ISSN 2278-3091
Volume 13, No.1, January - February 2024
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse011312024.pdf
https://doi.org/10.30534/ijatcse/2024/011312024

Enhancing Security and Access Control: A Biometric-Based Campus Area Network (CAN) Design for North Eastern Mindanao University (NEMSU) - Tagbina Campus

Flora Lou L. Calis[1], Dandy U. Dalina[2], Mildra March Tejano[3], Ervin Simon Uadan[4], Dr. Mark Van M. Buladaco[5]
[1]University of Southeastern Philippines – Obrero Campus, Philippines, fllcalis@usep.edu.ph
[2]Southern Philippines Agri-Business and Marine and Aquatic School of Technology, Philippines, dandydalena@gmail.com
[3]North Eastern Mindanao State University - Tagbina Campus, Philippines, mmtejano@nemsu.edu.ph
[4]North Eastern Mindanao State University - Tagbina Campus, Philippines, eduadan@nemsu.edu.ph
[5]Davao del Norte State College, Institute of Computing, Panabo City

Received Date : December 18, 2023 Accepted Date: January 19, 2024 Published Date: February 06, 2024

ABSTRACT

In this rapidly changing landscape of modern institutions, biometric technology has become a crucial part of strengthening security, enhancing productivity, and refining the overall campus experience. This study focuses on the implementation of a Campus Area Network (CAN) at the North Eastern Mindanao State University (NEMSU) - Tagbina Campus, with a specific emphasis on leveraging biometric technology for non-teaching and teaching personnel. By employing advanced methods such as fingerprint recognition and facial identification, institutions can ensure precise attendance records in real-time, replacing error-prone traditional methods. The proposed Campus Area Network (CAN) will serve as an integrated structure that establishes connectivity in both geographically separated Local Area Networks (LANs) and Metropolitan Area Networks (MANs) facilitating efficient data transfer and communication among various campus facilities. The primary goal of this study is to not only streamline administrative operations but also to establish a safer and more accountable educational environment, which will benefit both professors and students in the long run.

Key words: Biometric, CAN, LAN, MAN, Network

1. INTRODUCTION

In the changing world of institutions incorporating modern technologies has become crucial for improving safety, productivity, and the overall campus experience. Biometric technology drives the future direction of strong authentication. Biometric technology, which includes fingerprint recognition, facial identification, and other methods has become an advanced tool for improving security and optimizing various processes in different fields [1]. It provides highly accurate and reliable attendance records, eliminating errors and inaccuracies that can occur with traditional paper-based or manual methods. With a computer network, biometric attendance data can be collected and recorded in real-time. Although the employee's attendance will be recorded, it is unclear if the worker is actually present at work after reporting for duty. In this day and age of digitalization, it is seen that many employees leave the office after taking attendance in order to work on personal projects during business hours [2]. The enhancement of employee performance with the objective of delivering improved public service is a fundamental democratic principle upheld by the government. The provision of services is carried out within a transparent and responsible framework of governance [3]. This means that university administrators can access up-to-the-minute attendance information and respond to any issues promptly. The system network improves operational performance in many domains and institutions, like businesses and educational institutions. Computer networking plays a role in our society by facilitating the exchange of information. It allows different systems to connect with each other for the purpose of communication and ensures the transfer of data.

A Campus Area Network (CAN) is a type of network that comprises interconnected and dispersed Local Area Networks (LANs), resembling Metropolitan Area Networks (MANs). It is designed to give network coverage to buildings that are situated in close proximity to one another. By implementing biometric technology for faculty attendance using a computer network, universities cannot only enhance administrative processes but also create a more secure and accountable educational environment, ultimately benefiting both faculty and students. The implementation of a centralized IT infrastructure, facilitated by the use of a Controller Area Network (CAN), enhances operational efficiency and streamlines maintenance processes. By consolidating all network resources into a single entity, organizations can enhance their ability to effectively manage network security, quality of service, and other policy controls. This feature not only makes administrative tasks easier but also opens the door to better security and performance [4].

