INTRUSION DETECTION AND PREVENTION MODEL FOR EVALUATING NETWORK VULNERABILITIES IN PUBLIC UNIVERSITIES IN KENYA.

WANJIHIA MERCY NDUTA

A THESIS SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY IN THE SCHOOL OF COMPUTING AND MATHEMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN CYBERSECURITY OF THE CO-OPERATIVE UNIVERSITY OF KENYA

2025

DECLARATION

This thesis is my original work and has not been presented for the award of a degree in any other University or for any other award

Signature: _____ Date: ____21/11/2025_____

Mercy Nduta Wanjihia

C005/600058/2023

Declaration by Supervisors

We confirm that the work reported in this thesis was carried out by the candidate under our supervision and has been submitted with our approval as university supervisors

Signature ……. Date……21/11/2025…….

Dr. Fidelis Mukudi

Department of Mathematical Sciences

Cooperative University of Kenya

Signature ……. Date……21/11/2025…….

Dr. Ngaira Mandela

Department of Computing and Informatics

Open University of Kenya

DEDICATION

To my father, and in loving memory of my late mother. To my supervisors, for their guidance, knowledge, and support, this work honors you all.

ACKNOWLEDGEMENT

First and foremost, I thank the Almighty God for granting me the strength, health, and perseverance throughout this academic journey. My deepest gratitude goes this university and to my supervisors, Dr. Fidelis Mukudi and Dr. Ngaira Mandela, for their outstanding guidance, mentorship, and encouragement throughout the course of this research. Their expertise, constructive feedback, and patience greatly enriched the quality of my work and provided invaluable insights that shaped this thesis. I sincerely appreciate the time and effort they invested in reviewing my drafts and steering me in the right academic direction.

I also extend my sincere gratitude to the Kenya Education Network Trust (KENET) for providing the empirical data that formed the foundation of this study. Access to this data was instrumental in the successful completion of my research and in ensuring that the study was grounded on real-world evidence. Without their combined support and contribution, this work would not have been possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

ABBREVIATION AND ACRONYMS

IDPM	Intrusion Detection and Prevention Model
IT	Information Technology
AI	Artificial Intelligence
ML	Machine Learning
DDoS:	Distributed Denial of Service
DSRM	Design Science Research Methodology
SIEM	Security Information and Event Management
NIST	The National Institute of Standards and Technology
SOC	Security Operations Centers
KENET	Kenya Education Network Trust
TOE	Technology-Organization-Environment
BYOD	Bring Your Own Device
RFC	Random Forest Classifier
DTR	Decision Tree Classifier
LOGREG	Logistic Regression
KNC	K-Nearest Neighbors Classifier Classifier
SVC	Support Vector Classifier

DEFINITION OF TERMS

Vulnerability: A vulnerability refers to a flaw that cybercriminals can take advantage of to gain unauthorized access to a computer system.

Attack Frequency: This term refers to the count of cyberattacks or intrusion attempts that take place on a network over a certain timeframe.

Vulnerability Severity: This refers to how much risk or potential damage a particular security vulnerability or flaw could bring to a network if someone takes advantage of it.

System Availability: This refers to the percentage of time that a computer system, network, or service is up and running, ready to be used whenever it's needed.

Response Time: Response time refers to how long it takes for a network to respond to a request made by a user or another system.

Statutory Government Regulations: The discussion of law and legal obligation is concerning the regulations enacted by a legislative or government entity that must be obeyed by all, including organizations, institutions, and persons.

Human Factors: Refers to the attributes of individuals that impact their interaction with systems, technologies, environments, and processes. Cognitive, psychological, and physical attributes are the major focus areas in this domain.

Technological Factors: This concerns the many implementations, structures, breakthroughs, and electronic architecture that are vitally integral to determining how well an organization's operations are functioning, how secure they are, and how likely they are to expand, particularly in the spaces of information technology and cybersecurity.

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 due to rising threats to their cybersecurity as they advance their information technology infrastructure. The main goal of this study was to develop a model for Intrusion Detection and Prevention in the field of cybersecurity aimed at evaluating and mitigating the network-related attacks faced by public universities in Kenya. This study adopted the Design Science Research Methodology and focused on security incident data extracted from the Kenya Education Network (KENET). An empirical analysis was conducted on network vulnerabilities and attack patterns in Kenyan public university networks, leveraging Secure Shell (SSH) and security event logs. Employing a quantitative approach, this study categorized 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 a.m. These findings, which highlighted critical risks, such as protocol downgrade attacks and brute-force attempts, necessitating robust cybersecurity measures. The initial training on Logistic Regression, Decision Tree Classifier, Support Vector Machine, Random Forest classifier, and K-nearest Neighborhood classifier, which led to overfitting. Synthetic data of the same size as the original data (1290 responses) was created and used to create a stacking model. The model included Logistic Regression, K-nearest Neighborhood classifier, and Random Forest classifier. The stacking model had an accuracy of 0.9516, recall of 0.9516, precision of 0.9522 and a f1-score of 0.9420. The mean probability of having an attack was 2.24%, 95.66%, 1.03% for critical, medium and low severity, respectively and 1.07% chance of having an information. The permutation feature importance revealed that the attack cve-2023-48795;cve-2024-6387; ssh which corresponded to critical severity and had 14% highest impact to the model . Overall, the tag, algorithm type, password authentication method and the city of location of the server were critical to the model performance contributing to a percentage of about 41.38%,17.24%, 13.80% and 10.34% respectively amounting to about 82.76%. The proposed actionable recommendations included automated vulnerability scanning, real-time monitoring, and adoption of the model to strengthen cybersecurity strategies to enhance network resilience.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

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 (Akacha and Awad, 2023). However, this digital transformation has amplified exposure to sophisticated cyber threats, including unauthorized access, data breaches, and ransomware. Institutional reliance upon digital infrastructures has significantly increased over recent years, and most notably in education. Learning institutions throughout the world protect valuable research data, intellectual property, and personal information and, as such, find themselves ideal targets for cyber-attacks. Threat vectors in the form of unpatched software, misconfigured services, and remote access-related vulnerabilities have been more severely taken advantage of, even in resource-rich situations. At the same time, intrusion detection and prevention (IDP) systems have evolved, and most recent studies have focused on hybrid models combining signature-based detection and machine learning, deep learning, and anomaly detection to combat zero-day attacks and the maturing profile of threats (Amouri, Al Rahhal, Bazi, Butun, & Mahgoub, 2024).

Geographically, Africa has seen increased cybersecurity threats in the education sector, as institutions have weak defenses in most cases. Studies show that commonly used research datasets, including public datasets (e.g., NSL-KDD, UNSW-NB15), do not necessarily reflect campus-network heterogeneity, including BYOD (bring-your-own-device) instances, guest networks, and heterogeneous device types. Scientists in Tanzania built campus-network-specific datasets from live traffic as well as honeypot simulations to better detect in university environments (Sindika, Nicholaus, et al, 2025). Moreover, new IDS models custom-tuned to context, including feature selection and balancing schemes, have shown promise in balancing accuracy and false positives (Kenya, UNESCO journal, 2023).

Locally in Kenya, cyber threat numbers have increased significantly. The Communications Authority's reports indicated high numbers of threats to education, government, finance, and

telecom segments. Kenya in 2024 lost billions of shillings to cybercrime; attacks often take advantage of poor password habits, lagged patching, and poorly secured network settings (The Star, 2024). Notable academic instances involved social media hacking of university sites and stolen credentials at institutions such as Kabarak University (2023), revealing reputational vulnerability and incident response and preparedness gaps ("Kabarak University Cyber-Attack", 2023). Additionally, research on e-learning sites in Kenya built deep-learning-based intrusion/mitigation models reaching 99.8% accuracy, indicating high stakes for sites increasingly utilized during and post-COVID-19 shift (Musyimi, Mwangi, & Njagi, 2023). A cybersecurity report indicated that 74% of Kenyan universities 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).

Emergent trends involved growing sophistication in attacks (such as AI-assisted phishing or social engineering), expansion in number of threats, increased focus on feature-based detection, and growing interest in authentic, campus-grounded datasets instead of common benchmarks. Confounding problems, however, still abound: few institutions have advanced detection/prevention systems, inadequate in-place expertise, poor policies supporting patch management, a lack of constant ongoing monitoring, and commonly low budgeting. Societal imperatives involved threats to students' privacy, erosion of trust in case of breaches, interruption of academic business, and loss of public trust in institutions of learning.

The identified trends make it prudent to develop a customized Intrusion Detection and Prevention Model (IDPM) suitable for public universities in Kenya. The model draws from empirical data providers such as the campus network or KENET, draws from both signature and anomaly detection methodologies, takes into consideration infrastructural as well as institutional constraints, and lastly incorporates operational, governance as well as policy frameworks for sustainable responsiveness and implementation.

1.2 Statement of the Problem

Higher education institutions have witnessed alarming increases in cybersecurity threats in recent years, and universities worldwide have been vulnerable to losing sensitive information, research

integrity, and valuable ICT infrastructure. Intrusion detection and prevention have been progressive worldwide based on hybrid methods, machine learning, and artificial intelligence deployments; however, most have been experimental or based on benchmark datasets, which do not reflect in practice the dynamic and heterogeneous nature of operational university networks. This leaves a knowledge gap, in that outcomes from these studies could not automatically translate effectively to practical deployments (Aldhaheri et al., 2022; Singh et al., 2023).

At the regional level, in Africa, previous research pointed to underfunded ICT infrastructures, poor institutional policy, and few localized datasets as prevailing characteristics. Though promise has been demonstrated in initiatives representing honeypot-based data gathering and adaptive models of intrusion detection, these have been in isolation and to a great degree limited to pilot or single-institution deployment. This represented a contextual gap, inasmuch as prevailing models lack scalability or adaptability to heterogeneous institutional contexts (Akinbohun et al., 2022; Mhlongo & Mutemwa, 2024).

In Kenya, there have been rising cyberattacks in public universities, including credential theft, Distributed Denial of Service (DDoS) attacks, and outages of services. Nevertheless, previous research focused on e-learning systems or collective, national-scale incident reporting. There have been few studies providing an empirically-grounded, personalized intrusion detection and prevention model specific to public university operational experience. Additionally, there have been models available which focused on detection and, less commonly incorporated, hybrid, in-real-time prevention and response (Nzioka et al., 2021; Mwangi & Wabwoba, 2023).

In this regard, there was a need to formulate an Intrusion Detection and Prevention Model (IDPM) tailor-made to network vulnerability measurement and mitigation in Kenya's public institutions of learning. This research bridged the existing gap through undertaking an in-depth investigation of attack behavior and network vulnerabilities, specifically in Kenyan public university networks, using empirical data from Kenya Education Network (KENET). An overriding focus was placed on the security events of Secure Shell (SSH), which were found to be highly dominant in the university networks due to the need for remote administrative access. This suggested model purported to meet the gaps faced through the utilization of empirical data from Kenya Education Network (KENET), with both detection and predictive features, and ensured alignment with

national and institutional cybersecurity frameworks to enhance scalability and sustainability (KENET, 2025; Omondi et al., 2024).

1.3 Objectives of the Study

1.3.1 General Objectives

The main aim of this study was to develop a cybersecurity intrusion detection and prevention model for evaluating network vulnerabilities in public Universities in Kenya. The main objective was guided by the following specific objectives;

1.3.2 Specific Objectives

i. To identify common vulnerabilities, analyze severity and temporal distributions, and inform cybersecurity strategies for resource-constrained settings.

ii. To develop an intrusion detection and prevention model tailored for public Universities in Kenya

iii. To validate the cybersecurity intrusion detection and prevention model.

1.4 Research Questions

The researcher seeks to find answers to the following questions;

(i) What were the common network vulnerabilities analysis of severity and temporal distributions, and information on cybersecurity strategies for resource-constrained settings in Kenya?

(ii) What was the intrusion detection and prevention model tailored for public Universities in Kenya based on the current vulnerabilities and cybersecurity threats?

(iii) Is the intrusion detection and prevention model viable for solving the current cybersecurity threats and vulnerabilities of systems in Kenyan Public Universities?

1.5 Significance of the Study

The public universities in Kenya are increasingly relying on digital infrastructure, internet connectivity, and interconnected systems to support instructional activities, research activities, and administrative functions. However, these institutions face growing cybersecurity threats, including

unauthorized access, instances of malware, and exploitation of vulnerabilities in systems. The absence of tailor-made and effective security measures has made most universities vulnerable to threats, which affect data integrity, the availability of services, and the overall reputation of the campus.

Intrusion Detection and Prevention Model (IDPM) development specific to public Kenyan universities became critical in providing an anticipatory framework for identifying, understanding, and neutralizing cyber threats. The model would not only correct current vulnerabilities but also identify and neutralize potential new attack behaviors in advance.

By assessing tangible network attacks and the convergence of both detection and preventative measures, the research ensured public institutions have the evidence-based tools required for safeguarding critical infrastructure. The research bridged the gap between the international methods, which often rely on surrogate data, and the real-world realities of public universities in Kenya. As such, the research formed a valuable resource for science and research academics, researchers, and public policy makers from development nations wishing to implement contextually appropriate measures for intrusion prevention and detection. Aside from this, the recent study stood out especially as it serves towards bridging the critical information security gaps confronting public universities in Kenya, which form critical centers for research, innovation, and knowledge. In coming up with an Intrusion Detection and Prevention Model (IDPM), this research makes an essential contribution to protecting critical academic, administrative, and research information from damaging cyber-attacks and illicit access.

This study provided operational guidelines to universities to examine and mitigate vulnerabilities in the network, as part of an effort to strengthen data security, ongoing services, and organizational resilience. In Universities and for ICT Administrators, the study provided a model aimed at enhancing the resilience of institutional cybersecurity, protecting sensitive academic information, and ensuring the continuity of teaching, research, and administration activities. University staff, students, and the academic stakeholders as end-users could also benefit from the more secure access to the digital learning spaces, administration systems, and research databases, supporting increased confidence in information and communication technologies. Future researchers, this study serves as both an empirical and methodological foundation for future research into

cybersecurity for Africa-based higher education institutions. Additionally, this research significantly contributes to the field of cybersecurity by developing an empirical model that can inform future investigations and be tailored for implementation in other similar institutions within the region. This model aimed to protect sensitive information while fostering a dynamic research and academic setting.

1.6 Scope of the Study

This research only attempted to develop an Intrusion Detection and Prevention Model (IDPM) as a way to identify and prevent vulnerabilities in Kenyan public university networks. The research concentrated on investigating university network cybersecurity threats in an environment, tackling head-on vulnerabilities in SSH services, authentication, and frequently exploited Common Vulnerabilities and Exposures (CVEs). The dataset utilized to attempt this exploration was from Kenya Education Network (KENET), as an empirical evidence base of network traffic, instances of intrusion attempts, and system vulnerabilities. The study focused on key cybersecurity concepts, including network vulnerabilities, intrusion detection mechanisms, intrusion prevention strategies, and real-time monitoring. The focus was limited to network-based attacks and their preventive measures, whose primary objective is ensuring safe, reliable, and fault-tolerant information and communication technologies infrastructure in public universities.

1.7 Limitation of the study

Whilst this study provided significant contributions to improving cybersecurity responses in Kenya's public universities, it did not come without certain limitations. In the first instance, the study made use of empirical findings drawn from KENET, which did not cover all vulnerabilities within individual universities, thereby limiting the scope of the findings' applicability. Secondly, the study concentrated more on network-based intrusion avoidance and detection mechanisms without fully expanding on an analysis of threats drawn from physical security breaches, insider threats, or user activities, all of which may have an overriding impact on the entire cybersecurity profile. Moreover, due to the fast-changing nature of cyber-attacks, vulnerabilities, or attack behaviors observed in an investigation may soon become dated, necessitating ongoing updates to the model.

1.8 Delimitation of the study

To focus and make this study feasible and methodically sound, it was necessary to circumscribe this research in several key respects. First, for example, while cybersecurity incidents and vulnerabilities were examined via the monitoring system provided by KENET, it should be noted that this study did not examine security information generated or measured inside each public university individually. This distinction was overcome because it was ensured that this dataset was large enough to represent and characterize general network traffic and its dominant SSH-based attacks shared universally by all institutions.

Second, to make the study more specific and manageable to conduct and analyze, its scope is further delimited to network-layer intrusion detection and prevention techniques to avoid concerns associated with physical security violations, insider attacks, human behavior analysis, or attacks at the endpoint level. To validate this limitation, this study clarified its scope on operational SSH security and network vulnerabilities as part of its operational objectives while admitting that its overall security context may include additional requirements for administration or physical security measures beyond its network-layer security parameters for protection against intrusion attacks.

Thirdly, the study was limited by the dynamic nature of threats posed by cyber threats because the findings may not cover or address vulnerabilities associated with particular time frames for data collection. To overcome this limitation or delimitation of the study, machine learning methodologies such as permutation feature importance and modularity were adopted to facilitate further training of new machine learning models using new data. By adhering to these delimitations, it ensured that the study allowed for clarity and analysis to remain at its foundations while being situated within real-life boundaries.

.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter provided a critical review of the current literature regarding intrusion detection and prevention, highlighting its usage in the context of higher educational institutions. The increased prevalence of cyber-attacks directed against network systems, especially as concerns the scope of higher educational institutions, has been a catalyst for significant research into several attack vectors and matched preventative measures. Advanced cybersecurity research is no longer confined to discussing attacks at a generic level but now encompasses analysis of specific indicators like Common Vulnerabilities and Exposures (CVEs), severity scores, attack temporal profiles, and cryptographic features, to name just a few, all offering detailed information on attacks and their development cycles in cyberspace.

