ISSN: **2959-6386** (Online)
Journal of Knowledge Learning and Science Technology, Vol. 2, Issue 1, April 2023
Journal Homepage: http://jklst.org/index.php/home
DOI: https://doi.org/10.60087

DESIGN OF THE NETWORK SECURITY ARCHITECTURE FOR SMART CAMPUS IN THE PHILIPPINES

Yang Yuhong[1] , Song Zhuo[2], and Richard N Monreal[3]

[1]*University of the Cordilleras (Governor Pack Road, Baguio City 2600, PH)*
[2]*University of the Cordilleras (Governor Pack Road, Baguio City 2600, PH)*
[3]*University of the Cordilleras (Governor Pack Road, Baguio City 2600, PH)*

Correspondence Author: Song Zhuo **E-mail:** songzhuo360@gmail.com

| Abstract
This paper aims to study the existing network security framework of Philippine Smart Campuses and propose a more robust network security framework based on situational awareness which addresses emerging security challenges. By investigating and analyzing the current state of smart campus construction in the Philippines, the paper reveals the current problems and vulnerabilities in network security. As educational institutions increasingly adopt smart technologies, the need for a robust cybersecurity framework to protect sensitive data and ensure smooth campus operations becomes crucial. Consequently, a comprehensive network security framework is urgently needed to safeguard vital data and maintain the secure operation of smart campuses in the Philippines. It designs a comprehensive and effective network security framework by integrating relevant domestic and international research findings and experiences. The SA framework encompasses multiple security layers, including access control, authentication mechanisms, intrusion detection systems, and incident response. Results demonstrate the significant impact of the proposed cybersecurity framework on enhancing the security of Philippine Smart Campuses. The findings of this study contribute valuable guidance to the development of network security for Philippine smart campuses. By addressing the current network security landscape, identifying challenges, conducting a literature review, and designing the framework, this research presents a more robust network security framework and verifies its effectiveness through implementation. The framework leverages various security technologies and methods such as situational awareness, and zero-trust technology to enhance the security and reliability of smart campus networks. Moreover, it provides substantial support for securing smart campuses in the Philippines, ensuring the integrity of school data, and facilitating sustainable growth.

| Keywords
Network Security, Smart Campus, Situational Awareness, Threat Intelligence Analysis
| Article Information:

Accepted: 25/04/23 **Published:** 30/04/23 **DOI:** https://doi.org/10.60087/mrb0hh55

1. Introduction

In today's digital age, the construction of smart campuses has become an important measure to improve the quality of education and the efficiency of school management. The rapid development of smart campuses in the Philippines has brought many conveniences and opportunities to students and educational institutions. But at the same time, it also brings increasingly serious network security challenges. Issues such as cyber-attacks, data leakage, and information security threats have brought risks and challenges to the development of smart campuses in the Philippines. Therefore, it is necessary to study the current situation of Philippine smart campus network security and propose corresponding solutions.

In recent years, the Philippine Smart Campus has encountered a series of cyber-attacks. These attacks include data breaches, ransomware attacks, and phishing attempts targeting students, faculty, and staff. These cases have exposed the real threats and potential risks faced by smart campuses in the Philippines, highlighting the urgency and importance of network security. Cybersecurity has become a major issue. With the widespread use of the Internet and the rapid advancement of technology, network security threats have become increasingly complex and diverse. Hackers and malicious attackers take advantage of system vulnerabilities and technical vulnerabilities in an attempt to hack into networks, steal sensitive data, or disrupt network services. Smart campuses in the Philippines also face various cybersecurity challenges. On May 2, 2017, the newly established Department of Information and Communication Technology (DICT) of the Philippines released the National Cybersecurity Plan 2022 (National Cybersecurity Plan 2022) which also shows the government pays a lot of attention to cyber security[1]. The network security of smart campuses in the Philippines faces a series of challenges such as the single limitation of traditional firewall protection, lagging risk perception, untimely risk management, lack of coordinated response mechanism, and insufficient visualization of smart campus network security.

