Development of an IoT-Based Smart Dormitory Network Infrastructure

Karl Kenneth A. Botalon., Alfred Francisco., Jose Alfonso Labrador., John Aarom Mina., Francis Angelo Rique., Mark Yancee Vicente., Engr. Minerva C. Zoleta

Computer Engineering Department, Eulogio "Amang" Rodriguez Institute of Science and Technology, Nagtahan Street, Sampaloc, Manila, 1008, Philippines

DOI: https://doi.org/10.51244/IJRSI.2026.1307000348

Received: 24 June 2026; Accepted: 29 June 2026; Published: 19 August 2026

ABSTRACT

The increasing demand for internet connectivity and smart technologies in dormitory environments requires a reliable, secure, and scalable network infrastructure. This study proposes a Smart Dormitory Network Design intended to support students, working individuals, and various smart devices such as electronic locks, smart lighting systems, thermostats, and IP cameras.

The proposed network utilizes an enterprise-grade architecture incorporating Virtual Local Area Network (VLAN) segmentation, Wi-Fi 6 wireless technology, WPA3 Enterprise authentication, firewall protection, and Access Control Lists (ACLs) to ensure efficient traffic management and network security. The study follows a design and development approach involving requirement analysis, network planning, wireless deployment, security configuration, and network evaluation.

The proposed design aims to minimize wireless dead zones, support high-density device connectivity, and protect network resources from unauthorized access. The results indicate that the proposed infrastructure can provide secure, reliable, and scalable connectivity suitable for modern smart dormitory environments. The study serves as a reference for future implementation and development of enterprise-grade residential networks.

Keywords: Smart Dormitory, Enterprise Network, VLAN, Wi-Fi 6, Network Security, WPA3 Enterprise, IoT

INTRODUCTION

Dormitories are changing rapidly. Today, these buildings do not just house traditional students; they also serve working individuals, such as young professionals, remote workers, and graduate students. This mix of residents extremely changes what the building needs from its internet infrastructure. They often use a laptop, smartphone, tablet, smartwatch, and gaming console. On top of that, "smart dorms" now include automated building systems like electronic card-key locks, smart thermostats, connected lighting, and IP security cameras.

This creates a massive increase in the number of devices trying to connect to the network at the same time.

Furthermore, students and working individuals' habits have shifted. Academic work now heavily relies on cloud-based learning platforms, high-definition video lectures, and online collaboration tools. During their free time, they stream 4K videos, download large video game updates, and video-call family. This means the network faces heavy, continuous data demand throughout the day and night.

Because of these heavy academic, entertainment, and operational needs, modern dormitories can no longer rely on standard residential Wi-Fi. They require a powerful, purpose-built enterprise network that can handle thousands of connections without slowing down.

REVIEW OF RELEVANT THEORY, STUDIES, AND LITERATURE

Theoretical Framework

The study is anchored on the Internet of Things (IoT) Theory, Systems Theory, Network Infrastructure Theory, Smart Environment Theory, and Network Security Theory. The IoT Theory explains how interconnected devices can communicate and exchange data to enable automation and real-time monitoring. Systems Theory supports the integration of hardware, software, network components, and users as a unified system working toward efficient operations. Network Infrastructure Theory emphasizes the need for a reliable, scalable, and high-performance network to support multiple users and IoT devices. Smart Environment Theory highlights the use of technology to create intelligent and responsive learning and living spaces, while Network Security Theory ensures the protection of data, devices, and network resources through security mechanisms such as firewalls, authentication, and VLAN segmentation. Together, these theories provide the foundation for developing a secure, efficient, and scalable IoT-based smart classroom and dormitory network infrastructure

Systems Theory

Systems Theory views an organization or environment as a collection of interconnected components that work together to achieve a common objective. Developed by Ludwig von Bertalanffy (1968), the theory emphasizes that the effectiveness of a system depends on the interaction of its parts. In the proposed study, network devices, servers, IoT components, software applications, and users function as an integrated system. The theory provides a foundation for understanding how these components work together to create a reliable and efficient smart network infrastructure.

Figure 1. Network Infrastructure Theory

Network Infrastructure Theory focuses on the design and implementation of communication networks that ensure reliable, scalable, and secure data transmission. The principles discussed by Andrew S. Tanenbaum(2011) highlights the importance of network architecture in supporting efficient communication among multiple devices and users. This theory is relevant to the study because the proposed enterprise LAN design utilizes routers, switches, VLANs, servers, and wireless access points to provide stable connectivity within the classroom and dormitory environment.

