Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 3, June 2026, pp. 2373~2382
ISSN: 2302-9285, DOI: 10.11591/eei.v15i3.11299

Leveraging defense-in-depth through a deception-driven security model for smart university

Marlon A. Naagas, Anazel P. Gamilla, Mary Camille D. Rabang
Department of Information Technology, College of Engineering, Central Luzon State University, Science City of Munoz, Philippines

Article Info

Article history:

Received Aug 30, 2025
Revised Mar 11, 2026
Accepted Mar 31, 2026

Keywords:

Cybersecurity
Deception-driven security
Defense-in-depth
Security model
Smart university

ABSTRACT

Cybersecurity remains one of the biggest challenges to address as the education sector shifts to the smart university concept. The education sector has experienced in recent years a noticeable rise in cyberattacks, revealing limitations in relying solely on traditional defense-in-depth (DID) security strategies. In response, the study implements a deception-driven security model (D-DSM) designed for a campus network environment. The proposed model incorporates decoy resources managed through a centralized deception mechanism to mislead attackers, divert malicious activities away from critical assets, and provide meaningful indicators of attack behavior, resulting in a more effective way to mitigate attacks. Rather than replacing existing defenses, the model complements current security controls by improving the visibility of advanced and lateral attacks while helping reduce false alerts. Adding deception as an active security layer is a useful way to make networks more resilient and helps build smarter, safer, and more sustainable university infrastructures.

Corresponding Author:

Anazel P. Gamilla
Department of Information Technology, College of Engineering, Central Luzon State University
Science City of Munoz, Philippines
Email: apgamilla@clsu.edu.ph

1. INTRODUCTION

The smart university concept emerged from the principles of smart cities, applying them to university operations. It envisions a university as a platform that provides fundamental contextual data to shape the future of higher education [1]–[3]. In 2020, the COVID-19 pandemic forced organizations, including the academic sector, to pivot to a remote workforce. Universities had to switch to flexible learning, and the internet became the primary means of communication. The education and research sector has been severely impacted, experiencing an average of 2,454 attacks per organization each week, making it the most targeted industry [4], [5]. On the other hand, most of the universities have only implemented the defense-in-depth (DID) security model as a primary security defense mechanism [6]. This model serves as the foundation for protecting a campus network system [7]–[10]; however, this technique does not meet the demands of the dynamic and complex network environment [11]. Universities need to implement a security model that can effectively defend against complex and evolving threats [12].

The Philippines faces significant cybersecurity challenges, making it highly susceptible to cyberattacks. Recent trends show that ransomware attacks are on the rise in the Philippines, with finance, government, healthcare, education, and retail being the most common targets [13]. However, during the COVID-19 pandemic, the Commission on Higher Education (CHED) smart campus development project rolled out and provided grants of a maximum of PhP25 million each to State Universities and Colleges (SUCs). The grant priority areas are the campus area network, learning management system, and learners'

information system to support the operation of state colleges and universities during the pandemic. However, cybersecurity is missing in the priority list, despite many reports indicating that cyberattacks have increased by 500% since the pandemic [14], [15].

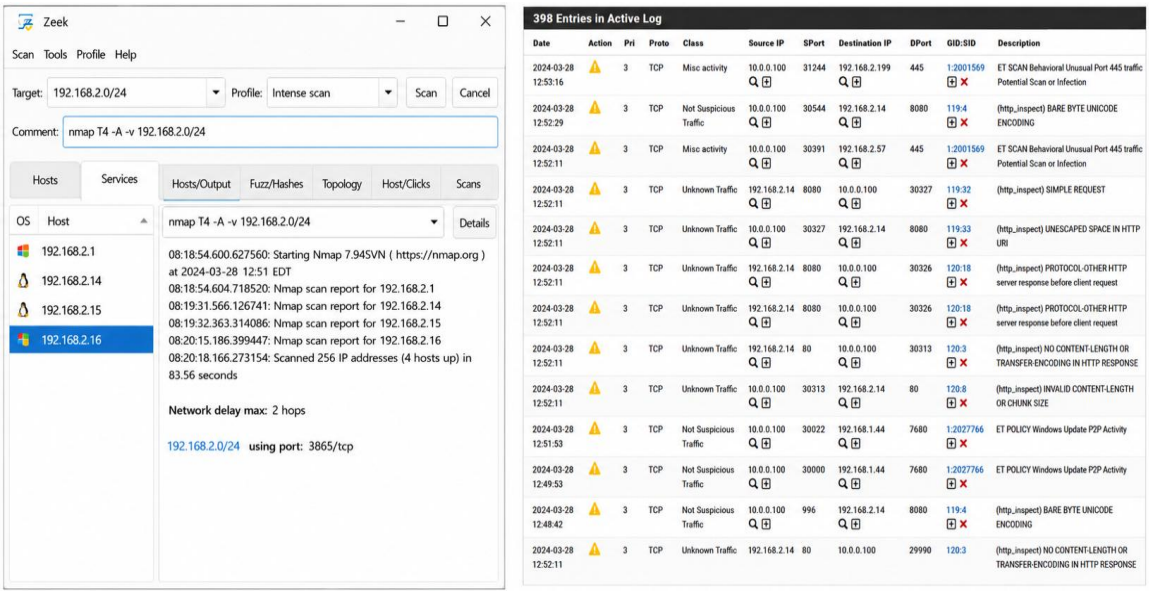
No security measure can prevent all attacks from occurring on a network. To protect the smart campus infrastructure, researchers designed and implemented a deception-driven security model (D-DSM) to address the issues and challenges in establishing and adopting a smart university network infrastructure. The proposed model enhances deception-driven strategies by implementing centralized management and expanding coverage of campus network threats. It utilizes deception technologies to reveal attacker behaviors beyond perimeter defenses, facilitating reliable detection of malicious activities. In addition, the study includes anomaly detection and correlation analysis which addresses credential-based attack data to spot unusual login patterns, while Pearson correlation analysis, which identifies relationships among attack vectors, improving alert interpretation and minimizing false positives. The study demonstrates that deception serves as an early warning system for malicious activities, decreases unnoticed intrusions, and mitigates the impact of attacks. The model proposed is foundational for universities aiming to enhance cybersecurity in future smart campus initiatives.

