Journal of
Cyber Security

Tech Science Press

Doi:10.32604/jcs.2025.069444

ARTICLE

AI-Driven Cybersecurity Framework for Safeguarding University Networks from Emerging Threats

Boniface Wambui[1,*], **Margaret Mwinji**[1] **and Hellen Nyambura**[2]

[1]School of Computing and Informatics, Mount Kenya University, Thika, 342-01000, Kenya
[2]School of ICT and Engineering, Zetech University, Nairobi, 2768-00200, Kenya

*Corresponding Author: Boniface Wambui. Email: bonniemwangi91@gmail.com

Received: 23 June 2025; Accepted: 24 September 2025; Published: 23 October 2025

ABSTRACT: As universities rapidly embrace digital transformation, their growing dependence on interconnected systems for academic, research, and administrative operations has significantly heightened their exposure to sophisticated cyber threats. Traditional defenses such as firewalls and signature-based intrusion detection systems have proven inadequate against evolving attacks like malware, phishing, ransomware, and advanced persistent threats (APTs). This growing complexity necessitates intelligent, adaptive, and anticipatory cybersecurity strategies. Artificial Intelligence (AI) offers a transformative approach by enabling automated threat detection, anomaly identification, and real-time incident response. This study sought to design and evaluate an AI-driven cybersecurity framework specifically for university networks in Kenya, focusing on detecting, preventing, and mitigating emerging cyber risks. Utilizing machine learning and deep learning techniques, the framework analyzed extensive network traffic to uncover anomalies and predict potential breaches. Data was collected from 150 university staff members, yielding 120 valid responses, with faculty and students being key participants. Findings showed high awareness (84.2%) and concern (74.2%) about cybersecurity, with phishing (38.3%) and unauthorized access (20%) reported as the most frequent threats. Although 96.7% of respondents employed strong passwords and multi-factor authentication (MFA), only 65.8% considered institutional cybersecurity training adequate. Notably, 95.9% supported AI-driven real-time threat detection, and 93.3% trusted AI to reduce unauthorized access. Statistical analysis revealed a moderate positive correlation (R = 0.466) between cybersecurity awareness and perceived AI effectiveness. The study emphasizes the urgent need for universities to integrate AI-powered security systems with continuous training programs to enhance resilience and create a safer academic digital environment.

KEYWORDS: Artificial intelligence; cyber security; threats; networks; university; detection

1 Introduction

As the digital transformation accelerates, universities are turning to networked systems for their academic, research, and administrative functions. Nevertheless, the increasing reliance on digital infrastructure has made these institutions vulnerable to complex cyber threats such as malware attacks, phishing schemes, ransomware incidents, and advanced persistent threats (APTs). Conventional cybersecurity measures like firewalls and signature-based intrusion detection systems frequently fall short in addressing the evolving nature of cyber risks. This has led to a pressing requirement for a cybersecurity strategy that is intelligent, adaptive, and anticipatory. As a result of its ability to facilitate automated threat detection, anomaly detection, and real-time response systems, Artificial Intelligence (AI) has developed into a significant asset for bolstering cybersecurity. Cybersecurity frameworks powered by AI utilize machine learning (ML) and deep learning (DL) methodologies to scrutinize extensive volumes of network traffic data, identify anomalies, and forecast possible security violations ahead of time. Universities can bolster their cybersecurity posture and mitigate cyber risks proactively by integrating AI-driven solutions, thereby ensuring data integrity, confidentiality, and availability [1].

This paper presents a cybersecurity framework powered by AI, aimed at protecting university networks from new threats. The framework includes sophisticated threat intelligence, behavioral analysis, and real-time security monitoring to effectively identify and counter cyber threats. The proposed framework seeks to offer a strong defense mechanism customized to the ever-changing cybersecurity environment of academic institutions by utilizing AI models for automated security analytics. The research examines how AI algorithms can be used for intrusion detection, endpoint security, and network anomaly detection, aiding in the creation of a robust cybersecurity ecosystem in university networks.