Although traditional firewall technology can provide basic network protection, its single-layer defense capability can no longer meet the complex and changeable network security requirements. Traditional firewalls are often unable to provide comprehensive protection against ever-evolving cyber-attacks and threats, thus bringing greater risks to smart campuses

Another challenge is the delay in risk perception. The security measures of the smart campus network are often difficult to identify emerging network threats and attack methods in a timely manner [2]. This vulnerability provides an opportunity for hackers to exploit, thereby increasing the risk of data leakage and system intrusion in Smart Campus Philippines.

In addition, the lack of visualization of smart campus network security is also an urgent problem to be solved. It is often difficult for school administrators to clearly understand the current situation and threats to network security, making it difficult to monitor and identify potential risks in real-time.

The objective of this paper aims to propose a new framework to solve the existing challenges facing the ever-evolving network threats and the increasingly intelligent campus environment, it is particularly important to study the network security of smart campuses. Ensuring the privacy and data security of students and teachers, protecting the integrity of academic research and intellectual property, and ensuring the operational stability of a smart campus all require a strong network security framework. The implementation of comprehensive network security measures can effectively respond to network attacks, prevent data leakage, and provide visual security monitoring and risk management, thereby ensuring the sustainable development of smart campuses.

2. Literature Review

2.1 Current Status of Network Security Research

Network security is a vast research field encompassing various aspects such as network attack defense, security measure design, and risk management. In the context of smart campus network security, researchers have explored different methods and solutions[3]. This section provides a comparative analysis of studies in three relevant areas to offer guidance for designing a cybersecurity framework for smart campuses in the Philippines.

2.2 Traditional Firewalls and Advanced Security Measures

Traditional firewalls are a fundamental component of network security in smart campuses. However, their functionality is limited to basic network access control and intrusion detection, often unable to cope with complex network attacks. In contrast, advanced security measures, like intrusion detection systems (IDS) and intrusion prevention systems (IPS), employ intelligent approaches to identify and block cyber-attacks [4]. For instance, an IDS can monitor network traffic and detect abnormalities based on known attack patterns and behavioral anomalies. Nevertheless, traditional firewalls and IDS/IPS technologies have their limitations when faced with unknown zero-day attacks and advanced persistent threats (APTs).

2.3 Risk Management and Threat Intelligence Analysis

Risk management plays a vital role in smart campus network security. By assessing and identifying potential security risks and implementing corresponding measures to mitigate and respond to these risks, the overall network security level of smart campuses can be enhanced [5]. SIEM is security information and event management. SIEM is a system model dedicated to collecting enterprise-level security logs, but it is much more powerful than simple log or event management. SIEM analyzes log and event data in real-time to provide threat monitoring, event correlation, and incident response, so it can be well integrated into a network situational awareness system as a module of the system[6]. Log analysis is emphasized here because it is the most intuitive way to perceive security information. Of course, network security analysis is not just log analysis, but also needs to integrate various data such as traffic and behavior.

2.4 Network Security Situational Awareness

In the rapidly evolving landscape of modern educational institutions, smart campuses have emerged as a cutting-edge solution that leverages advanced technologies to enhance learning, safety, and efficiency. These interconnected environments utilize the Internet of Things (IoT), cloud computing, and other digital innovations to create a seamless, data-driven educational experience[7]. However, with the integration of these technologies, the smart campus also becomes susceptible to various cyber threats, necessitating a robust Network Security Situational Awareness framework.

2.5 Literature Review Analysis and Conclusion

Firstly, although traditional firewalls play a fundamental role in smart campus network security, they have limitations when dealing with complex network attacks and advanced threats. Therefore, the adoption of advanced security measures such as IDS and IPS should be considered to enhance network defense capabilities. Secondly, risk management and threat intelligence analysis are crucial in smart campus network security. Accurate assessment and timely identification of security risks, coupled with insights gained from threat intelligence analysis, enable smart campuses to take appropriate measures to mitigate risks and respond to attacks. Furthermore, smart campus network security visualization provides managers with intuitive information regarding security status, facilitating a better understanding of the network

security landscape and potential risks. By visually representing network data, managers can swiftly detect abnormal behavior and security threats, enabling them to respond promptly.