2. SECURITY GAP OF TRADITIONAL CAMPUS NETWORK DESIGN

Typically, the traditional campus network follows the principles of the hierarchical design model, breaking the network into modular groups or layers. Breaking the design into layers allows each layer to perform specific functions, simplifying both network design and the deployment and management of the network [16]–[18]. Based on the number of end users or network elements (including routers, switches, wireless access controllers (ACs), access points (APs), and other devices), campus networks can be classified as small, medium, or large [19], [20].

2.1. Security test of traditional campus network security

The baseline security configuration places firewall inspection at the network boundary, supported by IDS/IPS and application-level protection mechanisms as part of the DID framework. However, antivirus software is usually deployed on endpoint devices for additional security measures [21]. The researchers tested the DID network security model by launching a reconnaissance attack tool to map the network subnet and observe how the security model reacts to the aforementioned attacks. As a result, Figures 1(a) and (b) shows the attacker can see the entire network subnet as revealed by the Nmap scan. In that case, the attacker can potentially perform several malicious actions, such as exploit services, move laterally across systems, disrupt network functionality, and potentially steal sensitive data.



(a) (b)

Figure 1. Network scanning and fingerprinting Nmap; (a) Nmap logs and (b) firewall logs test results of DID model

Moreover, the captured alert logs of the IDS provide a false positive and false negative state. A false positive result is an incorrect identification of a threat or vulnerability by a system or tool. This means that the system has detected something that is not actually a potential threat or vulnerability and has taken unnecessary action. However, a false negative result is a failure to identify a threat or vulnerability by a system or tool. This means that the system has missed a potential threat or vulnerability and has taken no action to mitigate or eliminate it. This type of result can be dangerous, as it can allow threats and vulnerabilities. Also, the results signify that the attacker gives a clear view of the target network and can easily determine who the victim is based on the successful reconnaissance phase and perform the chosen attack in the next phase [22], [23].

3. DECEPTION-DRIVEN SECURITY MODEL

The main component of our enhanced model adopts the core design of DID and adds another layer of defense through deception techniques. The DID approach involves implementing multiple layers of security controls to protect against threats and to mitigate the impact of security breaches [24].

On the other hand, the deception console was placed within the core of the distribution layer and firewall layer of the DID model to add more comprehensive threat detection and protection. The deception console provides a centralized platform for deploying, managing, and configuring multiple interactive decoys, such as multiple fake servers (FS), across the campus network [22], [25]. The decoys can strategically place on virtual local area networks (VLANs) (access layer) to simulate various network assets and the lure attackers [26]. When an attacker interacts with a decoy, the system generates an alert, indicating potential malicious activity. In addition, it can be deployed on both server and client VLANs to detect a wide range of attacks, from server-side vulnerabilities to client-side exploits like responder/link-local multicast name resolution (LLMNR) attacks. They were utilized to capture the attackers in case the firewall layer failed to protect against their attack methods. As a result, decoys served as the last line of defense, luring and capturing the attacker's activities instead of allowing them to directly target legitimate registered servers (RS). The D-DSM can read logs from network subnets, allowing organizations to hunt across all network and host logs simultaneously. This enhancement helps organizations augment traditional security measures and better defend against sophisticated and persistent threats. These techniques can identify attackers early in the attack lifecycle and disrupt their activities before they cause significant damage.