The emergence of Artificial Intelligence (AI) marks a pivotal moment for cybersecurity, signaling a basic shift in our strategies for fighting and dealing with cyber threats [2]. Once limited to the realms of science fiction and speculative futurism, AI has now crossed its conceptual boundaries, becoming a real and influential force with significant ramifications for cybersecurity. The emergence of AI marks the beginning of a new era of automated and intelligence-enhanced defense systems, as opposed to traditional cybersecurity methods that rely on manual supervision and fixed rule sets. Methodologies such as Machine Learning (ML) and Deep Learning (DL) are central to this paradigm shift [3], which provide AI systems the ability to analyze vast amounts of data with unmatched speed and complexity. Algorithms based on machine learning demonstrate an extraordinary capability to discern patterns and relationships in data, which enables them to identify minor anomalies that conventional rule-based detection approaches may overlook [4]. By means of ongoing education based on historical data and a skillfulness in adjusting to changing threat environments, machine-learning-driven systems can identify nascent threats with extraordinary accuracy, even in the absence of clear directives or preset guidelines.

Likewise, deep learning, subset of machine learning that draws inspiration from the neural networks of the human brain [5], greatly enhances the potential of artificial intelligence in the field of cybersecurity. Deep learning models, equipped with sophisticated neural architectures that can perform hierarchical feature extraction and representation learning, are able to autonomously identify complex features from raw data [6]. This allows them to uncover subtle indicators of cyber threats that may go unnoticed by human analysts, thereby strengthening the resilience of university cybersecurity systems. The objective of the study was to develop an AI-driven cybersecurity framework that enhances the protection of university networks by detecting, preventing, and mitigating AI-driven cyber threats. The study aims to implement machine learning-based threat detection, automated response mechanisms, and real-time monitoring to safeguard sensitive academic data and IT infrastructure.

1.1 Related Studies

1.1.1 Leveraging AI Technologies for Cyber Defense

According to [7], AI is applied in diverse and creative ways within cybersecurity practices, including threat detection, response strategies, and predictive analytics. Threat intelligence platforms driven by AI employ big data analytics to examine enormous datasets for potential threats prior to their occurrence, thereby greatly improving the proactive abilities of cybersecurity teams. Moreover, theoretical frameworks concerning the effects of AI on cybersecurity concentrate on comprehending the relationship between AI technologies and cyber threats. Frameworks like the Adaptive Security Architecture (ASA) provide perspectives on integrating AI into cybersecurity strategies to boost adaptability and resilience [8]. Research conducted by [9] employed a machine learning model to identify zero-day vulnerabilities with high precision, demonstrating the real-world advantages of AI in cybersecurity. Ref. [10] was the first to propose developing privacy-preserving deep learning (DL) within a distributed training framework. This enables multiple parties to collaborate in developing a precise neural network model without revealing their input datasets. Conversely, empirical research offers both quantitative and qualitative evaluations of the effectiveness of AI in particular cybersecurity applications. The upcoming section, however, outlines how Artificial Intelligence and Machine Learning contribute to detecting and alleviating cyber threats.

Threat detection: According to [11], Artificial Intelligence and Machine Learning excel in proactive threat detection. AI systems can identify the characteristics of cyber threats, ranging from phishing attempts to advanced persistent threats (APTs), with great accuracy by studying historical data [12].

Prediction: AI's ability to predict is revolutionary for cybersecurity. AI models can predict future threat trends by examining historical and current data, enabling organizations to prepare for and possibly avert attacks before they occur. Taking this proactive stance against cyber threats marks a significant departure from the reactive approaches of previous times.

Response: AI improves response strategies by rapidly assessing the extent of an attack and proposing or even automating suitable counteractions [13]. This ability to respond quickly mitigates damage and lessens the recovery time and resource expenditure necessitated by a security breach.

1.1.2 Cybersecurity Framework for Safeguarding University Networks

Universities are increasingly becoming targets for cyberattacks due to their open networks, diverse user populations, and the vast amounts of sensitive data they handle, including student records, research data, and financial information. With the incorporation of technologies such as Enterprise Resource Planning (ERP) systems, cloud services, and Internet of Things (IoT) devices, the attack surface has grown even larger, rendering conventional security measures insufficient. A study conducted on universities in Kenya found that although 66% have embraced international standards like ISO/IEC 27001:2013 for managing cybersecurity risks, there are considerable deficiencies in the implementation of policies and the allocation of resources. It is worth mentioning that 74% of these institutions faced cyberattacks within a five-year span, highlighting the critical necessity for a strong and customized cybersecurity framework [14].

The proposed cybersecurity framework for Kenyan universities focuses on a comprehensive strategy aligned with the ISO/IEC 27001:2022 standard to tackle these challenges. This framework entails grasping the university's context, pinpointing vital assets and processes, performing comprehensive threat evaluations, and applying risk treatment measures. Additionally, it emphasizes the need for ongoing supervision, participation from leaders, and the cultivation of a cybersecurity awareness culture. Through the adoption of such a structured approach, universities can take proactive measures to manage cybersecurity risks, safeguard critical assets, and uphold a resilient information security posture against evolving threats.