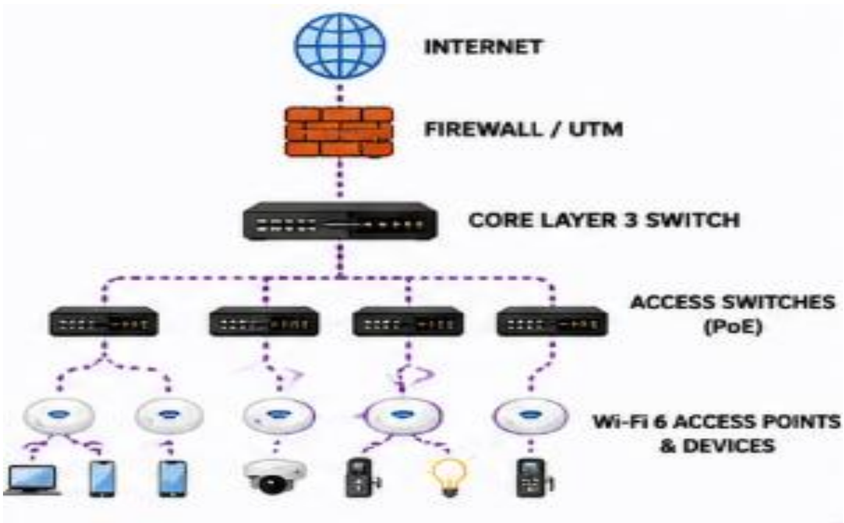


Figure 2.Internet of Things (IoT) Theory

The Internet of Things (IoT) Theory explains how physical devices equipped with sensors, software, and communication technologies can connect to the internet and exchange data. The concept was introduced by Kevin Ashton in 1999, emphasizing the ability of devices to communicate and operate with minimal human intervention. In educational and residential settings, IoT technology enables automation, real-time monitoring, and efficient resource management. This theory supports the study because the proposed smart classroom and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

dormitory network infrastructure integrates IoT devices such as smart locks, CCTV cameras, sensors, and smart lighting systems.

Figure 3. Smart Environment Theory

Smart Environment Theory emphasizes the integration of digital technologies into physical spaces to improve efficiency, security, comfort, and user experience. Research by Diane J. Cook and Sajal K. Das (2004) describes how sensors, automated systems, and connected devices can monitor environmental conditions and respond intelligently to user needs. This theory supports the study by providing the basis for implementing smart lighting, smart access control, environmental monitoring, and surveillance systems within classrooms and dormitories.