4. RESULTS AND DISCUSSION

This section presents the results of deploying the D-DSM in the campus area network. The findings show that D-DSM improves resilience, reduces false alerts, and strengthens smart university security.

4.1. Experimental setup and data analysis

To conduct the security test of the proposed model, the researchers established a network testbed at the host university. The logical diagram of the enhanced DID through the D-DSM network architecture, shown in Figure 2, was deployed in the research subnet of the university's network. The analysis follows a streamlined workflow as network traffic interacting with the deception layer generates logs that are collected and analyzed using combined anomaly detection and correlation analysis to produce validated alerts.

Traffic → Deception Layer → Logs → Anomaly and Correlation Analysis → Validated Alerts

The researchers employed a two-way deception security test. The first test was performed at the egress layer, where all incoming packets were redirected to the DMZ, where the honeypot sensor is located. This layer allows all the incoming traffic to be redirected to the trap, thereby deceiving the adversary and collecting logs to identify the attacker's attack pattern and methods. The captured data was used for data analysis.

The second test was conducted in the LAN of the deception layer. The initial security test involved performing network scanning and fingerprinting analysis by comparing the results of the abovementioned security test conducted on the traditional DID security model versus the D-DSM. Several data analysis tools, such as anomaly detection analysis, Pearson's correlation coefficient analysis [27], and comparison of false positives and false negatives between the two models, were performed in order to determine which model is more reliable in terms of reducing false positives and false negatives.

4.2. Network scanning and fingerprinting analysis of deception-driven security model

Figure 3 shows what the attacker(s) saw after the reconnaissance attack in the D-DSM. If the attacker bypasses the security of the DID, they will see several devices or servers without realizing that they

are decoys. The attackers become confused and are unsure which device is the real server, spending additional time investigating these server decoys, believing they are real. This technique can frustrate attackers by slowing down their reconnaissance attack and causing them to make mistakes when selecting exploits based on incorrect OS information, open ports, or network services. The results also show false device signatures designed to mislead attackers. By mixing real devices with decoy systems, deception makes it more difficult for attackers to distinguish between actual critical systems and bait. If the attacker decides to engage with the trap, it exposes their methods and triggers an alarm to notify the network administrator. Additionally, this technique serves to protect real assets by diverting attacks away from critical assets such as university servers and causing confusion during the attacker's reconnaissance process.