3. Methodology

3.1 Network Security Framework Requirements Analysis

Aiming at the cybersecurity challenges and needs of the Smart Campus in the Philippines, conducting a requirements analysis of a cybersecurity framework is a key step in designing a robust framework. The following is a demand analysis for the Philippine smart campus cybersecurity framework.

Multiple Layer	Requirements Analysis
IT Infrastructure layer	servers, databases, switches, routers, firewalls, and other networking components, etc.
Network Layer	the devices and protocols etc.
Application Layer	canvas, university portal, website, student portal, etc.
End Points Layer	IoT devices, laptops, computers, mobile phones, etc.
User Layer	Irregular online behavior, hacker attack

Figure 3.1 Network Security Framework Requirements Analysis

The network layer involves the devices and protocols used for routing and forwarding data across the university's network. The application layer involves the software and services running on the university's servers and systems. The endpoints layer refers to individual devices connected to the network, such as computers, laptops, smartphones, and IoT devices

3.2 Overall Architecture Design of NSSA Framework

Based on the above demand analysis, it is crucial to design an overall architecture of the network security framework applicable to the Philippine Smart Campus. The following is the overall architectural design of the network security framework.

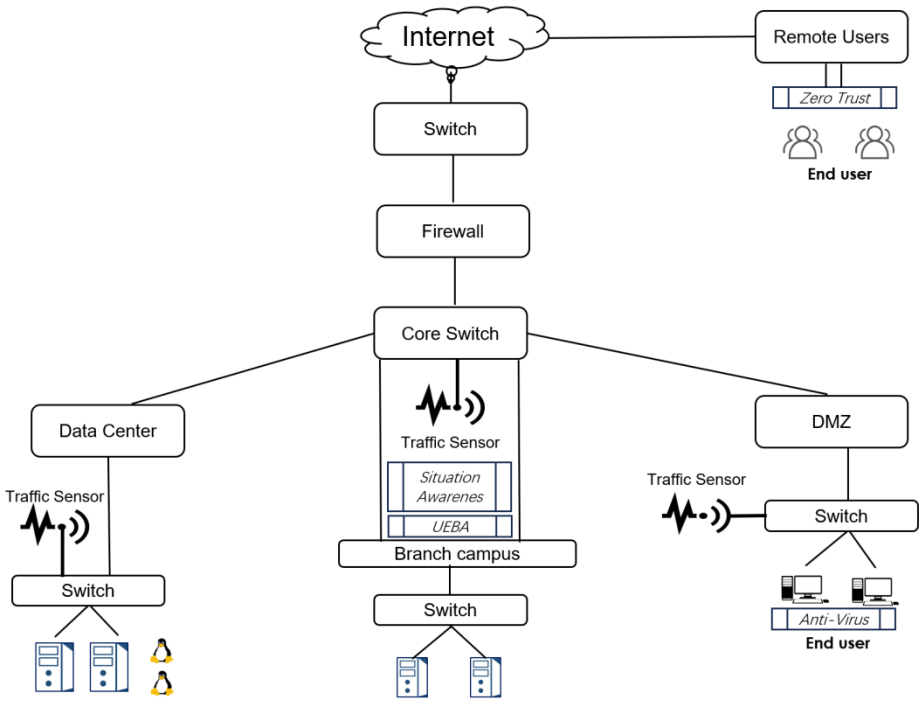


Figure 3.2 Overall Architecture Design of NSSA Framework

From the diagram, border security measures at the network entrance of the smart campus, including firewalls and NAC, etc. These measures can effectively prevent external attacks and malicious traffic from entering the campus network. Zero-trust identity authentication and access control for establishing a strong identity authentication and access control mechanism to ensure that only authorized users can access campus networks and resources. Threat monitoring and response introduce a threat monitoring system to monitor network traffic, logs, and events in real-time, and identify potential threats and abnormal behaviors. Adopt a real-time response mechanism to quickly take corresponding measures to deal with threats and attacks, including intrusion detection and prevention, abnormal behavior analysis, and malware detection. Security awareness training and education to carry out network security awareness training and education activities to improve the network security awareness and skills of teachers and students in the smart campus. By cultivating security awareness, reduce the risk of security breaches and user behaviors to network security.

