9, 130094-130110.

[15] White, B. (2022). The Influence of BYOD Security Risk on SME Information Security Effectiveness (Doctoral dissertation, Capella University).

[16] Uushona, J. N., Ndevaetela, V. I., Toivo, E. T., &Gamundani, A. M. (2021, November). Network Forensics in a BYOD Environment. In 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC) (pp. 1-5). IEEE.

[17] Guy, E. L. (2022). Analysis of Law Enforcement's Use of Internet of Things for Digital Evidence Collection in Metropolitan Atlanta (Doctoral dissertation, University of the Cumberlands).

[18] Demanuele, C., Lokker, C., Jhaveri, K., Georgiev, P., Sezgin, E., Geoghegan, C., ...& McCarthy, M. (2022). Considerations for Conducting Bring Your Own “Device”(BYOD) Clinical Studies. Digital Biomarkers, 6(2), 47-60.

[19] Rajagopalan, S. (2020, November). An Overview of SD-WAN Load Balancing for

WAN Connections.In 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1-4).IEEE.

[20] de-Marcos, L., Cilleruelo, C., Junquera-Sánchez, J., &Martínez-Herráiz, J. J. (2020). A Framework for BYOD Continuous Authentication: Case Study with Soft-Keyboard Metrics for Healthcare Environment. In Applied Informatics: Third International Conference, ICAI 2020, Ota, Nigeria, October 29–31, 2020, Proceedings 3 (pp. 347-358). Springer International Publishing.

[21] Balamurugan, K., Latchoumi, T. P., &Ezhilarasi, T. P. (2022). Wearables to Improve Efficiency, Productivity, and Safety of Operations. In Smart Manufacturing Technologies for Industry 4.0 (pp. 75-90). CRC Press.

[22] Daid, R., Kumar, Y., Hu, Y. C., & Chen, W. L. (2021). An effective scheduling in data centres for efficient CPU usage and service level agreement fulfilment using machine learning. Connection Science, 33(4), 954-974.

[23] Martínez-Herráiz, J. J. (2020, October). A Framework for BYOD Continuous Authentication: Case Study with Soft-Keyboard Metrics for Healthcare Environment. In Applied Informatics: Third International Conference, ICAI 2020, Ota, Nigeria, October 29–31, 2020, Proceedings (Vol. 1277, p. 347). Springer Nature.

[24] Narwal, A., &Dhingra, S. (2023). A novel approach for Credit-Based Resource Aware Load Balancing algorithm (CB-RALB-SA) for scheduling jobs in cloud computing. Data & Knowledge Engineering, 145, 102138.

[25] Hassan, M. A., &Khalifa, T. E. (2019). Data Protecting Techniques Transmitted from smartphone (Master's thesis, University of Science and Technology).

[26] Krishna, A. G., Rathore, D. S., Singh, N. S., &Anitha, H. M. (2021, October). Securing Data Workflows: An Insight into Cloud Security. In 2021 International Conference on Advances in Computing and Communications (ICACC) (pp. 1-5). IEEE.

[27] Kulkarni, M., Deshpande, P., Nalbalwar, S., &Nandgaonkar, A. (2022). Cloud computing based workload prediction using cluster machine learning approach. In Applied Computational Technologies: Proceedings of ICCET 2022 (pp. 591-601). Singapore: Springer Nature Singapore.

[28] Wardhani, R. S., Kant, K., Sreeram, A., Gupta, M., Erwandy, E., & Bora, P. K. (2022, September). Impact of Machine Learning on the Productivity of Employees in Workplace.In 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 930-934).IEEE.

[29] Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., &Tsatsoulis, C. (2019, May). Review of security and privacy for the Internet of Medical Things (IoMT). In 2019 15th international conference on distributed computing in sensor systems (DCOSS) (pp. 457-464). IEEE.