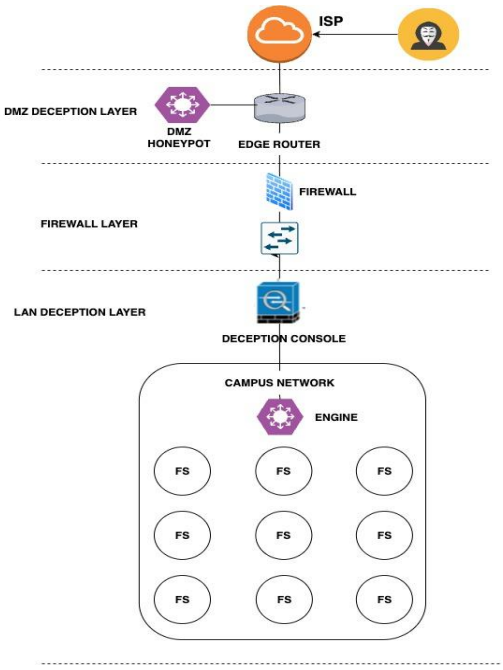


Figure 2. Enhanced DID through D-DSM network

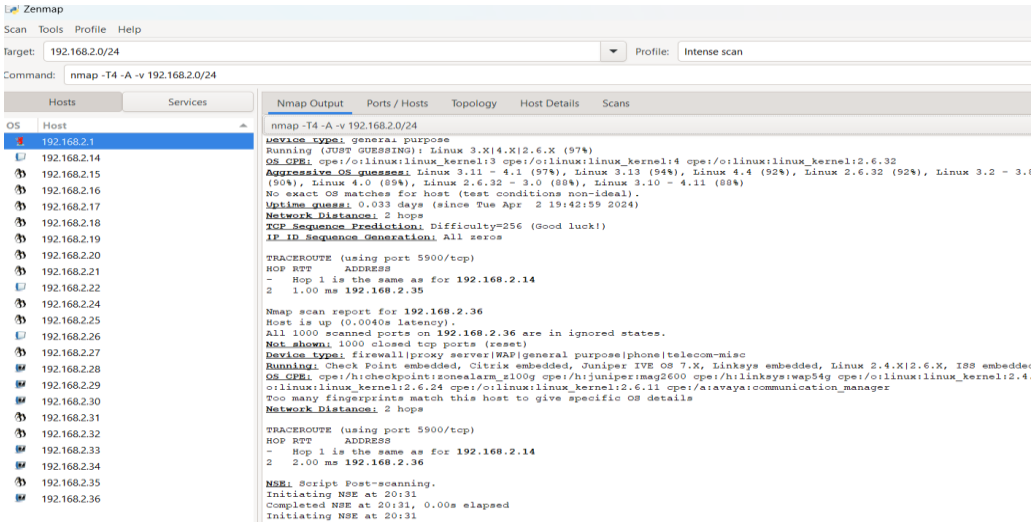
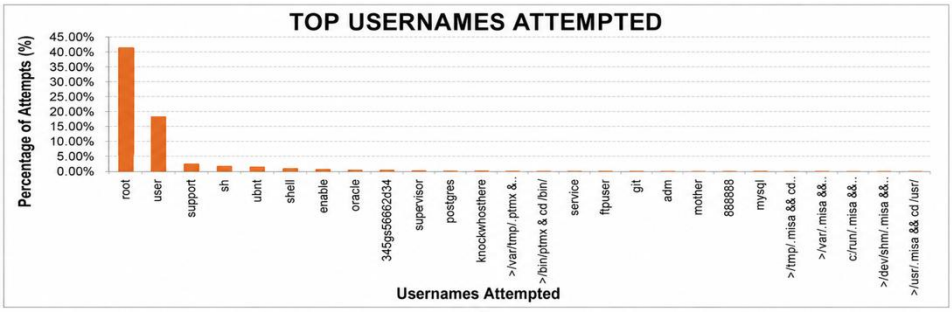


Figure 3. Network scanning and fingerprinting results of D-DSM

4.3. Anomaly detection analysis

This section describes the results of the anomaly detection analysis. Figures 4(a) and (b) present data on the most commonly attempted usernames and passwords during the login attempts. These results indicate

that attackers use methods such as brute-force or botnets. The username “root” dominates as it shown in Figure 4(a), representing over 40% of the login attempts. This means that adversaries primarily target systems with root-level administrative access. The second most attempted username is “user, accounting for just over 15%, while others such as “support,””sh,””ubnt,” and “oracle” have a lower percentage. Other usernames associated with the specific services, such as “postgres” and ftpuser”, may appear to path injection, further indicating attempts to exploit system vulnerabilities. On the other hand, the password “admin” is the most attempted password as shown in Figure 4(b), amounting over 12% of all attempts. Following “admin” and other attempted passwords such as “root,” “support,” and “ubnt,” are much less frequent and accounting for less than 2%. Moreover, other passwords such as > /tmp/.ptmx && cd /tmp/ and simple numeric sequences like "12345678" or "888888 are more likely a command injection, are also among the top attempted passwords. Indicating both common and sophisticated password-cracking attempts.



(a)

(b)

Figure 4. Anomaly detection; (a) usernames attempted and (b) passwords attempted

The anomaly detection model is applied [28], [29] to interpret the dataset as shown in Figures 4(a) and (b). Several username and password combinations stand out as anomalies based on their combined attempts and percent scores. Such anomalies could indicate common attack vectors or highly targeted username/password pairs, often exploited by botnets or brute-force attacks. Figure 5 shows the scatter plot that visualizes the anomalies in the combined username and password dataset. The blue points in the graph represent normal activity and the red points highlight the detected anomalies. The anomalies identified are likely to be highly targeted in brute-force attacks or automated scripts. These combinations are often used as default credentials in many devices, particularly internet of things (IoT) devices, routers, and other network equipment. The presence of such anomalies could indicate that these combinations are being exploited by botnets like Mirai, which scans the internet for devices using default or weak credentials.

4.4. Attack vectors correlation matrix and heatmap analysis

The Pearson's correlation coefficient [30] was utilized to measures the linear relationship between two variables [31]. The correlation matrix and heatmap as shown in Table 1 and Figure 6, explains how different types of attack behaviors are related to one another based on their frequency over time. Correlation values range from -1 to 1. 1: a perfect positive correlation, meaning when one attack vector increases, the other increases in the same proportion. 0: no correlation, indicating the two attack vectors are independent of each other, and -1: a perfect negative correlation, meaning when one attack vector increases, the other decreases. The high correlations between Scanning Port 443 and APACHED WEB SCANNER (0.999965), Scanning Port 80 and APACHE WEB SCANNER (0.904319), and Scanning Port 443 and Scanning Port 80 (0.904273) depicts that activity on these ports and the APACHE WEB SCANNER are closely related and tend to occur simultaneously. The moderate positive correlations between botnet activity and other attack vectors like Port 22 scanning and BRUTEFORCE attacks indicates that botnet activities are relatively independent against other types of attacks. Botnet operations might be focused on maintaining control over