Project Objectives

The main objective of this study is to comprehensively address the design and implementation of a Campus Area Network (CAN) at North Eastern Mindanao State University (NEMSU) - Tagbina Campus specifically on the following department buildings in Computer Science (DoCS), Business Management (DoBM), Agriculture (DA), Hospitality Management (DoHM) and General Teacher's Training (DGTT), focusing on both non-teaching and teaching personnel where biometric technology is employed. Scrutinizing the network connectivity solutions to ensure efficient data transfer and communication among department buildings and other campus facilities.

2. METHODOLOGY

Project Benefits

Biometric technology will help the North Eastern Mindanao State University (NEMSU) - Tagbina campus to enhance its security and ensure more accurate identification of its personnel and staff. It will improve their productivity by providing a real-time attendance tracking to minimize discrepancies which will result in a more efficient resource allocation and time management. Furthermore, automation of attendance records will help reduce the administrative burden, allowing staff to focus more on their core responsibilities.

Project Business and Technical Goals

The North Eastern Mindanao State University (NEMSU) - Tagbina campus Biometric-based Campus Area Network (CAN) aims to eliminate the administrative costs in manual attendance tracking through automation and optimize resource allocation. It also aims to boost the morale and reputation of the campus as technologically advanced to attract more students and faculty and guarantees to comply with the data and protection regulations while securing sensitive biometric data. With its implementation, the campus will have a chance for an efficient data transfer by connecting the LANs and MANs within the specified department buildings to operate in real-time attendance monitoring and reporting integrating fingerprint recognition and facial identification systems into the network infrastructure.

Project Gantt Chart

Table 1. Gantt Chart

Activities	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Network Planning												
Overall Analysis												
Requirements Determination												
Procurement												
Network Installation												
Line Testing												

Proposed Network Design

Network Analysis

Data Types

The network primarily deals with biometric authentication data, encompassing two key types: fingerprint and facial recognition data. Fingerprint data comprises digital representations of unique fingerprint patterns, collected through specialized scanners, while facial recognition data involves the capture and storage of facial features like facial geometry and texture.

Data Sources

Data generation within the network is initiated at various end stations (Department Offices), where biometric devices like scanners play a pivotal role. These biometric scanners capture two primary forms of data: fingerprint data and facial recognition data. Specifically, the scanners record and extract unique fingerprint patterns or facial features from individuals. Subsequently, the acquired data is transmitted to a centralized server for processing, storage, and authentication purposes. This data flow underscores the essential role of biometric devices in generating and relaying fingerprint and facial recognition data to the network's core, where it is harnessed for secure identity verification and access control.

Numbers of Users and Priority Level

Administrators and members of such departments will be the users at the state level. At any given time, the maximum projected number of users on the network is 150. Management (top priority), users (medium priority), and users (low priority) will all be supported. The prioritization of network management operations will be of utmost importance with a moderate level of priority assigned to the bulk of network processes. It is important to acknowledge that network administration generally utilizes a relatively small fraction of the available bandwidth. Consequently, support levels for both management and user processes are typically equivalent.

Transmission Speed Requirements

The primary objective of the network is to deliver a cohesive user experience by ensuring that biometric device-based applications operate remotely from the server. Ideally, operations performed from a distance should exhibit the same level of responsiveness as those executed directly on a user's local device.

Load Variation Estimates

Based on the available data, it is apparent that the time interval from 12:00 AM to 1:00 PM on weekdays demonstrates the highest mean traffic volumes. It is expected that network congestion will peak during two specific time periods each day: from midnight to noon, and from 5:00 PM to 6:00 PM in the evenings and weekends. During these times, network traffic is likely to decrease, except for the regular PC backups to the LAN servers. In order to mitigate consumer discontent, the network has been designed to effectively handle the most

demanding amounts of traffic at peak periods, prioritizing this aspect over average data performance.

