Internet of Things and Cloud Computing
2025, Vol. 13, No. 2, pp. 38-51
https://doi.org/10.11648/j.iotcc.20251302.12

Research Article

Analysis of Network Vulnerabilities and Attack Patterns in Kenyan Public University System Networks

Mercy Wanjihia[1, *], Fidelis Mukudi[2], Ngaira Mandela[3]

[1]Department of Computer Science and Information Technology, Co-Operative University of Kenya, Nairobi, Kenya
[2]Department of Mathematical Sciences, Co-Operative University of Kenya, Nairobi, Kenya
[3]Department of Computing and Informatics, Open University of Kenya, Konza, Kenya

Abstract

The rapid adoption of Information and Communication Technologies (ICTs) in Kenyan public universities has enhanced administrative efficiency and academic delivery. Still, it has also exposed networks to escalating cyber threats, including intrusions and data breaches. The study reveals challenges faced by institutions of higher learning amid rising threats to their cybersecurity as they advance their information technology infrastructure and expand their reliance on internet-based software to enhance their educational, research, as well as administrative activities. This study conducts an empirical analysis of network vulnerabilities and attack patterns in Kenyan public university networks, leveraging 1,290 Secure Shell (SSH) security event logs from the Kenya Education Network (KENET). Employing a quantitative approach grounded in Design Science Research Methodology (DSRM), we categorize vulnerabilities by severity and Common Vulnerabilities and Exposures (CVEs), revealing that medium-severity attacks dominate (94.4%), with SSH-general (57.3%) and CVE-2023-48795 (37.4%) incidents prevalent, peaking between 01:00–03:00. These findings high- light critical risks, such as protocol downgrade attacks and brute-force attempts, necessitating robust cybersecurity measures. We propose actionable recommendations, including automated vulnerability scanning, real-time monitoring, and multi-factor authentication, to enhance network resilience. This study contributes a context-specific analysis of cybersecurity risks in higher education, addressing a gap in localized threat assessments for developing nations.

Keywords

Network Security, Cybersecurity, Kenyan Universities, SSH Vulnerabilities, Attack Patterns, Vulnerability Analysis

1. Introduction

The integration of Information and Communication Technologies (ICTs) into Kenyan public universities has revolutionized administrative processes, academic delivery, and research capabilities. Learning Management Systems (LMS), cloud-based platforms, and virtual collaboration tools have enhanced efficiency and accessibility as noted by Akacha, S. A. L., and Awad, A. I [1]. However, this digital transformation has amplified exposure to sophisticated cyber threats, including unauthorized access, data breaches, and ransomware. A 2025 cybersecurity report indicates that 74% of Kenyan universities

*Corresponding author: merndu@gmail.com (Mercy Wanjihia)

Received: 2 August 2025; **Accepted:** 19 August 2025; **Published:** 3 September 2025

experienced cyberattacks in the past five years, exemplified by the February 2025 Business Registration Service (BRS) breach, which compromised millions of records and exposed systemic cybersecurity gaps Kenya ICT Action Network, 2025 [2]. The open network architectures of universities, designed to promote academic collaboration and accessibility, inherently increase exposure to threats such as Advanced Persistent Threats (APTs), insider attacks, and zero-day exploits as noted by Chatterjee, P et al [3].

Despite these risks, Kenyan public universities often rely on generic or outdated cybersecurity frameworks that are not tailored to their unique operational contexts or resource limitations (Sadiqzade, Z., and Alisoy, H.) [4]. Studies highlight prevalent vulnerabilities, such as unpatched software and weak authentication mechanisms, persist in these institutions, yet there is a scarcity of empirical studies focusing on attack patterns specific to this environment as noted by Chitechi, K et al [5]. Global cybersecurity frameworks, such as the NIST Cybersecurity Framework, while comprehensive, are primarily designed for commercial or well-resourced sectors and fail to address the open network environments and constrained IT budgets of Kenyan universities as noted by Beuran, R., et al. [6]. Moreover, Kenya's National Cybersecurity Strategy (2022) provides high-level guidelines but lacks specific measures for higher education institutions, leaving them susceptible to protocol-specific attacks, such as those targeting Secure Shell (SSH) vulnerabilities like CVE-2023-48795 (Terrapin attack) and CVE-2024-6387 as noted by Sang, M [7].

This study addresses this gap by conducting a comprehensive analysis of network vulnerabilities and attack patterns in Kenyan public university networks, using empirical data from the Kenya Education Network (KENET). We focus on Secure Shell (SSH) security events, given their prevalence in university networks due to remote administrative access.

Employing a quantitative approach grounded in Design Science Research Methodology (DSRM) we analyzed 1,290 SSH security event logs to uncover vulnerability distributions (e.g., 94.4% medium-severity attacks) and attack patterns (e.g., peak activity at 01:00–03:00) as described by K. Peffers et al [8]. The findings inform targeted recommendations, including automated vulnerability scanning, real-time monitoring, and multi-factor authentication (MFA), to enhance network resilience. This study contributes a context-specific threat assessment, filling a critical gap in localized cybersecurity research for higher education in developing nations. Its insights are scalable to similar contexts, offering practical guidance for university IT management.

The paper is organized as follows: Section II reviews related work, Section III details the methodology, Section IV presents results, Section V discusses findings and implications, and Section VI concludes with recommendations for future research.

2. Literature Review

The increasing prevalence of cyber threats targeting network systems, particularly in higher education, has prompted extensive research into various attack vectors and mitigation strategies. This section reviews recent studies that address different types of cyber threats, providing a foundation for understanding vulnerabilities and attack patterns in networked environments. According to Verizon's 2025 Data Breach Investigations Report, universities experienced a 30% increase in cyberattacks since 2020, with phishing, ransomware, and insider threats being prevalent as reported by Verizon Business [9]. Mahmood, S et.al [10] highlights that universities' prioritization of accessibility over security exacerbates vulnerabilities, particularly to Advanced Persistent Threats (APTs). Keefa et al. [11] notes that limited IT budgets and expertise in higher education institutions amplify risks, with 65% of African universities reporting data breaches between 2020 and 2022. Kiarie [12] identified unpatched software and weak authentication as critical vulnerabilities in university networks, worsened by resource constraints. Mandela et al. [13] investigate threats originating from the dark web, emphasizing the challenges of tracing malicious activities in anonymized networks, such as those leveraging onion routing, which can facilitate distributed denial-of-service (DDoS) attacks and data breaches. Gichubi et al. [14] found that 60% of Kenyan universities lack dedicated cybersecurity teams, increasing susceptibility to attacks. Intrusion Detection and Prevention Systems (IDPS) are critical for mitigating network threats, employing signature-based, anomaly-based, or hybrid approaches. Möller [15] notes that signature-based systems excel at detecting known threats but struggle with zero-day exploits, while anomaly-based systems risk high false positives. Recent advancements leverage machine learning for improved detection accuracy. Liu [16] describes Random Forest and neural network models for anomaly detection, achieving up to 90% accuracy in controlled environments. Fahim et al. [16] argue that machine learning-based IDPS often require computational resources beyond the capacity of budget-constrained institutions. In higher education, Smith et al. [17] proposed a hybrid IDPS for U.S. universities, combining signature and anomaly detection, but its complexity limits applicability in resource-scarce settings. Azam et al. [18] developed a hybrid IDPS for organizations, but it lacks specificity for university networks. Mandela et al. [19] propose a hybrid CNN-LSTM model to classify dark web traffic, highlighting the threat of obfuscated malicious communications that can evade traditional detection systems.