3.3 Technology involved in the framework

Designing a robust cybersecurity framework requires the consideration of multiple technologies and methodologies. The following are some key technical discussions involved in the Philippine Smart Campus network security Framework.

Situation Awareness: Situation awareness technologies are used to gain a comprehensive understanding of network security status and threat situations. By collecting and analyzing various security events and data, including logs, alerts, and threat intelligence, a situational awareness system can provide a comprehensive understanding of smart campus network security. It can help security teams quickly identify and respond to threats and improve the ability to detect network security incidents.

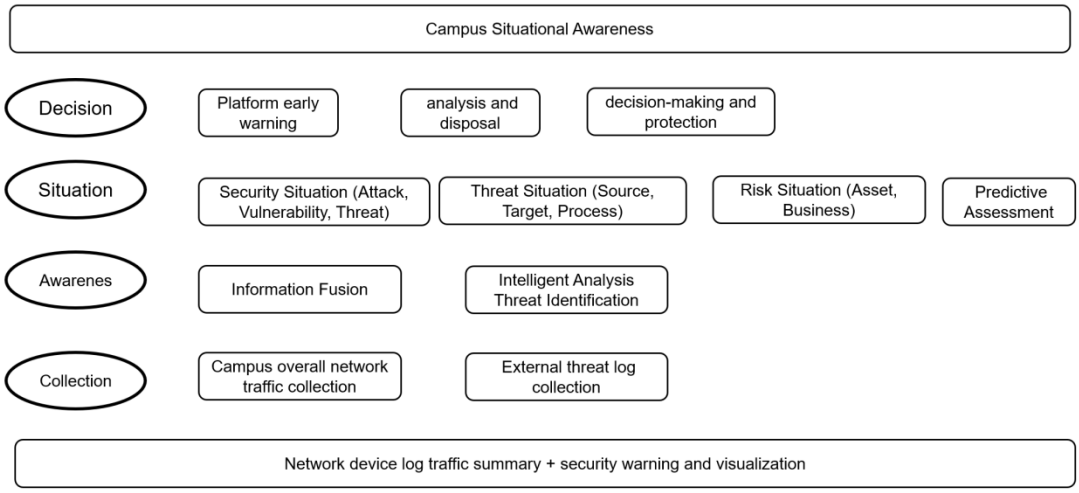


Figure 3.3 Campus Situation Awareness Diagram

Zero Trust Technology: The zero-trust model is a security strategy based on the principle of least privilege, which regards every user and device inside the network as a potential threat, requiring authentication and authentication on each access request. authorized. This model reduces potential attack surfaces and security risks by enforcing techniques such as multi-factor authentication, access control policies, and behavioral analytics to restrict user and device access.
Artificial intelligence and machine learning: Introduce artificial intelligence and machine learning technologies to realize intelligent threat detection and security response. By training the model, abnormal behaviors and unknown threats in the network can be identified, and corresponding defensive measures can be taken.

UEBA stands for User and Entity Behavior Analytics. It leverages machine learning, data analytics, and artificial intelligence to detect anomalous behaviors and potential security threats within an organization's network. UEBA focuses on monitoring the activities of users and entities (such as devices, applications, and servers) to identify deviations from typical patterns and uncover potential insider threats or external attacks. UEBA is applied in network security to strengthen an organization's ability to detect and respond to sophisticated cyber threats, including insider threats and external attacks.

Endpoints security protection is the key to protecting smart campus terminal devices and terminal users from threats. This includes using endpoint security software to detect and prevent the spread and intrusion of malware. In addition, terminal security also includes measures such as security patch management, access control, and enhanced identity authentication to ensure the security and reliability of terminal devices.