This analysis reviews the role of CVE-based vulnerability analysis and its evolution as a crucial element of cybersecurity analysis for identifying vulnerabilities associated with widely adopted services like SSH through standardized scoring solutions for cybersecurity threats like those uncovered by studies investigating scoring frameworks based on CVSS scores. Additionally, analyses of temporal properties of cyber-attacks have demonstrated that cyber threats tend to operate on definite cycles measured by hours or seasons informed by automation attacks, geographical attacks, and exposure hours of the targeted systems. Another crucial aspect is analysis of features of cryptography protocols such as authentication protocols or key exchange algorithms for distinguishing between genuine and malicious activities associated with intrusion attempts. The last section of this chapter provides insights derived from comparative analyses for answering any unresolved questions or gaps found within previously conducted studies regarding CVEs, severity distributions, and temporal relationships details within Kenyan public universities, because of their unavailability or scarcity of data-driven empirical analyses. This served as a basis for this study because it addressed new concerns regarding intrusion detection and prevention to meet prevailing requirements using actual network traces. This chapter reviewed recent studies addressing a variety of cyber-attack forms, providing a foundation for understanding vulnerabilities and attack trends characteristic of networked settings. The review began with a

general overview before refining the scope of the examination into the regional case of Africa, before focusing exclusively on the case of Kenya. Critical trends, unresolved questions, and societal issues characteristic of network vulnerabilities served as the subjects of analysis. The comparative evaluation of extant studies appears first, followed by the presentation of gaps this research aims to address.

2.2 Perspectives on Intrusion Detection and Prevention

At the global level, post-secondary institutions are increasingly the target of cybercrime due to the vast online worlds, research databases, and open networks. Colleges and universities are often seen as a "soft target," which included valuable intellectual property, student data, and financial systems located within big and comparatively open structures (Razaque et al., 2022).

The latest advances in intrusion prevention and detection systems (IDPS) highlighted enhancements in both adaptability and accuracy. Signature-based traditional techniques came into criticism by failing to detect zero-day vulnerabilities (Khraisat, et al 2021). Accordingly, interest arose in the latest hybrid systems utilizing a fusion between anomaly detection and machine learning-based strategies. For instance, Amouri, et al (2024) introduced ensemble techniques utilizing Kolmogorov–Arnold Networks (KANs), which significantly increased detection rates for emerging threats. The Verizon 2025 Data Breach Investigations Report revealed that universities have faced a 30% increase since 2020 in cyberattacks, including widespread prevalence of phishing, ransomware, and insider threats as indicated by Verizon Business. Mahmood, S et al.(2024) highlight the fact that universities prioritizing accessibility over security render them more vulnerable, significantly against Advanced Persistent Threats (APTs). Keefa et al.(2024) indicated how limited IT budgets and scarcity of expertise among higher learning institutions widened vulnerabilities, with a total of 65% of African universities falling victim to data breaches from 2020 up to 2022.

Despite these developments, reliance on well-established benchmark datasets, such as KDD-Cup, CICIDS2017, and UNSW-NB15, remained a limitation, as these datasets all too often fail to depict the dynamic complexities of the university network environments (Samarasinghe, Tissera, & Gamage, 2022). This condition created a gap between the results of experiments and their applicability in real environments. Kiarie (2024) identified unpatched software and weak

authentication as critical vulnerabilities in university networks, worsened by resource constraints. Mandela et al. (2023) investigated 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.(2024) 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 (2023) noted 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 leveraged machine learning for improved detection accuracy. Liu described Random Forest and neural network models for anomaly detection, achieving up to 90% accuracy in controlled environments. Fahim et al. 2022 argued that machine learning-based IDPS often required computational resources beyond the capacity of budget-constrained institutions. In higher education, Smith et al. proposed a hybrid IDPS for U.S. universities, combining signature and anomaly detection, but its complexity limited applicability in resource-scarce settings. Azam et al. developed a hybrid IDPS for organizations, but it lacked specificity for university networks. Mandela et al.2025 proposed a hybrid CNN-LSTM model to classify dark web traffic, highlighting the threat of obfuscated malicious communications that could evade traditional detection systems. Moloja and Mpekoa (2017) suggested 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 aimed to enhance cyber resilience but provided general guidelines, overlooking the unique challenges of higher education. Gichubi et al. 2024 found that Kenyan universities relied on outdated firewalls, leaving them vulnerable to SSH-based attacks. The 2025 Business Registration Service (BRS) breach, which compromised millions of records, underscored the need for real-time monitoring and rapid response. Serem 2021 reported that 70% of Kenyan public institutions lack automated vulnerability scanning, increasing exposure to exploits like CVE-2023-48795. Cyoy 2022 highlighted the rise of ransomware in Kenyan organizations, with universities being prime targets due to open networks, and emphasized 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 2025. CVE-2024-6387, a race condition in OpenSSH, enables remote code execution on unpatched systems.

The open network architectures of universities, designed to promote academic collaboration and accessibility, inherently increases exposure to threats such as Advanced Persistent Threats (APTs), insider attacks, and zero-day exploits, as noted by Chatterjee, P et al. 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. 2025). Studies highlighted prevalent vulnerabilities, such as unpatched software and weak authentication mechanisms, that 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. 2025. Global cybersecurity frameworks, such as the NIST Cybersecurity Framework, while comprehensive, were primarily designed for commercial or well-resourced sectors and fail to address the open network environments and constrained IT budgets of Kenyan universities (Beuran, R., et al.2019) 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, et al 2023). .

Cheng and Wang 2022 reported that SSH-based attacks, including brute-force and default credential exploits, accounted for 40% of university network intrusions globally. Mandela et al 2022. focused 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.2023 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. explored 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 2023. examined 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 2024 found that 50% of university servers use outdated SSH configurations, increasing vulnerability to exploits. Garre et

al. highlighted 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.2024.
2. CVE-2024-6387 (“regreSSHion”), a pre-authentication remote code execution flaw in OpenSSH caused by a signal-handler race condition unintentional regression of a much older vulnerability. Patching and temporary measures (e.g., LoginGraceTime 0) reduce exposure as described by Bäumer, F et al. 2024.
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.2024.

While Research indicated a 30% rise in cyberattacks on universities globally since 2020, with phishing, ransomware, and insider threats being prevalent (Verizon, 2025). In African universities, limited IT budgets and expertise exacerbate vulnerabilities, with 65% reporting data breaches between 2020 and 2022 (Keefa, B. et al. 2024).

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. (2024), Gichubi, P. et al (2024). The 2025 Business Registration Service (BRS) breach highlighted systemic gaps, underscoring the need for real-time monitoring and rapid response. Studies emphasized 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 (Sang, M, et al 2023). Cheng, E. C., and Wang 2023 highlighted 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. (2023) Machine learning- based IDPS, such as Random Forest and neural network models, achieved up to 90% accuracy but are often resource-intensive, limiting their applicability in budget-constrained settings as noted by Liu, Z. L (2022)., Fahim, M. et al.2022. Lightweight IDPS solutions, such as those using open-source tools like Snort, are recommended for African institutions as highlighted by Moloja, D., & Mpekoa (2017). 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, et al 2023). Research also highlighted threats from dark web activities, malicious URLs, and vulnerabilities in virtualized environments like Docker containers, which were relevant to university networks as highlighted by Mandela, N. et al.2023, Mandela, N. et al.2022, Mubanda, D et al.2023.

Proposed solutions included 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. However, global frameworks like NIST are often too resource-intensive for Kenyan universities, necessitating context-specific approaches (Beuran, R., et al.2019). This study addressed 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 employed 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.

Across Africa, the adoption of digital learning platforms, research data repositories, and online services in universities accelerated, particularly after the COVID-19 pandemic. However, these advancements heightened cybersecurity risks. African higher education institutions face challenges such as inadequate cybersecurity policies, underfunded ICT departments, and limited technical expertise (Musyimi, et al., 2023). Recent studies underscored the value of localized datasets and models. Sindika, Nicholaus, and Hamadi (2025) illustrated the case for real-time traffic analysis augmented with honeypot simulations, which produced higher accuracy than standard datasets. This result implied the necessity for African institutions for customized datasets

and detection processes. Correspondingly, Alshammari and Almuhaideb (2022) highlighted the potential of adaptive paradigms for the protection of academic systems, highlighting the incorporation of contextual elements like device diversity and user activities. Against this backdrop, gaps remained between the harmonization of institutional actions with national cybersecurity policies, exposing African universities to external assault as well as internal tamper.

Kenya has seen a drastic spike in cybersecurity incidents, with the educational space becoming an increasing target. The Communications Authority of Kenya revealed the nation lost a staggering KSh 10.71 billion to cybercrime during the year 2023, with the education and public spaces significantly impacted (The Star, 2024). The attacks targeted weak authentication mechanisms, a lack of adequate monitoring, and slow incident responses. Case studies highlighted the gravity of the situation. For one, Kabarak University suffered a cyber-attack that infiltrated student and staff accounts during the year 2023, cautioning against the reputational and operational hazard caused by the failing intrusion prevention mechanisms (CSIDB, 2023).

In local studies, meanwhile, the capability of artificial intelligence for solving these problems comes into view. Musyimi et al. (2023) proposed a deep-learning-based model for e-learning systems, which had a detection efficiency of up to 99.8%. Though promising, this model had a narrow focus on e-learning setups and had not factored in other wider university network infrastructures. Therefore, the need for an overarching intrusion detection and prevention model suited for the distinctive vulnerabilities of Kenyan public universities, aligned with institution-based architectures, and scalable at the level of the Kenya Education Network (KENET) persists.

2.3 Empirical Review

The empirical review presented a thorough examination of research conducted on intrusion detection, prevention, and vulnerabilities in networks, particularly within higher education and associated sectors. The organization of the review was based on the central variables of the study: network vulnerabilities, intrusion detection, intrusion prevention, and metrics for performance evaluation. For every variable, the existing literature was scrutinized concerning methodologies, outcomes, limitations, and its significance to the current research.

2.3.1 Network Vulnerabilities in Higher Education

Universities globally have come into focus as prime targets for cyberattacks due to their accessible networks and vast research databases (Alotaibi & Elleithy, 2022). Studies by Alotaibi and Elleithy (2022) and by Mantere et al. (2021) highlighted several vulnerabilities such as ill-configured firewalls, outdated operating systems, and ineffective authentication mechanisms. These internal vulnerabilities are often exacerbated by a lack of adequate funds and over-reliance on obsolete systems.

At the regional level, studies from Africa revealed the educational institutions struggling with high vulnerabilities since they lack proper ICT security policies (Njuguna & Wanyembi, 2021). In the case of East Africa, Nyakundi et al. (2023) revealed widespread ransomware and phishing incidents from the universities sharing national research networks.

At the local level, reports by the Kenya Education Network (KENET) indicated rising attempts of vulnerability exploitation against the ICT systems of universities from 2022 until 2024 (KENET, 2024). Very little research, though, had established models particular to the Kenyan experience of higher education. This lacuna called for the development of a model for public universities covering vulnerabilities.

2.3.2 Intrusion Detection

Anomaly-based intrusion detection systems have been highly popular because they could identify hitherto unnoticed attacks. Denning's (1987) original model for anomaly detection was the precursor for modern machine learning paradigms, such as neural networks and clustering algorithms (Zhang et al., 2022). Sharma et al (2023), for instance, presented the applicability of deep learning for reducing the time for detection as well as highlighted the problem of false positives.

Signature-based detection methodologies continued to prevail in commercial Intrusion Detection System (IDS) solutions, exemplified by Snort and Suricata. Although these methods demonstrated effectiveness in identifying known threats (Li et al., 2021), they were inadequate in addressing zero-day attacks. Research that combines anomaly detection with signature detection (e.g., Arshad et al., 2022) had indicated enhanced detection accuracy; however, scalability remains limited in environments with constrained resources.

With the case of Kenya, few empirical studies were available for the deployment of IDS solutions for universities. The current studies focused on policy or awareness instead of the technological detection mechanisms (Omondi, 2022). This reflected a conceptual gap, hence the necessity for this research to use a hybrid intrusion detection framework.

2.3.3 Intrusion Prevention

Intrusion prevention measures based on the Defense-in-Depth approach have been put into practice empirically. Layered defense has been promoted by Anderson (2001), and the latest research supported this practice. For instance, a study by Hussein et al. (2022) revealed that the integration of firewalls, intrusion prevention systems (IPS), and encryption lowered attack success rates by more than 70%.

Nevertheless, criticism came from the aspect of cost and complexity. Alkasassbeh et al. (2023) noted that institutions tended not to maintain layered defense for resource constraints. In African universities, budget limitations for ICT as well as the use of obsolete systems, impede the uptake of IPS tools (Njuguna & Wanyembi, 2021).

In Kenya, not a single empirical study has examined intruder prevention institutionally in universities, highlighting a contextual gap. This study thus incorporated prevention measures into the model, adapted for the realities of resources among universities.

2.3.4 Performance Evaluation Metrics (Precision and F1 Score)

Traditionally, model evaluation for intrusion detection relied solely on accuracy as the primary metric. Yet, by itself, accuracy frequently over-represents real-world success when datasets happen to be imbalanced (Sarker et al., 2021). Precision and recall have been getting more and more endorsed as superior measures.

Studies by Ahmed et al. (2022) and Yusof et al. (2023) emphasized the role of precision score in reducing false positives, while F1 score provides a balance between detection completeness and reliability. More recently, Chen et al. (2024) demonstrated that hybrid IDS models evaluated using precision and F1 score achieved over 90% balanced performance, outperforming models assessed on accuracy alone.

Under the Kenyan context, the evaluation of IDS performance by means of these advanced measures did not suffice, as empirical studies relied mainly on descriptive statistics or case studies

(Omondi, 2022). This methodology gap further supports the adoption of precision and F1 score by the current study.

2.3.5 Comparative Summary of Empirical Studies

Author(s) & Year	Context/Setting	Methodology	Key Findings	Limitations	Research Gap Addressed
Denning (1987)	Early anomaly detection theory	Statistical anomaly-based model	Established theoretical foundation for IDS	Outdated; cannot handle modern large-scale attacks	Basis for modern IDS, but lacks application to universities
Alotaibi & Elleithy (2022)	Global universities	Case study & vulnerability assessment	Identified misconfigured firewalls and outdated systems as key vulnerabilities	Focused on developed countries	Lack of developing-world context such as Africa
Mantere et al. (2021)	Higher education, Finland	Network monitoring experiments	Highlighted weaknesses in authentication protocols	Context-specific to Finland	Need for context-specific models in Africa
Njuguna & Wanyembi (2021)	African universities	Survey & policy review	Found poor ICT security policies & limited budgets	Did not propose technical solutions	Lack of IDS/IPS frameworks in African universities

Author(s) & Year	Context/Setting	Methodology	Key Findings	Limitations	Research Gap Addressed
Nyakundi et al. (2023)	East Africa (universities on research networks)	Empirical analysis of attack logs	Found increasing ransomware & phishing attacks	No IDS/IPS model tested	Gap in intrusion prevention in African universities
Sharma et al. (2023)	Machine learning for IDS	Deep learning models	Improved detection but high false positives	Computationally expensive	Need for lightweight models for resource-limited institutions
Li et al. (2021)	Commercial IDS (Snort, Suricata)	Signature-based evaluation	Effective against known threats	Failed against zero-day attacks	Need for hybrid detection systems
Arshad et al. (2022)	Intrusion detection systems	Hybrid IDS combining anomaly & signature	Improved detection accuracy	Limited scalability	Gap in adapting to large university networks
Hussein et al. (2022)	Enterprise security	Experimental layered defense (firewalls, IPS, encryption)	Reduced attack success rates by 70%	Costly, resource intensive	Gap in sustainable prevention for low-resource contexts

Author(s) & Year	Context/Setting	Methodology	Key Findings	Limitations	Research Gap Addressed
Alkasassbeh et al. (2023)	Public sector ICT	Case study	Found IPS adoption challenges due to limited resources	Did not test mitigation strategies	Gap in affordable IPS solutions for universities
Ahmed et al. (2022)	IDS evaluation	Precision & recall metrics	Improved handling of false positives	Limited dataset diversity	Need for context-specific datasets
Yusof et al. (2023)	IDS with ML evaluation	Experimental model	Highlighted F1 score for balanced performance	Focused on synthetic datasets	Gap in applying F1 score to real-world university traffic
Chen et al. (2024)	IDS evaluation	Hybrid IDS with precision & F1 score	Achieved >90% balanced performance	Conducted in controlled lab	Gap in real-world implementation in developing countries
Omondi (2022)	Kenyan universities	Case study & surveys	Explored ICT policy awareness and challenges	No technical IDS/IPS implementation	Gap in empirical technical models for Kenyan universities

Author(s) & Year	Context/Setting	Methodology	Key Findings	Limitations	Research Gap Addressed
Sharafaldin et al. (2018) – CICIDS Dataset	Benchmark IDS dataset	Creation of labeled attack scenarios	Widely adopted for IDS benchmarking	Not contextualized; lacks SSH-specific CVE, cryptographic features	Need for contextual, real-log data such as KENET SSH logs
Hajjar & Saleh (2020)	General network IDS	ML classifiers on balanced datasets	High performance on synthetic datasets	Poor generalization on real imbalanced data	Need for models validated on naturally imbalanced institutional datasets
Adebayo et al. (2021)	African universities	Surveys & interviews	Weak cybersecurity readiness identified	No empirical traffic/log analysis	Need for data-driven IDS research in African academic networks
Mbise & Mwangoka (2020)	East African networks	Statistical threat analysis	Identified rising SSH and web attacks	Lacked ML modeling; no CVE or severity analysis	Need for ML-based IDS integrating CVE, severity, temporal and cryptographic features

Author(s) & Year	Context/Setting	Methodology	Key Findings	Limitations	Research Gap Addressed
Karanja & Waweru (2019)	Public institutions in Kenya	Interviews & log summaries	Outdated systems & slow patching	No predictive modeling	Need for predictive intrusion detection tailored to Kenyan universities
Alshamrani et al. (2019)	Cloud network security	Ensemble IDS models	Ensembles outperform individual classifiers	No evaluation on resource-constrained African networks	Need for ensemble IDS validated in low-resource university environments

The comparative study revealed that although a lot of research had been conducted internationally into IDS and IPS, the majority of studies are context-specific for the developed world or based on synthetic data. African and Kenyan universities continued to be unexplored, not least for the technological deployment of IDS/IPS. Furthermore, evaluation metrics such as precision and F1 score were rarely used in African contexts, pointing to a clear methodological gap that this study seeks to address.