1.1.3 Role of AI in Identifying Unusual Activity

According to [15], anomaly detection is essential for spotting possible cybersecurity threats through the observation of network behavior for departures from set patterns. Anomaly detection systems have been significantly improved by AI through the application of machine learning algorithms that learn from large datasets and continually refine their ability to identify irregularities. Conventional approaches to anomaly detection depend on pre-established rules or signatures, which frequently fail to address new or quickly changing threats. Unlike traditional systems, those driven by AI can identify threats that were not known before through the analysis of behavioral patterns. This capability significantly enhances their effectiveness in real-time threat mitigation. Due to AI's capacity for processing and analyzing massive amounts of data, it can identify subtle irregularities that human analysts or conventional security systems might miss. For instance, machine learning algorithms can oversee network traffic, identify unusual login attempts, or highlight abnormal data transfers. By utilizing supervised learning, AI systems can learn to identify normal behavior within a network, while unsupervised learning methods can uncover previously unknown anomalies without prior knowledge of attack patterns. This adaptability renders AI indispensable for organizations confronting a constantly evolving landscape of cyber threats [16].

1.1.4 AI's Role in Predicting and Gathering Threat Information

Threat intelligence encompasses the collection, examination, and interpretation of data pertaining to possible cyber threats. This process is improved by AI through the automation of the gathering of large volumes of threat data from diverse sources, including open-source platforms, dark web forums, and network traffic logs. AI systems can analyze this data through filtering, classification, and correlation to forecast possible attacks, resulting in a more proactive approach to threat intelligence compared to traditional methods. With the help of AI, predictive analytics enables organizations to foresee future cyber threats by examining historical attack patterns. AI systems can analyze trends in threat data to predict the timing and location of potential attacks, enabling cybersecurity teams to make preparations ahead of time. This ability is essential to avert zero-day attacks, in which weaknesses are taken advantage of prior to their correction. The capacity of AI to perpetually learn from new data guarantees the enhancement of its predictions over time, aiding organizations in staying ahead of emerging threats. AI is essential for forecasting and compiling threat data, utilizing machine learning (ML) and deep learning (DL) models to identify and scrutinize cyber threats as they occur. Conventional cybersecurity methods frequently depend on established rules and signature-based detection, which can have difficulty keeping pace with new threats. Conversely, systems that utilize AI can handle enormous volumes of network traffic, detect irregularities, and discern patterns that signal cyberattacks ahead of time. As an example, platforms for threat intelligence that are powered by AI utilize automated data mining and natural language processing (NLP) to gather and examine data from cybersecurity forums, global threat databases, and dark web sources. This improves proactive defense mechanisms [17].

Moreover, AI improves predictive threat modeling by leveraging past attack data to anticipate potential security breaches. Advanced AI models like generative adversarial networks (GANs) and reinforcement learning simulate cyberattack scenarios and evaluate vulnerabilities within university networks. These models are capable of continuous learning based on new attack patterns, which enhances their detection accuracy as time goes on. In addition, security orchestration and automated response (SOAR) systems powered by AI facilitate swift threat mitigation through the implementation of predefined actions upon detection of a threat, thereby reducing potential harm [18]. Universities can improve their capacity to anticipate, avert, and address cyber threats in a rapidly evolving digital environment by incorporating AI into cybersecurity.

1.1.5 Approaches to Safeguarding Data in AI Systems

The vast amounts of data necessary for training and evaluating AI models complicate the task of safeguarding data in these models. With AI becoming increasingly integral to cybersecurity, implementing strategies that protect sensitive information across the data lifecycle is essential. Effective methods for guaranteeing privacy in AI models include encryption, anonymization, and federated learning. Encryption is essential for safeguarding data both at rest and in transit. Encryption prevents unauthorized access to sensitive data by converting it into an unreadable format, even if it is intercepted. AI systems can utilize encryption to safeguard both the raw data employed for model training and the outputs produced during operation, like threat intelligence reports. Depending on the use case, symmetric and asymmetric encryption algorithms can be utilized, with public-key cryptography being crucial for securing data exchanges [19].

Another important method is anonymization, especially regarding AI. This entails eliminating or disguising personally identifiable information (PII) from datasets, so that individuals cannot be recognized. This strategy is crucial for data gathered for the training of AI models, as it enables organizations to utilize valuable insights from extensive datasets while safeguarding individual privacy. As an example, a type of anonymization known as differential privacy adds noise to data in order to conceal individual contributions. This approach helps to avert re-identification, even when data is aggregated [20].