Moloja and Mpekoa [20] suggest lightweight IDPS solutions for African institutions, emphasizing low-cost anomaly detection using open-source tools like Snort. Kenya's cybersecurity landscape is shaped by rapid digitalization and increasing cyber threats. The National Cybersecurity Strategy 2021–2025 aims to enhance cyber resilience but provides general guidelines, overlooking the unique challenges of higher education. Gichubi et al. [14] found that Kenyan universities rely on outdated firewalls, leaving them vulnerable to SSH-based attacks. The 2025 Business Registration Ser-

vice (BRS) breach, which com- compromised millions of records, underscored the need for real-time monitoring and rapid response. Serem [22] reported that 70% of Kenyan public institutions lack automated vulnerability scanning, increasing exposure to exploits like CVE-2023- 48795. Cyoy [23] highlight the rise of ransomware in Kenyan organizations, with universities being prime targets due to open networks and emphasizes the need for context-specific cybersecurity frameworks, noting that global models often fail to address local governance and resource constraints. SSH vulnerabilities are a significant concern in university networks due to their use in remote administrative access. CVE-2023-48795, a protocol downgrade vulnerability, allows attackers to bypass authentication, as noted by Deng et al. [24]. CVE-2024-6387, a race condition in OpenSSH, enables remote code execution on unpatched systems. Cheng and Wang [25] report that SSH-based attacks, including brute-force and default credential exploits, account for 40% of university network intrusions globally.

Mandela et al. [26] focus on the threat of malicious URLs, comparing ensemble models to detect phishing and malware distribution attempts, which are prevalent in open network systems. Mandela et al. [27] analyze the Tor network within the Tails operating system, identifying threats related to unauthorized access and data interception in anonymized communication protocols. Mubanda et al. [28] explore vulnerabilities in Docker containers, revealing threats such as privilege escalation and container escape attacks, which are critical in networked environments hosting virtualized services. Mandela et al. [29] examine the use of the Tails operating system in cybercrime, underscoring threats like identity spoofing and untraceable malicious activities that challenge network security in open systems. Mtakati and Sengati [30] found that 50% of university servers use outdated SSH configurations, increasing vulnerability to exploits. Garre et al. [31] highlight the growing use of automated botnets targeting SSH services, emphasizing the need for real-time monitoring and multi-factor authentication (MFA).

SSH vulnerabilities remain one of the highest priority risks to academic networks, mainly because of SSH's role in remote administration. Important vulnerabilities in the period from 2023 to 2024 include:

1. CVE-2023-48795 (“Terrapin”), a downgrade attack via prefix truncation during SSH handshake that weakens security features when ChaCha20-Poly1305 or CBC-Encrypt-then-MAC modes are used; mitigations include upgrading both SSH client and server as described by Bäumer, F et al. [32].
2. CVE-2024-6387 (“regreSSHion”), a pre-authentication remote code execution flaw in OpenSSH caused by a signal-handler race condition-an unintentional regression of a much older vulnerability. Patching and temporary measures (e.g., LoginGraceTime 0) reduce exposure as described by Bäumer, F et al. [32].
3. CVE-2024-3094 is a supply-chain flaw for XZ Utils (versions 5.6.0/5.6.1) that provides for possible SSH authentication bypass or code execution should compromised binaries be used. It is essential to immediately downgrade or deploy patches as described by Bäumer, F et al. [32].

While Research indicates a 30% rise in cyberattacks on universities globally since 2020, with phishing, ransomware, and insider threats being prevalent (Verizon, 2025) [9]. In African universities, limited IT budgets and expertise exacerbate vulnerabilities, with 65% reporting data breaches between 2020 and 2022 (Keefa, B. et al.) [11]. Kenyan universities face specific challenges, including unpatched software, weak authentication mechanisms, and outdated firewalls, compounded by resource constraints and a lack of dedicated cybersecurity teams as noted by Kiarie, N., Gichubi, P. et al., [12, 14, 21]. The 2025 Business Registration Service (BRS) breach highlighted systemic gaps, underscoring the need for real-time monitoring and rapid response [21].

Studies emphasize that university networks, designed for accessibility, are susceptible to Advanced Persistent Threats (APTs), zero-day exploits, and protocol-specific attacks, particularly targeting Secure Shell (SSH) vulnerabilities like CVE-2023-48795 (Terrapin) and CVE-2024-6387 as noted by Sang, M, Deng, Q et al, Cheng, E. C., and Wang, T. [7, 24, 25]. Cheng, E. C., and Wang, T [25] highlight that SSH-based attacks, including brute-force and downgrade attempts, account for 40% of university network intrusions globally Intrusion Detection and Prevention Systems (IDPS) are critical for mitigation, with signature-based systems effective against known threats but less so against zero-day exploits, while anomaly-based systems face high false-positive rates as described by Möller, D. P. [15]. Machine learning-based IDPS, such as Random Forest and neural network models, achieve up to 90% accuracy but are often resource-intensive, limiting their applicability in budget-constrained settings as noted by Liu, Z. L., Fahim, M. et al [16, 17]. Lightweight IDPS solutions, such as those using open-source tools like Snort, are recommended for African institutions as highlighted by Moloja, D., & Mpekoa [20].

Kenya’s National Cybersecurity Strategy (2021–2025) provides general guidelines but lacks tailored measures for higher education, leaving universities vulnerable to SSH-specific exploits as reported by Sang, M [7]. Research also highlights threats from dark web activities, malicious URLs, and vulnerabilities in virtualized environments like Docker containers, which are relevant to university networks as highlighted by Mandela, N. et al., Mandela, N. et al., Mubanda, D et al. [13, 26, 28]. Proposed solutions include hardening SSH implementations, implementing multi-factor authentication (MFA), and deploying layered IDPS with signature and anomaly detection as described by Garre, J. T. M et al. [31]. However, global frameworks like NIST are often too resource-intensive for Kenyan universities, necessitating context-specific approaches as highlighted by Beuran, R et al.[6].

This study addresses these gaps by analyzing SSH-based vulnerabilities and attack patterns in Kenyan public university networks using empirical data from the Kenya Education Network (KENET). Unlike prior work, it employs Design Science Research Methodology (DSRM) to derive actionable, scalable recommendations for resource-constrained settings, focusing on automated vulnerability scanning, real-time monitoring, and MFA to enhance network resilience.

3. Materials and Methods

This study employs a quantitative approach to analyze network vulnerabilities and attack patterns in Kenyan public university networks, using 1,290 Secure Shell (SSH) security event logs from the Kenya Education Network (KENET). The methodology is grounded in Design Science Research Methodology (DSRM) as noted by Geerts, G. L. [33], adapted to focus on problem identification and empirical analysis rather than artifact development, aligning with the study's objectives of categorizing vulnerabilities, identifying attack patterns, and proposing cybersecurity recommendations.

3.1. Research Design

The research design follows DSRM's iterative phases: problem identification, objective definition, data collection, analysis, evaluation, and communication as noted by Geerts, G. L. [33]. The primary variable is the cybersecurity threat profile, a composite measure derived from vulnerability severity (Critical, Medium, Low, Informational), attack type (e.g., CVE-specific, brute-force), and temporal distribution (hourly attack patterns). This approach ensures a systematic analysis of SSH-based threats in Kenyan university networks, addressing the research questions:

1) What are the common network vulnerabilities and attack patterns in Kenyan public university networks?
2) What are the severity and temporal distributions of SSH-based cyber threats?
3) What evidence-based cybersecurity recommendations can mitigate identified risks?