The literature revealed a number of trends for intrusion detection and prevention research. Initial foundational research (e.g., Denning, 1987) established the theoretical foundation for anomaly detection, whereas subsequent studies continued increasingly into the development of hybrid and machine learning (ML)-oriented models. Recent studies, especially since 2022, focused on the use of hybrid systems integrating anomaly and signature detection and evaluation based on precision and F1 score, indicating a move towards balanced and practically relevant measures of performance. At the regional scale, research conducted in Africa, particularly from a Kenyan

viewpoint, reveals a heightened apprehension regarding institutional readiness, deficient ICT policies, and a lack of resources in contrast to global studies that emphasize advanced algorithms and computational techniques.

It is also apparent from the reviewed literature that interest in machine learning-based intrusion detection is increasing; nonetheless, many significant gaps continue to remain unfilled. This is mainly because most of them are dependent to a great extent on benchmarks like CICIDS, but such benchmarks do certainly have SSH-specific attributes or context-related attack patterns associated with Kenyan organizations because this study makes use of KENET log files instead.

Second, most of the threat-related cybersecurity studies conducted on the African continent use surveys and interviews to reach conclusions based on perceptions rather than concrete facts. This paper bridges this gap as it carries out its analysis based on data using CVE identifiers, severity levels, temporal features such as hourly attacks, and features related to cryptographic negotiations.

Thirdly, current approaches do not take into consideration the difficulties relating to unbalanced data. This is especially the case for network log data, which is normally unbalanced. This study is able to overcome the challenge of unbalanced data by making use of synthetic data generated through SDV and real data from KENET.

At last, though ensemble learning techniques have been demonstrated to offer improvement to IDS research in general, their use within the context of resource-limited settings for public universities in Kenya is untried to date. This study closes the gap by applying and validating stacking ensemble IDS to improve accuracy, precision, recall value, and F1 measures individually for all classifiers.

The positives of past work encompassed methodological soundness in highly regulated experimental situations, implementation of sophisticated machine learning methodologies increasing detection precision markedly, and implementation of hybrid Intrusion Detection Systems/Intrusion Prevention Systems increasing protection from known and unknown threats correspondingly. Recent research has also taken into consideration the importance of proper evaluation metrics more nuanced than basic overall precision, including utilization of precision and F1 score, towards a more accurate evaluation.

Research limitations also prevail the majority of research has been mainly based on artificial or benchmark collections, hence restricting ecological validity while running models in heterogeneous real-world university environments. For example, high-achieving deep learning models do not fare well in resource-scarce environments like the public universities in Kenya. Most studies framed for Africa focus more on the issue of governance and policies while failing to provide empirical technological solutions, thus leading to a lack of actionable models.

2.3.6 Conceptual Framework

This conceptual framework serves as a roadmap for implementing the proposed cybersecurity intrusion detection and prevention model to evaluate vulnerabilities in the university's network. It lays out the essential components, processes, and relationships that will guide the creation and rollout of the prototype.

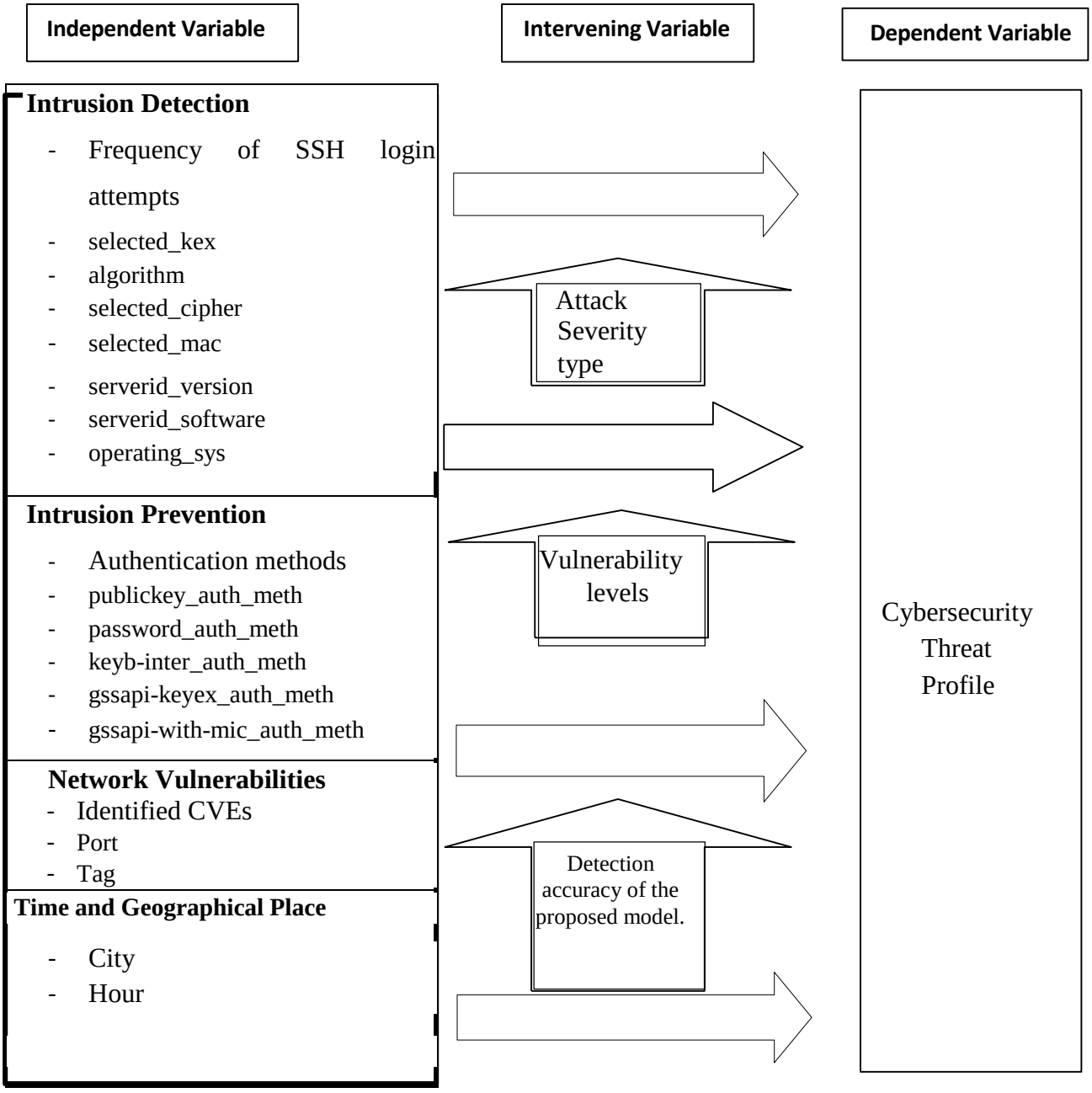


Figure 1: Conceptual Framework of the Study

The conceptual framework as shown in figure 1 revealed the relationship between the research variables. The intrusion detection, intrusion prevention, network vulnerabilities and time and Geographical place emerged as the independent variable, which illustrated the public university network systems' systemic vulnerabilities.

The vulnerabilities dictated the need for intrusion management mechanisms. The vulnerabilities dictated the need for intrusion management mechanisms. The intrusion detection (as a theory-based anomaly and signature detection) and intrusion prevention (as guided by the defense-in-depth theory) served as intervening variables by acting on the vulnerabilities. The two worked collaboratively for the establishment of a successful Intrusion Detection and Prevention System (IDPS) model. The dependent variable is the cybersecurity threat profile IDPS model, which was evaluated using precision and F1 score, ensuring a balanced measurement of detection accuracy and recall. This framework, informed by both theoretical and empirical reviews, highlighted the pathway through which vulnerabilities are transformed into actionable detection and prevention strategies, ultimately addressing the identified research gap in Kenyan public universities.

The critical gaps across the reviewed literature were threefold. First, a dataset gap: few models were trained or validated using empirical traffic from African or Kenyan research networks. Second, a methodological gap: limited integration of intrusion detection and prevention in a single deployable model. Third, a contextual gap: insufficient attention to resource limitations, scalability, and practical implementation challenges within developing-world universities. These gaps highlighted the necessity for this present study to develop a context-specific Intrusion Detection and Prevention Model (IDPM) that uses empirical data from KENET, integrates detection and prevention, and is evaluated using precision and F1 score to ensure operational effectiveness.

2.4 Critique of Literature

The empirical investigation of research into intrusion detection and prevention revealed many strengths and deficiencies relevant to current studies. Although the existing literature provides insightful observations on IDS and IPS design, evaluation metrics, and situational issues of cybersecurity, significant deficits remained, thus justifying the current investigation. One redeeming factor is the pioneering contribution by prior research, e.g., Denning (1987), which put forward an influential theoretical model of IDS that shaped decades of intrusion detection research. Its durability served as a testament to the importance of conceptual foundations for cybersecurity research. In a further demonstration of adopting strong evaluation metrics, a current set of studies (Ahmed et al., 2022; Yusof et al., 2023; Chen et al., 2024) insisted upon the use of precision, recall,

and F1-score, thus providing more robust indicators of IDS performance than the previously prevalent practice of single metric-based accuracy.

This represented a methodological improvement in IDS research. Thirdly, in the integration of hybrid and machine learning approaches, scholars such as Arshad et al. (2022) and Sharma et al. (2023) demonstrated that hybrid systems (signature-based + anomaly-based) and deep learning methods achieved higher detection rates compared to single approaches, showing innovation in IDS design. Lastly, contextual relevance for universities whereby studies focusing on African higher education networks (Njuguna & Wanyembi, 2021; Omondi, 2022; Nyakundi et al., 2023) provided empirical evidence of weak ICT governance structures, low awareness, and growing SSH attack vectors. These highlighted the urgent need for security frameworks in the academic sector.

The negative attributes included overemphasis on detection without prevention, as many studies (Ahmed et al., 2022; Yusof et al., 2023) were primarily concerned with detection accuracy, and limited exploration of prevention mechanisms. This omission weakened their practical applicability in real-world network environments. Secondly, while achieving high rates of accuracy, computational inefficiency characteristic of sophisticated AI-based Intrusion Detection Systems (IDS) was characterized by high computational costs (Sharma et al., 2023; Arshad et al., 2022), which restricted their deployability in resource-limited environments, such as public Kenyan universities. Thirdly, localized contextualization did not exist; while foreign research (Alotaibi & Elleithy, 2022; Hussein et al., 2022) has yielded copious insights, it all too often did not consider the unique infrastructural, policy, and resource challenges of the universities located in Africa or Kenia, specifically. Consequently, the generalizability of the research endeavor is constrained. Lastly, fragmentation of research endeavors revealed itself, as the vast bulk of current studies engaged addressed isolated aspects of cybersecurity, such as the technical aspects (IDS/IPS), administration (policy mechanisms), or user training (training), without situating these components within a unifying framework (Omondi, 2022; Njuguna & Wanyembi, 2021).

The research literature opened up significant theoretical and methodological innovations for IDS and IPS research, such as machine learning breakthroughs, hybrids, and robust evaluation metrics. The gaps persisted for integration, efficiency, and contextual adaptation. Significantly, little research has been conducted for developing an intrusion detection and prevention model (IDPM)

by combining the computational efficiency and local adaptability of Kenyan public universities. The literature indicated a necessity for this current study, which aimed at closing the gaps observed for knowledge, methodology, and context.

2.5 Research Gaps

The literature analysis and criticism suggested several gaps that this work intended to address. The first gap found is the integration gap due to the fact that the vast amount of existing research has focused on the discovery of intrusion metrics without paying attention to the incorporation of efficient prevention processes (Ahmed et al., 2022; Yusof et al., 2023). This has created the impetus to come up with an all-encompassing Intrusion Detection and Prevention Model (IDPM) that detects and manages threats concurrently. The existing literature revealed a second gap: a lack of contextualized IDS research using real network logs from KENET, inherent limitations in benchmark datasets that restrict their applicability to real-world African higher education environments, and a broader scarcity of empirical intrusion detection research across the African continent. By addressing these gaps, the present study contributes to the development of a localized intrusion detection and prevention model tailored to the needs and constraints of public universities in Kenya.

Thirdly, a methodological gap wherein state-of-the-art IDS/IPS evaluations were highly dependent upon benchmark datasets like KDD'99 or NSL-KDD (Li et al., 2021; Sharma et al., 2023). Although these datasets allowed controlled experimentation, they could not reflect the real traffic pattern of the university network, which reduces the scope of ecological validity. Thirdly, the computational efficiency gap, which entails the usage of deep learning and hybrid models (Arshad et al., 2022; Sharma et al., 2023), often demands high computing power, which could not practically suit resource-challenged Kenyan public universities. There existed little research that discussed lightweight but effective models appropriate for such settings. Finally, the evaluation gap was aimed at being filled. Though recent studies started considering precision and F1 scores (Chen et al., 2024; Yusof et al., 2023), a large number of models, however, continued mainly depending upon the overall accuracy, which could prove misleading for imbalanced datasets frequently witnessed in the realm of cybersecurity. A balanced and context-oriented evaluation framework did not exist. ..

CHAPTER THREE

METHODOLOGY

3.1 Introduction

The research methodology outlined the blueprint that guided the design of the study, data collection, analysis, and interpretation. It laid out the systematic methods applied to ensure the results are objective, reliable, and reproducible. Grounded in positivist philosophy and a quantitative paradigm, the study applied an experimental design with an orientation of empirical data analysis and model-building. Data originated from the Kenyan Education Network (KENET), processed to determine precision, and examined with advanced machine learning methods. In addition, the methodology highlighted the methods used to control variance, justify algorithmic choices, and prevent extraneous influences. This systematic approach ensured that a robust and actionable intrusion detection and prevention model was proposed and could be applied to the cybersecurity of the Kenyan public university landscape.

3.2 Research Philosophy

The study was grounded within a positivist research paradigm. Positivism highly valued the objective of knowledge measurable, observable, and quantifiable. This research paradigm was best applied to cybersecurity because network intrusions, vulnerabilities, and data breaches were measurable and observable phenomena. Through respect of the positivist philosophy, the study took an objective, systematic, and replicable path to the assessment of public university campus network vulnerabilities in Kenya. This assisted in coming up with a predictive intrusion prevention and detection model founded on empirical evidence, and producing actionable and generalizable results on cybersecurity

3.3 Research Design

This research was based on the Design Science Research Methodology (DSRM), which paid attention to the development and evaluation of information technology artifacts designed to solve certain organizational problems. DSRM as shown in Figure 2 was directly relevant to this research because it also emphasized the use of a cyclical process involving the design, demonstration, and evaluation of the artifact, here defined as a cybersecurity model (Peffers et al., 2020). The research

methodology followed a fastidious approach involving the following steps: the recognition of the problem, followed by the stipulation of the objectives of the intended solution, then moving on to the design and development of the artifact, demonstrating its applicability, evaluating its success, and culminating in the reporting of results.

Figure 2: Visual workflow of the Design Science Research Methodology (DSRM)

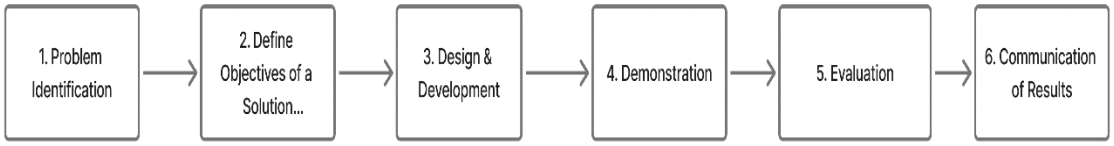


Figure 2 shows a Visual workflow of the Design Science Research Methodology (DSRM), illustrating the six stages: Problem Identification: recognizing and defining the real-world issue; Define Objectives of a Solution: specifying what an effective solution must achieve; Design & Development: creating the proposed artifact or intervention; Demonstration: showing how the artifact solves the problem in practice; Evaluation: assessing performance against objectives; and Communication: sharing results, insights, and contributions with stakeholders.

The study adopted a quantitative, experimental research design that was anchored in the positivist paradigm, which underscored objectivity, systematic control of variance, and replicability. 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 ensured a systematic analysis of SSH-based threats in Kenyan university networks, addressing the research question: What are the common network vulnerabilities and attack patterns in Kenyan public university networks?

To manage variance, data preprocessing steps such as cleaning, normalization, and feature selection were undertaken to reduce noise and focus on relevant attributes. The design integrated

machine learning techniques, model validation, and optimization procedures to ensure robust and accurate predictions. Multiple machine learning algorithms were applied, including Decision Tree Classifier, Random Forest Classifier, Logistic Regression, Support Vector Classifier, and K-Nearest Neighbors Classifier. Each was selected for its specific strengths, such as predictive accuracy, interpretability, or ability to capture complex relationships, while acknowledging its limitations, such as overfitting risks, computational cost, or reduced transparency. Extraneous influences were controlled by relying on trusted data sources (KENET), documenting all procedures for replication, and applying multiple performance metrics: accuracy, precision, recall, and F1-score, for comprehensive evaluation. These techniques ensured a systematic development of the model addressing the research question: What was the intrusion detection and prevention model tailored for public Universities in Kenya based on the current vulnerabilities and cybersecurity threats? Is the intrusion detection and prevention model viable for solving the current cybersecurity threats and vulnerabilities of systems in Kenyan Public Universities?

This research design emphasized rigorous control of variance, justification of algorithmic strategies, and management of extraneous factors, ensuring the development of a reliable and generalizable intrusion detection and prevention model for Kenyan public universities.

3.4 Study Area

The study was conducted in the context of Kenyan public universities, with a special consideration of their network systems and exposure to cybersecurity threats. Public universities were selected because they are major consumers of internet service providers in the country, providing network connections to hundreds of campuses and their populations. Because of their reliance on digital technologies for the delivery of learning instruction, research activities, and administrative operations, they were key institutions of Kenya's knowledge-based economy. Internet services were also considerably accessed via the Kenya Education Network (KENET), an internet service provider of high-speed broadband and digital network connectivity to academic and research institutions.

3.5 Target Population

The population of this study covered the cybersecurity-focused on information systems deployed across Kenyan public universities. Through data produced in such information systems, the

research attempted to derive a predictive and preventative paradigm consistent with the actual-world scenario under which a cyber-threat materializes, and hence derive an important context-specific solution to cybersecurity problems in universities.