Federated learning, a novel AI paradigm, boosts data privacy by enabling the training of machine learning models on decentralized devices without transferring raw data to a central server. This method reduces privacy risks by ensuring that personal data remains on each device, all the while allowing for the collaborative development of powerful AI models. In the field of cybersecurity, for instance, federated learning allows for the training of AI systems on threat patterns from multiple institutions without the need to share sensitive logs or data points. It boosts privacy and lessens the risk of a data breach, all the while preserving the effectiveness of AI-driven insights [21].

1.2 Research Gaps and Main Contributions

Considering the current attention to the utilization of AI technologies in the context of cyber defense, there are several existing research gaps that have not been addressed yet. To begin with, although the AI models have demonstrated positive results about the potential of detecting abnormal activity and anticipating threats, insufficient evidence is available to understand their flexibility and functionality in dynamic university applications where the user behavior is highly random and privacy of data is a key issue of concern. Second, traditional cybersecurity structures tend not to be latched up with progressive and self-learning AI-based threat intelligence evolved container to provide right up to date learning and contextual judgments. This leaves a vacuum in perceiving how AI can be successfully integrated in institution security measures to not only identify and address cyber threats but go further to collect, correlate, and act on the threat intelligence that is specific to academic infrastructures.

The primary contribution of this research is the creation and design of an AI-based approach to cybersecurity that is specifically targeted to protecting university networks against the rising forms of emerging cyber threats. It uses AI-enabled threat intelligence and behavioral analysis within a framework that allows anomaly detection in real-time, predictive threat mitigation, machine-driven criteria of threat response, and uninterrupted observation. Contrary to classical reactive, this method focuses on proactive security with data-driven knowledge and flexible learners. The framework is aligned with the ISO/IEC 27001:2022 standard, so it adheres to the international standards of information security applications and considers the specifics of vulnerabilities and resource limits of academic institutions. The architecture is holistic and smart and strengthens resilience and security of university IT ecosystems within a changing threat landscape.

2 Materials and Methods

2.1 Datasets

Large-Scale Intrusion Detection Dataset (BCCC-CSE-CIC-IDS2018) was used for the study. A sample containing 10,000 records was obtained on the basis of the Large-Scale Intrusion Detection Dataset (BCCC-CSE-CIC-IDS2018) to train and evaluate the model efficiently, ensuring the representativeness of the benign and malicious traffic. The initial data set consists of tens of millions of labeled instances which is valuable but computationally challenging to the iterations of an experiment. Thus, the stratified random sampling was applied in order to retain the original set of distribution on the different categories of attacks and normal traffic, i.e., 10,000 samples were chosen. It was then preprocessed in the removal of duplicates, addressing missing values, and normalization of features—and this was used to divide into 70 percent training and 30 percent testing. The smaller but balanced sample enabled the quicker application of experimentation and the optimization of machine learning algorithms, preserving, at the same time, the diversity of network events, therefore, meeting the reliability and validity of the outcomes.

2.2 Methods

A mixed-methodological approach was employed in this study, incorporating a descriptive research design [22]. Descriptive research design is a systematic approach used to observe, describe, and document characteristics of a phenomenon without manipulating variables. An experimental and descriptive research was adopted in the study. It entailed analyzing the primary data from the questionnaire feedback and developing a cyber security model framework for enhancing the security of university networks. The AI-driven cybersecurity framework played a crucial role in assessing the strengths and weaknesses of security services within university networks, as well as evaluating the effectiveness of implemented cybersecurity measures. This approach was essential since it provided the researcher with a deeper understanding of the study. The research focused on selected universities in Kenya, with a sample of 150 staff members, and 120 completed questionnaires were collected. Faculty and students were the primary target population for this study, as they are the key stakeholders in safeguarding university networks against emerging cyber threats.

A model framework for enhancing the threat detection was developed.

Fig. 1 presents an AI-driven cybersecurity framework designed to protect university networks from emerging threats. At its core, the framework integrates AI-driven security systems that operate across three critical phases: threat detection, threat prevention, and threat response. These components work in synergy to identify potential cyber threats such as phishing, malware, and unauthorized access, pre-emptively block or neutralize them, and swiftly respond to mitigate any impacts. Continuous monitoring ensures real-time analysis and situational awareness, while alignment with the ISO/IEC 27001:2022 standard emphasizes adherence to globally recognized information security practices. The ultimate goal of this layered and intelligent approach is to achieve robust and resilient university networks, safeguarded against evolving cyber risks.