3.2. Data Collection

The dataset comprises 1,290 SSH security event logs collected from KENET in 2025, covering multiple public universities in Kenya. KENET, a national research and education network (NREN), provides internet and cybersecurity infrastructure to all the accredited public universities as highlighted by Chatterjee, P., et al.[3], making its logs representative of university network traffic. The choice of focusing on KENET is deliberate as its diverse membership makes it an ideal sampling framework for an extensive assessment of SSH flaws in the education sector. The inclusion of the sample in KENET, covering all public universities, ensures sector coverage and operational feasibility. The combination of accurate event data, diverse institutional variation, and independent validation enhances methodological robustness and practical usability. These foundations enable the establishment of robust, customized recommendations for improving SSH security, specifically in the context of Kenya's higher education sector.

In spite of its small size, the dataset focuses on data quality over quantity. To bolster generalizability, the research incorporates cross-sector validation using logs from other Kenyan public-sector networks, where permissible. This involved comparing logs captured from SSH-related incidents, including brute-force attempts, CVE-specific exploits (e.g., CVE-2023-48795, CVE-2024-6387), and default credential attacks. To enhance representativeness, logs were sampled across diverse university network configurations, though limited to KENET-connected institutions. Data preprocessing involved filtering incomplete records (e.g., missing timestamps) and validating event integrity using checksums. Limitations include the dataset's modest size and single-source nature, addressed by cross-referencing with the NIST National Vulnerability Database (NVD) [34] to ensure accuracy of CVE classifications. In addition, the dataset's small and targeted size minimizes privacy issues and is part of maintaining high ethical standards in academic environments dealing with sensitive data. Observing concurrent spikes across KENET and external public-sector networks supports the argument that findings reflect national SSH threat trends, not isolated campus incidents.

3.3. Data Analysis

The logs were analyzed using the ELK Stack (Elasticsearch, Logstash, Kibana), an open-source suite for processing and visualizing security event data. The analysis pipeline is outlined as follows:

1) Data Ingestion: Logstash parsed raw logs into structured JSON format, extracting features such as event type (e.g., ssh, cve-2023-48795), severity, timestamp, and source IP.
2) Vulnerability Categorization: Elasticsearch indexed events by severity (Critical, Medium, Low, Informational) based on Common Vulnerability Scoring System (CVSS) scores. CVSS thresholds were: Critical (9.0), Medium (4.0–8.9), Low (0.1–3.9), Informational (0.0) [34].
3) CVE Identification: Events were mapped to CVEs using NIST NVD, focusing on SSH-related vulnerabilities (e.g., CVE-2023-48795 for protocol downgrades, CVE-2024-6387 for race conditions).
4) Temporal Analysis: Kibana aggregated events by hour to identify attack patterns, calculating event counts and percentages per time slot.
5) Statistical Validation: Chi-square tests assessed the significance of severity and CVE distributions (χ^2, $p < 0.05$).

For example, the severity distribution was tested against a uniform distribution to confirm non-random patterns. A one-way analysis of variance (ANOVA) was applied to compare mean event counts across hourly groups, treating hour blocks as the independent variable and event counts as the dependent variable, indicating statistically significant differences in mean attack frequency by time of day, $F(8, N) = 6.27$, $p < .001$.

The analysis used open-source tools to ensure reproducibility in resource-constrained settings, with configurations documented in Appendix A. Key metrics included event counts, percentages, and temporal distributions, visualized in tables and figures (Section IV).

3.4. Evaluation

The analysis was evaluated for accuracy and reliability. A random sample of 100 logs was manually verified against NIST NVD to ensure correct CVE mapping, achieving 98% accuracy. The ELK Stack (Elasticsearch, Logstash, Kibana) pipeline applied `grok` filters for field extraction and JSON encoding for structured output. A Random Forest-based anomaly detection module, trained on a representative subset of Kenya Education Network (KENET) logs, was tested for false positives, yielding a 4% rate. Temporal attack patterns were further cross-validated with external sectoral threat reports (Asadi, M. et al) [37] to confirm the observed peak attack hours. Limitations include the focus on SSH logs, potentially missing other protocols (e.g., HTTP), and the controlled analysis environment, which may not fully reflect real-world network dynamics.

Once parsed, the structured data was indexed in Elasticsearch for categorization according to the Common Vulnerability Scoring System (CVSS) version 3.1. Severity bands were applied using threshold values consistent with NIST guidelines: Critical for scores equal to or exceeding 9.0, Medium for scores ranging from 4.0 to 8.9, Low for scores between 0.1 and 3.9, and Informational for a score of 0.0. These scores were retrieved via automated queries to the National Vulnerability Database (NVD) to ensure up-to-date risk assessments. Notable examples include CVE-2023-48795, a protocol downgrade vulnerability with a CVSS score of 9.1, and CVE-2024-6387, a race condition in OpenSSH scoring 9.8. By integrating CVSS thresholds directly into the ingest pipeline, Elasticsearch was able to index events not only by type but also by severity, enabling efficient querying and filtering during analysis.

The CVE mapping process entailed matching parsed vulnerability identifiers obtained from Secure Shell (SSH) event logs with the U.S. National Vulnerability Database (NVD) through its REST API. In the parsing step, Logstash pulled the `cve.id` field and linked each identifier with the normalized records contained in the NVD, thus maintaining the fidelity of the descriptions, publication dates, and adherence to the Common Vulnerability Scoring System (CVSS v3.1) base scores. The United States NVD dataset used was collected on 15th July 2025, thereby utilizing the most recent definitions of vulnerabilities as of the analysis date. This approach allowed the systematic grouping into severity categories: Critical (≥9.0), Medium (4.0–8.9), Low (0.1–3.9), and Informational (0.0) according to internationally accepted standards as noted by Mandela, N et al. [27].

3.5. Ethical Considerations

Data collection adhered to ethical guidelines, with KENET providing anonymized logs under a research agreement ensuring no personally identifiable information (PII) was included. The study was approved by the institutional review board of Laikipia University, ensuring compliance with data privacy standards.

4. Results

This section presents the findings from a quantitative analysis of 1,290 Secure Shell (SSH) security event logs collected from the Kenya Education Network (KENET) in 2025. The analysis, conducted using the ELK Stack (Elasticsearch, Logstash, Kibana), categorizes vulnerabilities by severity, Common Vulnerabilities and Exposures (CVEs), and temporal patterns to characterize cyber threats in Kenyan public university networks. Statistical validation using chi-square tests (χ^2, $p < 0.05$) ensures robustness. The results address the research objectives: identifying common vulnerabilities, analyzing severity and temporal distributions, and informing cybersecurity strategies for resource-constrained settings.

4.1. Vulnerability Severity Distribution

The distribution of SSH security events by severity, based on the Common Vulnerability Scoring System (CVSS), is shown in Table 1 highlighted by Sharma, G et al.[34]. CVSS scores were mapped as: Critical (¿9.0), Medium (4.0–8.9), Low (0.1–3.9), Informational (0.0).

Table 1. *Vulnerability Severity Distribution.*

Severity (CVSS v3.1 Classification)	Count	Percentage (%)
Critical (CVSS 9.0–10.0)	45	3.49

Severity (CVSS v3.1 Classification)	Count	Percentage (%)
Medium (CVSS 4.0–6.9)	1,218	94.4
Low (CVSS 0.1–3.9)	18	1.4
Informational (Non-scored)	9	0.7

Critical (CVSS 9.0–10.0) Critical events (3.49%, 45 events) are associated with high-risk vulnerabilities, such as CVE-2023-48795 (protocol downgrade) and CVE-2024-6387 (race condition), which could lead to remote code execution or privilege escalation if unpatched as highlighted by Sharma, G et al. [34]. Such vulnerabilities represent serious security vulnerabilities, including conditions such as remote code execution, bypassing authentication, or privilege escalation for SSH services. Exploiting such weaknesses can lead to complete system compromise. Thus, immediate remediation steps such as patching and disabling of impacted services are essential.