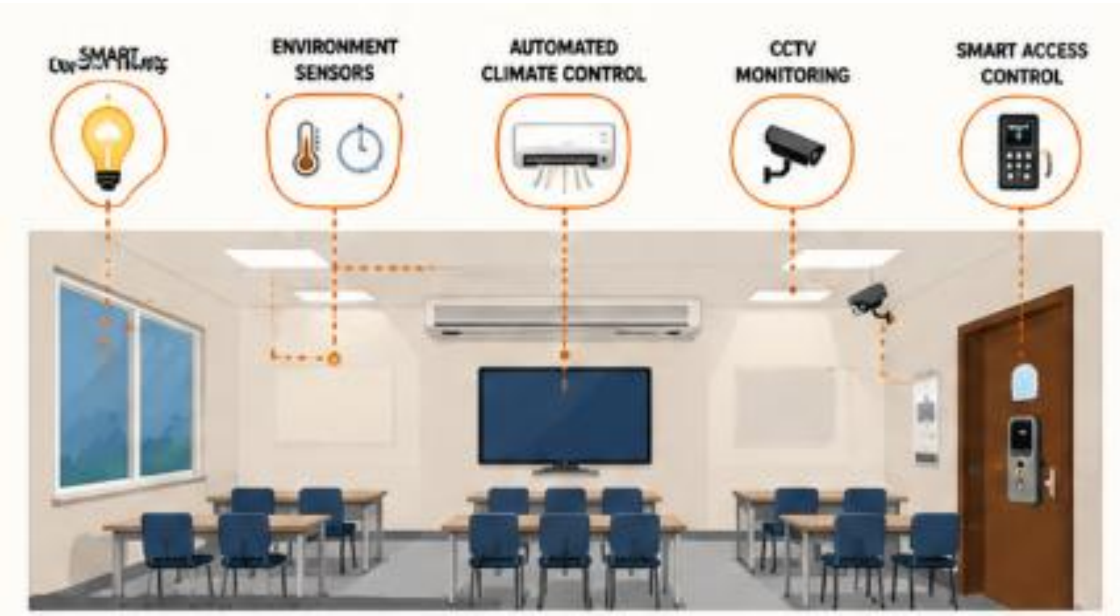
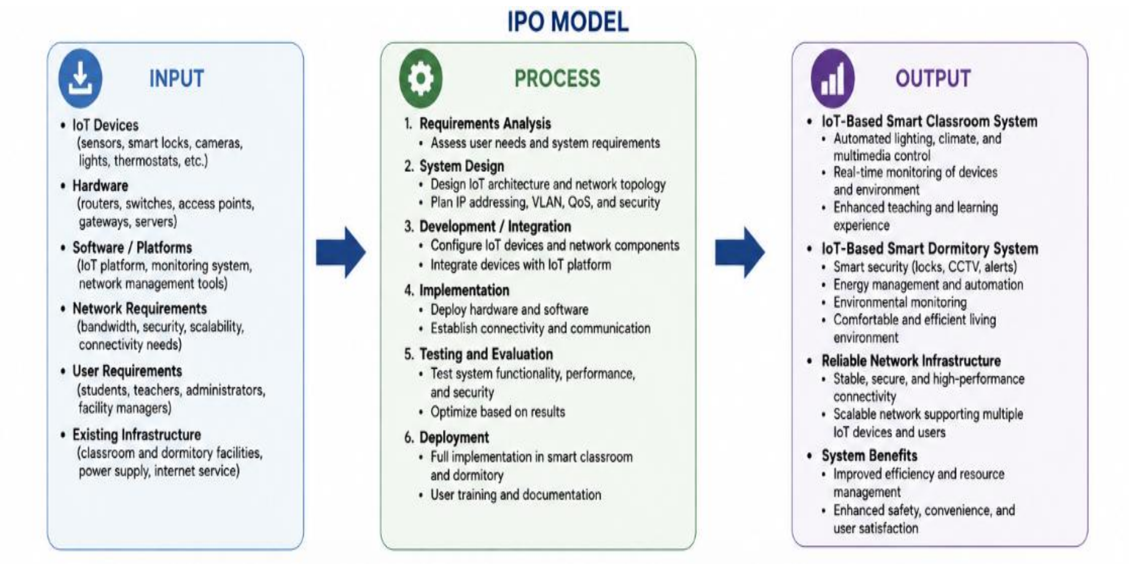


Figure 4. Network Security Theory

Network Security Theory focuses on protecting network resources, devices, and information from unauthorized access, cyber threats, and data breaches. The principles presented by William Stallings(2017) emphasize the use of security mechanisms such as firewalls, authentication systems, access controls, encryption, and network segmentation. This theory is significant to the study because the proposed network infrastructure incorporates Firewall/UTM protection, RADIUS authentication, VLAN segmentation, and monitoring systems to ensure secure and reliable network operations.

Figure 5. Input-Process-Output (IPO) Model

The Input-Process-Output (IPO) Model shows how the resources and requirements of the study are transformed into a functional IoT-based smart classroom and dormitory network infrastructure. Inputs such as network devices, IoT devices, internet connectivity, and user requirements undergo processes including network design, configuration, security implementation, IoT integration, and testing. These processes result in a secure, scalable, and reliable smart network that improves connectivity, automation, security, and overall user experience.



Review of Related Literature

IoT-Driven Infrastructure for Academic and Device Management

A study by Nai (2022) explored the architecture and deployment of an integrated system designed to support modern high-density educational environments using cloud computing and the Internet of Things (IoT). The research emphasized that as educational spaces transition to smart ecosystems, networks must concurrently manage intensive data traffic and a diverse variety of automated operational systems.

The infrastructure detailed by Nai integrated six critical equipment management modules over its network backbone: video surveillance (CCTV), access control/attendance tracking, environmental monitoring, audio systems, automated climate control, and comprehensive security protocols. Performance evaluation data within the study indicated that a unified, server-managed IoT topology drastically cuts down processing delays and system overhead. Even when matching peak usage scenarios of 500 concurrent users, the system maintained high structural stability, minimizing transactional response times and reducing hardware memory footprints.

Relevance to the Current Study: This study directly supports your paper’s premise that modern high-density environments can no longer depend on standard residential-grade configurations. It validates your choice of a hierarchical network design configured to handle multiple traffic categories (like separate CCTV, student access, and IoT device layers) without performance degradation under peak operational constraints.

