CYBERHYGIENESCAN (CHS): A NETWORK-BASED SYSTEM FOR ASSESSING AND ENHANCING CYBER HYGIENE IN EDUCATIONAL INSTITUTIONS

Onwubiko Davidson Chisom[1], Odikwa Ndubuisi Henry[2], Ukabuiro Ikenna Kelechi[3]
[1, 2 ,3,] *Computer Science Department, Abia State University, Uturu*

Abstract

This article establishes and develops a cyber hygiene (CHS) framework for network-based system for assessing and enhancing cyber hygiene in educational institutions. Cyber Hygiene Scan (CHS) is a network-based system developed to evaluate, monitor, and enhance cyber hygiene in educational environments. CHS integrates real-time network scanning, vulnerability detection, endpoint compliance monitoring, and risk scoring into a unified dashboard accessible through a secure web interface. The increasing reliance on digital infrastructure in educational institutions has amplified the need for robust cybersecurity practices, particularly in maintaining high standards of cyber hygiene. Despite this need, many institutions lack effective mechanisms to assess and improve their cyber hygiene posture. A total of ten (10) universities located in South-eastern universities with over three hundred (300) systems were selected and their systems' vulnerabilities analyzed. The vulnerabilities helped in building a cyber hygiene scan built using Python, Nmap, OpenVAS, and SNMP for network data collection, and supported by a PostgreSQL as the back-end. A modular architecture enables seamless deployment across varying network sizes, while the integrated policy engine maps CHS's effectiveness in identifying vulnerabilities such as outdated software, miss-configured services, and weak authentication practices. Our findings suggest that CHS can serve as a vital tool for educational institutions aiming to fortify their cyber security resilience through proactive hygiene management and informed decision-making.

Keywords: cybersecurity, hygiene, vulnerability, risks, network.

1. Introduction

It is not an overstatement that security is key to protecting vital documents in any organization. Weak security poses vulnerabilities to important documents, thereby making it prone for hackers to perpetrate their heinous crimes hence the need for a cyber hygiene scan [9]. Cyber hygiene, akin to personal hygiene in the digital world, refers to the regular practices and precautions users take to maintain the health and security of information systems and data [12]. In recent years, the expansion of digital infrastructures in educational institutions has created both opportunities for innovation and significant vulnerabilities. With increasing reliance on networked resources, online assessments, remote learning platforms, and

administrative digitization, educational environments have become prominent targets for cyber threats such as ransomware, phishing, and data breaches [11].

Despite growing awareness of cyber security risks, educational institutions often operate with limited cyber security budgets, insufficient skilled personnel, and weak enforcement of security policies [3]. These factors contribute to poor cyber hygiene, particularly in developing countries and under-resourced institutions where digital adoption has outpaced security readiness. Existing solutions for cyber security assessment are typically enterprise-focused, expensive, and difficult to deploy in educational environments with diverse user populations and limited IT staff.

This paper presents the design and implementation of Cyber Hygiene Scan (CHS), a lightweight, network-based system tailored to assess and improve cyber hygiene practices in educational institutions. CHS addresses critical security domains such as vulnerability detection, endpoint configuration compliance, network asset visibility, and risk prioritization. The system is built on open-source technologies, integrating tools like Nmap, OpenVAS, and SNMP-based monitoring to automate real-time scanning and generate actionable reports via a user-friendly dashboard.

2. Literature Review

Much works have not been done in the area of cyber hygiene. It is inadequate to compare previous attempts in enhancing cyber hygiene to the present day where treats and system vulnerability have been on the increase. Some key literature features on cyber hygiene are discussed.

Concept of Cyber Hygiene

Cyber hygiene refers to the habitual practices and strategies employed by individuals and organizations to maintain the security, health, and integrity of their digital systems and data [4]. Similar to personal hygiene, cyber hygiene emphasizes routine behaviors such as updating software, managing passwords securely, and using firewalls and antivirus tools. The National Institute of Standards and Technology [8] outlines cyber hygiene as foundational to organizational cyber security resilience, especially in environments with dynamic users and devices such as educational institutions.