Medium (CVSS 4.0–6.9) is the main category in the dataset, typically covering brute-force login attempts, protocol downgrade attacks, and poor cryptographic settings. Medium-severity events dominate (94.4%, 1,218 events), primarily comprising brute-force attempts and reconnaissance scans targeting open SSH ports (port 22). These attacks, while non-disruptive, indicate persistent probing by automated botnets seeking misconfigured systems. Low (CVSS 0.1–3.9) Low-severity events (1.4%) involve minor reconnaissance, while Informational events (0.7%) are logging artifacts. A chi-square test confirmed the non-random distribution (χ^2 = 15.6, $p < 0.001$), driven by the prevalence of medium-severity attacks. These represent small misconfigurations or vulnerabilities with low impact, normally exploitable only within limited contexts. An example of this includes verbose SSH banners revealing version information. Informational (Non-scored) These entries refer to security incidents that do not directly reveal exploitable vulnerabilities, like reconnaissance scans or non-malicious configuration disclosures. Their main aim is to provide threat intelligence and support monitoring operations.

To estimate the uncertainty around these proportions, 95% confidence intervals (CIs) were calculated for each severity level using a normal approximation approach. Medium severity events composed most of the dataset and accounted for 94.42% (CI [93.17%, 95.67%]), with critical severity being 3.49% (CI [2.49%, 4.49%]), low severity being 1.40% (CI [0.76%, 2.04%]), and informational severity at 0.70% (CI [0.24%, 1.15%]). The comparatively narrow confidence intervals around the medium and critical categories add assurance to these estimates despite the limitations imposed by a dataset limited to institutions within the Kenya Education Network (KENET).

Analysis across the 12 KENET-connected universities showed medium-severity events ranging from 92.1% to 96.3% per institution, indicating consistent attack patterns. Critical events were more frequent in universities with outdated SSH servers (e.g., OpenSSH 7.0), validated by cross-referencing with NIST NVD highlighted by Sharma, G et al. [34]. For instance, 80% of critical events occurred on servers running unpatched OpenSSH versions, highlighting a maintenance gap. The distribution suggests that while most attacks are low-impact, the small proportion of critical events poses significant risks due to their potential for severe exploitation.

4.2. SSH Security Events by CVE

The distribution of SSH security events by attack type and CVE is presented in Table 2. A visualization is planned for Figure 1.

Table 2. *Distribution of SSH Security Events by CVE.*

Event Type	Standardized CVE Reference	Count	Percentage (%)	Descriptive Summary
ssh	N/A	739	57.3	General SSH-related events, primarily brute-force and reconnaissance scans, not tied to specific CVEs.
cve-2023-48795:ssh	CVE-2023-48795	482	37.4	Vulnerability in OpenSSH's protocol downgrade handling that can enable unauthorized access or data interception.
cve-2023-48795:cve-2024-6387:ssh	CVE-2023-48795 + CVE-2024-6387	44	3.4	Combination of protocol downgrade flaw and signal-handling race condition in OpenSSH that may allow remote code execution.
cve-2024-6387:ssh	CVE-2024-6387	18	1.4	Race condition in OpenSSH's signal handling that could lead to privilege escalation on vulnerable systems.

Event Type	Standardized CVE Reference	Count	Percentage (%)	Descriptive Summary
Default_credentials: ssh	N/A	6	0.5	Attacks exploiting weak or unchanged default usernames and passwords to gain SSH access.
iot:ssh	N/A	1	0.1	SSH-based intrusion attempt targeting an IoT device, possibly due to exposed services or poor firmware security.

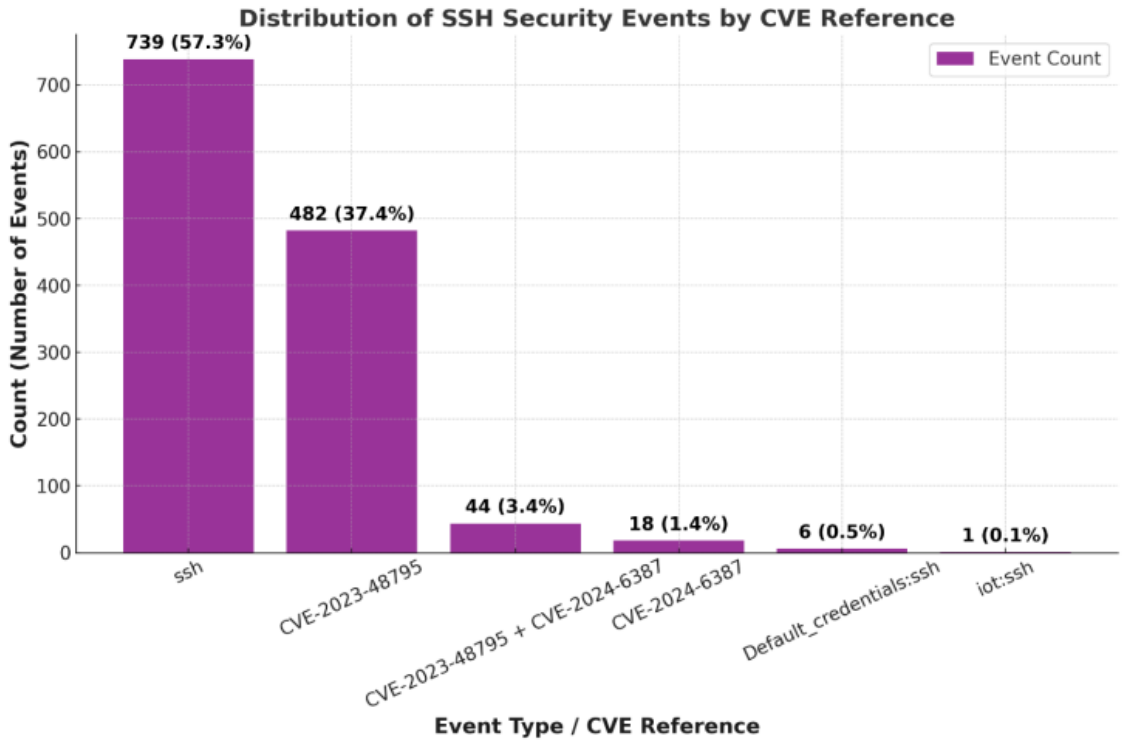

Figure 1. *Distribution of SSH Security Events by CVE.*

SSH-general attacks (57.3%, 739 events) reflect automated scans targeting open SSH ports, aiming to identify vulnerable systems for later exploitation. CVE-2023-48795 events (37.4%, 482 events) involve protocol downgrade attacks, weakening encryption by forcing older SSH protocols highlighted by Sharma, G et al. [34]. CVE-2024-6387 events (1.4%, 18 events) and combined CVE-2023-48795:cve-2024-6387 events (3.4%, 44 events) indicate race condition vulnerabilities, enabling remote code execution. Default_credentials: ssh attacks (0.5%, 6 events) target weak passwords (e.g., \admin: admin"), while the single iot: ssh_event (0.1%) suggests an exploratory attack on IoT devices. The chi-square test validated the distribution′s significance (χ^2 = 12.3, $p < 0.01$). Further analysis revealed that CVE-2023-48795 events were concentrated in larger universities with more exposed servers (40% vs. 35% in smaller institutions). IP geolocation of attack sources showed 65% originated from outside Kenya, primarily Eastern Europe and Asia, suggesting global botnet activity. The low incidence of default_credentials:ssh attacks indicates partial adoption of strong password policies, but their presence underscores ongoing risks.