The technical specifications for the framework included: We examined deep learning and classical machine learning architectures for our security framework. While gradient boosted trees were employed in the early prototype, random forests were used for anomaly detection. It could manage the aspects of network flow.

The integration of deep learning methods like recurrent neural networks (RNN) and coevolutionary neural networks (CNN) formed the framework's fundamental elements. The chronology of university records was subjected to CNN. The temporal dependencies between the network streams were modeled using RNN. The framework was trained and validated on a publicly available dataset. An architecture that could record real-time network traffic was used to perform real-time model monitoring. The piped data streams were recorded using Kafka. Each network session is converted into a numeric feature vector, which is then fed into the trained models and processed by efficient inference engines to make the inference on the fly. The model's detection accuracy was 98% and its F1-score was near 0.97 on held-out testing sets.

The Algorithm 1 for the model entailed AI Driven Cybersecurity Framework().

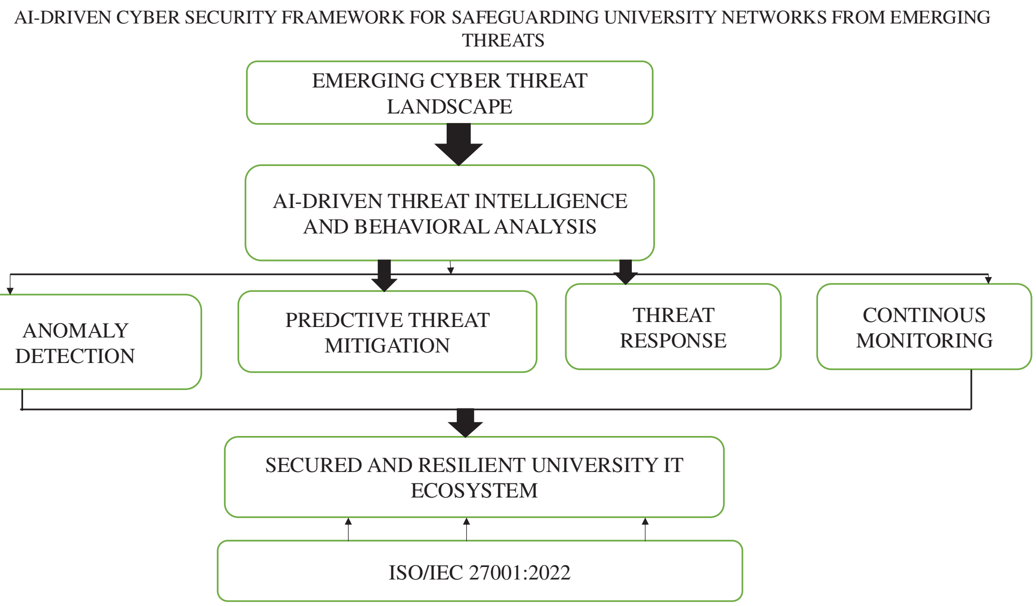
AI-DRIVEN CYBER SECURITY FRAMEWORK FOR SAFEGUARDING UNIVERSITY NETWORKS FROM EMERGING THREATS
EMERGING CYBER THREAT LANDSCAPE
AI-DRIVEN THREAT INTELLIGENCE AND BEHAVIORAL ANALYSIS
ANOMALY DETECTION
PREDCTIVE THREAT MITIGATION
THREAT RESPONSE
CONTINOUS MONITORING
SECURED AND RESILIENT UNIVERSITY IT ECOSYSTEM
ISO/IEC 27001:2022

Figure 1: Developed AI-driven cyber security framework

Algorithm 1: AI driven cybersecurity Framework()

```
while True:
    # Step 1: Collect and preprocess network data
    network_data = collect_network_data()
    cleaned_data = preprocess(network_data)
    # Step 2: Perform AI-driven threat intelligence and behavioral analysis
    behavior_profiles = analyze_behavior(cleaned_data)
    threat_signals = analyze_threat_intelligence_feeds()
    suspicious_behavior = correlate (behavior_profiles, threat_signals)
    # Step 3: Detect anomalies in behavior
    anomalies_detected = detect_anomalies(behavior_profiles)
    if anomalies_detected:
        # Step 4: Predict and mitigate threats
        predicted_threats = predict_threats(suspicious_behavior)
        mitigation_actions = generate_mitigation_plan(predicted_threats)
        execute_mitigation(mitigation_actions)
        # Step 5: Respond to threats
        send_alert()
        initiate_containment()
        collect_forensic_data()
    # Step 6: Continue monitoring for new threats
    wait(monitoring interval)
```