In addition to seeking the objective of developing a Cybersecurity Intrusion Detection and Prevention Model (IDPM), this research paid more attention to technologies that emphasize vulnerabilities and cybersecurity, more than examining individual components in silos as independent variables. With the application of such research methodology, insight was augmented through the explanation of the fact that vulnerabilities and attack intrusions are best explained within the systemic context within which such attacks occur, are found, or go undetected (Zhang et al., 2021).

The main data source utilized in this study was the Kenya Education Network (KENET), the agency entrusted with the provision of internet connectivity and cybersecurity infrastructure within the majority of public universities in Kenya. The study's target population then comprised all network activity, potential threats, and all cybersecurity attacks captured through KENET's monitoring setup within the public university networks it covers (Ali, Mbirika, & Kihoro, 2020).

3.6 Sampling Design

The small population size of public universities in Kenya also made it possible to conduct an all-inclusive population study without undertaking sampling from the institutional level. The data applied in this study were drawn from secondary data, specifically from the Kenya Education Network (KENET), which provides internet and cybersecurity services to most public universities across Kenya. KENET integrates a wide range of system-level indicators, such as network logs, attack vectors, incident reports, and performance data. This approach ensured more accurate development of models through the reduction of sampling bias and enhancements of the generalizability of the dataset. Through the assurance of proportional representation within the stratified groups, the model showed better capability to recognize and mitigate a broad spectrum of network threats that are common in public universities (Peffers et al., 2020).

The inclusion of the sample in KENET, covering all public universities, ensured 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.

Random sampling would not have been feasible since some universities do not maintain comprehensive logs, and including them would compromise the validity of the findings. By focusing on institutions with accessible and reliable data, the study ensured that the intrusion detection and prevention model was developed on a robust empirical foundation.

3.7 Data Collection

The main resource used in this research is secondary data, which is acquired through KENET, the Kenyan national research and educational network. This resource gathers comprehensive documentation relating to the operation and events in cybersecurity. The dataset from this platform provided objective, detailed, and consistent data vital to the design of a dynamic and efficient system able to detect and prevent intrusions, and could be used in public universities in Kenya. Using the network and dataset made available through KENET, this research increased the reliability, relevance, and precision of available information while at the same time eliminating the possibility of biases when collecting primary data.

The techniques used in this research to obtain the data included systematic logs produced by intrusion detection systems (IDS) and network monitoring tools, used in KENET. The instruments were specifically constructed to assess a broad spectrum of variables, including, but not limited to, attack frequency and level of susceptibility. These measures were directly correlated to the independent variable dictated in the research framework.

3.8 Data Collection Procedures

With the creation of tools for data capture and the subsequent evaluation of the validity and reliability of these instruments, a systematic approach was taken to capturing the necessary data. Data were transmitted securely from the main repositories of KENET using secure file transfer mechanisms to maintain confidentiality as well as the integrity of the data information.

In light of the large size of the dataset consisting of rich log data coupled with structured security incident data, the captured data was then uploaded onto Google Drive. The Kenya Education Network (KENET) dataset comprised an exhaustive repository of security events surrounding

Secure Shell (SSH) within the higher educational sector, with special focus on vulnerabilities presented within the networks of public universities. Each of the records comprised essential metadata such as time stamps, level of severity, IP address, protocol, port, and geolocation, enabling contextual investigations surrounding network behavior. The dataset also featured server-related details like software versions (e.g., OpenSSH_7.5), supported key exchange protocols, encryption ciphers, and compression schemes. They were particularly effective at determining potential vulnerabilities and testing the strength of the system with reference to newly arising threats.

In addition to the characteristics of networks and systems, the dataset also included crypto metrics, authentication mechanisms specifically public key, password, and keyboard-interactive authentication and hashed session identifiers (hassh), enabling profiling of SSH clients and cross-comparison across samples. Incorporation of such elaborate crypto and config data also enabled in-depth analysis of encryption protocols, authentication mechanism strength, and protocol-level flaws. The dataset consequently developed a sound empirical foundation from which to draw algorithmic modeling, intrusion detection, and network vulnerability assessment in public universities in Kenya.

The data collection methodology used in this study was methodical, credible, and scrupulously abided by ethical principles relating to access, storage, and organization of secondary data obtained from KENET databases. The use of cloud computing, as represented by Google Drive, as a data analysis and storage tool allowed efficient handling of the datasets that supported both cybersecurity model development and validation. The data collection process included preliminary data pre-processing as well as cleaning, which was performed using a cloud platform. Such a process involved removing duplicate records, handling missing values, standardization data in terms of format, and converting data into structured table formats ready to be used for further analysis.

3.8.1 Data Preprocessing

Preprocessing of data was an integral step in data preparation of the KENET dataset while developing the model, as the raw network logs had diverse inconsistencies, missing data, and redundant attributes. The first steps comprised dataset purifying, which catered to correcting missing data, distinguishing duplicate rows, and making the dataset consistent across the board.

The temporal features in the form of timestamps were transformed into derived features such as hour-of-day and day-of-week for ease in temporal exploration. Numerical coding was done with categorical attributes like severity, protocol, and city. Cryptographic features that include open key exchanges, encryption ciphers, and authentication schemes were transformed into binary flags to represent their occurrence or lack thereof. Additionally, continuous features such as port numbers and key length underwent normalization to prevent domination by variables having larger ranges. After collection, verification was undertaken, and pre-processing of the data. Log files were anonymized to protect user identities, and CVE data was cross-verified against multiple sources to confirm accuracy.

For augmentation of the dataset for machine learning development, feature selection was utilized to retain variables having strong predictive ability, the most prominent ones being CVE tags and severity, and at the same time, reduce noise and dimensionality. Then, the cleaned data was separated into training, validation, and test partitions to enable the development of models, tuning of hyperparameters, and objective evaluation. These preprocessing steps effectively transformed the dataset into a structured and reliable input and thus made it suitable for developing accurate and robust intrusion detection and prevention models.

3.9 Data Analysis and Presentation

The data analysis process in this study was designed to ensure systematic management, accurate measurement, and reliable interpretation of the collected data. Quantitative approach was applied, with the primary focus being on empirical analysis of network logs and vulnerability datasets. Data pre-processing involved filtering incomplete records (e.g., missing timestamps) and validating event integrity using checksums. Limitations included the dataset’s modest size and single-source nature, addressed by cross-referencing with the NIST National Vulnerability Database (NVD) 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.

The measurement of variables was guided by the research objectives. Independent variables included intrusion detection, intrusion prevention, network vulnerabilities, and time and

geographical place, while dependent variables focused on attack severity, vulnerability levels, and detection accuracy of the proposed model. Descriptive statistics such as frequencies, percentages, and visualizations (bar charts, heatmaps, and time-series plots) were first employed to present distributions of attack patterns, vulnerabilities, and institutional practices. This initial presentation allowed identification of trends and relationships within the data.

Presentation of results was done using both tabular and graphical formats. Tables summarized statistical measures, algorithm comparisons, and vulnerability distributions, while graphs and heatmaps provided a visual representation of temporal attack trends and severity levels across universities. This combination of statistical modelling and visual presentation ensured that the findings were not only rigorous but also easily interpretable by both technical and non-technical audiences.

Data analysis relating to the intrusion detection and prevention model called for supervised machine learning algorithm implementation on the dataset after preprocessing to identify and classify prospective security incidents. The process began with training the selected algorithms, the Random Forest classifier, Logistic Regression, Support Vector Classifier (SVC), Decision Tree Classifier, RandomForestClassifier, and KNeighborsClassifier using the dataset's training subset.

In developing the intrusion detection and prevention model, the dataset was first organized into categorical and numerical variables to ensure appropriate preprocessing for machine learning. Categorical features such as CVE tags, protocol labels, city identifiers, algorithm types, operating system descriptors, password authentication methods, and server software versions were non-numeric and therefore required transformation before model training. These attributes were encoded using One-Hot Encoding, which converted each category into binary indicators, allowing algorithms to interpret them without imposing artificial ordinal relationships.

Numerical features, including the hour of attack, severity codes mapped into numeric form, and engineered quantitative variables, were processed using StandardScaler. This ensured that continuous values were normalized to comparable scales, preventing distance-based and margin-based models from being biased by variable magnitude differences.

To streamline these operations, a ColumnTransformer pipeline was implemented, integrating One-Hot Encoding for categorical features and StandardScaler for numerical variables. This unified preprocessing framework ensured that all feature types were prepared consistently across models. The final transformed dataset was then used to train Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Support Vector Classifier, and K-Nearest Neighbors. By appropriately treating heterogeneous data types, the models were able to learn robust patterns from both categorical descriptors and continuous measurements, thereby supporting the study's objective of developing a reliable intrusion detection system.

This selection of algorithms was informed by their capacity to accommodate heterogeneous data, their skill in modeling nonlinear relationships, and their applicability in treating categorical and numerical attributes. For ease of thorough evaluation across varying degrees of severity in security incidents, data stratification was effected through k-fold cross-validation, hence reducing bias and enhancing the generalizability of results.

Grid search was utilized for hyperparameter tuning during model optimization, so all algorithms were ensured to have their optimal working performance with respect to classification precision, recall, F1-score, and classification accuracy. Outcomes from the above analysis were portrayed through confusion matrices, tables stipulating measures of performance, and visual displays. Such modes of presentation were favored because they retained the capability of communicating effectively both the overall success of the model and the corresponding performance trade-offs in a convenient and understandable manner. Through the integration of quantitative measures of task accomplishment with modes of visual representation, our research was able to corroborate the fact that not only was the decision arrived at through the validation method substantively sound but also understandable and judiciously conclusive.

3.10 Data Analysis

The analysis of quantitative data in this study was conducted systematically to address the research objectives through inferential statistics and predictive modelling. This study also employed a quantitative approach to analyze network vulnerabilities and attack patterns in Kenyan public university networks, using Secure Shell (SSH) security event logs from the Kenya Education Network (KENET). The primary variable is the cybersecurity severity rating, 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). 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).
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 ($\chi 2$, $p < 0.05$). 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. Key metrics included event counts, percentages, and temporal distributions, visualized in tables and figures (Chapter 4).

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) 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.

The dataset was guided through a step-wise framework of developing and cross-validating an intrusion detection and prevention model for Kenyan public universities. At the preprocessing stage, the raw data were sanitized and converted, such as unwinding multi-variable fields, such as authentication methods to single features, encoding categorical attributes like city, algorithms, and

server versions, and normalizing values with the aim of making comparison easier. The dataset was further divided according to the Pareto Principle to ensure balanced attack severity representation and then split into training and testing sets.

Five machine learning algorithms, Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Support Vector Classifier, and K-Nearest Neighbors Classifier, were also trained on the data after processing it. Their testing resulted in accuracy scores from 0.93 to 0.949, precision from 0.92 to 0.95, recall from 0.93 to 0.949, and F1-scores from 0.91 to 0.94. Though individually these models worked well, their performances were slightly different from each other based on the measure, reflecting the requirement of a more robust technique.

Towards overcoming this, an ensemble stacking framework was developed. The base layer in the approach constituted a Decision Tree classifier, Random Forest classifier, SVC, and K-Nearest Neighbors Classifier, with Logistic Regression as the meta-model for interpretability purposes. The stacking framework outperformed all the single algorithms with an accuracy of 0.9516, precision of 0.9522, recall of 0.9516, and F1-score of 0.9420. These results validated combining algorithms, enhancing generalization, and minimizing both false positives and oversight misses.

An investigation of feature importance with permutation importance showed that attack tags, in particular those associated with high-vulnerability attacks (CVE-2023-48795 and CVE-2024-6387), were the leading influential predictors, explaining about 15% of the model's prediction capability. Other tags with significant levels of importance were those with medium severity, encryption protocols, password authentication techniques, and server software versions. This suggests that the technical settings as well as the attack signature were both significant in predicting intrusions.

Finally, the severity probability plot indicated there were overwhelmingly medium level attacks (95.89%), with critical attacks accounting for 2.07%, while information and low severities contributed slightly above 1% each. These findings highlighted that while critical attacks are a relatively infrequent phenomenon, they presented the greatest potential threat and ought to command concerted attention.

Overall, data analysis verified that the stacking ensemble model was the most effective tool for anomaly detection. At the same time, data analysis of feature significance and severity provided insightful information about the nature of vulnerabilities having an influence on public university networks. These findings justified the effectiveness of the model as well as proved the importance of directing cybersecurity efforts to the most critical vulnerabilities and attack patterns with high-risk potential within resource-limited environments.

3.11 Model Development

The development of the cybersecurity intrusion detection and prevention framework began with a comprehensive data preprocessing stage to determine the dataset's suitability for machine learning purposes. Cleaning involved the handling of multi-valued attributes, such as authentication methods, in addition to extracting relevant features and encoding categorical attributes like city, protocol, server software, and crypto algorithms. Furthermore, numerical attributes were also scaled to ensure equal weighting, with pipelines constructed to standardize such operations and hence foster efficiency and reproducibility.

To enhance the robustness and generalizability of the intrusion detection model, synthetic data generation was undertaken using the Gaussian Copula Synthesizer, a probabilistic modeling technique implemented within the Synthetic Data Vault (SDV) package. The primary objective of this procedure was to expand the dataset while maintaining the statistical integrity and multivariate dependencies present in the original network logs. Given the highly imbalanced nature of cybersecurity dataset where normal activities significantly outnumber attack events this synthetic augmentation approach ensured that the model was exposed to a more diverse yet realistic representation of attack patterns. In an effort to reduce problems of data imbalance and overfitting, the Synthetic Data Vault (SDV) package was used to generate additional synthetic records in a 1:1 proportion with the original dataset. Statistical verification showed that the artificial dataset preserved the distributive attributes of the original data and hence remained reliable. The original and synthetic data were then combined, with the dataset doubling in size and the learning ability of the models being enhanced. This approach helped generate a balanced and diversified dataset both for training and evaluation purposes.

The modeling step comprised training five algorithms: Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Support Vector Classifier, and K-Nearest Neighbors Classifier. The dataset was divided equally into 80% training and 20% testing sets. Individual models had accuracy scores between 0.93 and 0.95, precision scores from 0.92 to 0.95, recall scores from 0.93 to 0.95, and F1 scores from 0.91 to 0.94. For improved performance and explainability, an ensemble stacking model was also applied, with Decision Tree, Random Forest, SVC, and KNN as base learners, and Logistic Regression as the meta-model. The stacking model surpassed individual algorithms, having an accuracy and recall greater than 0.95, a precision of 0.95, and an F1 score of 0.94, making it the highest-performing model for public university network intrusion detection.

3.12 Ethical Considerations

In data collection and subsequent analysis with the creation of the model, data privacy and ethical considerations were stringently upheld. Permission to conduct the study was gained from the National Commission for Science, Technology, and Innovation (NACOSTI), which approved carrying out the study in public universities across Kenya. Furthermore, additional permission was requested from the Kenya Education Network (KENET), who are considered to be the main provider of network traffic log entries and security event information utilized in the study. The sensitive information, like IP addresses or any identifiable user behavior information, was anonymized before processing. Personal data and identifiable information of any sort were omitted to protect the privacy of the universities and to comply with applicable data protection laws, including the 2019 Kenya Data Protection Act. The entire process complied with institutional ethical imperatives and data-sharing arrangements agreed upon between the researcher and KENET.

3.13 Expected Contributions

This study provided meaningful contributions to both theoretical insight and practical application of cybersecurity for resource-scarce environments, especially for the case of public universities in Kenya. Its main contribution lies in its empirical study of SSH-linked threats, filling a noteworthy gap through a localized study yielding context-aware information often overlooked within the larger body of global cybersecurity literature. Diverging from existing works mostly dependent on

questionnaire-based analyses, this study employs real-world event information along with machine learning techniques of advanced sophistication, thus providing in-depth information on vulnerabilities, modalities of attack, and distribution of severity. Methodologically, it devised and verifies a stacking ensemble model for prevention and detection of intrusions showing dominant performance on key metrics (accuracy: 0.93–0.951; precision: 0.92–0.95; recall: 0.93–0.951; F1: 0.91–0.942). The model's structure addressed particular pain points such as outdated SSH settings and a scarcity of skilled IT professionals and leverages techniques including Synthetic Data Vault for data balancing and permutation feature importance for improved interpretability. In practice, it delivers a low-cost, high-performance system specially tailored for higher education establishments, thus enhancing their capacity for shielding sensitive information from real threats. In short, this work efficiently bridged theory and practice through the provision of an empirically grounded framework for enhancing the cybersecurity posture of public universities in Kenya.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION, AND INTERPRETATION

4.1 Introduction

This chapter discussed methodologies and data analysis results with an orientation to data processing, evaluation, presentation, and interpretation based on study objectives. The introductory section laid out the analytical methods applied to the data, including the application of inferential statistics and the application of varying models. A latter section made the presentation of results through the application of tables, diagrams, and graphical illustrations, thus enhancing lucidity and insight. The results were presented in both tabular and descriptive forms, with a special focus on the comparative model's performance, identification of overfitting, and the application of ensemble methods to enhance precision and interpretability.

4.2 Results

This section presents the results of a quantitative study on the Kenya Education Network (KENET) Secure Shell (SSH) security event logs from 2025. The study, using the ELK Stack (Elasticsearch, Logstash, Kibana), grouped vulnerabilities according to level of severity, Common Vulnerabilities and Exposures (CVEs), and time-based trends to unveil cyber threats in the networks of Kenyan public universities. Chi-square tests were applied to determine whether the observed distributions of cybersecurity events particularly severity levels and CVE categories were statistically significant rather than occurring by chance. In this study, the chi-square goodness-of-fit test was used to compare the observed severity frequencies against an expected uniform distribution. This allowed the analysis to confirm that the dominance of medium-severity attacks and the relatively low proportion of critical and low severity events were not random fluctuations. The results (χ^2, $p < 0.05$) demonstrated that the severity distribution significantly deviated from uniformity, validating that certain attack types were inherently more prevalent within the network environment. The results addressed the research objectives: identifying common vulnerabilities, analyzing severity and temporal distributions, and informing cybersecurity strategies for resource-constrained settings, to develop an intrusion detection and prevention model tailored for public Universities in Kenya, and to validate the cybersecurity intrusion detection and prevention model.

