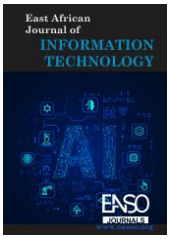
Article DOI: https://doi.org/10.37284/eajit.3.1.153



East African Journal of Information Technology
eajit.eanso.org
Volume 3, Issue 1, 2021
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security

Wycliffe Lamech Ogogo[1*]

[1] Kisii University, P. O. Box 408 – 40200, Kisii, Kenya.
[*] ORCID: https://orcid.org/0000-0002-7441-6020; Author for correspondence email: pricelamech@gmail.com.

Article DOI: https://doi.org/10.37284/eajit.3.1.153

Date Published:

04 March 2021

Keywords:

Real-Time Monitoring, Network Devices, Network Intrusion, Network Security.

ABSTRACT

The business world has been significantly affected by network intrusion leading to infringement of privacy and unprecedented economic losses. Therefore, real-time monitoring of network devices is important due to the enhanced and complex network systems in organizations and associated cyber threats. Real-time monitoring provides adequate alerts and updates regarding specific networks and their performance as soon as they occur. Constant monitoring of devices also makes it possible for organizations to detect any possible challenges that the networks may be encountering. This paper examines the effectiveness of real-time monitoring of network devices in a bid to enhance network security. The study was an empirical review of recently published research papers, journals, internet sites, and books with relevant content. The findings of this study revealed that Real-time device monitoring has many potential advantages to organizations by securing their systems thereby enhancing their overall performance.

APA CITATION

Ogogo, W. L. (2021). Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security. *East African Journal of Information Technology*, *3*(1), 1-6. https://doi.org/10.37284/eajit.3.1.153

CHICAGO CITATION

Ogogo, Wycliffe Lamech. 2021. "Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security." *East African Journal of Information Technology* 3 (1), 1-6. https://doi.org/10.37284/eajit.3.1.153.

HARVARD CITATION

Ogogo, W. L. (2021) "Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security," *East African Journal of Information Technology*, 3(1), pp. 1-6. doi: 10.37284/eajit.3.1.153.

Article DOI: https://doi.org/10.37284/eajit.3.1.153

IEEE CITATION

W. L. Ogogo, "Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security," *EAJIT*, vol. 3, no. 1, pp. 1-6, Mar. 2021.

MLA CITATION

Ogogo, Wycliffe Lamech. "Real-Time Monitoring of Network Devices: Its Effectiveness in Enhancing Network Security." *East African Journal of Information Technology*, Vol. 3, no. 1, Mar. 2021, pp. 1-6, doi:10.37284/eajit.3.1.153.

INTRODUCTION

Due to the high costs of development and research, many technology-based companies worldwide have shifted towards the use of network systems that provide real-time device monitoring to promote upgraded operations with effective and secure network systems. The security of network monitoring is fundamental in detecting threats that originate from the external network and can be applied to detect network threats from within. Network monitoring refers to consistently overseeing computerized network devices for any deficiencies or failures to ensure the effectiveness of network devices and a continuous network performance. For instance, network monitoring will ensure that network components' conditions are adequately and effectively monitored, including firewalls, servers, and routers (Tsai et al., 2018),

According to Gupta et al. (2016), network monitoring is the worldwide monitoring of fundamental network devices for performance, fault, and is often evaluated to optimize and maintain their availability and effectiveness. It promotes proactive monitoring of network systems and identifying problems at early stages, thus preventing failures and network downtime. According to Yuan et al., (2017), network monitoring offers important information to many network administrators in real-time, such as using a network device and proactively identifying any possible deficiencies and optimizing network efficiency. Network systems majorly include hardware tools and software which can track different aspects of network operations such as uptime, bandwidth utilization, and traffic.

According to Woodall et al. (2017), network monitoring involves applying intensive technologies towards ensuring networks deliver consistent and effective performance that is predictable. It begins with the discovery process, where the device is analysed. After the discovery process is completed, the network system is monitored and a road map that can ensure effective network monitoring is established. According to Brueckner and Donovan (2018), Real-time monitoring of devices has created a roadmap that enables easy identification of weaknesses in network security that is likely to lead to errors and provide recommendations and means of protecting network services while in transit and at rest. The roadmap will also enable easy identification of weaknesses in network security and provide recommendations to protect the network in motion or static state.