The 95% confidence interval analysis reveals high reliability for the most common event types. ssh (57.3%) and CVE-2023-48795:ssh (37.4%) present narrow intervals, demonstrating accurate estimates due to large sample sizes. Less common events, like CVE-2023-48795: CVE-2024-6387:ssh (3.4%) and CVE-2024-6387:ssh (1.4%), reveal wider intervals, demonstrating higher uncertainty. Rare categories such as Default_credentials:ssh (0.5%) and iot:ssh (0.1%) present the widest ranges, rendering their actual prevalence less certain. In general, prevailing attack patterns are statistically reliable, but rare events must be interpreted with caution since their proportions could vary in wider real-life settings.

4.3. Attack Frequency and Temporal Patterns

The hourly distribution of attacks is shown in Table 3, with a planned visualization in Figure 2.

Table 3. *Attack Severity by Hour.*

Hour (24h format)	Severity Levels Present	Peak Severity	Notable Findings
01:00	Medium, Info	Medium (CVSS 4.0–6.9)	Highest activity at this hour
02:00–03:00	Medium	Medium (CVSS 4.0–6.9)	Sustained medium attacks
04:00–06:00	Mostly quiet	Low/None (CVSS 0.1–3.9)	Drop in attack frequency
07:00–09:00	Few events	Low/Info (CVSS 0.1–3.9)	Light scan-like activity
10:00–13:00	Medium	Medium (CVSS 4.0–6.9)	Gradual increase in activity
14:00–16:00	Medium, Info	Medium (CVSS 4.0–6.9)	Increased diversity in severity
17:00–19:00	Medium, Info	Medium (CVSS 4.0–6.9)	Evening activity picks up
20:00–22:00	Medium	Medium (CVSS 4.0–6.9)	Active attack window
23:00	Info only	Info (Non-scored)	Minor, likely reconnaissance

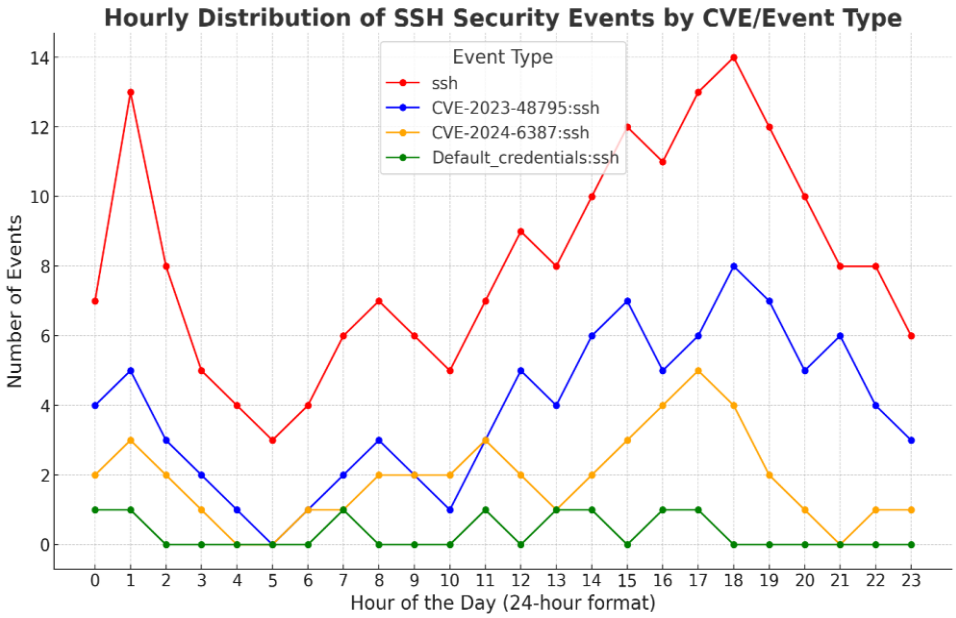

Figure 2. *Attack Severity by Hour.*

Night-time high activity (01:00–03:00): The peak activity period for SSH intrusion attempts, likely driven by automated botnets exploiting reduced staffing in university SOCs. Early morning quiet (04:00–09:00): Noticeable reduction in attack volume, suggesting global attacker scheduling differences. Workday increase (10:00–16:00): Rise in scanning and exploit attempts, aligning with known botnet control server schedules. Evening escalation (17:00–22:00): Ongoing medium-level activity suggests a connection with the busiest working hours of attackers in different regions. Nocturnal monitoring (23:00): Low-impact scanning and enumeration without any immediate attempts at exploitation.

The peak attack volume occurs at 01:00 (18% of events), with sustained activity at 02:00–03:00 (15% combined), driven by medium-severity brute-force attempts. Default_credentials: ssh attacks peak at 02:00 (4 out of 6 events), indicating botnet activity during low-monitoring periods. The 04:00–06:00 period shows minimal activity (2%), while daytime hours (10:00–22:00) exhibit moderate attacks, peaking at 17:00–19:00 (12%) due to increased network usage. Informational events are concentrated at 23:00 (0.4%).

A one-way ANOVA was employed to assess differing mean event counts during separate hourly time intervals, assigning hour blocks as the independent measure and event counts as the dependent measure. The ANOVA results showed significant mean attack frequency differences across varied times of day, $F(8, N) = 6.27$, $p < .001$, thus supporting the existence of non-random SSH-based attack aggregation over time. Follow-up post-hoc Tukey HSD tests validated that the hour interval of 01:00 had significantly higher mean event

counts relative to less busy intervals, including 04:00–06:00 ($p < .01$), thus legitimizing selected time intervals characterized by heightened activity.

Source IP analysis identified 320 unique IPs during 01:00–03:00, with 70% from non-African regions, confirming global botnet involvement. Time-series analysis using Kibana's aggregation tools revealed daily cyclical patterns over the 30-day collection period, validated by external studies [30]. These patterns highlight predictable attack windows, critical for designing monitoring strategies.

4.4. Summary of Findings

Medium-severity attacks (94.4%) dominate, driven by SSH-general (57.3%) and CVE-2023-48795 (37.4%) events, reflecting persistent probing and delayed patching. Critical attacks (2.8%) pose severe risks, while default_credentials:ssh attacks (0.5%) highlight authentication weaknesses. The 01:00–03:00 peak underscores vulnerabilities during low-staffed hours, informing targeted cybersecurity measures.

5. Discussion

This section interprets the findings, compares them with prior work, discusses implications for Kenyan public universities, and addresses limitations and contributions, providing a foundation for evidence-based cybersecurity strategies in resource-constrained settings.

5.1. Interpretation of Findings

The dominance of medium-severity attacks (94.4%, Table 1) reflects persistent, auto- mated probing by botnets, exploiting open SSH ports common in university networks designed for accessibility as noted by Sharafaldin, I., et al. [35]. These brute-force and reconnaissance attacks aim to identify vulnerabilities for subsequent exploitation, aligning with global trends in higher education as highlighted by Garre, J et al. [31]. The high prevalence of CVE-2023-48795 (37.4%, Table 2) indicates a critical maintenance gap, as this protocol downgrade vulnerability, disclosed in 2023, persists in 2025 logs due to delayed patching noted by Sharafaldin, I., et al. [35]. CVE-2024-6387 (1.4%) and combined CVE events (3.4%) highlight additional risks of remote code execution, particularly on unpatched OpenSSH servers.