infected machines or launching distributed attacks rather than engaging in the initial reconnaissance or exploitation seen with other vectors. Botnets, such as Mirai, often focus on exploiting weak devices across a variety of ports and services, but their activity is not strongly linked to SSH-specific attacks. This could imply that the botnet's targets are spread across different protocols or that the scanning phase of SSH targets does not necessarily coincide with botnet operations. Moreover, weak correlations between BRUTEFORCE and Scanning Port 80 (0.007602), Scanning Port 443 (0.018484), APACHE WEB SCANNER (0.019309), and Scanning Port 22 (0.035206) depicts minimal to no relationship between these attack vectors, indicating that their occurrences are likely independent of each other.

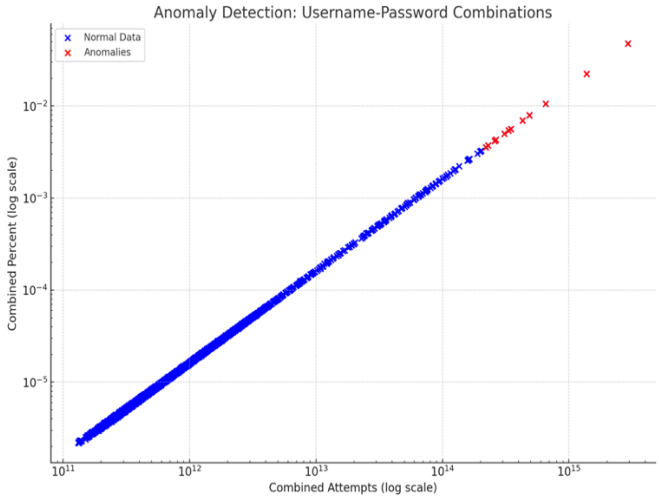


Figure 5. Anomaly detection of username and password combination

Table 1. Correlation matrix of attack vectors

Attack vector	Scanning Port 21	Scanning Port 22	Scanning Port 443	Scanning Port 80	Apache web scanner	Botnet	Bruteforce
Scanning Port 21	1.000000	-0.102206	-0.251962	-0.186107	-0.252745	-0.087422	-0.059622
Scanning Port 22	-0.102206	1.000000	0.176507	0.216295	0.178213	-0.032371	0.035206
Scanning Port 443	-0.251962	0.176507	1.000000	0.904273	0.999965	0.331109	0.018484
Scanning Port 80	-0.186107	0.216295	0.904273	1.000000	0.904319	0.233231	0.007602
Apache web scanner	-0.252745	0.178213	0.999965	0.904319	1.000000	0.329794	0.019309
Botnet	-0.087422	0.032371	0.331109	0.233231	0.329794	1.000000	0.082592
Bruteforce	-0.059622	0.035206	0.018484	0.007602	0.019309	0.082592	1.000000

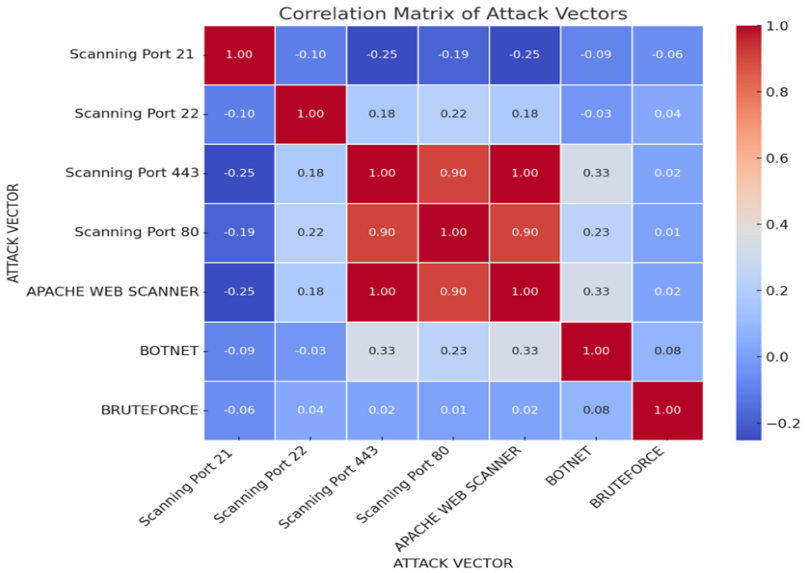


Figure 6. Attack vectors correlation heatmap

4.5. Comparison of false positives and false positives of two models

The comparison between the datasets were focused on minimizing false positives and false negatives which influence accuracy was also employed in this study [32]–[36]. The analysis shown in Figure 7, that the deception dataset appeared to have more reliable alerts compared to the DID dataset. The DID dataset had 290 false positives, mostly triggered by benign HTTP traffic inspections (e.g., HTTP server responses without a client request). These alerts were not associated with actual attacks or malicious behavior.