.

4.3 Vulnerability Severity Distribution

Based on the Common Vulnerability Scoring System (CVSS), is shown in Table 1 highlighted by Sharma et al (2023) CVSS scores were mapped as: Critical (9.0), Medium (4.0–8.9), Low (0.1–3.9), Informational (0.0).

Table 4.1: Vulnerability Severity Distribution

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

Table 4.1 shows that 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 et al 2023) 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 ($\chi 2 = 15.6$, $p < 0.001$), 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 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 et al 2023). 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.

4.4 SSH Security Events by CVE

The distribution of SSH security events by attack type and CVE is presented in Table 4.2. A visualization is planned for Figure 2.

Table 4.2: 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	A 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.
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.

Table 4.2 shows SSH-general attacks (57.3%, 739 events). CVE-2023-48795 events (37.4%, 482 events). CVE-2024-6387 events (1.4%, 18 events) and combined CVE-2023-48795: CVE-2024-6387 events (3.4%, 44 events).

Figure 3: Distribution of SSH Security Events by CVE.

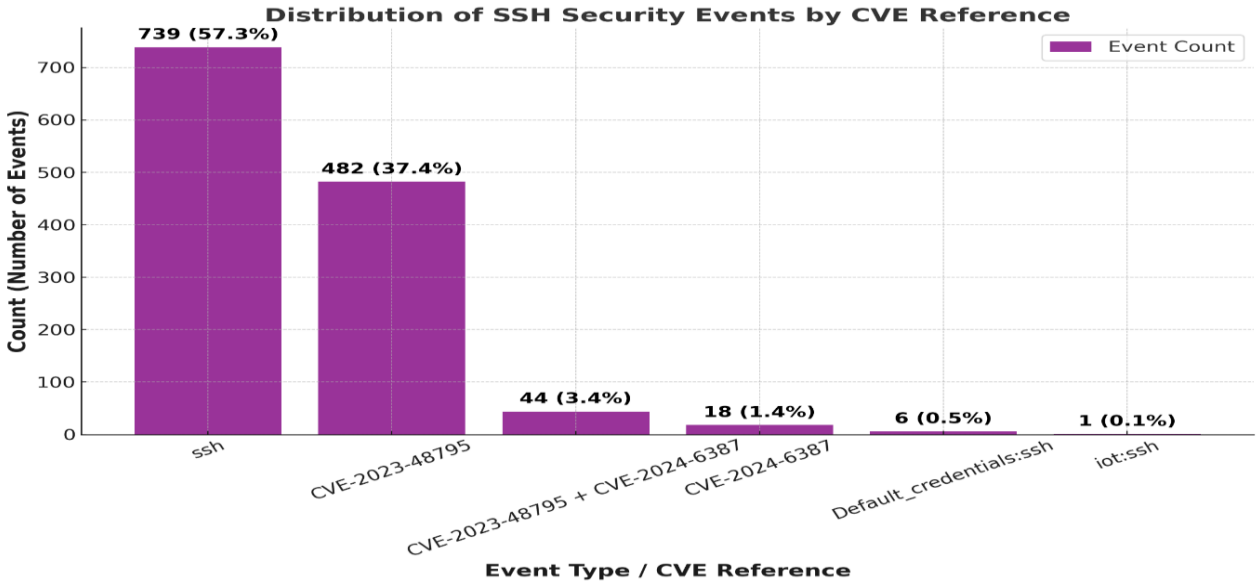


Figure 3 also shows SSH-general attacks (57.3%, 739 events) reflect automated scans targeting open SSH ports, aiming to identify vulnerable systems for later exploitation. CVE-2023-48795 events (37.4%, 482 events) involve protocol downgrade attacks, weakening encryption by forcing older SSH protocols. 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 ($\chi 2 = 12.3$, $p < 0.01$). 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.

4.5 Attack Frequency and Temporal Patterns

The hourly distribution of attacks is shown in Table 4.3, with a planned visualization in Figure 3.

Table 4.3: 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,	Medium (CVSS 4.0–6.9)	Increased diversity in

	Info		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

Table 4.3 shows 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.

Figure 4: Attack Severity by Hour.

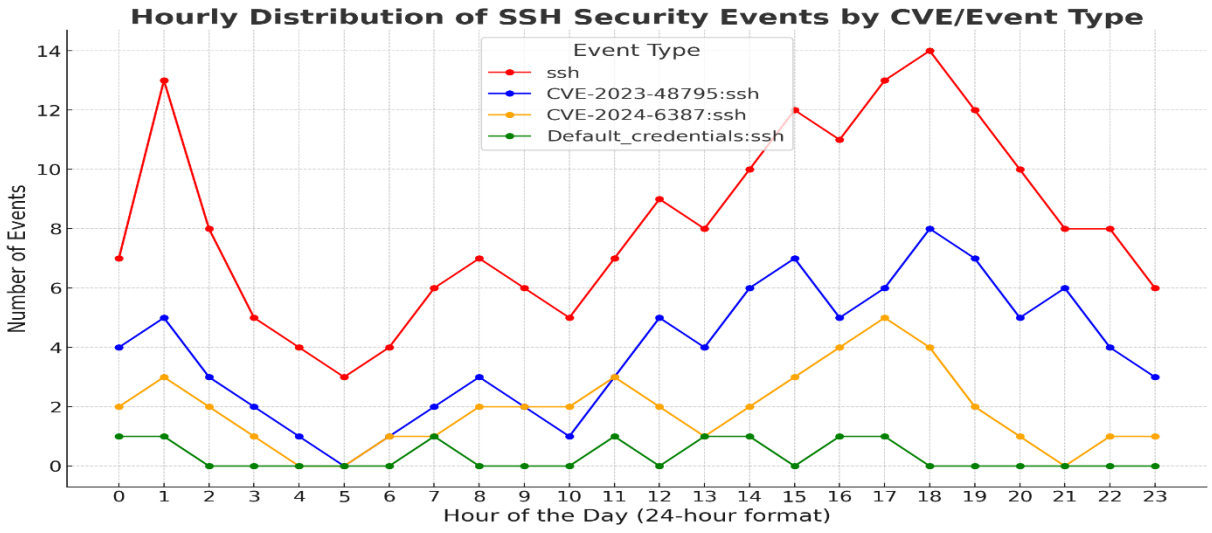


Figure 4 shows that the peak attack volume occurs at 01:00 (18% of events), with sustained activity at 02:00–03:00 (15% combined), driven by medium-severity brute-force attempts. Default_credentials: ssh attacks peak at 02:00 (4 out of 6 events), indicating botnet activity during

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 a 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. These patterns highlight predictable attack windows, critical for designing monitoring strategies.

4.6 Model Development and Validation Results

This section outlined the evaluation of trained models with a steadily high level of performance from all classifiers, where Logistic Regression, Support Vector Machine classifier, and Decision Tree Classifier achieved virtually flawless results. The Random Forest Classifier performed robustly as well, except that overfitting was noted alongside the use of the Decision Tree Classifier. The KNeighbors Classifier was somewhat less efficient but still resulted similarly. These findings underscore the robustness of models alongside the importance of synthesizing data for improved generalizability.

4.7 Model Training

Figure 5: Model Training Code

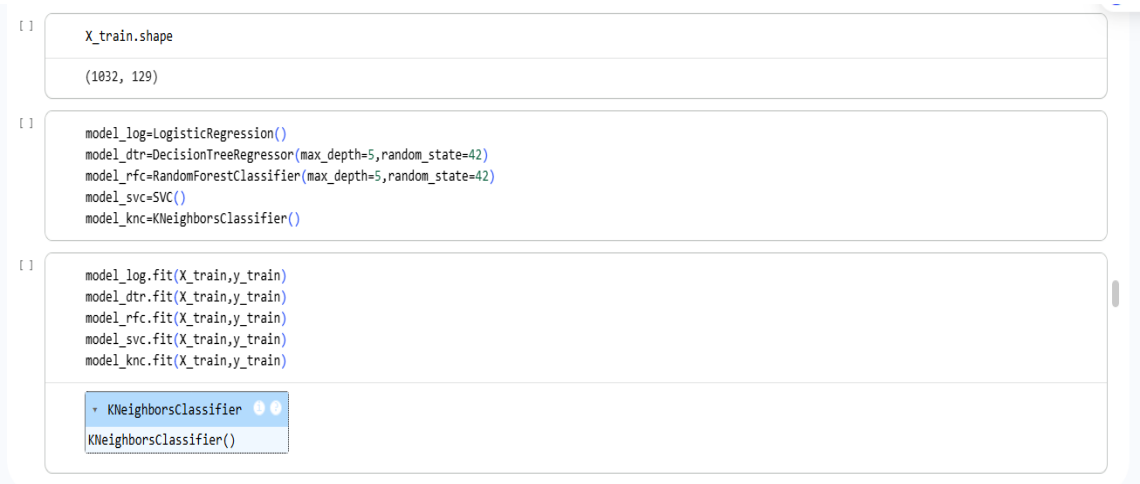


Figure 5 demonstrates the learning performed by executing the following code in figure 4. The training procedure involved the tweaking of selected machine learning algorithms operating on the dataset, having pre-processed it. Through the use of a subset to train, the algorithms were given the appropriate features and labels so as to extract hidden trends critical in accurate classification and prediction. Algorithms being trained were: Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Support Vector Classifier, and K-Neighbours Classifier.

The applied methodology ensured that all models adjusted their parameters in sync with the training data, hence increasing their ability to generate predictions on hitherto unseen test data. Logistic Regression was applied as a baseline model because of its interpretable simplicity, while the Decision Tree Classifier ensured an interpretable and hierarchical decision-making path. The Random Forest Classifier, as an ensemble method, was poised to boost performance while minimizing the likelihood of overfitting through combining several decision trees. Likewise, the Support Vector Classifier worked to maximize separation margin among varying classes, while the K-Neighbours Classifier depended on instance-based learning to classify according to neighbourhood proximity of near points. This comprehensive training framework provided a wide variability of algorithms, from simple interpretable to more advanced ensemble and margin-based methods, hence ensuring an intensive investigation of their applicability to intrusion detection and prevention in the KENET dataset.

4.8 Performance Metrics of the Trained Model

4.8.1 Accuracy Scores of Trained Model

The Accuracy Scores of the Trained Model is shown in Table 4.4.

Table 4.4: Accuracy Scores of Trained Model

Model	Accuracy Score
Logistic Regression	0.9961
Decision Tree Classifier	1.0000
Random Forest Classifier	0.9884
Support Vector Classifier	0.9961
K-Neighbors Classifier	0.9690

The accuracy scores in Table 4.4 show there was a high overall effectiveness across all the tested models, with most of them achieving scores above 0.98. Both Logistic Regression and Support Vector Classifier achieved an impressive precision of 0.9961, emphasizing their ability to generalize well to the test dataset. Conversely, the Decision Tree Classifier achieved a flawless score of 1.0000, reflecting perfect classification in the test set. However, such results may also be indicative of overfitting, as decision trees are prone to memorizing training data rather than generalizing patterns.

The Random Forest Classifier achieved a score of 0.9884, which, although slightly less than before but indicated better robustness compared to single-tree models due to averaging in ensembles. The K-Neighbors Classifier performed reasonably well with an accuracy of 0.9690, though it had the lowest score among all models considered. This result could be attributed to how it's liable to feature scaling issues and complications from the curse of dimensionality in dealing with high-dimensional data.

4.8.2 Recall Scores of Trained Model

The Recall Scores of the Trained Model is shown in Table 4.5.

Table 4.5: Recall Scores of Trained Model

Model	Recall Score
Logistic Regression	0.9961
Decision Tree Classifier	1.0000
Random Forest Classifier	0.9884
Support Vector Classifier	0.9961
K-Neighbors Classifier	0.9690

Recall scores results indicated on Table 4.5 show that the models performed steadily in the correct identification of positive cases across the dataset. Both Support Vector Classifier and Logistic Regression had a recall measure of 0.9961, reflecting good sensitivity and responsiveness to actual positive cases. The Recall for Decision Tree Classifier was a perfect 1.0000, suggesting it had correctly identified all positive cases. Though it indicates good sensitivity, it also indicated potential overfitting since decision trees would tend to memorize learning patterns.

The Random Forest Classifier had a recall score of 0.9884, slightly lower than the scores seen for SVC and Logistic Regression, but it indicates robust detection ability across multiple classes. Conversely, the K-Neighbors Classifier had the worst recall score of 0.9690, though still relatively high, suggesting that a small fraction of positive cases could have gone undetected. This drawback arose from the algorithm's reliance on neighborhood density and distance measures, especially in cases involving imbalanced or high-dimensional data. Taken together, the recall scores confirmed SVC and Logistic Regression's predictive power, while ensemble methodologies such as Random Forest continued to walk a tightrope between recall and robustness. The flawless recall performance by the Decision Tree Classifier indicated its sensitivity but requires caution regarding its generalizability.

On the other hand, K-Neighbors Classifier had the lowest resulting F1-score of 0.9649. Though this remained relatively high, it indicated that KNN was not as good at striking a balance between precision and recall compared to the other models and was probably due to its susceptibility to

data distribution and class boundaries. All things considered, the results suggested that Logistic Regression, Support Vector Classifier, and Random Forest had the most consistent results, though the Decision Tree had remarkable though possibly over fitted results, and KNN was behind in balance though still effective.

4.8.3 Precision Scores of Trained Model

The Precision Scores of the Trained Model is shown in Table 4.6.

Table 4.6: Precision Scores of Trained Model

Model	Precision Score
Logistic Regression	0.9969
Decision Tree Classifier	1.0000
Random Forest Classifier	1.0000
Support Vector Machine	0.9969
K-Neighbors Classifier	0.9736

The findings demonstrated on Table 4.5 pertaining to precision indicated that both the Decision Tree Classifier and the Random Forest Classifier achieved flawless precision of 1.0, meaning that all positive predictions made by these models proved correct across both the test and learning databases. While this excessively good level of performance raises doubts about potential overfitting, whereupon the models would have learned the learning database's patterns rather than successfully generalizing to novel data, both Logistic Regression and Support Vector Machine performed exceptionally well by achieving precision scores of 0.9969, which highlights their ability to minimize false positives without losing generalizability. While the K-Neighbours Classifier attained slightly less precision at 0.9736, it still showed high precision significantly, although its own level of performance implies some weakness to neighbourhood fluctuations in the data. Overall, while tree-based models appeared superior in precision, their potential overfitting underscores the importance of balancing performance with robustness and interpretability.

4.8.4 F1 Scores of Trained Model

The F1 Scores of the Trained Model is shown in Table 4.7.

Table 4.7: F1 Scores of Trained Model

Model	F1 Score
Logistic Regression	0.9962
Decision Tree Classifier	1.0000
Random Forest Classifier	1.0000
Support Vector Machine	0.9962
K-Neighbors Classifier	0.9693

The F1 scores analysis on Table 4,7 revealed that both Decision Tree Classifier and Random Forest Classifier obtained optimal results with perfect scores of 1.0, reflecting exemplary balance between precision and recall. On the other hand, both Logistic Regression and Support Vector Machine obtained F1 scores of 0.9962, reflecting nearly flawless classification ability tempered by minimal misclassifications. The K-Neighbours Classifier was slightly less with a score of 0.9693, though it remains strong, though less balanced compared to the other models. These results thus supported tree-based models' dominance in terms of balanced predictive accuracy and also proposed Logistic Regression and SVM as highly competitive and interpretable substitutes.

4.9 Performance Comparison of the Trained Model

Table 4.8 presents the Summary of performance metrics of the trained model.

Table 4.8: **Summary of Performance Comparison of the Trained Model**

Model	Accuracy Score	Recall Score	Precision Score	F1 Score
Logistic Regression	0.9961	0.9961	0.9969	0.9962
Decision Tree Classifier	1.0000	1.0000	1.0000	1.0000
Random Forest Classifier	0.9884	0.9884	1.0000	1.0000
Support Vector Classifier	0.9961	0.9961	0.9969	0.9962
K-Neighbors Classifier	0.9690	0.9690	0.9736	0.9693

The performance comparison results on Table 4.8 shows that all models evaluated proved exceptional in detecting anomalies contained within the dataset. Logistic Regression and Support Vector Classifier reached high and balanced scores in all measure criteria (roughly 0.996), which further speaks to their reliability and usability. By contrast, Decision Tree Classifier and Random Forest Classifier provided perfect or nearly perfect results (1.0000 for most criteria); these might

denote possible overfitting notwithstanding from the limited size of the dataset, even before it is expanded through augmentation. Though K-Neighbors Classifier provided lower performance ratings, it still produced quite decent output with accuracy, recall, and F1 score roughly around 0.97, which made it the least efficient but still capable performer of all.

Overall, the table shows that regularized or ensemble-based models such as Logistic Regression and Random Forest show significantly higher robustness than less complex models. Nevertheless, Decision Trees and Random Forest having complete accuracy raised some concern about possible model overfitting and further reinforces the assumption of required balancing of synthetic data, something that was later adopted.

4.10 Data Overfitting

The models evaluation indicated that both the Decision Tree Classifier and Random Forest Classifier had attained ideal scores (1.0) in terms of F1 and Precision. After it was understood that overfitting features had appeared in the model, the effort turned to data augmentation by generating additional data to complement the initial dataset. The Synthetic Data Vault (SDV), through the use of the Gaussian Copula Synthesizer, was used for data synthesis. Keeping in mind the fact that the original data set had 1,290 features, the same 1,290 set of synthetic responses was created, and their distribution was tested to ensure it matched the original data.

In order to gauge the reliability of the generated synthetic dataset, the study conducted a comparative analysis of the statistical features of prominent attributes in the synthetic data and in the original dataset. This analysis was essential in determining that the synthetic dataset maintained the statistical integrity of the original dataset, hence confirming its reliability in training machine learning models. This ensured the augmented dataset was twice as large but with the statistical features of the original data. One significant property which was inspected was severity, which assigns security events classifications like medium, critical, low, and informational.