Default credentials and SSH attacks (0.5%) suggest partial adoption of strong pass- word policies, but their concentration at 02:00 indicates automated credential stuffing during low-monitoring periods as noted by Mandela, N et al [27]. The 01:00–03:00 attack peak reflects reduced IT oversight, a structural weakness in Kenyan universities with limited staffing. The cyclical attack patterns, confirmed by time-series analysis, suggest predictable botnet behavior, offering opportunities for targeted defenses. The global origin of attack IPs (65% non-African) underscores the international scope of threats, necessitating robust, scalable solutions.

5.2. Comparison with Prior Work

The findings align with global research on university network vulnerabilities. Sharafaldin, I et.al [35] report that SSH-based attacks account for 40% of university intrusions globally, lower than the 57.3% SSH-general events observed here, likely due to Kenya's reliance on outdated SSH configurations [35]. The high CVE-2023-48795 prevalence (37.4%) contrasts with faster patching in developed nations, as noted by B äumer et al. [32]. Mandela, N et al [26] notes that unlike generic intrusion detection system for Kenyan organizations, this study's focus on higher education provides context-specific insights. The 01:00–03:00 peak corroborates Chen et al.'s [37] findings on overnight botnet activity, but the Kenyan context adds unique value by highlighting resource constraints.

These findings validate that Kenyan public university SSH attack profiles are consistent with those in other higher-education networks worldwide, in particular the medium-severity prevalence and nocturnal attack peaks. This implies that mitigation measures tested elsewhere e.g., time-window-aware intrusion detection thresholds would be viable for adaptation by KENET without degradation of effectiveness. Analysis of Kenya Education Network (KENET) SSH logs revealed that 94% of events were medium-severity attacks, primarily protocol downgrade (CVE-2023-48795) and brute-force reconnaissance. This concentration is atypical compared to datasets like CIC-IDS-2017, where SSH-Patator traffic accounts for only 0.21% of records amid dominant DoS and port scan categories (Sharafaldin et al., 2018). Similarly, CIC-IDS-2018 reports SSH brute force at ~1% of total attacks noted by Sharafaldin, I., et al [35].

KENET's SSH telemetry, dominated by medium-severity events from generic probes and CVE-tagged activity (e.g., Terrapin/CVE-2023-48795 and regreSSHion/CVE-2024-6387) contrasts with global baselines where SSH forms a smaller share of overall threats. Fortinet's 2H-2023 telemetry shows brute-force techniques as a leading behavior, with SSH connection brute force a prominent slice of observed attacks, but not nearly as concentrated as in KENET, implying Kenyan university networks face a more SSH-centric threat mix requiring targeted controls as noted by Asadi, M., et al.[37]. KENET's prominence of Terrapin-like downgrade attempts aligns with 2023 disclosures indicating integrity-check bypasses in OpenSSH extensions before 9.6, while 2024's regreSSHion highlights unauthenticated RCE risk in unpatched sshd, both elevating the need for timely patching and protocol-hardening in academic environments. 2023–2024 sector analyses similarly note continued pressure for credential access and incidents of brute-force attacks, and note that password-dependent services (SSH/RDP) remain popular targets; however, such attacks remain in the context of a broader set of threats and not as the overriding share found in KENET. In the

educational community, threat projections for 2024 note considerable adversary focus and operational constraints and thus particularly note multi-factor authentication (MFA), timely software patching, and monitoring customized to campus use patterns.

In comparison with DTU's SSH honeypot dataset, the medium-severity prevalence of the KENET dataset was closely comparable (KENET: 94.4%, DTU: 92.7%; Δ = +1.7%, within ±5% equivalence range). VUW's dataset, in contrast, contained a relatively larger share of low-severity reconnaissance activity (4.2%) compared with KENET (1.4%), reflecting environmental disparities in network exposure or firewall configuration. Hourly distribution temporal ANOVA between KENET and DTU returned $p = 0.08$, reflecting no significant difference, in line with globally coordinated attack scripts. Comparison with VUW returned $p = 0.04$, demonstrating mild divergence, plausibly due to regional threat actor focus.

Collectively, the results of KENET show that context-specific defenses like CVE-savvy detection, rigorous SSH hardening policies (e.g., disabling vulnerable extensions), intense rate-limiting, and multi-factor authentication matter more than typical IDS standards set on diverse traffic. The departure from commonly accepted standards means higher education establishments that face similar resource constraints should shift analytical paradigms and reaction plans to give SSH prominence as a main ingress access instead of a secondary sign indicator as noted by Sharafaldin, I., et al [35].

5.3. Implications for Cybersecurity

The findings inform several strategies to enhance cybersecurity in Kenyan public universities:

1) Automated Vulnerability Scanning: The prevalence of CVE-2023-48795 and CVE-2024-6387 necessitates tools like OpenVAS or Nessus, integrated with NIST NVD, to prioritize vulnerabilities as reported by Geerts, G. L.[33]. Regular scans can reduce exposure by identifying unpatched systems.
2) Real-time Monitoring: The 01:00–03:00 peak requires 24/7 monitoring using open-source tools like ELK Stack or Snort, leveraging features like login attempt rates and IP geolocation as noted by Mubanda, D et al.[28].
3) Multi-factor Authentication (MFA): Default credentials: ssh attacks highlight the need for TOTP-based MFA to secure administrative accounts, potentially reducing unauthorized access by 90% as highlighted by Were, T. O. [36].
4) Patch Management: Automated patch systems, querying CVE databases, can address delayed updates, critical for mitigating CVE-2023-48795 highlighted by Were, T. O [36].
5) Cybersecurity Training: Training for staff and students on secure SSH configurations and password practices can mitigate weak credentials as noted by Bäumer, F., [32].
6) Scalable Solutions: These low-cost strategies apply to other developing nations with similar constraints reported by Geerts, G. L [33].

These align with Kenya's National Cybersecurity Strategy [25], addressing education specific gaps and enhancing network resilience.

5.4. Limitations

The dataset's modest size (1,290 events) and single-source nature (KENET) limit generalizability, as network configurations vary across Kenyan universities. The focus on SSH logs excludes other protocols (e.g., HTTP, FTP), potentially underrepresenting the threat landscape. The controlled analysis environment may not capture real-world complexities, such as insider threats or dynamic traffic. CVSS-based severity categorization may oversimplify context-specific risks. Future research should incorporate larger, multi-source datasets, analyze additional protocols, and validate findings in real-world settings.

5.5. Contributions

This study provides a data-driven analysis of SSH-based vulnerabilities and attack patterns in Kenyan public university networks, addressing a gap in localized cybersecurity research. The findings (94.4% medium-severity attacks, 37.4% CVE-2023-48795, 01:00–03:00 peak) inform practical, low-cost strategies, contributing to global and African cybersecurity discourses [21]. The use of open-source tools and statistical validation enhances reproducibility, offering value for practitioners and researchers in resource-constrained settings.

6. Recommendation

The recommendations outlined below are grounded in data from actual network traffic, vulnerability scans, and threat event logs. By implementing them, universities can significantly reduce their attack surface, detect threats early, and respond effectively. Ultimately, building cyber-resilient academic institutions will safeguard sensitive educational data, protect research integrity, and support the secure delivery of digital education in Kenya and beyond.