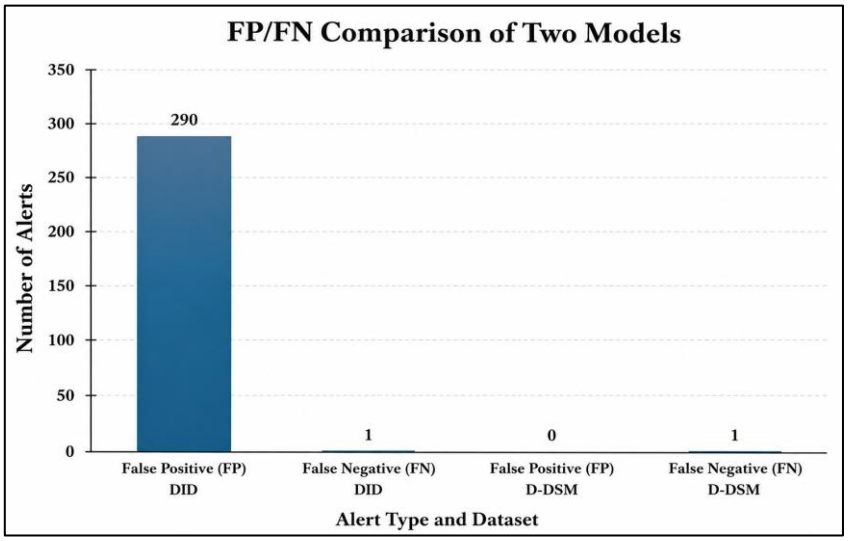


Figure 7. FP/FN comparison of two models

The deception dataset had 0 false positives, indicating that all the events recorded in this dataset were genuine and related to actual network activity or potential threats. Both datasets experienced 1 false negative related to an ICMP ping event that was missed by the DID alert system, meaning a legitimate attack was not flagged. However, the deception dataset is more reliable than the DID dataset due to having no false positives and only one false negative, while DID generate 290 false positives, leading to unnecessary alerts and reduced effectiveness in detecting real threats. The D-DSM dataset demonstrates higher accuracy than the DID dataset, as it eliminated false positives while maintaining the same false negative rate, thereby improving alert precision and reducing alert fatigue.

5. CONCLUSION

The study demonstrates that integrating the deception model within a DID architecture enhances network resilience in a smart university. The D-DSM adds layers of protection by attracting attackers to interact with decoys, gathering critical intelligence while minimizing damage. The model reduces false positives and false negatives and offers important information about attacker behavior. Anomalies in login attempts and attack patterns were identified, and correlation analyses showed significant relationships between attack vectors. Unlike zero-trust and blockchain-based frameworks that emphasize access control and data integrity, the proposed model focuses on network-level attack detection through deception. The findings emphasize the importance of proactive measures like deception techniques in strengthening cybersecurity for smart universities. This study was based on a simulated campus network, indicating a need for further validation to confirm scalability in diverse university environments. Future research may enhance the model using AI for security management to detect and analyze threat anomalies.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to Central Luzon State University for providing the funding and resources necessary to complete this study.

FUNDING INFORMATION

This research was funded by the Central Luzon State University through the Deception-Driven Security Project.

AUTHORS CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Marlon A. Naagas	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anazel P. Gamilla	✓	✓		✓		✓	✓	✓		✓				
Mary Camille D. Rabang		✓	✓	✓	✓		✓	✓		✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data supporting this study are available from the corresponding author upon request but are not publicly shared due to privacy restrictions.

REFERENCES

[1] CommScope, "Smart Campus Security." [Online]. Available: https://www.commscope.com/globalassets/digizuite/62438-sb-smartcampus-security-co-113893-en.pdf. (Accessed: Sep. 25, 2024).

[2] M. C. F. Raguro, A. C. Lagman, and R. Juanatas, "Technology Management Framework for Smart University System in the Philippines," in *2021 The 9th International Conference on Information Technology: IoT and Smart City*, Dec. 2021, pp. 372–380, doi: 10.1145/3512576.3512642.

[3] G. Suster, C. A. Popescu, T. Iancu, G. Popescu, and R. Ciolac, "The Synergy of Smart Campus Development with Smart City Policies and the New European Bauhaus with Implications for Educational Efficiency," *Sustainability*, vol. 17, no. 17, p. 8078, Sep. 2025, doi: 10.3390/su17178078.