Storage Requirements

The storage capacity must be sufficiently extensive to accommodate the entirety of the biometric data. The utilization of fingerprint and facial recognition for the storing of users' data suggests that an allocation of approximately 1 MB of data space will be required per user on average. Furthermore, it should be noted that there is a strict limit of 20 users allocated to any individual department. The network operating system is expected to consume around 500 megabytes of storage space on the local area network (LAN) server.

Reliability Requirements

In accordance with the user requirements and prevailing industry standards, it is expected that both Local Area Networks (LANs) and Wide Area Networks (WANs) will strive to achieve a significant degree of dependability, with a target uptime of 99.9% and an exceptionally low error rate of 0.001%.

Physical Design

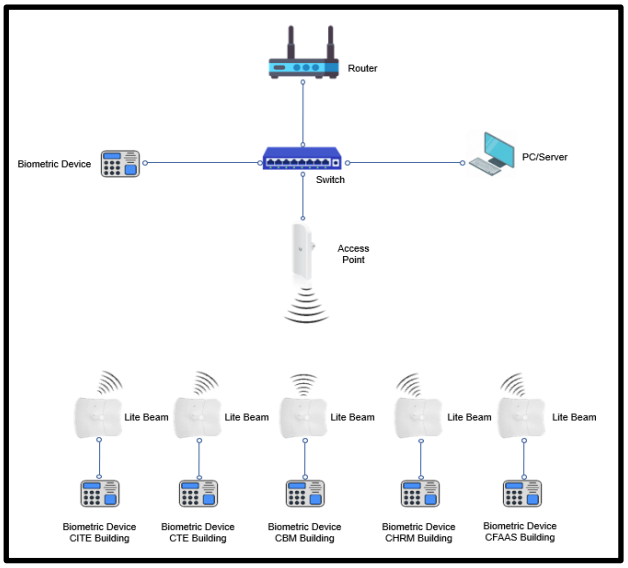

Figure 1: Physical Network Design

The proposed Campus Area Network (CAN), illustrated in Figure 1, employs Lite Beam technology to interconnect multiple buildings namely the College of Information Technology Education (CITE), College of Teacher Education (CTE), College of Business Management (CBM), College of Hospitality and Restaurant Management (CHRM), and College of Forestry, Agriculture, and Aquatic Sciences (CFAAS) buildings all link to the Access Point in the Administration Office as part of the comprehensive network infrastructure design. Additionally, the Biometric Device is located within the Administration Office and is connected to the switch. The Access Point is strategically positioned within the Administration Office and is connected to a router in order to facilitate connectivity for various devices throughout the entirety of the university campus.

Logical Design

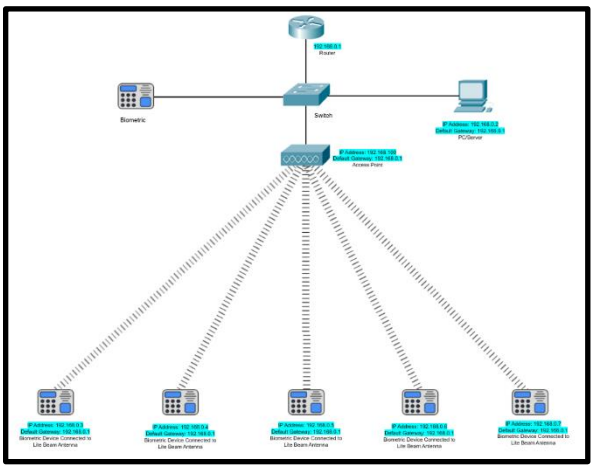

Figure 2: Network Logical Design for Biometric System of each Department

The network setup shown in Figure 2, features a router and a switch configuration within a Campus Local Area Network (LAN). Oversight of network management falls under the switch, acting as the designated trunk switch to facilitate access for devices within the Campus Local Area Network. Specific IP addresses are allocated to various components: the PC/Server is set at 192.168.0.2, the Access Point at 192.168.0.100, the College of Information Technology Education (CITE) Building at 192.168.0.3, the College of Teacher Education (CTE) Building at 192.168.0.4, the College of Business Management (CBM) Building at 192.168.0.5, the College of Hospitality and Restaurant Management (CHRM) Building at 192.168.0.6, and the College of Forestry, Agriculture and Aquatic Sciences (CFAAS) Building at 192.168.0.7. The network's assigned network address is 192.168.0.0, with the gateway IP Address configured as 192.168.0.1.