Cyber security Challenges in Educational Institutions

Educational institutions face distinct cyber security challenges due to their open and heterogeneous network environments, which support a wide range of users including students, faculty, staff, and external collaborators. Studies have reported an increase in ransomware attacks and data breaches targeting schools and universities, exploiting weak endpoint security, miss-configured services, and poor password hygiene [2],[6]. Additionally, institutions often struggle with a lack of formalized cyber security policies, limited funding, and inadequate awareness training among users [5].

Tools for Cyber Hygiene Assessment

A variety of tools and frameworks exist to assess cybersecurity risks. Commercial

solutions such as Nessus, Qualys, and Rapid7 provide comprehensive vulnerability scanning and threat analytics, but are often cost-prohibitive and complex to deploy in academic environments [10]. Open-source tools like Nmap and OpenVAS offer lightweight alternatives, though they require significant configuration and domain knowledge. Moreover, most existing solutions are not designed with cyber hygiene specifically in mind, and they lack support for educational-use cases such as multi-user awareness, policy education, and institution-specific compliance metrics.

Recent research has focused on developing more context-aware and adaptive cyber security systems. For instance, Kumar and Sengupta [7] proposed a modular threat detection framework tailored for public institutions, while Tang and Lee [8] explored student-centric security awareness platforms. However, few systems provide a holistic view of cyber hygiene that integrates automated scanning, policy compliance, risk scoring, and educational feedback in a single platform.

[13] Vigneswari, emphasized on the need to safeguard institutional sensitive data against cyber treats such as phishing, ransomeware, insider attacks etc.

[4], opined that cyber hygiene can drastically reduce online child exploitation in the era of digital technology. The study identified several child exploitation vulnerabilities and suggests that cyber hygiene is a vital tool to be employed in our educational institutions. [1] identified two major cyber hygiene services which includes vulnerability scanning meant for continuous monitoring and assessment of internet accessible network assets

3. Materials and Methods

This section illustrates the materials and methods used in achieving the cyberhygiene scan (CHS). It also depicts the population sample used, the method of data collection and the processes employed in developing the cyber hygiene scan.

3.2 Method of Data Collection

The method of data collection for this research paper is through primary method by using interviews. The interviews were carried on the information and communication technology administrators and other It staff in the universities. The aim is to ascertain the level of intrusion and vulnerabilities of their educational systems, the prospects and constraints militating or enhancing cyber hygiene.

3.1 Simple Random Sampling

This research work employed simple random sampling in selecting the universities and their corresponding systems. It is a probability sampling or chance sampling. This type of sampling was used because of the many institutions in Nigeria, narrowed to south eastern parts.

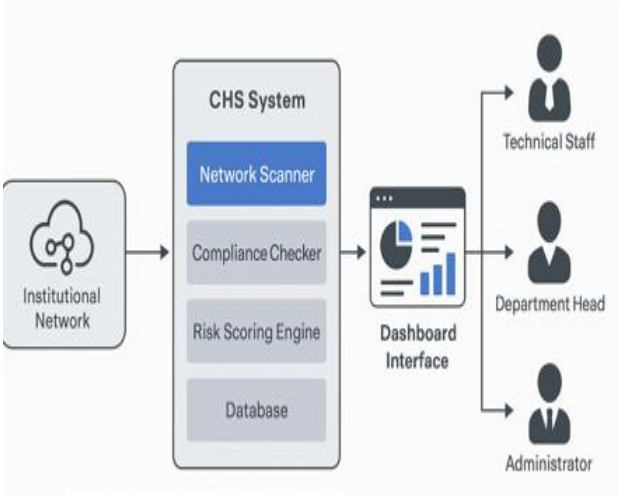
3.2 Population Sample

This research used a population sample size of ten (10) universities. From the ten universities, a selection of 40 information and communication technology administrators and other IT staff. They were randomly selected from 10 (ten) of the universities in south eastern parts of Nigeria, namely; Abia State University, Michael Okpara University of Agriculture, Imo State University, Odumegwu Ojukwu University, Enugu State University, University of Nigeria Nzukka, Ebony State University, Nnamdi Azikwe University, Federal University, Ndufu Alikwo and Federal University of Technology, Owerri. The