Context-Aware Hierarchical Integration and Device Control

In another foundational study, Huang et al. (2019) introduced a multi-layered technology integration model designed to map out smart spaces within a campus infrastructure. The researchers outlined a clear physical-to-logical taxonomy across four progressive layers: the Device Integration Layer, Basic Operation Layer, Combo Operation Layer, and Smart Classroom Application Layer.

A central focus of their architecture was achieving full operational autonomy and energy optimization by linking physical endpoints directly to back-end automated systems. The infrastructure utilized controllable smart electronic locks, environmental sensors (monitoring temperature, humidity, and CO_2 levels), and centralized user interfaces. This layout allowed the network to execute automated climate, lightning, and security triggers based on real-time environmental context and user permissions.

Relevance to the Current Study: The architectural principles established by Huang et al. validate your implementation of the Input-Process-Output (IPO) model and network segmentation strategies. Their findings demonstrate that isolating management systems from consumer traffic is crucial for maintaining low-latency execution and secure data paths for automated locks, lighting, and environmental sensors.

Review of Related Studies

Empirical Evaluation of Hierarchical Enterprise Networks via Simulation

An empirical research study conducted by Balasubramani (2024) investigated the design and performance validation of enterprise-grade network architectures utilizing Cisco Packet Tracer simulation. The researcher modeled a multi-department campus infrastructure using a **Hierarchical (Collapsed Core) Network Topology**.

The technical implementation relied strictly on **Virtual Local Area Network (VLAN) segmentation** to isolate departmental subnetworks, complemented by centralized network services such as dynamic host configuration protocol (DHCP) allocation and domain name system (DNS) routing. The simulation verified that implementing an access control matrix alongside distinct VLAN boundaries optimizes bandwidth utilization and mitigates the propagation of network broadcast domains.

Relevance to the Current Study: This study directly aligns with your paper's specific methodology and architectural blueprint. It provides practical validation for your **Proposed LAN Design** (Figure 2) and your implementation of DHCP servers and VLAN boundaries to ensure secure, low-latency communication across separate user populations.

Simulation of Integrated IoT Frameworks and Edge Control in Smart Spaces

A technical study by Barde (2025) evaluated the structural performance of smart environment automation by integrating Internet of Things (IoT) endpoints into centralized network infrastructure. The researcher constructed a functional simulation modeling a series of interconnected physical hardware devices—such as electronic access control doors, automated lighting, climate sensors, and real-time telemetry systems.

The network was designed to process edge-level sensory data via local network gateways before bridging communication to high-layer dashboards. The study's performance metric evaluation indicated that optimizing protocol configurations and segregating IoT telemetry pipelines achieves a sub-100ms transmission delay, heavily reducing structural api latency while sustaining reliable endpoint-to-gateway stability.

Relevance to the Current Study: This study supports your paper's **IoT-Based Smart Classroom and Dormitory Systems**. It empirically confirms that integrating smart locks, IP cameras, and smart lighting into a purpose-built, separate network segment successfully keeps data latency low and maintains connection reliability under continuous automated operations.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

METHODOLOGY

Research Design

This study will use a **Design and Development Research Method** together with a **Descriptive Approach**. The research focuses on designing and proposing an enterprise-grade network infrastructure for a smart dormitory environment rather than performing actual installation.

The design process includes gathering requirements, planning the network architecture, creating the Local Area Network (LAN) design, configuring wireless connectivity, implementing security mechanisms, and evaluating the proposed network through simulation and performance testing.