Organization Security Policy

In order to limit access for persons who lack authorization, the implementation of a firewall will be undertaken. The security protocols will encompass the implementation of user accounts and passwords, which will be assigned with different levels of authorization to network administrators and standard users.

Network Cost of Ownership

Table 2. Network Cost of Ownership

Capital Expenditures	
Particulars	**Estimated Cost**
Network Equipment (Hardware)	100,000.00
Storage	50,000.00
Software License	50,000.00
Installation	30,000.00
Total Capital Expenditures	**130,000.00**
Operating Expenditures	
Electricity Expenses	100,000.00/year
Salaries and Wages	280,000.00/ year
Internet Subscription	156,000.00/ year
Total Capital Expenditures	**130,000.00**
Total Capital and Operating Expenditures for the First Year of Implementation	**666,000.00**

3. RESULT AND DISCUSSION

Implementation

The main objective of this study is to create the optimal campus local area network that can be integrated with the biometric system of every department and administration building located at the Tagbina Campus of North Eastern Mindanao State University that is resilient to the demanding use process. The management of network operations Table 1 presents the Gantt Chart that illustrates the implementation of activities in accordance with the recommended network design. Furthermore, it is advisable to consult Table 2 in order to obtain details regarding capital expenses related to the procurement of network equipment, storage devices, computer specs, subscriptions, and communication services. In order to mitigate potential complications, it is imperative to stick to the prescribed network logical configuration with a reduced number of settings. It is advisable for the administrator to adhere to the project's timeline for planning and implementation, which spans a duration of one year.

Building Floor Plan

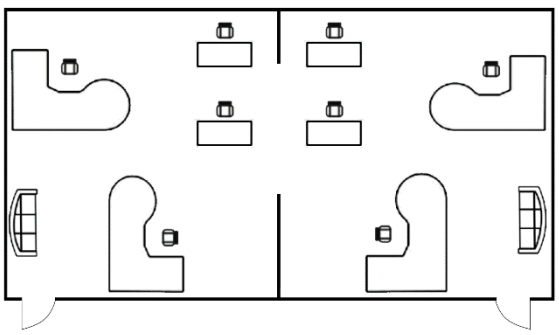

Figure 3: Administration Building (Second Floor)