respondents are grounded in the field of IT support across academic divide. The respondents are responsible for formulating policies and actions aimed at safeguarding the sensitive information for their various higher institutional systems.

3.3 Methodology

The methodology follows the system architecture presented in figure 1. The **Cyber Hygiene Scan (CHS)** system is designed as a modular, network-based solution to evaluate and enhance cyber hygiene in educational environments.



Fig, 1: CHS System Architecture

The process follows the design and development of cyber hygiene scan which determines the vulnerability of network-based institutional systems. Then,follows the components parts such as network scanner module, compliance checker, risk scoring, the database and the dashboard as depicted in figure 1. These components collaborate to make informed decisions to the administrators and departmental heads.

a. Network Scanner Module

This module uses Nmap and OpenVAS to discover active devices, open ports, running services, and known vulnerabilities. Scans can be scheduled or triggered manually and are optimized for low-bandwidth and mixed-environment networks typical in educational settings.

b. Compliance Checker

This component is a rule-based compliance engine which evaluates endpoint configurations (e.g., patch levels, firewall status, antivirus presence) against defined institutional cyber security policies. The engine is extensible, enabling administrators to tailor checks to their specific IT governance frameworks.

c. Risk Scoring Engine

The system integrates CVSS (Common Vulnerability Scoring System) scores from vulnerability databases and combines them with contextual institutional priorities (e.g., exposed student records, open remote desktop ports) to calculate risk levels. Risks are categorized as low, medium, high, or critical.

d. Reporting and Visualization Dashboard

CHS includes a web-based dashboard built with Flask and React.js that presents scan results, compliance status, and risk scores in real time. Role-based access control ensures that technical staff, department heads, and administrators see relevant information only. Reports can be exported in PDF and CSV formats for audits and training purposes.

4. Experimental Results

In this research work, the dash board of the system was built and deployment was made following the universities security peculiarities on mostly their compromised educational facilities including database. CHS

was deployed on a virtualized Ubuntu server hosted within the campus data center. Docker Compose was used to orchestrate containers for the scanner, web app, database, and OpenVAS server. The system was tested in a real-world departmental network with over 280 active endpoints.