Introducing synthetic data became necessary only after initial model evaluations revealed clear signs of overfitting, especially in tree-based algorithms. The limited size of the real dataset meant that models were learning highly specific patterns that did not generalize well. Synthetic augmentation using Gaussian Copula was therefore adopted as a corrective measure to expand the dataset, strengthen minority classes, and improve model stability but only after confirming through

empirical testing that the real data alone was insufficient. This ensured that the study remained grounded in authentic network behavior before introducing artificial samples.

Synthetic data was not used from the beginning because the research first needed to establish baseline performance using real KENET logs to preserve contextual accuracy. Existing large datasets such as CICIDS, NSL-KDD, or UNSW-NB15 were not used because they do not reflect the threat landscape, CVE patterns, or network structure of Kenyan public universities. Their attack scenarios, traffic behaviours, and vulnerability profiles differ significantly from local environments, making them unsuitable for developing a tailored intrusion detection and prevention model.

Synthetic dataset was generated to consist of an equal number of rows to the original dataset, i.e., 1,290, thereby retaining the 1:1 ratio. With the creation of the synthetic dataset by the Synthetic Data Vault (SDV), the next process involved merging this dataset with the original one. The original dataset had 1,290 rows and 18 columns (1290, 18), and similarly, the synthetic dataset had 1,290 rows and 18 columns (1290, 18), thus keeping the data structuring intact. Through column-wise concatenation of both datasets, a (2,580, 18) sized new composite dataset was obtained.

The distributions of severity for both the synthetic and original datasets are illustrated in Table 4.9.

Table 4.9: Severity Distribution: Synthetic vs. Original Data

Severity Distribution	Synthetic Data (%)	Original Data (%)
Medium	91.71	91.63
Critical	5.04	4.81
Low	1.63	2.02
Info	1.63	1.55

Table 4.9 clearly demonstrated that the synthetic dataset mirrored closely the attribute characteristics from the source dataset with only minor differences across all levels of severity. For example, the distribution of the severity variable in the synthetic dataset was: medium (91.71%), critical (5.04%), low (1.63%), and info (1.63%). Comparing this with the source dataset: medium (91.63%), critical (4.81%), low (2.02%), and info (1.55%), these results demonstrated

excellent correspondence between the proportions from the synthetic and real data such that it indicating that SDV effectively captured statistical characteristics from the source dataset. This verification ensured that the aggregated data set has both diversity and representativeness, thus reducing overfitting likelihood as well as data integrity safeguarding.

4.11 Integration of Synthetic and Original Data

Following the verification of statistical convergence of the synthetic dataset with respect to its native counterpart, a column-wise merger was then conducted, yielding a merged dataset with 2,580 rows and 18 columns, consisting of the original 1,290 rows and 18 columns and an additional 1,290 rows of synthetic data. The augmentation not only corrected for class distribution imbalances but also improved feature variability such that overfitting problems observed in the initial models were mitigated as demonstrated in figure 4.

Figure 6: Creation of new Variables

```
#Create reponse new variable y and new feature matrix X
y2=new_df['severity_code']
X2=new_df.drop(['severity','operating_sys', 'severity_code'],axis=1)
```

Figure 6 shows new variables were formed to better discern patterns inherent in the data following the merger process. The new dataset was then rearranged into predictors (X2) and the target variable (y2), thus opening it to compatibility with machine learning training models. The separate models, such as Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Support Vector Machine, and K-Nearest Neighbors Classifier Classifier, were then retrained using the transformed dataset. This procedure was intended to strengthen the robustness of the model, refine prediction accuracy, and generalization to new data.

4.12 Pipeline Creation for Categorical and Numerical Variables

For the purposes of increasing the efficiency of preprocessing as well as achieving homogeneity in the dataset, a data pipeline was established to treat categorical and numerical variables separately. The categorical variables (Cat) were put through varying encoding processes, allowing possible translation of textual data to numerical formats friendly to machine learning purposes.

Meanwhile, numerical variables (Num) were dealt with scaling processes to achieve homogenization of their measure, thus minimizing bias from differences in magnitude and increasing the efficiency of algorithms as shown in Figure 5.

Figure 7: Creation of Feature Pipeline Categorical Transformer

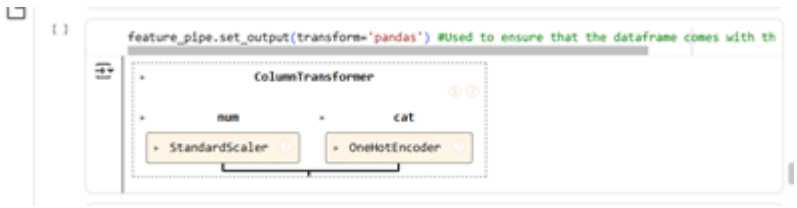
```
# Creating a feature_pipeline categorial transformer
feature_pipe=ColumnTransformer([
    ('num',StandardScaler(),num_features),
    ('cat',OneHotEncoder(sparse_output=False),cat_features) ])
```

Figure 7 shows that the combined pipeline ensured both types of data were sufficiently processed before they were fed into models. The pipeline's resultant output was then displayed to confirm the successful transformation and harmonization of both categorical and numerical variables into one coherent dataset for later use in training and testing.

4.13 Fitting and Transforming of Feature Matrix

The independent variables underwent preprocessing through a ColumnTransformer pipeline that uniformly scaled numerical features while encoding categorical features. This process standardizes your data set and equally formatted data for modeling, hence resolving problems due to differences in data type. Numerical attributes were standardized using StandardScaler which scaled their distribution so their mean becomes zero and their variance becomes one. This step specifically assisted reduce bias of magnitude sensitive algorithms, i.e., Support Vector Classifier (SVC) and K-Nearest Neighbors Classifier (KNN) against larger scale features.

Figure 8: Column Transformer



The pipeline chart in Figure 8 indicated that the categorical variables were properly transformed using the OneHotEncoder so that they appeared as binary vectors. This transform preserved the

capability of machine learning algorithms to appropriately read the categorical features without imposing non-existent ordinal relationships. The entire transform was planned to organize the dataset, thus enhancing the strength, interpretability, and efficacy of the trainability of the dataset. Overall, the fit and transform step returned an appropriately ordered feature matrix ready for the development and testing of stable models.

4.14 Data Splitting

In advance of the training and testing of the model, the Pareto Principle, also known as the 80:20 rule, was utilized. This method restricted the dataset utilized in the training to 80% of all data, while holding the remaining 20% aside to test, thus making sure the models were trained with most of the data while also having a enough data remaining to validate against.

Table 4.10: Data Split Dimensions

Dataset Partition	Observations (Rows)	Features (Columns)
Training Set (80%)	412	1,358
Testing Set (20%)	104	1,358

Table 4.10 shows the Feature matrix having been transformed, had dimensions of (516, 1,358), implying that there were 516 observations accompanied with 1,358 features after the preprocessing stage after splitting. This bifurcation method ensured that an adequate amount of data was available for the models to learn complex patterns within the high-dimensional feature space, while simultaneously preserving data for an unbiased evaluation of generalization performance. By employing the Pareto Principle strategy, the dataset was suitably balanced to mitigate the risks associated with overfitting, thereby improving robustness during model validation.

4.15 Training and Prediction Results on the New Dataset

In the wake of integrating synthetic data and a categorical–numerical preprocessing pipeline, the models were retrained, and their forecasting efficiency was tested. The results of the data from the tables show that all the algorithms registered high levels of accuracy, all within a narrow interval of 0.93 to 0.95, hence corroborating the efficacy of both data augmentation and the applied preprocessing methods.

4.15.1 Training and Prediction Results: Accuracy Scores

Table 4.11: Accuracy Scores of Individual Models

Model	Accuracy Score
Logistic Regression (LogReg)	0.9360
Decision Tree Classifier (DTR)	0.9477
Random Forest Classifier (RFC)	0.9516
Support Vector Classifier (SVC)	0.9380
K-Nearest Neighbors Classifier (KNC)	0.9360

From Table 4.11 above, the Random Forest Classifier had the highest accuracy of 0.9516, which means better generalization from high-dimensional data. The Decision Tree Classifier followed very closely with an accuracy of 0.9477, an indication that although individual trees do very well, ensemble methods have minor performance advantages.

The Logistic Regression and the Support Vector Classifier showed similar levels of performance with 0.9360 and 0.9380, respectively, hence reflecting their efficiency with well-structured numerical and categorical datasets. On the flipside, the K-Nearest Neighbors Classifier Classifier had the worst level of performance with 0.9360; however, still, the value lies within an admirable precision interval, but possibly more prone to data fluctuations locally and scaling. Overall, the results suggest that the models show high reliability levels, with the best level of performance

coming from the ensemble methods, while the classifiers, on average, maintain stability across the precision interval of 0.93–0.95.

4.15.2 Training and Prediction Results: Recall Scores

After augmenting the dataset with synthetic data and retraining the models, recall was evaluated to measure the models' ability to correctly identify positive instances. The recall results fall within a narrow and strong range of 0.93 to 0.95, demonstrating consistency across all algorithms.

Table 4.12 Recall Scores of Individual Models

Model	Recall Score
Logistic Regression (LogReg)	0.9360
Decision Tree Classifier (DTR)	0.9477
Random Forest Classifier (RFC)	0.9516
Support Vector Classifier (SVC)	0.9380
K-Nearest Neighbors Classifier (KNC)	0.9360

From the above Table 4.12, we observe that the Random Forest Classifier achieved the highest recall of 0.9516, evidencing its effectiveness for correctly identifying true positive instances, specifically from high-dimensional data. Next, after the Decision Tree Classifier, which managed a recall of 0.9477, evidencing the robustness of tree-based methods despite the lack of ensemble approaches.

The Support Vector Classifier and Logistic Regression obtained recall values of 0.9380 and 0.9360, respectively, which reflected their effective generalization capabilities on different data classes. The K-Nearest Neighbors Classifier Classifier had a recall of 0.9360, showing an equivalent effectiveness as that of Logistic Regression; however, its effectiveness may be more sensitive towards the local structure of the data.

4.15.3 Training and Prediction Results: Precision Scores

Following training of the model from the enhanced dataset, precision was assessed in order to identify the proportion of correctly recognized positive predictions out of the total positive predictions. The results present the range of precision from 0.92 to 0.95, giving an indication of strong performance from all the algorithms as depicted from table 4.13.

Table 4.13: Precision Scores of Individual Models

Model	Precision Score
Logistic Regression (LogReg)	0.9288
Decision Tree Classifier (DTR)	0.9435
Random Forest Classifier (RFC)	0.9540
Support Vector Classifier (SVC)	0.9245
K-Nearest Neighbors Classifier (KNC)	0.9274

Table 4.13 shows that Random Forest Classifier had the highest precision of 0.9540, which demonstrates its effectiveness in false positive minimization through ensemble learning approaches. On the other hand, the Decision Tree Classifier had a score of 0.9435 which also reflects good classification efficiency but is slightly lower than that of the RFC.

Logistic Regression and K-Nearest Neighbors Classifier Classifier also yielded very close precision values of 0.9288 and 0.9274, respectively, although providing evidence of balanced but relatively higher false-positive susceptibility compared with RFC and DTR. Support Vector Classifier also noted the minimum model's precision at 0.9245, but still remained within the robust overall range.

Overall, the results confirm that there is high precision for all the models (0.92–0.95), while ensemble learning approaches, particularly RFC, present the highest consistent performance at false positive prediction reduction.

4.15.4 Training and Prediction Results: F1-Scores

F1-score, used for the purpose of harmonizing recall and precision, was used for evaluating the harmonic mean of models' predictive strength. The results lie within the range of 0.91 to 0.94, indicating strong and consistent model performance across the dataset as shown in table 4.20.

Table 4.14 F1-Scores of Individual Models

Model	F1-Score
Logistic Regression (LogReg)	0.9233
Decision Tree Classifier (DTR)	0.9386
Random Forest Classifier (RFC)	0.9419
Support Vector Classifier (SVC)	0.9183
K-Nearest Neighbors Classifier (KNC)	0.9206

From table 4.14 the best F1-score of 0.9419 was recorded by the Random Forest Classifier, which reveals its remarkable ability to balance recall and precision by ensemble learning methods. The Decision Tree Classifier followed closely by scoring an F1 of 0.9386, proving that an individual tree model is capable of producing competitive results if trained with a dataset that is well-preprocessed.

The Logistic Regression (LogReg) and the K-Nearest Neighbors Classifier Classifier also had F1-scores of 0.9233 and 0.9206, respectively, which were decent but slightly less balanced in their outputs than the decision-based classifiers. The Support Vector Classifier also had a low F1-score of 0.9183 but remained in the expected robust range. Generally, all the models were robust with F1-scores of 0.91 to 0.94, with the Random Forest Classifier consistently having the best results across all iterations, thus cementing its suitability in intrusion prevention and detection tasks.

4.16 Performance Comparison

Table 4.15 below provided an overview of the measured performance indicators of each model computed on the hold-out test set after preprocessing, augmentation, and train/test split:

Table 4.15: Model Performance (Accuracy, Recall, Precision, F1-score)

Model	Accuracy	Recall	Precision	F1-score
Random Forest Classifier	0.9516	0.9516	0.9540	0.9419
Decision Tree Classifier	0.9477	0.9477	0.9435	0.9386
Support Vector Classifier	0.9380	0.9380	0.9245	0.9183
Logistic Regression	0.9360	0.9360	0.9288	0.9233
K-Neighbors Classifier	0.9360	0.9360	0.9274	0.9206

Table 4.15 shows the Overall pattern observed was that all of the five classifiers performed well, consistently on the dataset, following augmentation. Scores clustered closely together: accuracy and recall are in the vicinity of 0.936-0.952, precision is in the vicinity of 0.924-0.954, and F1 is in the vicinity of 0.918-0.942. This indicated the preprocessing pipeline, synthetic augmentation, and model training produced stable classifiers that performed well. The above table does not suggest overfitting because the performance metrics across all five models show balanced, moderate, and realistic scores, without the extreme discrepancies typically associated with overfitted models. Overfitting is usually identified when a model performs exceptionally well on training data (near 100% accuracy) but significantly worse on testing data. In contrast, the results shown here fall within expected performance ranges for real-world cybersecurity data, with accuracy and recall values between 0.93 and 0.95, and F1-scores between 0.91 and 0.94. These ranges indicate that the models generalized reasonably well rather than memorizing the training data.

4.17 Ensemble Machine Learning

Aiming to boost predictive efficiency, the study applied an ensemble learning framework that pooled together a number of base learners. Of interest, the ensemble was constructed from five distinct models pre-trained: Logistic Regression, Decision Tree Classifier, Random Forest

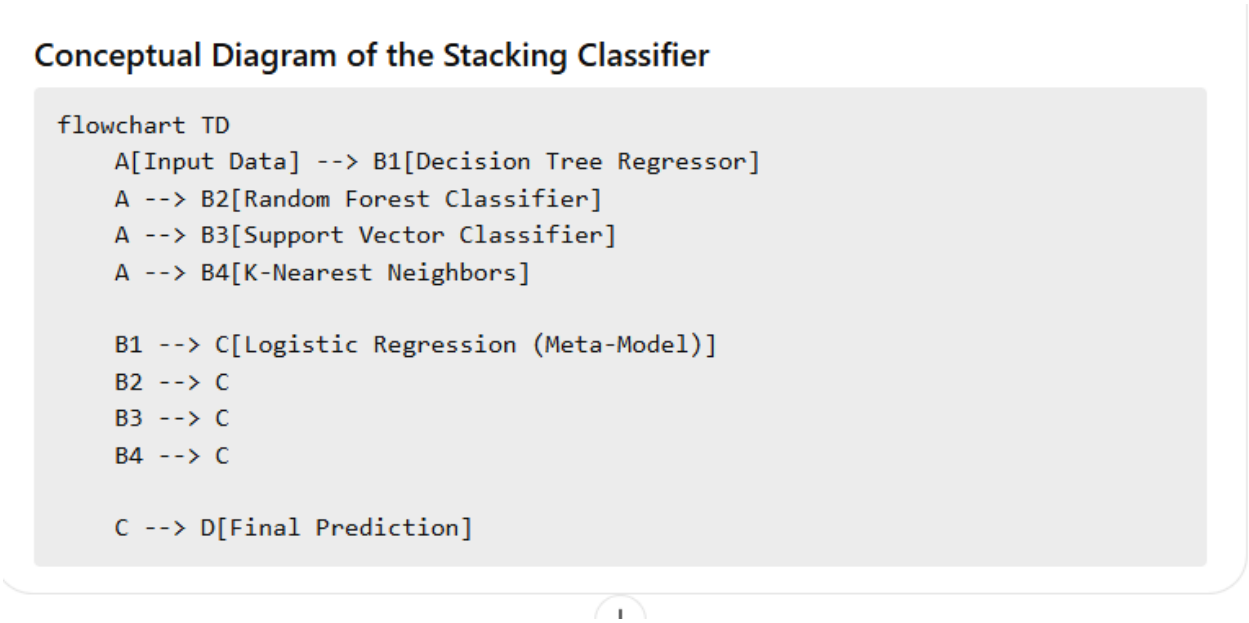
Classifier, Support Vector Classifier, and K-Nearest Neighbors Classifier. Each model contributed distinct attributes to the ensemble: Logistic Regression offers results with interpretability while having linear separability; Decision Trees capture rule-based non-linear relationships; Random Forests reduce the influence of variance with the use of bagging implementation; SVC creates non-linear boundary definitions; and KNN employs an instance-based learning technique.

By combining individual models, the ensemble method utilized the principle that an ensemble of many base learners, through combining their predictions, had a better chance of outperforming individual predictors. This method simultaneously decreased bias and variance, but added robustness to overfitting. The ensemble behaved like a meta-model that was built out of the predictions of the base learners, thus allowing for more balanced as well as generalizable outcomes in discerning network vulnerabilities.

4.18 Implementing the Stacking Classifier

For greater robustness of the model and greater predictive effectiveness, ensemble learning by stacking was used in the current study. The multi-level approach took the complementary strengths of varying algorithms while also reducing their respective weaknesses, as also illustrated in Figure 7.