To sum up, security technologies such as NDR technology, situation awareness, endpoints security protection, zero trust technology, data encryption, and privacy protection play an important role in the design of the Philippine smart campus network security framework. Through the comprehensive use of these technologies, a comprehensive, intelligent, and credible network security defense system can be established to improve the security and reliability of the smart campus network. At the same time, in the design of the Philippine smart campus network security framework, we also consider the requirements of

border security, identity authentication, and access control, threat monitoring and response, data encryption and secure transmission, and security awareness training and education.

4. Results and Discussion

This section is a comparative or descriptive analysis of the study based on the study results, previously literature, etc. The results should be offered in a logical sequence, given the most important findings first and addressing the stated objectives. The author should deal only with new or important aspects of the results obtained. The relevance of the findings in the context of existing literature or contemporary practice should be addressed.

4.1 Framework Assessment Design

By implementing a comprehensive situational awareness framework, real-time monitoring and analysis of the security status of the smart campus network can be achieved. The framework implementation diagram mainly includes the following diagram and components.

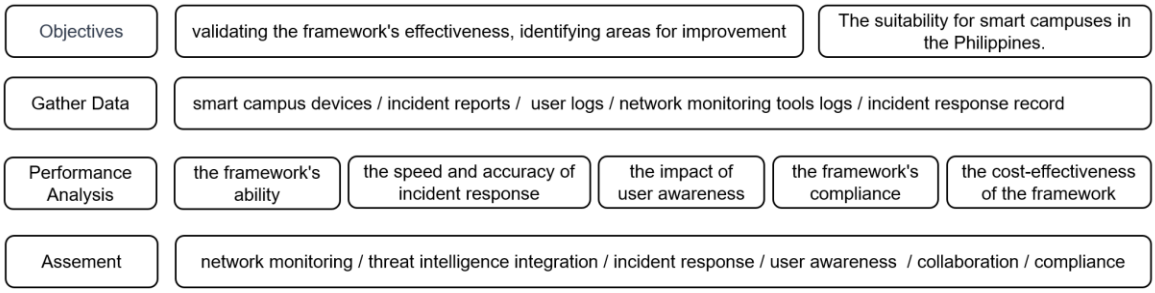


Figure 4.1 The Assessment Framework Diagram

4.2 Result Analysis

The assessment aims to evaluate the framework's effectiveness, efficiency, and practicality in addressing the specific security challenges faced by different campuses. To conduct a comprehensive evaluation, it simulated the configuration information, generated test data, and compared the results with baseline data to assess the framework's impact on enhancing network security. To generate realistic test data, it incorporated a wide range of simulated security threats and incidents that may encounter.

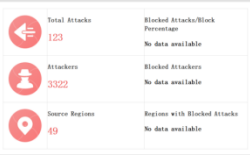
SA Framwork	Forensics	Intelligence	UEBA
Framwork Simulation Setup	VM: Windows 2012 / CentOS Linux 8 RAM: 32G STORAGE: 128G SOFTWARE: vFW / vSensor / SIP / Anylogic / Wireshark		
Simulation Configuration Information	Network Topology: switches, routers, access points, firewall, sip . Smart Devices: IoT devices, smartboards, and security cameras . Security Solutions: Integrated the proposed situation awareness framework into the simulation environment. Network monitoring tools: threat intelligence feeds, incident response procedures, and user awareness training modules.		
Simulation Test Data	Malware Attacks: Various types of malware, including viruses, ransomware, and trojans. Insider Threats: an unauthorized individual attempted to gain access to sensitive information or disrupt network. Phishing and Social Engineering to check awareness and preventing successful attacks. Network Anomalies: port scans, brute force attacks, and DDoS attempts .		
Results and Findings	IP Address :122 Type : hosts and servers Risk Level :Compromised Threats :Virussality \ vobfusworm \skeeyahtrojan \MiningSVCCTL \skeeyahtrojan \ injectortrojan\agenttrojan	Specific Intelligence: sync.malwareprotectionlive.com DNS Server: 10.114.134.252 Resolved IP: 199.59.243.233 Src IP: LACJrHigh1 (10.134.137.160) Src Port: 65026 Dst IP: 199.59.243.222(-) Dst Port: 66743 Protocol: dns	

Figure 4.2 Situation Awareness Framework Analysis

The framework assessment analysis confirmed that the proposed situation awareness framework is a valuable addition to smart campus network security in the Philippines. It offers enhanced threat detection capabilities, quicker incident response, increased user awareness, and improved compliance. The findings indicate that the framework effectively addresses the unique security challenges faced by educational institutions and is well-suited for implementation in other smart campuses.