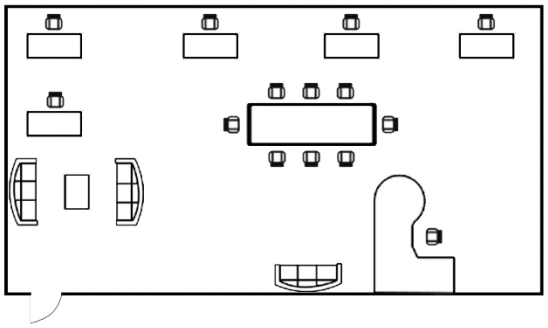

Figure 4: College of Business Management Building

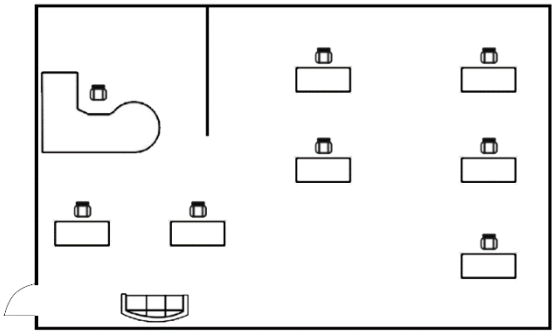

Figure 5: College of Information Technology Education Building

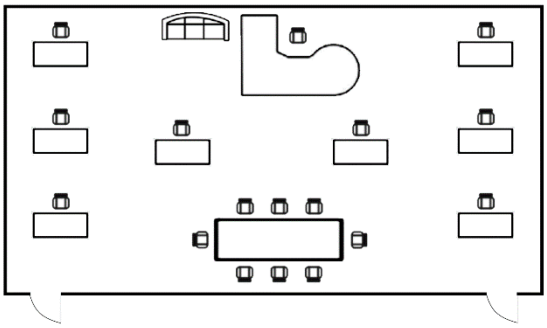

Figure 6: College of Teacher Education Building

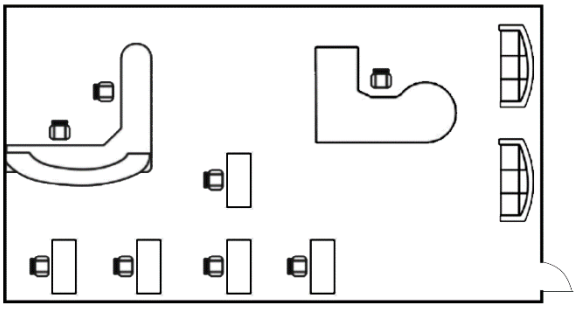

Figure 7: College of Hospitality Restaurant Management Building

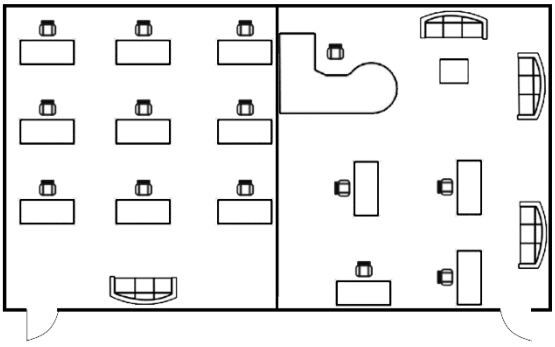

Figure 8: College of Forestry Agriculture and Aquatic Sciences Building

4. CONCLUSION AND RECOMMENDATIONS

In conclusion, the proposed Campus Area Network (CAN) at North Eastern Mindanao State University (NEMSU) - Tagbina Campus integrating biometric technology holds significant potential for enhancing security, improving personnel identification accuracy, and streamlining attendance tracking processes. The project aligns with the goal of reducing administrative burdens and optimizing resource allocation, fostering a more efficient and technologically advanced campus environment. The detailed network design, encompassing both physical and logical aspects, showcases a robust infrastructure capable of handling biometric authentication data and meeting the specified reliability requirements. Additionally, the implementation plan, illustrated in the Gantt chart and cost estimates, provides a clear roadmap for successful execution. Recommendations include meticulous adherence to the network's logical setup, continuous adherence to security policies, and strict compliance with data protection regulations. The projected cost of ownership and the potential benefits in terms of security, productivity, and efficiency support the feasibility and long-term sustainability of the proposed CAN. Overall, the successful implementation of this project is anticipated to position the North Eastern Mindanao State University (NEMSU) - Tagbina Campus as a technological leader, attracting more students and faculty while ensuring a secure and technologically advanced learning environment.

REFERENCES

[1] M. Down and R. Sands, “Biometrics: An Overview of the Technology, Challenges and Control Considerations” 2004 Information Systems Audit and Control Association. [Online] Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b148ea42d3d6ab78484476a96e6666ab3992398e

[2] H. Adal, N. Promy, S. Srabanti and M. Rahman, "Android based advanced attendance vigilance system using wireless network with the fusion of biometric fingerprint authentication," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea (South), 2018, pp. 217-222, doi: 10.23919/ICACT.2018.8323702.

[3] Seng Chun Hoo, Haidi Ibrahim, "Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements", Journal of Sensors, vol. 2019, Article ID 7410478, 25 pages, 2019. https://doi.org/10.1155/2019/7410478.

[4] ThreeIC, “What Is a Campus Area Network?” 2022. [Online] Available: https://www.threeic.com/resources/campus-network-solution/campus-area-network/