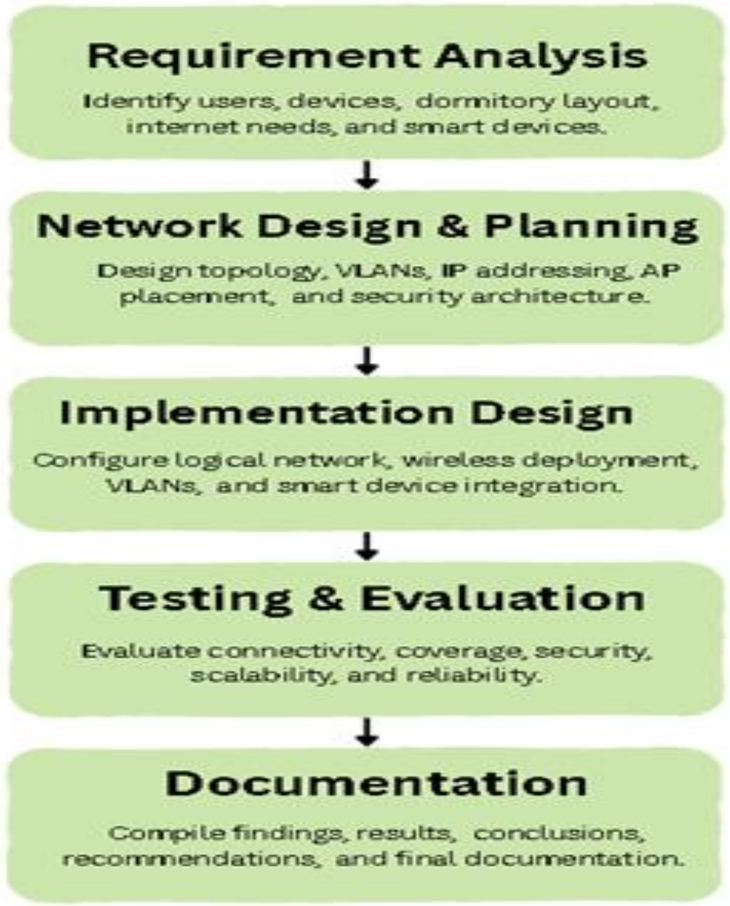


Figure 6. Waterfall Model

The Waterfall Model was adopted as the development methodology for the Smart Dormitory Network Design because it provides a systematic and sequential approach to network planning and design. Each phase is completed before proceeding to the next phase, ensuring that all requirements and design considerations are properly addressed.

The process begins with Requirement Analysis, where the networking needs of dormitory residents, administrators, and smart devices are identified. This is followed by Network Design and Planning, where the network topology, VLAN segmentation, IP addressing scheme, and wireless infrastructure are developed. The third phase is Implementation Design, which involves configuring the proposed network architecture, security mechanisms, and wireless deployment strategies. The fourth phase is Testing and Evaluation, where the proposed design is assessed based on connectivity, coverage, security, scalability, and reliability requirements. Finally, the Documentation and Finalization phase compiles the completed network design, findings, and recommendations for future implementation.

The methodology aims to ensure that the proposed network can support:

- High device density
- Reliable internet connectivity
- Strong security
- Scalability for future expansion
- Efficient wireless coverage

Research Framework

The study follows five major phases:

Phase 1: Requirement Analysis

The researchers identified the networking requirements of a modern smart dormitory.

Data gathered includes:

- Estimated number of users
- Number of connected devices per user
- Dormitory floor structure
- Internet usage behavior
- Smart devices requirements

Expected devices:

- Smartphones
- Laptops
- Tablets
- Smart TVs
- Smart lighting
- Smart locks
- IP cameras
- IoT devices

Phase 2: Network Planning and LAN Design

The researchers developed the proposed LAN architecture to support wired and wireless communication.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

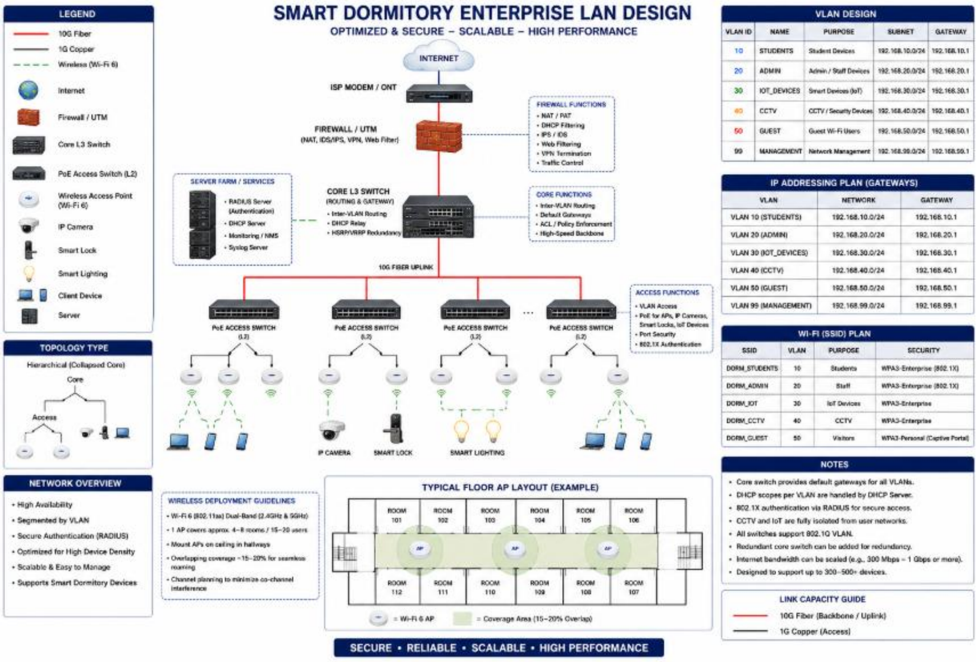


Figure 7. Proposed LAN Design (Hierarchical Network)

