

ABSTRACT

This project investigates the existing network infrastructure of Bolgatanga Technical University (BTU) with a focus on identifying security vulnerabilities and proposing practical, research-based solutions. Through a combination of direct observation, informal interviews with IT personnel, and the review of institutional network practices, the study revealed several weaknesses in the university's network setup.

Key issues identified include the absence of secure Wi-Fi authentication, lack of network segmentation, no enforceable Acceptable Use Policies (AUP), and unrestricted access to core administrative systems from potentially unsecure personal devices. These vulnerabilities expose the institution to various cyber threats such as unauthorized access, data breaches, and malware propagation.

The study recommends a series of non-invasive but impactful solutions, including the implementation of email-based Wi-Fi login systems, the adoption of VLAN segmentation, policy development and enforcement, access restrictions for core systems, and basic network monitoring tools. Additionally, it emphasizes the importance of user awareness training to build a security-conscious campus environment.

While the study does not implement these recommendations, it serves as a strategic blueprint for future network security planning and improvements within the university setting.

Keywords: Network Security, Wi-Fi Authentication, Acceptable Use Policy, VLAN, Access Control, University Network, Cyber Threats

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

In today's technology-driven academic environment, universities rely heavily on computer networks for administration, research, teaching, communication, and student engagement. These networks allow access to critical services such as email, e-learning platforms, examination systems, and online libraries. As these systems become more interconnected and accessible, they also become more vulnerable to cyber threats.

At Bolgatanga Technical University (BTU), the network infrastructure is a vital component of both academic and administrative operations. Students and staff depend on it for accessing educational content, submitting assignments, and performing daily tasks. However, like many institutions, BTU's network may face challenges such as inadequate security controls, outdated devices, weak access restrictions, and lack of awareness among users — all of which can expose the network to significant risks.

With the increasing number of cyberattacks targeting educational institutions globally, it is necessary to ensure that university networks are adequately secured. This project seeks to investigate common network security issues within the context of Bolgatanga Technical University and propose practical, cost-effective measures to strengthen the university's infrastructure against current and emerging threats.

1.2 Problem Statement

Despite the increasing dependence on IT infrastructure, many universities in Ghana — including Bolgatanga Technical University — face challenges related to network security. Common problems include unsecured wireless access points, weak user authentication, poor access control, lack of regular system updates, and absence of well-defined security policies.

These weaknesses can lead to various threats, including data breaches, unauthorized access to sensitive information (such as exam records), malware infections, and service disruptions. In most cases, these threats are not detected or addressed early enough due to limited technical capacity or lack of awareness. The absence of a structured network security framework increases the risk of compromise.

1.3 Aim of the Study

The aim of this project is to assess the current network security challenges at Bolgatanga Technical University and propose practical and effective measures to enhance the security of its network infrastructure.

1.4 Objectives of the Study

The specific objectives of the study are as follows:

1. To identify common network security threats affecting university networks, particularly at BTU.
2. To assess existing weaknesses in the network infrastructure and management policies.
3. To propose technical and administrative solutions for improving network security.
4. To provide general recommendations to promote network security awareness and best practices.

1.5 Significance of the Study

This study will help the management and IT staff of Bolgatanga Technical University to understand key vulnerabilities in their current network setup. The proposed recommendations can serve as a guide for improving network security, reducing downtime, and protecting sensitive academic and administrative data. Furthermore, this research can serve as a reference for other technical universities in Ghana facing similar issues.

1.6 Scope and Limitations of the Study

The scope of this study is limited to the analysis of common network security issues within the main network infrastructure of Bolgatanga Technical University. The project does not include advanced penetration testing or full implementation of proposed solutions but is focused on research, observation, and recommendation.

Limitations include restricted access to some internal configurations and possible unavailability of some network data due to institutional privacy policies. As such, some assumptions are based on common practices in similar institutions.

1.7 Organization of the Report

This report is organized into six chapters:

- **Chapter One** provides an introduction to the study, outlining the background, problem statement, objectives, and scope.
- **Chapter Two** reviews relevant literature on network security and common issues in university networks.

- **Chapter Three** describes the research methodology used to gather data and analyze the current situation.
- **Chapter Four** presents the findings from the research and discusses identified security issues.
- **Chapter Five** outlines proposed solutions and best practices for securing the network.
- **Chapter Six** summarizes the study, draws conclusions, and provides recommendations for future improvements.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Network security has become a major concern for educational institutions worldwide. Universities, like Bolgatanga Technical University, operate complex networks that support thousands of users across students, faculty, and administrative staff. These networks often manage sensitive data, such as examination records, personal information, and financial details. Without adequate security measures, these systems become easy targets for cybercriminals, unauthorized users, and malware. This chapter reviews the basic concepts of network security, identifies common threats in university environments, and highlights best practices relevant to the context of BTU.