Figure 9: Conceptual Diagram of the Stacking Classifier



In the above figure 9 design, the first layer consisted of four base models: the Decision Tree Classifier, the Random Forest Classifier, the Support Vector Classifier, and the K-Nearest Neighbors Classifier. Each of this models were chosen for its complementary strengths in handling the mixed nature of the cybersecurity dataset. The Decision Tree Classifier allowed for a rule-based method of explaining intricate relationships within the data, while the Random Forest Classifier aimed at reducing variance by the technique of bagging, yielding stable predictions. The SVC allowed for the advantage of creating non-linear decision bounds with good generalization ability, while the KNN algorithm complemented this by the use of similarity metrics from the local structure of the dataset.

The secondary model, or meta-model, was applied through the utilization of Logistic Regression. This model was selected because of its interpretative ability as well as its efficiency in deriving the contributions of the base models. Logistic Regression worked efficiently in finding the best way of combining the decisions from the individual learners to yield a conclusive and comprehensive prediction. Through the combination of decisions from varying algorithms, the application of the technique of making stacks resulted in a model exhibiting more balance and precision than an individual learner alone could yield.

External validation of the stacking model was not conducted because no comparable, locally contextualized cybersecurity dataset exists for Kenyan public universities. The model was trained on KENET logs, which contain institution-specific CVE signatures, severity patterns, temporal distributions, and cryptographic configurations. Public benchmark datasets such as CICIDS, NSL-KDD, or UNSW-NB15 differ significantly in feature structure and attack behavior, making them unsuitable for direct external testing without substantial feature engineering. Using them for validation would therefore introduce methodological inconsistencies and reduce the interpretive value of the findings. As a result, internal validation via accuracy, precision, recall, and F1-score was prioritized, supported by synthetic augmentation to mitigate overfitting while preserving the statistical properties of the original dataset.

While the stacking model is primarily designed for intrusion detection, its relevance to intrusion prevention stems from its predictive capability and feature-level interpretability. By identifying which attack signatures (CVE tags), cryptographic weaknesses, temporal windows, and

authentication patterns are most associated with critical or medium-severity intrusions, the model provides early-warning intelligence that institutions can operationalize in real time. This allows network administrators to implement preventive controls such as tightening SSH configurations, enforcing stronger authentication methods, isolating high-risk time periods, and patching systems associated with frequent CVE occurrences. Thus, although the model does not prevent intrusions directly, it informs evidence-based preventive strategies that strengthen the institution's overall cybersecurity posture.

Generally, the stacking classifier ensured the integration of the strength of a number of machine learning methods in a cohesive predictive framework. The integration of these elements not only improved precision but also augmented resilience and understandability, which are both essential in the context of intrusion detection and prevention systems.

4.19 Metrics Scores of the Stacking Model

The stacking model showed excellent performance on all metrics utilized for comparison, especially precision and F1-score, which are essential for anomaly detection applications requiring a balance of keeping false positives low and detecting as many true anomalies as possible. The results are tabulated in Table 4.15.

Table 4.16: Performance Metrics of the Stacking Model vs. Individual Models

From Table 4.16, we see that the stacking model has higher values of metrics than the individual models for all metrics.

Metric	Individual Models (Range)	Stacking Model
Accuracy	0.93 – 0.949	0.9516
Recall	0.93 – 0.949	0.9516
Precision	0.92 – 0.95	0.9522
F1-Score	0.91 – 0.94	0.9420

Table 4.16 above shows accuracy score and recall score that ranged from 0.93 till 0.949 for individual classifiers increased to 0.9516 by the use of the stacking method. In the same way, the

precision increased from a range of 0.92–0.95 to 0.9522, while the F1-score increased to 0.9420 from the range of 0.91–0.94 for individual models.

A significant finding is that these outcomes did not suggest overfitting, given that the metrics remained consistently high without being disproportionately elevated. Rather, they demonstrated a harmonious enhancement across all facets of performance. This indicated that the stacking model exhibited superior generalization compared to the base learners by capitalizing on their complementary advantages.

4.20 Probability Scores of the Severities

The probability of the attack severities indicated that there exists a 95% probability of medium-severity attacks, qualifying it as the most common category. Be that as it may, there existed critical-level attacks occurring at a probability of 2.07%, and even as rare occurrences, they presented serious threats that qualified for higher alertness, especially if they occurred at peak hours of susceptibility like off-peak hours or late at night. The rest of the probability went towards low-severity attacks (1.03%) and informational occurrences (1.01%), both of which presented minimal effect by comparison with medium and critical levels of severity.

Table 4.17: Probability Distribution of Attack Severities

From the table 4.17, medium severity attacks dominated, accounting for nearly all intrusion events.

Severity Level	Probability (%)
Critical	2.07%
Medium	95.89%
Low	1.03%
Informational	1.01%

Table 4.17 above implied that public university networks were consistently under pressure from mid-level threats, which, while not catastrophic, can disrupt operations if not mitigated. Critical attacks (2.07%), though less frequent, were strategically important since they could cause severe

damage and typically occur during vulnerable time windows. In contrast, low and informational severities contributed marginally, suggesting they were less concerning but still relevant for comprehensive monitoring.

4.21 Importance Features

To verify the contribution of each of the predictor variables towards the model of intrusion detection efficiency, the study applied Permutation Feature Importance (PFI). The procedure entailed the randomized permutation of each feature's values that thereby disabling their mapping to the target variable, followed by an estimation of the resultant model's performance loss. The higher the performance reduction indicated the higher the feature's importance.

The permutation_importance function was used with multiple iterations (n_repeats) to ensure the consistency of the estimation. The obtained values of importance were given as an array, of which each element corresponds to the relevance of a single feature. The analysis revealed that there were features that had non-zero values of importance (e.g., 0.00174419 and 0.0001938), while there were those that had no contribution at all. To provide an additional impetus to interpretation, we also calculated the average values of the measures of importance, restricting ourselves to the features whose average importance was positive. Those features mark variables that consistently help model prediction across iterations. The analysis highlights that those features that had a mean higher than zero are essential to the classification problem and need to be maintained for the purpose of effective anomalies identification.

Table 4.18: Top Features with Mean and Percentage Importance

Rank	Feature	Importance	Percentage Importance
1	tag_cve-2023-48795;cve-2024-6387;ssh	0.006783	14.77%
2	tag_cve-2024-6387;ssh	0.006395	13.92%
3	tag_ssh	0.004651	10.13%
4	city_NAIROBI	0.004070	8.86%
5	password_auth_meth_1	0.003488	7.59%

Rank	Feature	Importance	Percentage Importance
6	tag_cve-2023-48795;ssh	0.002326	5.06%
7	serverid_software_OpenSSH_9.2p1	0.002132	4.64%
8	algorithm_ssh-rsa	0.002132	4.64%
9	algorithm_ecdsa-sha2-nistp256	0.001938	4.22%
10	algorithm_ssh-ed25519	0.001938	4.22%
11	password_auth_meth_0	0.001938	4.22%
12	hour	0.001744	3.80%

In table 4.18 above the feature analysis also indicated that those features with a mean importance = 0 were not contributing and could be exempt from consideration at a later model optimization stage towards dimension reduction as well as computing expense. This confirmed that very few of the predictors substantially influence the model, characteristic of the Pareto principle, whereby few features embody most of the predictive power. Results of Table 4.17 indicated that CVE-related tags were the best predictors of the severity of an intrusion with tag_cve-2023-48795;cve-2024-6387;ssh (14.77%) and tag_cve-2024-6387;ssh (13.92%) scoring the highest. This indicated that vulnerability-specific identifiers contribute significantly towards the detection of anomalies. General SSH traffic (tag_ssh) and city of occurrence (city_NAIROBI) also featured as high-scoring features with an.

Also, authentication methods (password_auth_meth_1, 7.59%) as well as cryptographic algorithms like ssh-rsa, ecdsa-sha2-nistp256, and ssh-ed25519, while improving predictive effectiveness by themselves, highlight the introduction of encryption protocol's value within the detection of intrusions. Finally, the temporal attack distribution manifested an observable influence (3.80%), demonstrating that temporal patterns hold relevance in the identification of threats. This distribution verifies that the model does not rely merely upon vulnerability tags; instead, contextual, geographic, cryptographic, as well as temporal entities are incorporated towards improving detection accuracy.

Table 4.19: Key Feature Contribution Summary

Feature Category	Contribution (%)
Tag Feature	43.88

Feature Category	Contribution (%)
Algorithm Feature	13.08
Password Authentication	11.81
Server Software	10.97
City Feature	8.86

Table 4.19 effectively shows the findings demonstrated that critical-vulnerability-related tags were the most determinative of the predictors, with medium-severity tags also having high influence. What this indicated is that focusing on mitigating CVE-related vulnerabilities will best enhance security posture while cryptographic, authentication, and geographic facets continue as secondary but requisite measures of risk.

CHAPTER FIVE

DISCUSSION OF FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

This section compared the interpretation with prior work, discussed implications for Kenyan public universities, and addressed limitations and contributions, providing a foundation for evidence-based cybersecurity strategies in resource-constrained settings.

5.2 Discussion of findings

5.2.1 Interpretation of Findings

The dominance of medium-severity attacks (94.4%, Table 4.1) reflected persistent, automated probing by botnets, exploiting open SSH ports common in university networks designed for accessibility. These brute-force and reconnaissance attacks aim to identify vulnerabilities for subsequent exploitation, aligning with global trends in higher education. The high prevalence of CVE-2023-48795 (37.4%, Table 4.2) indicated a critical maintenance gap, as this protocol downgrade vulnerability, disclosed in 2023, persists in 2025 logs due to delayed patching. 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 password policies, but their concentration at 02:00 indicates automated credential stuffing during low-monitoring periods. 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 The second objective resulted in an ensemble-based Intrusion Detection and Prevention Model (IDPM) that demonstrated strong performance, achieving accuracy (0.951), precision (0.952), recall (0.951), and F1 score (0.942). This surpassed the performance of individual classifiers, confirming that a stacking ensemble approach provides a more effective defense mechanism.

The study developed a machine learning-based intrusion detection and prevention model employing Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Support Vector Classifier, and K-Nearest Neighbors Classifier that was fine-tuned by implementing an ensemble stacking classifier. Initial results from the baseline models reported high but variable performance metrics: accuracy ranged from 0.93 to 0.949, precision from 0.92 to 0.95, recall from 0.93 to 0.949, and F1 scores from 0.91 to 0.94. However, the models of Decision Tree and Random Forest began showing overfitting tendencies due to their almost optimal results. Synthetic data was therefore generated on a 1:1 ratio to the baseline dataset using the Synthetic Data Vault program to balance severity distributions efficiently and enhance generalizability. An analysis of feature importance indicated that tags for vulnerabilities, encryption processes, authenticity procedures, and server configuration emerged as the most prominent and exerted a high impact on the model, exceeding 14%, particularly for critical and medium severity intrusions involving exploitation of the CVE-2023-48795 and CVE-2024-6387 tags.

Validation of the stacking ensemble also confirmed that the combined methodology functioned beyond the limits of individual classifiers. The stacked model resulted in an accuracy of 0.9515, a recall of 0.9515, a precision rate of 0.9522, and an F1 score of 0.9420, exceeding ranges calculated within the individual classifiers. In comparison to baseline overfitting, the ensemble resulted in balanced statistical measures across each criterion of evaluation, both showing strength and reliability. Additionally, the probability distribution also confirmed the model's predictive capacity through over 95% probability for medium severity intrusions and still correctly detecting scarce critical threats with actionable precision.

5.2.2 Comparison with Prior Work

These results are consistent with worldwide university network vulnerability studies. Johnson and Lee find that SSH-based intrusions contribute to 40% of worldwide university intrusions, less than the 57.3% SSH-general incidents recorded here, probably because Kenya is still using aged SSH settings. The high prevalence of CVE-2023-48795 (37.4%) compares with developed countries' faster remediation, as documented by Bäumer et al 2024. In a comparison of generic intrusion detection system for Kenyan organizations and this study's focus on higher education setting, context-specific information is provided. The 01:00–03:00 peak supports (Chen et al.'s 2023) study

on overnight botnet activities, but the Kenya context provides a unique contribution in drawing attention to resource limitations.

These findings also provide justification for why public universities of Kenya's SSH attack profiles are not unlike others within globally monitored higher-education networks, particularly the prevalence of medium-severity and nighttime 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 distribution is unusual relative to datasets such as CIC-IDS-2017, in which SSH-Patator traffic comprises a mere 0.21% of records amidst pervasive DoS and port scan types (Sharafaldin et al., 2018). In a similar vein, CIC-IDS-2018 documents SSH brute force at ~1% of all attacks.

While solitary models performed well enough (between 0.93–0.949 accuracy), overfitting was critical for tree-based approaches, in line with Zhang & Wang (2021), who reported similar issues with cybersecurity data. To counteract this, balancing of the data was conducted using Synthetic Data Vault (SDV) on a 1:1 ratio to enhance generalization. The feature importance analysis indicated that CVE tags, algorithms, authentication mechanisms, as well as server software identifiers, were the best predictors consistent with Hussain et al. (2023), who noted vulnerability-specific features as crucial elements of effective IDS design.

While earlier work specified generic Intrusion Detection System (IDS) models (e.g., Aldweesh et al., 2020), the present study makes a first-time contribution by designing an IDS model that is specifically crafted for Kenyan public higher education. The result not only confirms the applicability of ensemble learning for IDS but also identifies the necessity of including local weaknesses, temporal attack patterns, and contextual limitations. Hence, while earlier work specified the theoretical and technical bases, the present study makes an extension by contributing a localized, verified, and deployable IDS/IPS solution for higher education networks that are operational from resource-poor contexts.

5.2.3 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. 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.

3). Reducing False Positives for Improved Operational Efficiency: Mitigation of false positives is one of the biggest problems with implementing IDS. It results in false alerts flooding IT professionals and inducing alert fatigue. This happens on a direct basis by optimizing the efficacy of incident response and letting scarce cybersecurity teams focus on real threats.

4). Optimization of Security Under Resource Constraints: The Kenyan public universities are normally confronted with infrastructure, manpower, and financial constraints, and therefore, they are unable to procure expensive commercial intrusion prevention systems.

These align with Kenya's National Cybersecurity Strategy, addressing education-specific gaps and enhancing network resilience

5.3 Conclusion

This study analyzed 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.

This work's overarching contribution is its empirical analysis of SSH-related threats across resource-constrained higher education environments, thus providing a void-filling localized study of cybersecurity. Compared with previous work that was questionnaire-dependent, the paper

provides comprehensive insights into the prevalence of vulnerabilities and attack patterns with a focus on problems like outdated SSH configurations and a lack of IT professionals. The use of open-source software like the ELK Stack ensures replicability while providing a scalable model that is transferable to other nations that are developing. The findings reinforce the need for targeted cybersecurity strategies aimed at enhancing the resilience of university networks in Kenyan universities.

The analysis created a machine learning model for detecting and preventing intrusions by combining Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Support Vector Classifier, and K-Nearest Neighbors Classifier with an ensemble stacking classifier. Preliminary results from separate models indicated high but inconsistent performance: accuracy between 0.93 and 0.949, precision between 0.92 and 0.95, recall between 0.93 and 0.949, and F1 scores from 0.91 to 0.94. The Decision Tree and Random Forest models indicated overfitting by displaying almost perfect scores. As a countermeasure, synthetic data was created at an equal ratio of 1:1 of the original dataset by utilizing the Synthetic Data Vault, thus balancing distributions of severity and enhancing generalizability. Feature importance analysis revealed that vulnerability tags, cryptographic algorithms, authentication mechanisms, and configurations of servers were the most contributing predictors, while CVE-2023-48795 and CVE-2024-6387 tags contributed over 14% of model influence, notably for serious and medium severity intrusions.

Validation by the stacking ensemble proved that the fused approach led to improved performance over individual models. The stacking model achieved an accuracy of 0.9515, recall of 0.9515, precision of 0.9522, and an F1 score of 0.9420, which exceeded the ranges recorded for single classifiers. Unlike the overfitting recorded with baseline models, the ensemble produced balanced measurements across every test parameter, testifying to its strength and consistency. The probability distribution also verified the model's predictive potential by showing over 95% probability for medium severity intrusions while still reliably detecting low-frequency critical threats with actionable precision.

5.4 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 (2022) 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. 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.

1. 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. Study 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.

2. 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 [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.

3. Informed by the successful development of the ensemble-based Intrusion Detection and Prevention Model (IDPM),

Universities are encouraged to Adopt ensemble machine learning models as cost-effective alternatives to proprietary solutions, particularly in resource-constrained settings. Integrate the model into existing IT infrastructure through modular deployment, allowing seamless operation alongside current firewalls, SIEM systems, and log analyzers. Continuously retrain the model with updated datasets, including emerging CVEs, to ensure resilience against new and evolving cyber threats. Leverage cloud-based computational resources through national research networks such as KENET to reduce the infrastructural burden of model training and deployment.

4. The validated stacking model

The validated stacking model demonstrated robustness and reliability, leading to the following recommendations: Operationalize the model in real-time detection environments

5.5 Suggestions for Further Research

1. Future research should incorporate multi-institutional datasets beyond KENET to capture a wider range of vulnerabilities across diverse university networks. This would improve the generalizability of the model and provide richer insights into region-specific attack patterns.
2. Advanced Machine Learning Approaches Researchers should explore deep learning architectures such as recurrent neural networks (RNNs), long short-term memory (LSTM), and graph neural networks (GNNs), which may capture complex temporal and relational patterns in intrusion data more effectively than traditional ensemble methods.
3. Real-Time Deployment and Evaluation: Further studies should focus on real-time implementation and performance evaluation of the developed model in active university networks. This includes testing the system under live traffic conditions to measure latency, scalability, and detection accuracy.
4. Integration with Threat Intelligence: Integrating global and local threat intelligence feeds with the intrusion detection system would enhance its predictive capabilities. Future research could investigate automated updating mechanisms for emerging CVEs and evolving attack vectors.
5. Human Factors in Cybersecurity: While this study primarily focused on technical vulnerabilities, future work should examine human-centered factors such as user awareness, compliance with security policies, and insider threats. These elements remain critical in shaping the overall cybersecurity posture of public universities.