LITERATURE REVIEW

According to a study by Ambika and Nataraj (2013) on architecture for real-time modelling and monitoring of network behaviour to enhance network security, it was found that the rise in the need for network security has led to the development and application of Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) in network systems to prevent illegal access. An IDS is a system that facilitates monitoring and analysis of events taking place in a network system to identify the signs of possible incidents. The illegal incidents may include threats or violations about to take place to violate the computer and standard security policies. The lack of reliable security measures can lead to network attacks by intruders who take hold of a user's account or the legitimate information in a networking device. In case of any intrusion, the IPS reports to the system administrator and takes appropriate action such as configuring firewalls or closing access points to prevent further attacks. IPS solutions are also used to determine employees in an organization, identify the key issues with corporate security policies, and prevent network guests from violating the guidelines and policies.

Article DOI: https://doi.org/10.37284/eajit.3.1.153

It is essential to monitor the vital signs of possible violations, imminent threats, and incidents in a typical network with many access points. The same is because the current network threats are more sophisticated and can infiltrate the most robust security networks or solutions. On the other hand, IDS are designed to monitor the network and send alerts to the administrator after detecting a threat. However, an IDS is not designed to block threats or attacks. An IPS works by scanning all network traffic and preventing security threats such as Denial of Service (DoS) attacks, DDoS attacks, worms, various types of exploits, and viruses. Importantly, IPS performs real-time inspection of a packet by deeply inspecting every packet travelling across the entire network. If IPS detects a malicious packet, it will terminate the TCP session and block the offending user account or source IP address from assessing an application in the system. It also reconfigures or reprograms the firewall to prevent a future attack. Lastly, it removes and replaces any suspicious content left in the network after an attack by removing header information, repackaging payloads, and removing any infected attachments in an email or file.

The monitoring of network devices has effectively promoted an improved healthcare system. Different healthcare institutions have benefited from effective firewall management in healthcare companies and organizations; where linked computers are left exposed to varieties of potential threats without any protection. An installation of a firewall in every computer network is the first defence against viruses and malware penetrating the system. A weakened firewall is one of the causes of medical errors in electronic health records. With a disabled firewall, the health facility might lose all the patients' details through malware and virus penetration (Bettany & Halsey, 2017). With the penetration of malware into the patients' medical records, the records might be lost, compromising the credibility of the records provided to the patients. With the loss of records, patients might be supplied with the wrong medication, hence, adversely impact them. The hospitals might also lose the patient's financial records and result in great losses in health facilities. Active monitoring of firewall has significantly reduced network insecurity in medical institutions regarding Electronic Health Record.

Moreover, device monitoring has enhanced the security of software used by medical institutions. A compromised system is a computer network system whose availability, integrity and confidentiality have been majorly affected either unintentionally or intentionally by a foreign source. Compromised software has led to the loss of health records in various health facilities impacting the credibility of the treatment procedures provided to the patients (Ondiege, Clarke & Mapp 2017). Monitoring of network devices as promoted increases confidentiality, privacy, transparency, and integrity with these institutions. It promotes the detection of risk as they occur and thus enhances the organization's security of important software. Real-time device monitoring has also brought many potential advantages to these organizations by securing the financial records and economic prosperity in different organizations, including healthcare institutions.

A research study by Sohail (2010) on automation of network management and various multidisciplinary concepts found that today's computer networks and management systems should have dynamic real-time decision making and an experience-based self-adaptation. It should also have the ability to facilitate intellectual reasoning. Furthermore, with the increase in the complexity and size of computer networks, the network's management system should be automated. Automation minimizes human involvement, hence saving time by facilitating dynamic supervision of the heterogeneous and large systems. Automation of a network management system is also necessary to solve the challenges faced by network professionals in balancing the ongoing responsibilities while at the same time reacting to daily events. Furthermore, automation saves time by reducing the period spent on responding to unanticipated business requirements or putting out the fires at the expense of dealing with feeding or caring for network operations.

Programmable logic is used to manage the network services and resources in a network system. Network automation allows for the configuration, scaling, protection, and integration of a network infrastructure. It also quickens application services performed by manual users. Since IT operations should be more flexible and responsive to change, automation helps enhance the IT operations'

Article DOI: https://doi.org/10.37284/eajit.3.1.153

flexibility. More visibility is gained by understanding the network operations in a network system hence upholding the ability to adapt to the network changes or needs. Additionally, automation of repetitive tasks that are subject to mistakes and human errors makes a company increase its productivity to drive innovation and increase performance.