4.3 Discussion

Through the implementation of the situational awareness framework, the security situational awareness of the Philippine smart campus network can be effectively improved.

Security event detection capability: Through the implementation of the framework, real-time detection and analysis of security events in the smart campus network can be performed. Through accurate detection and rapid response to security incidents, the impact of potential threats on the smart campus can be reduced, and corresponding measures can be taken in time to deal with security incidents.

Threat intelligence analysis: Through the threat intelligence analysis technology in the implementation of the framework, information about current threat intelligence can be obtained and correlated with real-time monitored network traffic and event data for analysis. This can improve the awareness and understanding of threats, and help the smart campus network security team to better develop security policies and response measures.

Real-time monitoring and visual display: After the framework is implemented, through the display of the visual interface, smart campus managers and security teams can monitor the security situation and threats of the network in real-time. By graphically displaying information such as network topology, security events, alarms, and risk assessments, you can more intuitively understand the security status of the smart campus network and take corresponding security measures in a timely manner.

Decision support capability: After the framework is implemented, the use of decision engines can provide decision support for smart campus managers and security teams. By comprehensively analyzing and evaluating the data collected by the framework, the decision-making engine can generate corresponding decision-making suggestions and response measures to help managers better deal with cybersecurity threats and incidents.

By implementing a situational awareness framework, the security and reliability of the Philippine smart campus network can be improved. The design of the framework implementation diagram, the selection of equipment deployment mode, and the analysis of the implementation results are the keys to ensure the effectiveness of the framework. Through continuous monitoring, analysis, and adjustment, the framework can be continuously optimized to further enhance the security defense capabilities of the smart campus network.

5. Conclusion

This paper proposed a more robust situation awareness framework through the study of cybersecurity in smart campuses in the Philippines. This framework is of great significance for the construction of a smart campus in the Philippines. It can improve the security and reliability of the smart campus network, and reduce the impact of network threats and security vulnerabilities on smart campuses. Through the analysis of the framework, comprehensive perception and timely response to the network security situation can be achieved, and the level of network security in smart campuses can be improved.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Smith, J., & Johnson, L. (2018). Enhancing Network Security in Smart Campus Environments. *Journal of Information Systems Education, 29(3)*, 211-220.

[2] Wang, H., Zhang, H., & Li, L. (2020). A Threat Intelligence-Based Risk Management Framework for Smart Campus Networks. *IEEE Access, 8,* 186532-186542.

[3] Liu, Y., Huang, Z., & Chen, L. (2019). Visualizing Network Security for Smart Campus: A Case Study. *Proceedings of the 2019 4th International Conference on Network and Computing Technologies,* 1-5.

[4] Gao, S., Wang, Q., & Yang, B. (2021). Smart Campus Network Security: Current Status and Challenges. *International Journal of Online and Biomedical Engineering, 17(8),* 50-60.

[5] Zhang, Y., Li, M., & Wang, X. (2019). Design and Implementation of Smart Campus Security System Based on Big Data Analysis. *Proceedings of the 2019 8th International Conference on Educational and Information Technology*, 121-125.

[6] Chen, J., Chen, M., & Lu, K. (2020). Risk Assessment and Decision-Making Framework for Smart Campus Security. *Proceedings of the 2020 IEEE International Conference on Systems, Man, and Cybernetics*, 2332-2337.

[7] Yang, S., Sun, W., & Zhu, L. (2021). A Visualization Approach for Cybersecurity Situation Awareness in Smart Campus. *Security and Communication Networks, 2021*, Article ID 6631306.