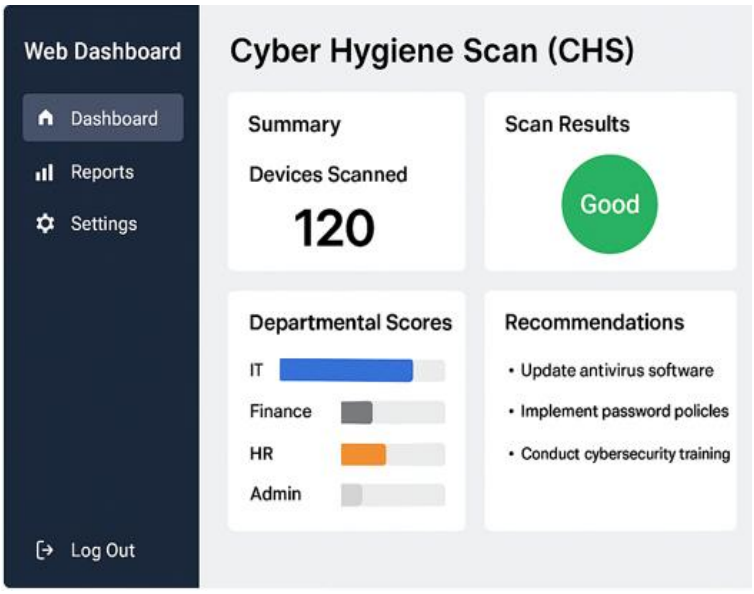


Fig.2: Web Dashboard Interface

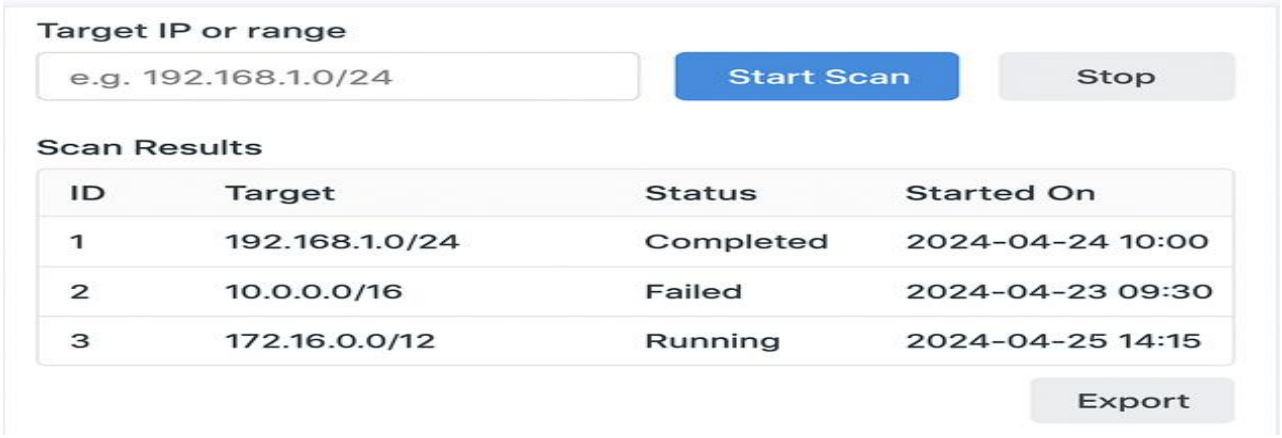


Fig. 3: The Net Scanner Interface

Fig. 4: Reporting and Visualization Dashboard

Fig. 5: Risk Scoring Engine

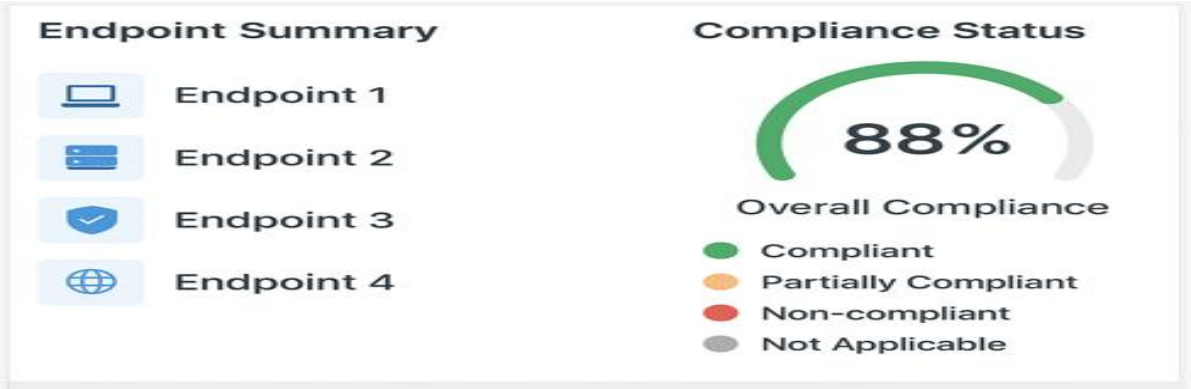


Fig. 6: The Compliance Checker

Table 1: Distribution of identified vulnerabilities by level of severity.