[4] C. P. Research, "Check Point Research warns every day is a school day for cybercriminals with the education sector as the top target in 2024," 2024. [Online]. Available: https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/. (Accessed: Sep. 25, 2024).

[5] T. Favale, F. Soro, M. Trevisan, I. Drago, and M. Mellia, "Campus traffic and e-Learning during COVID-19 pandemic," *Computer Networks*, vol. 176, p. 107290, Jul. 2020, doi: 10.1016/j.comnet.2020.107290.

[6] L. Zhang and V. L. L. Thing, "Three decades of deception techniques in active cyber defense - Retrospect and outlook," *Computers & Security*, vol. 106, p. 102288, Apr. 2021, doi: 10.1016/j.cose.2021.102288.

[7] L. Zhang and W. Song, "Research on Intrusion Detection Algorithm Based on Smart Campus Network Security," in *Proceedings of the 2020 International Conference on Aviation Safety and Information Technology*, Oct. 2020, pp. 446–449, doi: 10.1145/3434581.3434627.

[8] L. Huang, "Research on Campus Network Security Management Technology Based on Big Data," in *2019 International Conference on Smart Grid and Electrical Automation (ICSGEA)*, Aug. 2019, pp. 571–575, doi: 10.1109/ICSGEA.2019.00133.

[9] J. Lu, "Research and Implementation of Security Technology in Campus Network Construction," in *2019 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, Sep. 2019, pp. 219–224, doi: 10.1109/ICCNEA.2019.00050.

[10] M. Huang, W. Luo, and X. Wan, "Research on Network Security of Campus Network," *Journal of Physics: Conference Series*, vol. 1187, no. 4, p. 042113, Apr. 2019, doi: 10.1088/1742-6596/1187/4/042113.

[11] S. K. Jangam and P. S. R. P. Muntala, "Comprehensive defense-in-depth strategy for enterprise application security," *International Journal of Multidisciplinary on Science and Management*, vol. 1, no. 3, pp. 62–75, Sep. 2024, doi: 10.71141/30485037/V1I3P106.

[12] M. L. Flores, "IT Security Management Challenges of State Universities and Colleges," *Cognizance Journal of Multidisciplinary Studies*, vol. 4, no. 9, pp. 18–37, Sep. 2024, doi: 10.47760/cognizance.2024.v04i09.003.

[13] CYFIRMA, "Philippines threat overview," CYFIRMA Research, 2024. [Online]. Available: https://www.cyfirma.com/research/philippines-threat-overview/. (Accessed: Sep. 25, 2024).

[14] A. M. Al Shabibi and M. N. Al-Suqri, "Cybersecurity Awareness Among Students During the COVID-19 Digital Transformation