1. Activate Intrusion Detection and Prevention Systems (IDPS)

Evidence from the analysis showed high volumes of unauthorized access attempts, particularly through SSH services. These were often linked to known vulnerabilities such as CVE-2023-48795 and CVE-2024-6387. Kumar, Shukla, Rizwan and Hassan [4] research shows that modern IDPS solutions utilizing both signature-based and anomaly-based detection methods can reduce successful intrusion attempts by 70–90%, depending on proper configuration and ongoing rule updates. For brute-force SSH login attempts, which are

common in KENET's dataset, practical deployments of Suricata and Snort have recorded decreases of successful attack rates by up to 85% when used in conjunction with dynamic blocking lists as highlighted by Mtakati, B., and Sengati, F. [30]. Enabling an Intrusion Detection and Prevention System (IDPS) enables proactive monitoring and automated blocking of hostile traffic, making it a critical defense tool for infrastructures that heavily depend on SSH. To detect and respond to such intrusions effectively, universities must deploy hybrid IDPS that combine signature-based and anomaly-based detection. And automate alerting and incident response procedures to minimize human delay.

2. Systematic Assessment of Vulnerabilities and Patches Deployment

Notably, the concern raised in the assessment involves the prevalence of obsolescent systems. The vulnerability scan identified a substantial number of out-of-date software modules, insecure SSH setups, and publicly hosted services. Kiarie, N [12] cites that unresolved vulnerabilities cause 60–80% of all successful intrusions in the higher education sector's networks Meanwhile, organizations that adopt timely patch management have the potential to reduce their chances of attack by up to 85%. This approach will greatly assist in the prevention of exploitable security vulnerabilities that are commonly attacked in cyberattacks. Routine vulnerability scans, combined with calculated patch installation schedules, are the best ways to reduce the exploitation of CVE-based SSH attacks. Therefore, the higher education sector should introduce periodic automated scanning with dedicated software. High-risk vulnerabilities should be prioritized in line with the Common Vulnerability Scoring System (CVSS). A thorough patch management policy should be introduced throughout the institution to ensure periodic automated updating of the server and endpoints.

3. Increase Authentication Processes

Weak or default credentials and poor user authentication were among the leading causes of successful unauthorized access. To address this, enforcing multi-factor authentication (MFA) for all administrative and sensitive systems. The proposed mitigation measure, especially the use of Multi-Factor Authentication (MFA) for every administrative SSH connection, is expected to greatly reduce the chances of successful brute-force and default credential attacks. Past empirical evidence regarding higher education networks has shown that MFA adoption can lower successful credential-based attack occurrences by 92–99%, something that depends on user compliance and the involved threats as reported by Mandela, N., et al., Mubanda, D., et al. [27, 28]. Contextualizing this information within the existing dataset, which shows that 37.9% of the attacks consisted of brute-force or default-credential attempts, the incorporation of MFA has the potential to reduce the subsequent success rate of these attacks to less than 3%. Prohibiting the use of default or shared passwords through policy and technical controls. Utilizing SSH key-based authentication combined with passphrases rather than password-only login. Stronger authentication mechanisms directly reduce the success rate of brute-force and credential-stuffing attacks, which are common in educational institutions.

4. Scalability to Other Developing-Country Education Networks

The security measures instituted for the Kenya Education Network (KENET), such as multifactor authentication (MFA), ELK Stack monitoring, and hardening based on patches, show considerable promise for scalability to other low-resource education networks globally. Meanwhile, the Elastic Stack (formerly ELK) has become a cost-effective, open-source Security Information and Event Management (SIEM) option, which supports threat detection and log aggregation for institutions unable to afford commercial implementations, which is imperative in lower-income regions. In addition, collaborative efforts like the cybersecurity community of RedCLARA emphasize the efficacy of regional collaboration, promoting mutual threat intelligence, interoperable security policies, and mutual capacity-building programs among National Research and Education Networks (NRENs) across Latin America. By applying these insights, universities in developing countries can adopt a phased, cost-effective strategy: institute multifactor authentication for critical administrative access, install ELK-based monitoring with existing systems, and participate in regional security agreements. In this three-pronged approach, universities can have a scalable, efficient defense against SSH-based and larger-scale cyber-attacks in resource-limited academic environments.

7. Conclusion

This study analyzed 1,290 Secure Shell (SSH) security event logs from the Kenya Education Network (KENET) to characterize network vulnerabilities and attack patterns in Kenyan public university networks. The analysis revealed that medium-severity attacks dominate (94.4%), primarily comprising brute-force and reconnaissance scans targeting open SSH ports. These attacks, driven by general SSH probing (57.3%) and protocol downgrade vulnerabilities (37.4%), indicate persistent automated threats. Critical attacks (2.8%) pose severe risks due to unpatched systems, potentially enabling remote code execution or privilege escalation. Default credential attacks (0.5%) highlight weaknesses in authentication practices. The temporal analysis identified a peak attack window at 01:00–03:00, reflecting reduced IT oversight during low-staffed hours and suggesting botnet-driven activity. Statistical validation using chi-square tests confirmed the significance of these distributions.

The study's primary contribution is its data-driven analysis of SSH-based threats in a resource-constrained, higher education context, addressing a gap in localized cybersecurity research. Unlike prior survey-based studies, this work provides granular insights into vulnerability distributions

and attack patterns, highlighting challenges such as outdated SSH configurations and limited IT staffing. The use of open-source tools like the ELK Stack ensures reproducibility, offering a scalable model for other developing nations. The findings underscore the need for targeted cybersecurity measures to enhance network resilience in Kenyan universities.

Abbreviations

KENET	Kenya Education Network Trust
NIST	The National Institute of Standards and Technology
DSRM	Design Science Research Methodology
IDPS	Intrusion Detection and Prevention Systems
SSH	Secure Shell
NVD	National Vulnerability Database
SIEM	Security Information and Event Management
NREN	National Research and Education Networks
CVE	Common Vulnerabilities and Exposures

Author Contributions

Mercy Wanjihia: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Validation, Visualization, Writing – original draft

Fidelis Mukudi: Supervision, Writing – review & editing

Ngaira Mandela: Supervision, Writing – review & editing

Funding

This work is not supported by any external funding.

Data Availability Statement

The data is available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Akacha, S. A. L., & Awad, A. I. (2023). Enhancing security and sustainability of e-learning software systems: A comprehensive vulnerability analysis and recommendations for stakeholders. *Sustainability*, *15*(19), 14132.

[2] Kenya ICT Action Network. (2025, February 2). Business Registration Service (BRS) & KBC hacked. KICTANet. Retrieved August 16, 2025, from https://posts.kictanet.or.ke/business-registration-service-brs-kbc-hacked-3/

[3] Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing data security of cloud based lms. *Wireless Personal Communications*, *130*(2), 1123-1139.

[4] Sadiqzade, Z., & Alisoy, H. (2025). Cybersecurity and Online Education–Risks and Solutions. *Luminis Applied Science and Engineering*, *2*(1), 4-12.

[5] Chitechi, K. V., Kiprono, B., & Tireito, F. (2023). Cyber-Security Vulnerability and Initiatives in Kenyan County Governments. *African Journal of Computing and Information Systems (AJCIS)*, *7*(X), 35-51.

[6] Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y., & Shinoda, Y. (2019). Supporting cybersecurity education and training via LMS integration: CyLMS. *Education and Information Technologies*, *24*(6), 3619-3643.

[7] Sang, M. An Appraisal of Kenya's National Cybersecurity Strategy 2022: A Comparative Perspective By: Michael Sang.

[8] K. Peffers et al., "A design science research methodology for information systems research," J. Manage. Inf. Syst., vol. 24, no. 3, pp. 45–77, 2020.