Severity Level	**Number of Findings**
Critical (CVSS ≥ 9)	31
High (CVSS 7–8.9)	87
Medium (CVSS 4–6.9)	112
Low (CVSS < 4)	68

5. Result Discussion

The evaluation of the CyberHygieneScan (CHS) system was conducted to assess its effectiveness, accuracy, usability, and overall impact on the cyber hygiene posture of educational institutions. The system was deployed in a real-world scenario within the Faculty of Physical Sciences at public Universities, targeting departmental networks, labs, and administrative offices. Over a period of four weeks, CHS was used to scan and analyze the

digital infrastructure, consisting of more than 120 endpoints including desktops, laptops, printers, routers, and servers. After the development of the network-based cyber hygiene scan as shown in figure 2, the pilot test shows summary of devices scanned (120), the result scan is good with recommendations for update of antivirus. The update on antivirus as detected by the application is imperative to prevent virus attacks. Another recommendation from the application is the creation of policy passwords to safeguard the systems against unauthorized users. Finally, the system recommended cyber security training for most of the staff to keep them updated with the current technology.The successful detection of nearly 200 vulnerabilities in a limited-scale institutional deployment underscores the latent cyber hygiene challenges present in typical educational networks among the universities educational systems.

Many of these vulnerabilities, particularly those classified as high or critical, could have facilitated unauthorized access, data breaches, or malware propagation had they remained undetected. After the vulnerability tests and recommendations, the system scanning is done through the net scanner interface shown in figure 4 for further checks. This region reflects the network-based systems based on their internet protocol address range. Any network system that falls into this address domain and bar would automatically be scanned to ascertain its health. Any system that failed during the scanning is termed to be on the red alert and informed decision is made by the application to correct the anomalies. The risk scoring dashboard shown in figure 5. retrieves CVE data from the OpenVAS feed and maps it to each identified vulnerability. The engine calculates a risk score using a weighted formula that includes:

- CVSS base score
- Asset criticality (defined by role, e.g., student records server)
- Network exposure (e.g., public vs. private IP)

Notably, over 40% of detected vulnerabilities were remediated within two weeks after CHS reports were circulated and acted upon by the departmental IT teams.

The final score shown in table 1 categorizes threats as **Low (0–3.9)**, **Medium (4.0–6.9)**, **High (7.0–8.9)**, or **Critical (9.0–10)**. figure 8 shows the compliance status of the scanned systems. The green light is an indicator of a full compliance with cyber security hygiene, the amber light shows a system that partially complies with the cyber hygiene while red light is a red flag that the system is not compliant in anyway to cyber scan hygiene. The implementation and evaluation of the CyberHygieneScan (CHS) system highlight several critical insights about cyber hygiene practices and the cybersecurity readiness of educational institutions. The applications deployment yielded significant improvements in vulnerability visibility, policy compliance, and user engagement factors that are often underdeveloped in resource-constrained academic environments. Feedback from institutional IT staff highlighted the systems' usability, especially the simplified risk breakdown and action-oriented remediation suggestions. Performance benchmarks showed:

- Average scan time: 3–7 minutes per 50 devices
- Risk score generation latency: < 5 seconds
- Dashboard response time: < 1.2 seconds under normal load

4.1 Post Tests by the IT Administrators

A post-deployment survey was administered to 40 IT staff and 6 administrative users. Key findings include:

91% of respondents found the dashboard intuitive and easy to navigate.

83% rated the vulnerability reports as useful for prioritizing remediation.

75% noted that CHS improved their understanding of institutional cyber risks.

Suggestions for improvement included expanding reporting granularity and adding customizable alert thresholds.

6. Conclusion

This paper presented the design, implementation, and evaluation of Cyber Hygiene Scan (CHS), a network-based system aimed at improving cyber hygiene practices in educational institutions. CHS addresses critical gaps in cyber security readiness by providing an integrated platform that combines vulnerability scanning, compliance assessment, risk scoring, and actionable visualizations. The system's modular architecture, reliance on open-source tools, and user-friendly dashboard make it specially suitable for deployment in resource-constrained academic environments.