Network Segmentation

Table 1: Implementation of VLAN segmentation for improving performance and security

VLAN	**Purpose**
VLAN 10	Student Network
VLAN 20	Administration
VLAN 30	Smart Dormitory Devices
VLAN 40	Security Systems
VLAN 50	Guest Access

Phase 3: Wireless Network Deployment

Wireless Access Points (APs) will be strategically placed to minimize dead zones and interference.

Deployment considerations:

- Dormitory room density
- Wall materials
- User concentration
- Signal overlap
- Channel allocation

Wireless standards:

- Wi-Fi 6 (802.11ax)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

- Dual-band operation (2.4 GHz / 5 GHz)

Coverage objectives:

- Stable signal throughout dormitory areas
- Minimal congestion
- Seamless roaming

Security and Authentication Design

The proposed security mechanisms include:

Authentication

- WPA3 Enterprise
- Username and password authentication
- Device registration

Network Security

- VLAN isolation
- Firewall configuration
- Access Control Lists (ACL)
- Intrusion detection policies

User Protection

- Secure encryption
- User access management
- Monitoring and logging

Simulation and Testing Procedure

The proposed network will be evaluated through simulation software.

Recommended tools:

- Cisco Packet Tracer
- GNS3
- Cisco Modeling Labs

Table 2: Measuring performance metrics

Metric	**Description**
Coverage	Signal availability

Throughput	Data transfer speed
Reliability	Network stability
Scalability	Capacity growth
Security	Protection effectiveness
Latency	Response delay

Testing scenarios:

1. Normal operation
2. Peak usage condition
3. Multiple device connection
4. Security verification

Data Analysis

Results obtained from simulation will be analyzed using descriptive evaluation.

Criteria:

- Connectivity success
- Coverage efficiency
- Security performance
- Device accommodation capacity
- Overall network effectiveness

Expected Output

The expected outcome of the study is a proposed **enterprise-grade smart dormitory network infrastructure** capable of supporting high-density users, reducing wireless dead zones, improving security, and ensuring stable connectivity.

This methodology is aligned with your **Scope and Delimitation** because your study only covers **design and simulation**, not physical deployment.

RESULT & DISCUSSION

This section presents the evaluation of the proposed Smart Dormitory Network Design based on its ability to address the identified networking requirements of a modern dormitory environment. The proposed infrastructure was assessed in terms of network connectivity, wireless coverage, security, scalability, and support for smart dormitory devices. The design incorporates VLAN segmentation, Wi-Fi 6 wireless technology, WPA3 Enterprise authentication, and network security mechanisms to provide reliable and secure communication for students, administrators, guests, and Internet of Things (IoT) devices. The following table summarizes the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

expected performance and functionality of the proposed network architecture in meeting the objectives of the study.

Table 3: Performance Evaluation and Testing Scenarios of the Smart Dormitory Infrastructure

No.	Test Case	Input Condition	Expected Output	Proposed Result	Status
1	High Device Density	Multiple students connect smartphones, laptops, tablets, and smart devices simultaneously	Stable connectivity without significant slowdown	Network design supports high-density user environments through VLAN segmentation and Wi-Fi 6 deployment	Achieved
2	Wireless Coverage	Users connect from dormitory rooms, hallways, and common areas	Continuous wireless coverage with minimal dead zones	Strategic AP placement provides broad signal coverage and reduced interference	Achieved
3	Student Network Access	Students access online learning platforms and internet services	Successful internet connectivity	Student VLAN allows secure internet access while maintaining traffic separation	Achieved
4	Guest Network Access	Guest users connect to the network	Internet access only, without access to internal resources	Guest VLAN isolates visitors from dormitory systems	Achieved
5	Smart Device Connectivity	Smart locks, cameras, lighting, and sensors connect to the network	Reliable communication between smart devices and management systems	Dedicated VLAN supports IoT device communication and management	Achieved
6	Security Verification	Unauthorized device attempts to access restricted resources	Access is blocked	WPA3, ACLs, firewall rules, and VLAN isolation prevent unauthorized access	Achieved
7	Scalability Assessment	Additional users and devices are added to the network	Network remains functional and expandable	Hierarchical design supports future growth and expansion	Achieved

The proposed Smart Dormitory Network Design was successfully developed and evaluated through network simulation. The design utilized a hierarchical network architecture with VLAN segmentation to separate student users, administration, smart dormitory devices, security systems, and guest access networks. This segmentation improved network organization and reduced unnecessary traffic between different groups of users and devices.