The use of multidisciplinary concepts from machine learning, artificial intelligence, and artificial neural networks in a network system facilitates self-healing and experience-based learning in network management systems. Dynamic real-time supervision of large network connections with many components is impossible without the automation of network connections and the use of multidisciplinary concepts. The approach helps to address traffic characterization, and network intrusion detection in a security management system.

Real-time device monitoring has led to ensuring the security of different companies and organizations from malware attacks, which may compromise the effectiveness of their network security. Malware is software that is created to infect and harm host systems. Advance malware, for example, ransomware, is used in committing numerous frauds by using them to extort critical information and resources from the computers of an organization. With the penetration of malware into a company's network system, the system might experience various irregularities and losses (Chakkaravarthy, Sangeetha & Vaidehi, 2019). However, Real-time monitoring has ensured the protection of network systems from malware attacks. Ensuring there is no malware, spyware and ransomware in the system, monitoring would recommend a need to install malware/antivirus software, which would help identify the malware by the computer system and necessitate effective and timely elimination. Companies have also benefited by detecting network insecurities and thus can ensure that the antivirus software is kept up to date. Real-time monitoring of network devices also emphasizes the importance of regular scanning of the system using the antivirus software and ensuring the network operating system is kept current.

Monitoring network devices has ensured that damaged and corrupted database systems are improved through improved data recovery plans and intensive network security that is reliable and convenient to minimize network insecurities (Cox *et al.*, 2017). It has also emphasized the need for organizations and companies to adopt an effective system for backup information systems by integrating cloud-based backup procedures that promote complete backup processes and protect confidential information through secure network regulations. It has emphasized the need to perform regular scanning of the network system using the antivirus software and ensuring the Network Operating System is kept current.

According to Shin et al. (2016), Software Defined Networking (SDN) is a network architecture that helps to uphold network security in a management system by enabling programmatical and central configuration of networks to improve its monitoring and performance. In other words, it makes a network system more of cloud computing than traditional network management. SDN addresses the issue of traditional management in a static architecture since such a network architecture is complex and decentralized as compared to the current network, which is easy to troubleshoot and requires more flexibility. SDN opts to centralize network intelligence in a single network component through disassociation of the data plane or network packets forwarding from the control panel or the routing process. A control plane comprises one or more controllers that act as the brain of the SDN network that incorporates the whole intelligence. However, intelligent centralization has some negative implications on the system's scalability, security, and elasticity.

At first, SDN was associated with the OpenFlow protocol used for remote information sharing with a network plane element to determine the network packet path in a network switch. However, advancements have made OpenFlow an inappropriate solution after adding proprietary techniques such as Nicira's network virtualization platform and Cisco System's Open Network environment. Moreover, SD-WAN enables the application of similar technology to a WAN. SDN has also been availed for industrial control application that needs an extremely fast failover.

Article DOI: https://doi.org/10.37284/eajit.3.1.153

One of the benefits of SDN is that it is directly programmable since it is decoupled from the available forwarding functions. It is also managed centrally since a network intelligence is logically centralized in an SDN controller software-based to maintain a global network view.

The network view appears to policy engines and applications as a single logical switch. Additionally, SDN is configured programmatically to enable network managers to configure, secure, optimize, and manage the network resources quickly and dynamically through an automated SDN program. The programs can write themselves since they do not rely on proprietary software. Lastly, SDN is vendor-neutral and open standard-based hence simplifying the network operations or design since the SDN controller provides the instructions rather than the multiple vendor-specific device and protocol.

According to Li et a. (2019), integrating multi-layered security in a network system makes it possible for network managers to identify and isolate any threat or possible attacks before they spread. However, for the multi-layered security system to be more effective in preventing an attack, it should be combined with a powerful protocol, intrusion prevention, application control, behaviour analysis, and vulnerability management. Other network defences found in firewalls will also help to reduce the exposure to other threats. It is also important to counter check whether all these layers are enabled to ensure that they work effectively as a multi-layered system. To fight against potential security threats, the layers should be harmonized appropriately.