2.2 Overview of Network Security in Educational Institutions

Network security involves protecting the usability, integrity, and safety of a network and its data. In universities, this includes securing internet access, email systems, campus Wi-Fi, web applications, student portals, and administrative tools. According to [Cisco, 2023], the core goals of network security are:

- **Confidentiality** – ensuring that data is accessible only to authorized users.
- **Integrity** – preventing unauthorized changes to data.
- **Availability** – ensuring the network and systems are reliably accessible.

Most university networks are exposed to threats due to open-access environments, a large number of users, bring-your-own-device (BYOD) cultures, and limited technical enforcement of security policies.

2.3 Common Network Security Issues in University Networks

Several issues have been identified as frequent in campus networks, many of which apply directly to Bolgatanga Technical University:

2.3.1 Insecure Wireless Network Access

One of the main concerns at BTU is the use of a **shared Wi-Fi password** without proper **authentication or identity management**. While the infrastructure supports **email-based login**, it is not yet implemented. As a result, anyone who obtains the Wi-Fi password can freely connect to the network, whether they are a student, staff member, or an outsider.

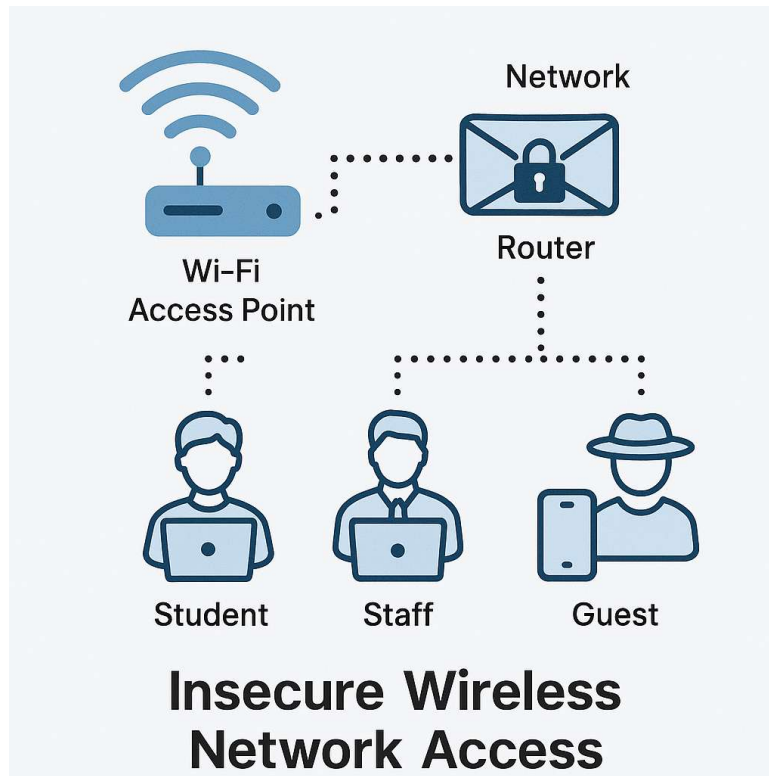


Figure 2.1: Insecure Wireless Network Access

Risks:

- Unauthorized users gaining access to internal systems.
- Potential data interception by rogue users.
- Difficulty in monitoring who accessed the network and when.

Best Practice:

- Implementing **802.1X authentication** using university emails.
- Using **RADIUS server integration** for user-level login on Wi-Fi.
- Generating user-specific access logs.

2.3.2 Lack of Network Usage Policies

BTU currently lacks a well-defined and publicly available **network usage policy**. Users do not have clear guidelines on acceptable or prohibited behavior on the university network.

Risks:

- Students or staff unknowingly engaging in risky activities (e.g., downloading malware).

- Legal liability in case of abuse or attacks originating from the network.
- Lack of enforcement makes accountability difficult.

Best Practice:

- Drafting and distributing a **Network Acceptable Use Policy (AUP)**.
- Including clauses on user responsibilities, prohibited actions, data protection, and consequences of violations.

2.3.3 Uncontrolled Access to Core Systems (e.g., School Management Software)

The current setup at BTU allows staff to access the school management system from any personal device, including personal laptops which may not meet security standards.

Risks:

- Personal devices may be infected with malware, keyloggers, or have outdated antivirus.
- If such a device is compromised, attackers could access sensitive academic or administrative data.
- Risk of data leaks or unauthorized data manipulation.

Best Practice:

- Limiting system access to **secured, university-provided devices**.
- Enforcing **endpoint security policies** such as antivirus, device encryption, and OS updates.
- Implementing **Virtual Private Network (VPN)** for secure remote access.