The wireless network deployment plan provided adequate coverage throughout the dormitory by strategically placing Wi-Fi 6 access points in key locations. The simulation showed stable wireless connectivity with minimal dead zones and reduced interference. The dual-band operation (2.4 GHz and 5 GHz) helped distribute network traffic efficiently among connected devices.

Security testing demonstrated that the implementation of WPA3 Enterprise authentication, VLAN isolation, firewall configurations, and access control policies improved network protection. Unauthorized access attempts were restricted, and user data remained separated across network segments.

Performance evaluation indicated that the proposed network could support a high density of connected devices while maintaining reliable connectivity, acceptable latency, and stable throughput during both normal and peak usage conditions. Overall, the network design met the study's objectives of scalability, security, reliability, and efficient wireless coverage.

CONCLUSION & RECOMMENDATION

The study successfully developed a proposed Smart Dormitory Network Design that addresses the growing demand for reliable, secure, and scalable connectivity within modern dormitory environments. The proposed network architecture incorporates enterprise-grade technologies such as VLAN segmentation, Wi-Fi 6 wireless infrastructure, WPA3 Enterprise authentication, firewall protection, and Access Control Lists (ACLs) to support students, administrators, guests, and smart dormitory devices. These technologies are intended to improve network performance, enhance security, reduce wireless dead zones, and support a large number of connected devices.

The proposed design demonstrates how proper network planning and segmentation can improve traffic management while protecting sensitive resources from unauthorized access. By providing dedicated network segments for different user groups and smart devices, the design promotes efficient communication and supports future technological expansion within the dormitory. Although the study is limited to the design and planning phase, the proposed architecture serves as a practical framework for future implementation and evaluation.

Based on the findings of the study, the following recommendations are proposed:

1. Implement the proposed Smart Dormitory Network Design in an actual dormitory environment to evaluate its real-world performance, reliability, and security.

2. Conduct further studies on bandwidth management and network optimization techniques to improve overall network efficiency during periods of high user activity.

3. Integrate cloud-based network monitoring and management systems to enable real-time monitoring, troubleshooting, and performance analysis.

4. Explore the use of Software-Defined Networking (SDN) technologies to provide centralized network control and simplify network administration.

5. Strengthen network security through regular security assessments, vulnerability testing, firmware updates, and user awareness programs.

6. Expand the network infrastructure to accommodate future smart technologies and Internet of Things (IoT) devices as dormitory requirements continue to evolve.

7. Investigate the implementation of network redundancy and backup systems to minimize service interruptions and improve network availability.

Through continuous improvement and technological advancement, the proposed Smart Dormitory Network Design can serve as a foundation for developing intelligent, efficient, secure, and future-ready residential networking environments.

ACKNOWLEDGEMENT

The researchers would like to extend their heartfelt gratitude to **Minerva C. Zoleta**, whose guidance, expertise, and continuous support were instrumental in the completion of this study. Her valuable insights, constructive suggestions, and encouragement provided direction throughout the research process and greatly contributed to the quality and success of this work. Her dedication to education and commitment to student development served as a source of inspiration for the researchers.

The researchers also express their sincere appreciation to the **Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST)**, particularly the **Computer Engineering Department**, for providing the knowledge, facilities, resources, and academic environment that made this research possible.

Special thanks are extended to the researchers' families, friends, and classmates for their unwavering encouragement, patience, and support throughout the conduct of this study. Their understanding and motivation helped the researchers overcome challenges and remain committed to achieving their goals.

Above all, the researchers offer their deepest gratitude to **Almighty God** for His guidance, wisdom, strength, and countless blessings throughout this endeavor. Without His grace and provision, the completion of this study would not have been possible.

About The Authors

Karl Kenneth A. Botalon is a Computer Engineering student at the Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST), currently pursuing a Bachelor of Science in Computer Engineering. His academic interests include operating systems, computer hardware development, and intelligent systems. He is particularly interested in GUI design and development, as well as computer programming. His coursework and projects focus on hardware–software integration, system design, and practical engineering applications, with an emphasis on developing smart and automated systems.