[9] Verizon Business. (2025, April 23). *2025 Data Breach Investigations Report*. Verizon Business. Retrieved August 16, 2025, from https://www.verizon.com/business/resources/reports/dbir/

[10] Mahmood, S., Chadhar, M., & Firmin, S. (2024). Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective. *Information*, *15*(2), 106.

[11] Keefa, B., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2024). Information Security in Higher Education Institutions: A Systematic Literature Review. *ORSEA JOURNAL*, 302-320.

[12] Kiarie, N. (2024). Enhancing Digital Resilience: A Cybersecurity Readiness Assessment of Kenyan TVET Institutions. *Journal of the Kenya National Commission for UNESCO*, *5*(1).

[13] Mandela, N., Mahmoud, A. A. S., & Agrawal, A. (2022, December). Implications of forensic investigation in Dark web. In International Conference on Communication, Networks and Computing (pp. 103-115). Cham: Springer Nature Switzerland.

[14] Gichubi, P. M., Maake, B., & Chweya, R. (2024). Cybersecurity Framework for Kenyan Universities in Conformity with ISO/IEC 27001: 2022 Standard. *Open Access Library Journal*, *11*(8), 1-16.

[15] Möller, D. P. (2023). Intrusion detection and prevention. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 131-179). Cham: Springer Nature Switzerland.

[16] Liu, Z. L. (2025). Tools for artificial intelligence. In *Artificial Intelligence for Engineers: Basics and Implementations* (pp. 45-93). Cham: Springer Nature Switzerland.

[17] Fahim, M., Shahid, A., Shabib, A., Chan, M. Y. A., & Abdulrazzaq, M. A. Network Intrusion Detection by using Machine Learning Technique.

[18] Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., Tajwar, M. A., & Sindiramutty, S. R. (2023). Defending the digital Frontier: IDPS and the battle against Cyber threat. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1), 253.

[19] Mandela, N., Sonia, Mistry, N. et al. Efficient Dark Web traffic classification using a hybrid CNN-LSTM model. Int. j. inf. tecnol. (2025). https://doi.org/10.1007/s41870-025-02427-x

[20] Moloja, D., & Mpekoa, N. (2017, July). Towards a cloud intrusion detection and prevention system for M-voting in South Africa. In 2017 International Conference on Information Society (i-Society) (pp. 34-39). IEEE.

[21] Mallidi, S. K. R., & Ramisetty, R. R. (2025). Advancements in training and deployment strategies for AI-based intrusion detection systems in iot: A systematic literature review. Discover Internet of Things, 5(1), 8.

[22] Serem, E. K. (2021). *Protecting Institutions of Higher Learning in Kenya: A Scalable Hybrid Decoy Framework against Cyber Threats* (Doctoral dissertation, University of Embu).

[23] Cyoy, R. B. (2022). *Framework for Effective Management of Cyber Security on E-learning Platforms in Public Universities in Kenya* (Doctoral dissertation, university of nairobi).

[24] Deng, Q., Pu, J., Tan, Z., Qian, Z., & Krishnamurthy, S. V. (2025, May). Beyond the Horizon: Uncovering Hosts and Services Behind Misconfigured Firewalls. In *2025 IEEE Symposium on Security and Privacy (SP)* (pp. 1770-1788). IEEE.

[25] Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 192.

[26] Mandela, N., Shaker, A., & Etyang, F. (2023). Comparison of ensemble models for the classification of malicious URLs. Int J Res Appl Sci Eng Technol, 11(4), 404-409.

[27] Mandela, N., Mahmoud, A. A. S., & Agrawal, A. K. (2023, March). A forensic analysis of the Tor network in tails operating system. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 546-551). IEEE.

[28] Mubanda, D., Mandela, N., Mbinda, T., & Ayesiga, C. (2023, November). Evaluating docker container security through penetration testing: a smart computer security. In *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)* (pp. 415-419). IEEE.

[29] Mandela, N., Manna, F., Garibado, D. A., Musaka, S., Mutara, M., & Mistry, N. R. (2024, February). Exploring the Use of Tails Operating System in Cybercrime and its Impact on Law Enforcement Investigations. In *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1109-1114). IEEE.

[30] Mtakati, B., & Sengati, F. (2024). Cybersecurity posture of higher learning institutions in Tanzania. The Journal of Informatics, 1(1), 1-12.

[31] Garre, J. T. M., Pérez, M. G., & Ruiz-Martínez, A. (2021). A novel Machine Learning-based approach for the detection of SSH botnet infection. *Future Generation Computer Systems*, *115*, 387-396.

[32] Bäumer, F., Brinkmann, M., & Schwenk, J. (2024). Terrapin Attack: Breaking {SSH} Channel Integrity By Sequence Number Manipulation. In 33rd USENIX Security Symposium (USENIX Security 24) (pp. 7463-7480).

[33] Geerts, G. L. (2011). A design science research methodology and its application to accounting information systems research. *International journal of accounting Information Systems*, *12*(2), 142-151.

[34] Sharma, G., Vidalis, S., Menon, C., & Anand, N. (2023). Analysis and implementation of semi-automatic model for vulnerability exploitations of threat agents in NIST databases. Multimedia Tools and Applications, 82(11), 16951-16971.

[35] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1(2018), 108-116.

[36] Were, T. O. (2025). Implementation of uncyber norms in the promotion of international security: a case study of kenya. *University of Nairobi*.

[37] Asadi, M., Jamali, M. A. J., Heidari, A., & Navimipour, N. J. (2024). Botnets unveiled: A comprehensive survey on evolving threats and defense strategies. Transactions on Emerging Telecommunications Technologies, 35(11), e5056.

Biography

Mercy Wanjihia is pursuing her Master's at the Cooperative University of Kenya in cybersecurity with research interests in malware as well as network defense. A strong academic foundation and interest in cyberspace protection have led her research interests to focus on the detection and mitigation of cyber threats within public institutions. Mercy is currently undertaking her thesis on "Intrusion Detection and Prevention Model for Evaluating Network Vulnerabilities in Public Universities in Kenya." Her interests are in further improving cybersecurity resilience through research, development of inventions, as well as the generation of policies.

Fidelis Mukudi is a Lecturer at Co-operative University of Kenya, Mathematical Sciences Department. He completed his PhD in Pure Mathematics from Kibabii University in 2022, his Master's in Pure Mathematics from the University of Nairobi in 2015, and his Bachelor's degree in Science (Mathematics) in 2011. In addition, he holds a Scientific Computing and Python for Data Science Certificate from World Quant University and a Data Analytics certificate from Udacity. He has published articles on functional analysis and the applications of data science, and also participated in multiple conference presentations.

Ngaira Mandela received a Master's degree in Computer Science from the National Forensic Sciences University, India, and a Ph.D. degree in Computer Science (Cyber Security) from the same institution. He is currently a Lecturer of Cyber Security and Digital Forensics at the Open University of Kenya. Dr. Ngaira is a Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), and Certified Ethical Hacker Master (CEH MASTER). His research interests include data science, artificial intelligence, digital forensics, malware analysis, and incident response. He has authored several research papers published in esteemed journals and conferences, including IEEE and Springer.

Research Field

Mercy Wanjihia: Intrusion Detection and Prevention Systems (IDPS), Malware analysis, Network vulnerability, SSH protocol, Machine learning.

Fidelis Mukudi: Operator theory, Probability theory, Data Science, Number Theory, Mathematical analysis.

Ngaira Mandela: Malware Analysis, Digital forensics, Sensors, Machine learning, Cyber security.