of Education: A Case Study at the Muscat (Oman) Schools," in *Future Trends in Education Post COVID-19*, Singapore: Springer Nature Singapore, 2023, pp. 39–51, doi: 10.1007/978-981-99-1927-7_4.
[15] A.-L. Enterprise, "Smart campus security," White Paper, 2024. [Online]. Available: https://www.al-enterprise.com/-/media/assets/internet/documents/smart-campus-security-white-paper-en.pdf. (Accessed: Sep. 25, 2024).
[16] B. Sánchez-Torres, J. A. Rodríguez-Rodríguez, D. W. Rico-Bautista, and C. D. Guerrero, "Smart Campus: Trends in cybersecurity and future development," *Revista Facultad de Ingeniería*, vol. 27, no. 47, pp. 104–112, Jan. 2018, doi: 10.19053/01211129.v27.n47.2018.7807.
[17] Y. Zhang, "Research of Campus Network Information Security," in *Proceedings of the 2018 8th International Conference on Mechatronics, Computer and Education Informationization (MCEI 2018)*, 2018, pp. 198–201, doi: 10.2991/mcei-18.2018.38.
[18] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.
[19] L. Huawei Technologies Co., "Typical Networking Architectures for Campus Networks and Case Practice," in *Data Communications and Network Technologies*, Singapore: Springer Nature Singapore, 2023, pp. 471–500, doi: 10.1007/978-981-19-3029-4_15.
[20] R. Alexander, "Using Linear Regression Analysis and Defense in Depth to Protect Networks during the Global Corona Pandemic," *Journal of Information Security*, vol. 11, no. 04, pp. 261–291, 2020, doi: 10.4236/jis.2020.114017.
[21] X. Qin, F. Jiang, C. Dong, and R. Doss, "A hybrid cyber defense framework for reconnaissance attack in industrial control systems," *Computers & Security*, vol. 136, p. 103506, Jan. 2024, doi: 10.1016/j.cose.2023.103506.
[22] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, and Ata-ur-rehman, "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, Jan. 2019, pp. 1–6, doi: 10.1109/ICOMET.2019.8673520.
[23] A. P. Gamilla, T. D. Palaoag, and M. A. Naagas, "Enhancing reconnaissance security: a 2-tier deception-driven model approach (2TDDSM)," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 3, p. 1999, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1999-2006.
[24] K. Neupane, R. Haddad, and L. Chen, "Next Generation Firewall for Network Security: A Survey," in *SoutheastCon 2018*, Apr. 2018, pp. 1–6, doi: 10.1109/SECON.2018.8478973.
[25] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Computers & Security*, vol. 140, p. 103792, May 2024, doi: 10.1016/j.cose.2024.103792.
[26] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Computing Surveys*, vol. 52, no. 4, pp. 1–28, Aug. 2019, doi: 10.1145/3337772.
[27] P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K. K. R. Choo, and H. H. S. Javadi, "Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 865–889, 2019, doi: 10.3745/JIPS.03.0126.
[28] E. Muhati and D. Rawat, "Data-Driven Network Anomaly Detection with Cyber Attack and Defense Visualization," *Journal of Cybersecurity and Privacy*, vol. 4, no. 2, pp. 241–263, Apr. 2024, doi: 10.3390/jcp4020012.
[29] Z. Yang *et al.*, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," *Computers & Security*, vol. 116, p. 102675, May 2022, doi: 10.1016/j.cose.2022.102675.
[30] P. Chen, F. Li, and C. Wu, "Research on Intrusion Detection Method Based on Pearson Correlation Coefficient Feature Selection Algorithm," *Journal of Physics: Conference Series*, vol. 1757, no. 1, p. 012054, Jan. 2021, doi: 10.1088/1742-6596/1757/1/012054.
[31] J. Li, J. Liu, and R. Zhang, "Advanced Persistent Threat Group Correlation Analysis via Attack Behavior Patterns and Rough Sets," *Electronics*, vol. 13, no. 6, p. 1106, Mar. 2024, doi: 10.3390/electronics13061106.
[32] M. Abbas-Escribano and H. Debar, "An Improved Honeypot Model for Attack Detection and Analysis," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, Aug. 2023, pp. 1–10, doi: 10.1145/3600160.3604993.
[33] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," in *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, Sep. 2017, pp. 000277–000282, doi: 10.1109/SISY.2017.8080566.
[34] A. A. Ghorbani, W. Lu, and M. Tavallaee, *Network Intrusion Detection and Prevention: Concepts and Techniques*. New York, NY, USA: Springer, 2009.
[35] S. V. N. S. Kumar, M. Selvi, and A. Kannan, "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things," *Computational Intelligence and Neuroscience*, vol. 2023, Jan. 2023, doi: 10.1155/2023/8981988.
[36] A. H. Ali, M. Charfeddine, B. Ammar, B. B. Hamed, F. Albalwy, A. Alqarafi, and A. Hussain, "Unveiling machine learning strategies and considerations in intrusion detection systems: a comprehensive survey," *Frontiers in Computer Science*, vol. 6, Jun. 2024, doi: 10.3389/fcomp.2024.1387354.

BIOGRAPHIES OF AUTHORS

Dr. Marlon A. Naagas holds a Doctorate degree in Information Technology (DIT) from the University of the Cordilleras (UC-BCF), Philippines. A Professor at Department of Information Technology, College of Engineering, and Dean of Admissions at Central Luzon State University (CLSU). He is a CISCO Cyber Security Scholarship Awardee, passed CCNA – CyberOps and CCCA. His current research interests include computer networks, cyber security, ethical hacking, and has four research publications in the said field. He can be contacted at email: manaagas@clsu.edu.ph.

Dr. Anazel P. Gamilla holds a Doctorate degree in Information Technology (DIT) from the University of the Cordilleras (UC-BCF), Philippines. An Assistant Professor of the Department of Information Technology, College of Engineering, and the Chief of Network, Cybersecurity, and Technical Support Division (NCTSD) under the Management Information Systems Office at Central Luzon State University (CLSU). She is also a trainer for the Department of Information Technology and Communications Technology (DICT-ILCDB). She can be contacted at email: apgamilla@clsu.edu.ph.

Mary Camille D. Rabang holds a Bachelor degree in Information Technology (BSIT), an Instructor of the Department of Information Technology, College of Engineering, at Central Luzon State University. Her current research interests include information systems, software design, data management systems and R&D, and it has one research publications in the said field. She can be contacted at email: camillerabang@clsu.edu.ph.