2.4 Other Common Network Threats in University Environments

In addition to the issues at BTU, other known threats in similar university networks include:



Figure 2.2: Common network security threats

2.4.1 Malware and Ransomware Attacks

Universities are common targets for malware due to the high number of connected users and systems. A single infected machine can quickly spread viruses throughout the network if no controls are in place.

Best Practice:

- Enforce regular antivirus updates across all devices.
- Use firewalls and content filtering to block malicious websites.

2.4.2 Insider Threats

Some of the most damaging attacks come from users who have legitimate access to the network but misuse it. This could be an angry staff member, a careless student, or even a technician with elevated access.

Best Practice:

- Apply the **principle of least privilege** – users should only have access to what they need.

- Enable **activity logging and monitoring**.

2.4.3 Poor Network Segmentation

Many universities use a flat network where all devices (student and administrative) share the same network space. This increases the risk of lateral movement in the event of a breach.

Best Practice:

- Use **VLANs (Virtual LANs)** to separate traffic between students, staff, and sensitive systems.
- Control inter-VLAN routing using firewalls or access control lists (ACLs).

2.5 Summary of Reviewed Concepts

This chapter has discussed the foundational concepts of network security and identified threats commonly affecting university environments. Specific to BTU, the unsecured Wi-Fi access, lack of user policy, and unregulated system access present real risks. The reviewed best practices and technologies provide a roadmap for mitigating these risks in a cost-effective and practical manner, especially for educational institutions with limited resources.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methods used to investigate common network security challenges at Bolgatanga Technical University (BTU) and to propose appropriate solutions. Since the project is research-based and not implementation-focused, the methodology emphasizes observation, informal interviews, and the review of existing configurations and network practices. The goal is to gather practical data about the current state of the network, identify vulnerabilities, and recommend realistic improvements.

3.2 Research Design

The research adopted a **descriptive and exploratory design**, focusing on understanding the security posture of BTU's network infrastructure. It was qualitative in nature, relying on observations, staff input, and comparison with industry best practices. The study did not involve technical implementation or penetration testing, but rather an investigative review to identify weaknesses and propose solutions.

3.3 Data Collection Methods

To gather relevant information, the following methods were used:

3.3.1 Observation

- The physical and logical structure of the network was observed.
- Public access points (e.g., Wi-Fi) and access to sensitive systems (like the school management platform) were examined.
- Network equipment such as routers and switches were reviewed visually for security configurations.

3.3.2 Informal Interviews

- Informal discussions were held with selected IT support staff and a few teaching staff to understand how the network is used and managed.
- Questions focused on Wi-Fi access management, antivirus usage, update policies, and access to internal systems.

3.3.3 Document Review

We couldn't have access to documents so we made assumptions base on the standard practices and Little information about the current policies from ICT Directorate staff.

3.3.4 Case Study Comparison

- The study referenced network security measures used in other Ghanaian universities or global educational institutions to benchmark BTU's situation.
- These comparisons helped in generating practical, proven recommendations.

3.4 Research Tools Used

Although this project does not involve actual network scanning or testing, certain **research tools and reference models** were used to assess the current security state. These include:

- **Network Security Checklists** – based on best practices from organizations like Cisco and NIST.
- **Sample Network Policies** – templates from similar educational institutions were reviewed.
- **Visual Mapping Tools** – used to conceptualize the network's structure and flow of information.