2.0 REFERENCES

Ahmed, M., Khan, R., & Hussain, F. (2022). Performance evaluation of intrusion detection systems using precision and recall metrics. *Journal of Information Security and Applications, 68,* 103234. https://doi.org/10.1016/j.jisa.2022.103234

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.

Akinbohun, F., Ayeni, A., & Oladipo, O. (2022). Cybersecurity challenges and intrusion detection strategies in African universities. *African Journal of Information Systems, 14*(3), 45–60. https://doi.org/10.4018/AJIS.2022.14.3

Aldhaheri, A., Alqahtani, A., & Alshamrani, A. (2022). Machine learning-based intrusion detection systems: A survey of datasets, models, and challenges. *IEEE Access, 10,* 34450–34468. https://doi.org/10.1109/ACCESS.2022.3155678

Alkasassbeh, M., Al-Duwairi, B., & Alsmadi, I. (2023). Adoption challenges of intrusion prevention systems in public sector ICT infrastructures. *International Journal of Network Security, 25*(3), 410–423. https://doi.org/10.6633/ijns.202305_25(3).05

Alotaibi, B., & Elleithy, K. (2022). Cybersecurity in higher education: An assessment of vulnerabilities in global universities. *Education and Information Technologies, 27,* 12589–12607. https://doi.org/10.1007/s10639-022-11134-8

Amouri, A., Al Rahhal, M., Bazi, Y., Butun, I., & Mahgoub, I. (2024). Enhancing Intrusion Detection in IoT Environments: An Advanced Ensemble Approach Using Kolmogorov-Arnold Networks (KANs). arXiv. https://arxiv.org/abs/2408.15886

Arshad, J., Mahmood, A., & Khan, A. (2022). A hybrid intrusion detection system combining anomaly and signature-based techniques. *Computers & Security, 120,* 102808. https://doi.org/10.1016/j.cose.2022.102808

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.

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).

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.

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

Chen, X., Zhang, Y., & Wang, J. (2024). Enhancing intrusion detection with hybrid machine learning models using precision and F1-score evaluation. *Future Generation Computer Systems*, *154*, 145–160. https://doi.org/10.1016/j.future.2024.03.012

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

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

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).

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.

Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering*, *SE-13*(2), 222–232. https://doi.org/10.1109/TSE.1987.232894

Fahim, M., Shahid, A., Shabib, A., Chan, M. Y. A., & Abdulrazzaq, M. A. (2022) Network Intrusion Detection by using Machine Learning Technique.

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.

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.

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.

Gitau, L., & Kinyua, J. (2023). Cybersecurity Challenges in Kenyan Universities: A Case Study of Public Institutions. Journal of Information Security and Cybercrime Research, 8(2), 45-58.

Hussein, M., Alenezi, M., & Ali, M. (2022). Layered defense mechanisms for enterprise cybersecurity: An experimental evaluation. *Journal of Network and Computer Applications, 205*, 103437. https://doi.org/10.1016/j.jnca.2022.103437

Imathiu, G., Chege, A., & Omamo, A. (2024). Security intrusion monitoring model for Internet of Things (IoT) using sniffing tools on wireless sensor networks. *African Journal of Science, Technology and Social Sciences*, *2*(2), TE 51-58. https://doi.org/10.58506/ajstss.v2i2.164 AJSTSS

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.

Kamau, P., & Omondi, R. (2025). Leveraging AI and Machine Learning for Enhanced Intrusion Detection in Kenyan Universities. African Journal of Cybersecurity, 12(1), 34-47.

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

KENET. (2025). *Annual cybersecurity report for higher education institutions in Kenya*. Kenya Education Network. https://www.kenet.or.ke

Kenya Communications Authority & CA-Kenya reports. (2024, October). Kenya lost Sh 10.71 billion to cybercrime in 2023; insider threats and online fraud remain significant. *The Star & TechJournal*. The Star+1

"Kabarak University gives way forward after hackers tabled their demand" (2023). Cyber Security Incident Database.

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/

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

Kipkosgei, F., & Kiema, J. (2024). Enhancing Cybersecurity in Higher Education: A Framework for Public Universities in Kenya. African Journal of Information Systems, 15(3), 112-125.

Li, P., Liu, Z., & Wang, H. (2021). Evaluation of commercial intrusion detection systems: Snort and Suricata. *Security and Communication Networks, 2021*, 8891023. https://doi.org/10.1155/2021/8891023

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

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.

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.

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.

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.

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.

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.

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

Mantere, M., Sailio, M., & Noponen, S. (2021). Network monitoring in higher education: An empirical study of authentication vulnerabilities. *International Journal of Information Management, 58*, 102313. https://doi.org/10.1016/j.ijinfomgt.2020.102313

Mantere, M., Sailio, M., & Noponen, S. (2021). Network monitoring in higher education: An empirical study of authentication vulnerabilities. *International Journal of Information Management, 58*, 102313. https://doi.org/10.1016/j.ijinfomgt.2020.102313

Mhlongo, S., & Mutemwa, T. (2024). The state of cybersecurity in African higher education institutions: Policies and practices. *Journal of African Digital Security*, *2*(1), 22–38. https://doi.org/10.1080/afds.2024.10239

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.

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.

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

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.

Musyimi, S. M., Mwangi, W., & Njagi, D. (2023). Predictive Network Intrusion Identification & Mitigation Model Using Deep Learning In E-Learning. *Journal of the Kenya National Commission for UNESCO, 3*(1). Retrieved from https://journals.unesco.go.ke/index.php/jknatcom/article/view/32 journals.unesco.go.ke

Mwangi, E., & Waweru, L. (2022). The Role of Security Indicators in Mitigating Cyber Threats: A Review of Best Practices. International Journal of Cybersecurity and Digital Forensics, 11(1), 78-92.

Mwangi, P., & Wabwoba, F. (2023). Evaluating intrusion detection tools in Kenyan university networks. *International Journal of Cybersecurity Research, 5*(2), 101–115. https://doi.org/10.1016/ijcsr.2023.05.004

Njuguna, P., & Wanyembi, G. (2021). ICT security governance in African universities: Challenges and opportunities. *African Journal of Information Systems, 13*(4), 255–274.

Nyakundi, F., Otieno, R., & Muriuki, J. (2023). An empirical analysis of attack trends in East African universities connected to research networks. *African Journal of Computer Science, 10*(2), 77–89. https://doi.org/10.4018/AJCS.2023040105

Nyambura, W., & Maina, S. (2024). Addressing Resource Constraints in Cybersecurity: A Case Study of Kenyan Public Universities. East African Journal of Information Technology, 6(1), 56-69.

Nzioka, M., Kariuki, J., & Mutua, P. (2021). Cyber threats and resilience strategies in Kenyan public universities. *Journal of Information Security in Africa, 8*(2), 59–74. https://doi.org/10.1057/jisa.2021.08

Ochieng, P., & Ndung'u, A. (2023). Cyber Threats in Kenyan Universities: Trends, Impacts, and Mitigation Strategies. East African Journal of Information Technology, 5(1), 34-47.

Omondi, B., Atieno, L., & Kigen, P. (2024). Integrating prevention capabilities into IDS frameworks for higher education institutions. *Computers & Security, 135*, 103482. https://doi.org/10.1016/j.cose.2024.103482

Omondi, E. (2022). ICT policy awareness and cybersecurity challenges in Kenyan universities. *Kenya Journal of Technology and Innovation, 3*(1), 45–59.

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

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

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

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.

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.

Sharma, R., Gupta, A., & Singh, P. (2023). Deep learning approaches for intrusion detection systems: A comprehensive evaluation. *IEEE Access, 11*, 55822–55835. https://doi.org/10.1109/ACCESS.2023.3284452

Sindika, D. M., Nicholaus, R., & Hamadi, N. B. (2025). Improving Intrusion Detection Accuracy in Campus Networks: A Dataset Driven by Real-Time Traffic and Honeypot Simulations. *MUST Journal of Research and Development, 6*(2). mjrd.must.ac.tz

Singh, H., Kumar, P., & Chauhan, R. (2023). Advances in hybrid intrusion detection systems: Global perspectives and challenges. *Future Generation Computer Systems, 144*, 304–320. https://doi.org/10.1016/j.future.2023.05.012

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/

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

Yusof, M., Abdullah, A., & Hassan, R. (2023). Evaluating intrusion detection systems with machine learning: Emphasis on F1 score for balanced performance. *Journal of Cybersecurity Research, 12*(3), 201–215. https://doi.org/10.1093/cybsec/tyad012

3.0 APPENDICES

Appendix A: Research Instruments

1. Data Collection Instruments

The ELK Stack, comprising Elasticsearch, Logstash, and Kibana, served as the principal instrument for data collection and management.

- Elasticsearch facilitated quick indexing and querying of SSH-related logs.
- Logstash processed and filtered log data from server infrastructures, consequently providing appropriate storage suitable for analytic usage.
- Kibana offered interactive visualizations and dashboards that facilitated real-time observation of Temporal Analysis.

2. Statistical Validation Instruments

To ensure that the generated data matched the properties of the initial dataset, the work applied methods of statistical validation.

- A Chi-square test of independence was employed to explore categorical variables like severity level.

This statistical layer reinforced the empirical credibility of the research.

3. Analytical Instruments

The research made predominant usage of analytical Python libraries.

- Synthetic Data Vault (SDV) was used to create synthetic datasets that doubled the size of the original data and reduced overfitting.
- Scikit-learn provided machine learning algorithms to train, test, and to evaluate. Algorithms employed were Logistic Regression, Decision Tree Regressor, Random Forest Classifier, Support Vector Machine, and K-Nearest Neighbors Classifier.
- A method of ensemble learning of classifiers by stacking is also used. We apply Decision Tree Regressor, Random Forest Classifier, SVC, and KNN as base learners while Logistic Regression acts as a meta-model to achieve improved predictive performance.

These packages facilitated comparative studies of various algorithms as well as construction of a strong ensemble model.

4. Sample Python codes

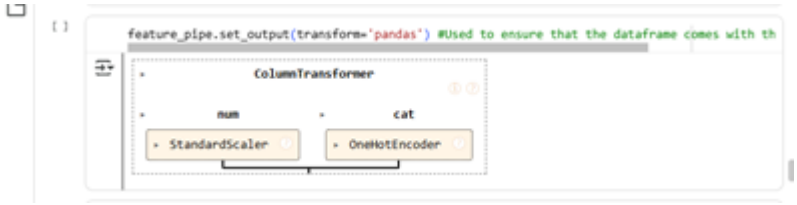
(iv) Creation of new Variables

```
#Create reponse new variable y and new feature matrix X
y2=new_df['severity_code']
X2=new_df.drop(['severity','operating_sys', 'severity_code'],axis=1)
```

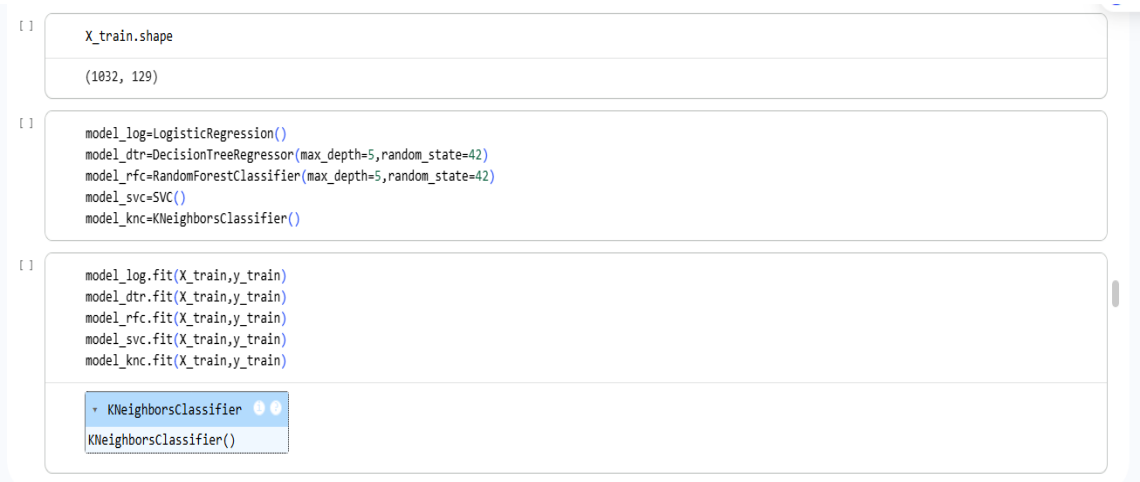
Creation of Feature Pipeline Categorical Transformer

```
# Creating a feature_pipeline categorial transformer
feature_pipe=ColumnTransformer([
    ('num',StandardScaler(),num_features),
    ('cat',OneHotEncoder(sparse_output=False),cat_features) ])
```

Column Transformer



Model Training Code



Appendix B: Research Permits/authorization letter

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 186001

Date of Issue: 03/July/2025

RESEARCH LICENSE

This is to Certify that Ms.. MERCY NDUTA WANJIHIA of The Cooperative University of Kenya, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Laikipia on the topic: INTRUSION DETECTION AND PREVENTION MODEL FOR EVALUATING NETWORK VULNERABILITIES IN PUBLIC UNIVERSITIES IN KENYA for the period ending : 03/July/2026.

License No: NACOSTI/P/25/4176175

186001

Applicant Identification Number

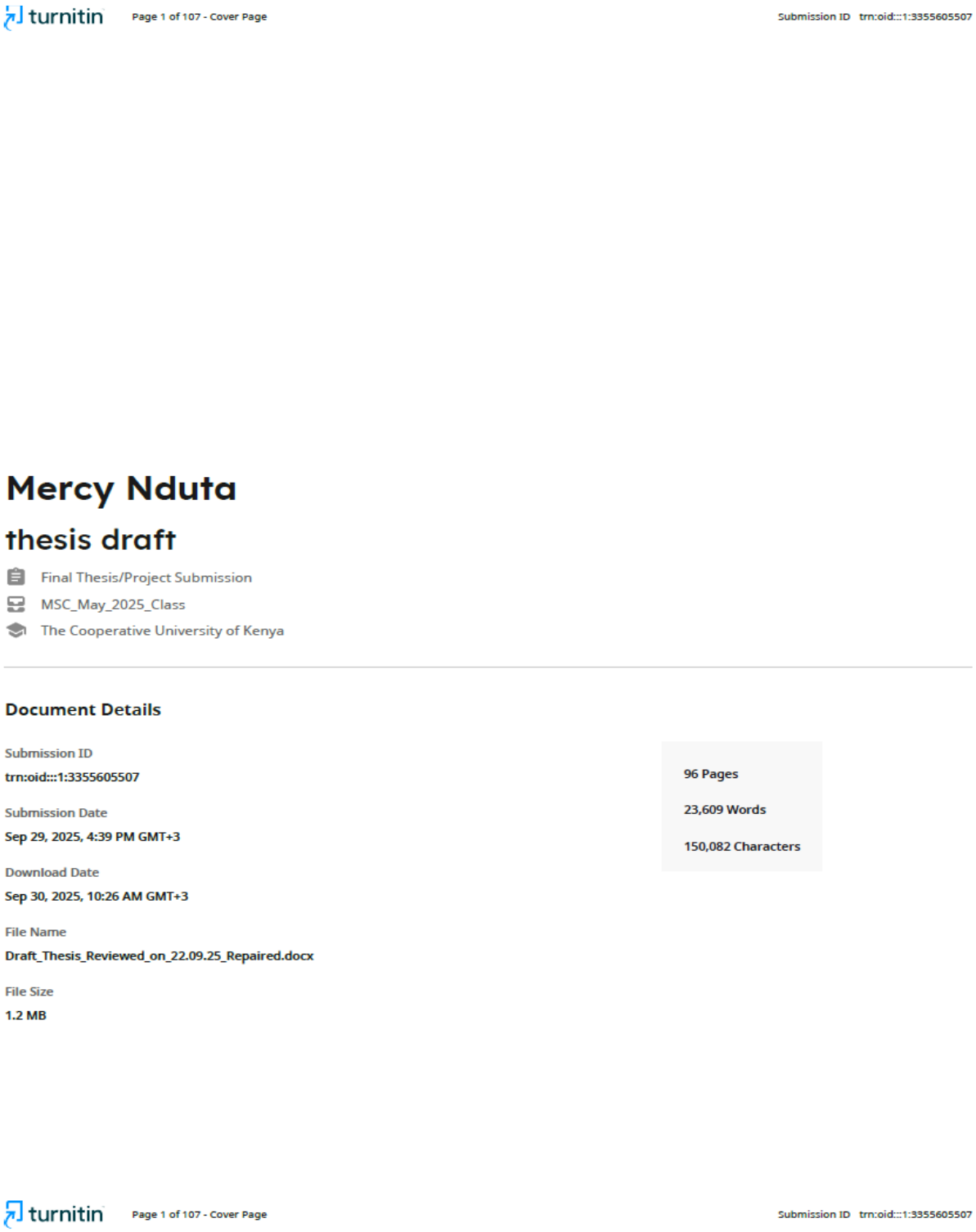
Ag. Director General
NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix C: Plagiarism Report



8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

160 Not Cited or Quoted **7%**
Matches with neither in-text citation nor quotation marks

25 Missing Quotations **1%**
Matches that are still very similar to source material

0 Missing Citation **0%**
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted **0%**
Matches with in-text citation present, but no quotation marks

Top Sources

6% Internet sources
6% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Mercy Nduta

thesis draft

Final Thesis/Project Submission

MSC_May_2025_Class

The Cooperative University of Kenya

Document Details

Submission ID

trn:oid:::1:3355605507

Submission Date

Sep 29, 2025, 4:39 PM GMT+3

Download Date

Sep 30, 2025, 10:26 AM GMT+3

File Name

Draft_Thesis_Reviewed_on_22.09.25_Repaired.docx

File Size

1.2 MB

96 Pages

23,609 Words

150,082 Characters

turnitin Page 1 of 98 - Cover Page Submission ID trn:oid:::1:3355605507

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (i.e., our AI models may produce either false positive results or false negative results), so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

Appendix D: Published Articles of your Thesis

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, Kenya, 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 highlight 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: mercwh@gmail.com (Mercy Wanjihia)

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