Insiders' attack leads to data loss, which can be prevented by implementing an automated corporate policy to catch data loss incidences before the data leaves the system or organization. Data Loss Prevention (DLP) is an effective tool used to prevent any attack that leads to data loss. It also prevents misused or access to data by unauthorized users. DLP solves three main objectives of an organization or network system that includes personal information protection, data protection, and intellectual property protection. It also prevents threats caused by negligent or unintentional data exposure that occurs when an employee in an organization fails to adhere to the organizational policies' access to data. The system is used along with an antivirus to prevent attackers from compromising sensitive information or systems. Similarly, a firewall is used to block unauthorized personnel from accessing the system that stores sensitive or confidential information.

Device monitoring has also provided the efficiency and effectiveness of patches, which help to fix network security. Real-time monitoring of network security in every company and organization ensures that network security is their priority and concern (Rath et al., 2018). While ensuring that the patches work and provide protection to the network system, there is a need to apply patch testing before rolling them out to all the network devices in organizations to make the right balance between keeping the company’s network system up to date and stable.

CONCLUSION

Monitoring of network devices as promoted increases confidentiality, privacy, transparency and integrity with these institutions. It promotes the detection of risk as they occur and thus enhances the organization's security of important software. Real-time device monitoring has also brought many potential advantages to these organizations by securing the financial records and economic prosperity in different organizations, including healthcare institutions. Indeed, Real-time monitoring of devices has created a roadmap that enables easy identification of weaknesses in network security that is likely to lead to errors and provides recommendations and means of protecting network services while in transit and at rest.

REFERENCES

Ambika, M., & Nataraj, R. V. (2013). Architecture for real-time monitoring and modeling of network behavior for enhanced security. *International Journal of Computer Applications*, *64*(8).

Bettany, A., & Halsey, M. (2017). Malware Defense in Depth. In *Windows Virus and Malware Troubleshooting* (pp. 21-39). Berkeley, CA: Apress.

Article DOI: https://doi.org/10.37284/eajit.3.1.153

Brueckner, S. K., & Donovan, M. P. (2018). *U.S. Patent No. 10,083,624*. Washington, DC: U.S. Patent and Trademark Office.

Chakkaravarthy, S. S., Sangeetha, D., & Vaidehi, V. (2019). A Survey on malware analysis and mitigation techniques. *Computer Science Review*, *32*, 1-23.

Cox, J. H., Chung, J., Donovan, S., Ivey, J., Clark, R. J., Riley, G., & Owen, H. L. (2017). Advancing software-defined networks: A survey. *IEEE Access*, *5*, 25487-25526.

Gupta, A., Birkner, R., Canini, M., Feamster, N., Mac-Stoker, C., & Willinger, W. (2016, November). Network monitoring as a streaming analytics problem. In *Proceedings of the 15th ACM Workshop on Hot Topics in Networks* (pp. 106-112).

Li, Y., Huang, G. Q., Wang, C. Z., & Li, Y. C. (2019). Analysis framework of network security situational awareness and comparison of implementation methods. *EURASIP Journal on Wireless Communications and Networking*, *2019*, (1) 205.

Ondiege, B., Clarke, M., & Mapp, G. (2017). Exploring a new security framework for remote patient monitoring devices. *Computers*, *6*(1), 11.

Rath, M., Swain, J., Pati, B., & Pattanayak, B. K. (2018). Network security: attacks and control in MANET. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 19-37). IGI Global.

Shin, S., Xu, L., Hong, S., & Gu, G. (2016, August). Enhancing network security through software-defined networking (SDN). In the *2016 25th international conference on computer communication and networks (ICCCN)* (pp. 1-9). IEEE.

Sohail, S. (2010). Automation of network management with multidisciplinary concepts. *International Journal of Computer Technology and Applications*, *1*(1), 71-77.

Tsai, P. W., Tsai, C. W., Hsu, C. W., & Yang, C. S. (2018). Network monitoring in software-defined networking: A review. *IEEE Systems Journal*, *12*(4), 3958-3969.

Woodall, W. H., Zhao, M. J., Paynabar, K., Sparks, R., & Wilson, J. D. (2017). An overview and perspective on social network monitoring. *IISE Transactions*, *49*(3), 354-365.

Yuan, Y., Lin, D., Mishra, A., Marwaha, S., Alur, R., & Loo, B. T. (2017, August). Quantitative network monitoring with NetQRE. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication* (pp. 99-112).