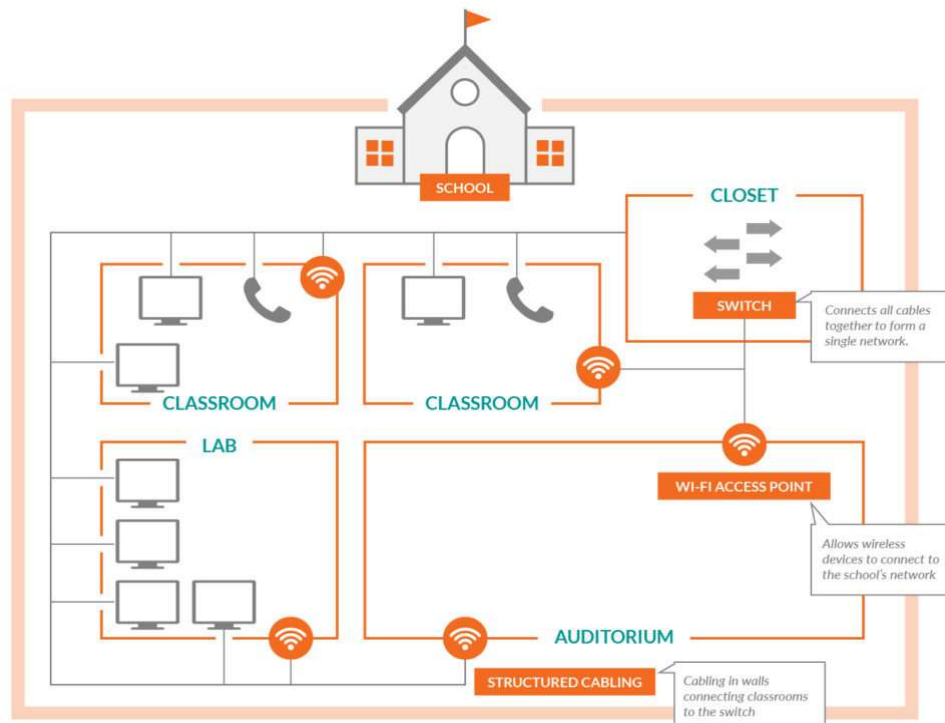


Figure 3.1 Visual Mapping Tools

- **Basic Interview Guides** – to guide conversations with staff on daily operations and concerns.

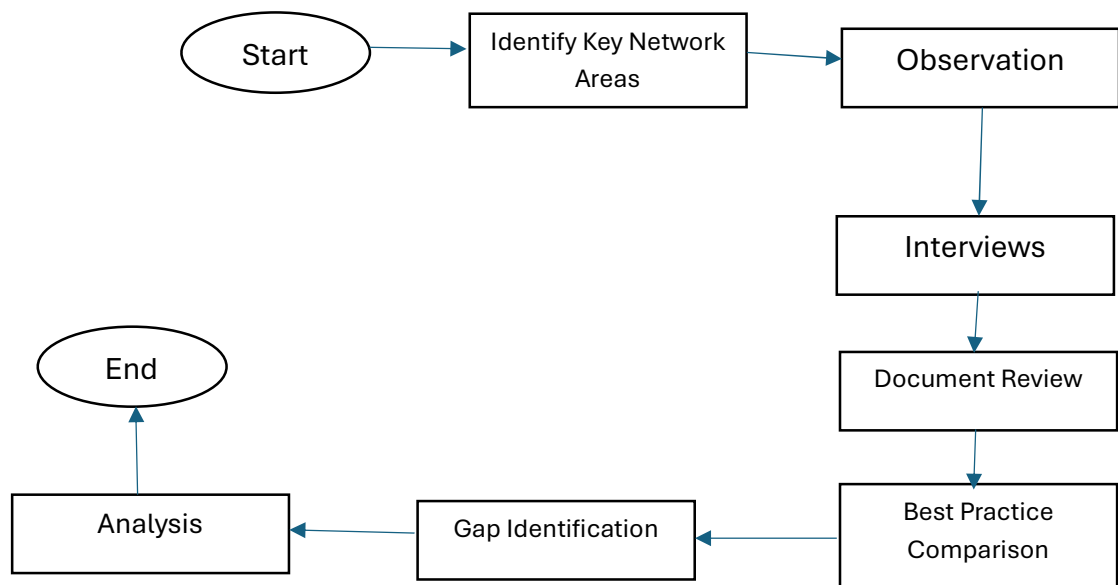


Figure 3.2 Data Collection Process – Flowchart

3.5 Data Analysis Method

The data collected was analyzed through the following steps:

1. **Categorization of Issues:** Network problems were grouped under headings like “Access Control,” “Device Security,” and “Policy Gaps.”
2. **Gap Identification:** Each finding was compared against known best practices to identify vulnerabilities.
3. **Risk Analysis:** The potential impact of each issue (e.g., malware infection, unauthorized access) was considered in relation to the University's operations.
4. **Proposal of Solutions:** For each problem area, one or more practical and affordable solutions was recommended.

3.6 Ethical Considerations

As the project involved observational research and informal staff input, ethical measures were taken to ensure:

- No sensitive or confidential data was disclosed in the report.

- Staff opinions were used anonymously and with consent.
- No network devices or systems were modified or interfered with during the research process.

3.7 Limitations of the Methodology

- Access to full network documentation and configuration files weren't available.
- Formal interviews with all relevant departments (e.g., administrative staff) were not possible.
- Some assumptions were made based on the best global practices where local data was unavailable.
- The study could not include real-time monitoring, or system logs due to privacy and access restrictions.

3.8 Summary

This chapter has outlined the methodology used to explore and understand network security challenges at Bolgatanga Technical University. Through observation, staff engagement, document review, and comparison with best practices, the study was able to identify key weaknesses and prepare a foundation for recommending meaningful security improvements in the next chapters.