Alfred Francisco is a Computer Engineering student at the Eulogio “Amang” Rodriguez Institute of Science and Technology. He holds a National Certificate Level III in Visual Graphic Design, earned during senior high school, and a National Certificate Level II in Computer System Servicing, achieved in his first year of college. With this blend of creative and technical expertise, he is committed to applying his skills to both engineering and design challenges.

Jose Alfonso P. Labrador is a 3rd year Computer Engineering Student at Eulogio “Amang” Rodriguez Institute of Science and Technology. He excels in hardware mechanics and software development, with a strong interest in embedded systems and electronics.

John Aarom P. Mina is a 3rd year Computer Engineering Student at Eulogio “Amang” Rodriguez Institute of Science and Technology. He has a growing interest in computer hardware, basic electronics, and programming. He is motivated to improve his technical skills through hands-on projects and collaborative learning experiences.

Francis Angelo Q. Rique is a 20-year-old Computer Engineering student at the Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST). He is currently pursuing a Bachelor of Science in Computer Engineering with academic interests in operating systems, computer hardware development, and intelligent system development. His areas of interests include GUI design and development, and computer programming. His coursework and projects emphasize hardware–software integration, system design, and hands-on engineering applications, with a strong focus on developing smart and automated systems.

Mark Yancee P. Vicente is a 3rd year Computer Engineering Student and Chairman of VSA (Volunteer Student Assistant) at Eulogio “Amang” Rodriguez Institute of Science and Technology. He is the ongoing chairman of VSA for 2 years.

Engr. Minerva C. Zoleta, a Professional Computer Engineer, is a dedicated Computer Engineering Professor at the Eulogio “Amang” Rodriguez Institute of Science and Technology in the Philippines, specializing in Embedded Systems, Operating Systems, and Computer Network and Security. With a strong background in

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

academia and industry. She has been instrumental in shaping the next generation of Engineers through innovative teaching methods and hands-on research. Engr. Zoleta holds a Master's degree in Electrical Engineering major in Computer Engineering at Technological University of the Philippines, Manila and is pursuing her doctorate degree in Engineering with specialization in Computer Engineering AT Technological Institute of the Philippines. She has presented published research on topics such as Embedded System, IoT applications, and wireless communication international conferences and journals. . Passionate about technology-driven solutions, She has led various projects integrating smart systems into real-world applications, contributing to the advancement of local and international engineering communities.

REFERENCES

1. Al-Ofeishat, H. A., & Alshorman, R. (2024). Build a Secure Network Using Segmentation and Micro-segmentation Techniques. International Journal of Computing and Digital Systems, 16(1), 1499–1508.
2. Cisco. (n.d.). Cisco Packet Tracer. Cisco Networking Academy. https://www.netacad.com/cisco-packet-tracer
3. Comer, D. E. (2018). The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works (5th ed.). CRC Press.
4. IBM. (n.d.). What is Computer Networking? https://www.ibm.com/think/topics/networking
5. Kallatsa, M. (2024). Strategies for Network Segmentation: A Systematic Literature Review. University of Jyväskylä.
6. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164–173.
7. Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview. Internet Society.
8. TP-Link. (n.d.). What is an Enterprise Network? Types and Concepts. https://www.tp-link.com/ph/blog/1727/what-is-an-enterprise-network-types-concepts/
9. Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of Things. International Journal of Communication Systems, 25(9), 1101–1102.
10. Ye, J., et al. (2024). Exposed by Default: A Security Analysis of Home Router Default Settings. Proceedings of the ACM Asia Conference on Computer and Communications Security, 63–76.
11. Huang, L. S., Su, J. Y., & Pao, T. L. (2019). A context aware smart classroom architecture for smart campuses. Applied Sciences, 9(9), 1837. https://doi.org/10.3390/app9091837 Cited by: 167
12. Nai, R. (2022). The design of smart classroom for modern college English teaching under Internet of Things. PLOS ONE, 17(2), e0264176. https://doi.org/10.1371/journal.pone.0264176 Cited by: 39
13. Balasubramani, G. (2024). Design and implementation of hierarchical enterprise architectures and internal services using Cisco Packet Tracer. Department of Electronics and Communication Engineering, St. Joseph's Institute of Technology.
14. Barde, A. (2025). Real-time telemetry optimization and edge gateway processing for multi-endpoint IoT environments. Journal of Smart Systems and Automation, 4(1), 112–125.