The empirical evaluation demonstrated that CHS can significantly enhance an institution's cyber hygiene posture by identifying configuration weaknesses, facilitating rapid remediation, and raising awareness among IT staff and administrators. The system's deployment in a real-world educational setting resulted in measurable improvements in compliance scores and vulnerability reduction, underscoring its practical value. Its architecture emphasizes scalability, low-cost deployment, and usability, particularly in institutions with limited cyber security resources. CHS systematically scans networked assets, detects vulnerabilities, evaluates endpoint configurations, and aligns findings with institutional policies. It provides role-based access to results and recommendations through a secure web interface, thereby supporting both technical and non-technical stakeholders.

The design goal of CHS is to operationalize cyber hygiene practices by providing visibility into security gaps, quantifying risks, and recommending prioritized actions. The system's modularity allows institutions to adopt and scale CHS according to their network complexity, security maturity, and available infrastructure.

7.Acknowledgement

The authors wish to specially thank the vice chancellor of Abia State University, Uturu, Abia State Nigeria, Professor James Okeudo for his untiring efforts towards promoting staff development in the University

8. References

[1] American Cyber Defense Agency (2025). Cyber Hygiene Services

[2] Hadlington, L. (2021). *Cyber hygiene and the human factor: Addressing user behavior in cybersecurity*. Cyberpsychology, Behavior, and Social Networking, 24(5), 341–347. https://doi.org/10.1089/cyber.2020.0773

[3] Hadlington, L. (2021). *Cyber hygiene and the human factor: Addressing user behavior in cybersecurity*. Cyberpsychology, 15(3), 1–12. https://doi.org/10.1016/j.chb.2021.106897

[4] Ifeoluwa, E. (2024). Cyber Hygiene: Enhancing Cyber Hygiene Practices to

Mitigate Child Exploitation in the Online Environment. International Journal of Education and Social Science Research. 7(2), 273-278.

[5] Johnson, M., Green, J., & Adeyemi, T. (2021). Cybersecurity capacity in higher education:
An evaluation of organizational readiness. *Journal of Educational Technology & Society*, 24(1), 33–45.
https://www.jstor.org/stable/26915192

[6] Kaspersky. (2022). *The state of cybersecurity in education: 2022 report*. Retrieved from
https://www.kaspersky.com

[7] Kumar, V., & Sengupta, S. (2022). A modular threat detection system for public sector
cybersecurity. *International Journal of Cybersecurity Intelligence and Cybercrime*, 5(2),
45–59.

[8] National Institute of Standards and Technology (NIST). (2022). *Cybersecurity Framework*.
U.S. Department of Commerce.
https://www.nist.gov/cyberframework

[9] Onwubiko, D.C., Odikwa, H.N., Ukabuiro, I.K., & Agomah, S.A. (2025). Threat Intelligence Driven Detection Of CryptoCurrency Fraud: a Proactive Security Approach. Global Scientific Journal. 13(5), 406-413.

[10] Patel, R., & Morris, D. (2020). Evaluating open-source and proprietary tools for network
vulnerability assessment. *Cybersecurity Review*, 8(1), 11–20.

[11] Ponemon Institute. (2023). *Cost of a data breach report 2023*. IBM Security.
https://www.ibm.com/reports/data-breach

[12] Tang, S., & Lee, C. Y. (2023). Enhancing cybersecurity awareness in university students
through interactive simulations. *Journal of Information Security Education*, 17(1), 1–15.

https://jise.org/volume17/JISEv17n1p1.html

[13] Vigneswari, T., Pramila, S., Gomathi, V., & Madhumitha, M. (2025). Enhancing Cybersecurity in Educational Institutions: Challenges and Strategies. Researchgate. 32-66.