The flowchart below (Fig. 2) depicts an AI-powered cybersecurity framework that uses intelligent threat response techniques and ongoing monitoring to protect university networks from new attacks. Network data is first gathered and processed, after which it is analyzed for trends using behavioral analysis and threat intelligence powered by artificial intelligence. To find anomalies that would indicate possible cyberattacks, these behavior profiles are compared to the threat intelligence currently in place. The system anticipates and reduces potential hazards if abnormalities are found, then reacts appropriately to eliminate them. If no irregularities are discovered, the system keeps an eye out for fresh dangers, generating an ongoing feedback loop that strengthens the network's resilience and proactively guards the university's digital infrastructure against changing cyberthreats.

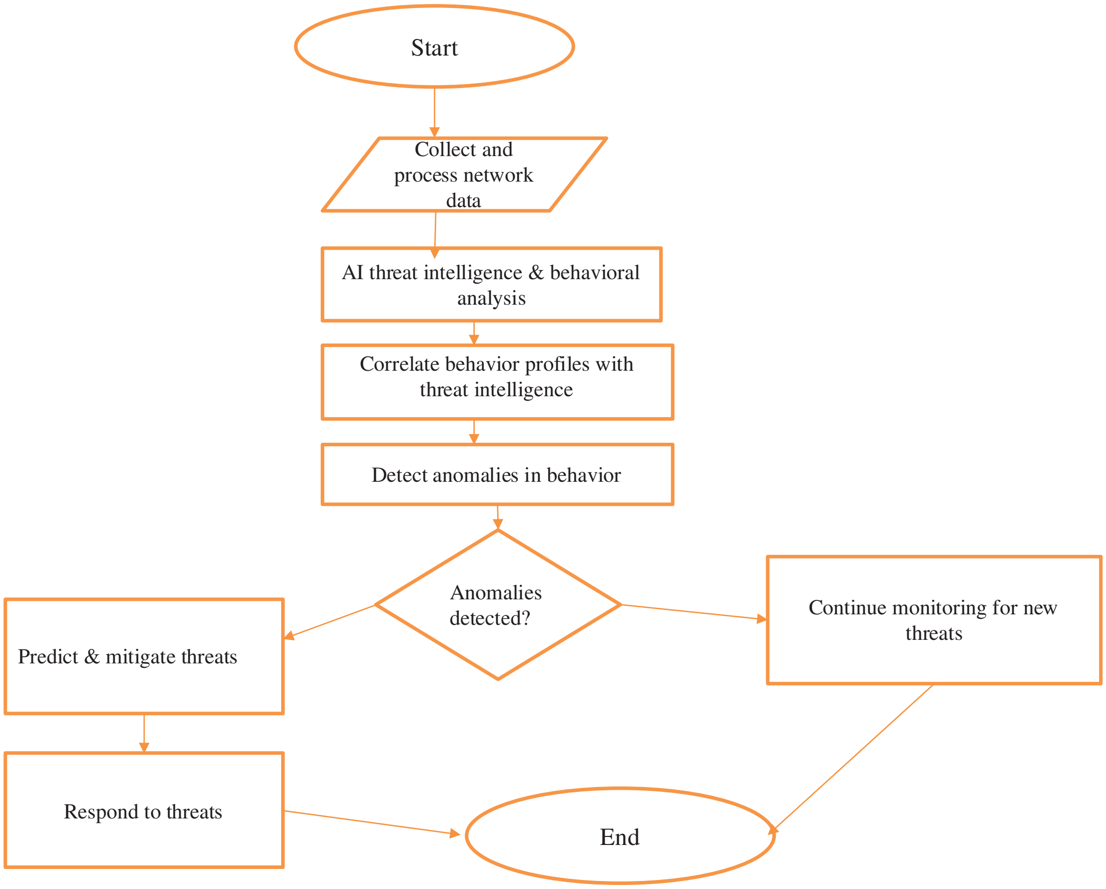
Start
Collect and process network data
AI threat intelligence & behavioral analysis
Correlate behavior profiles with threat intelligence
Detect anomalies in behavior
Anomalies detected?
Predict & mitigate threats
Continue monitoring for new threats
Respond to threats
End

Figure 2: Flowchart for the model

3 Results

3.1 Questionnaire Response Rate

During the data collection process, the researcher distributed 150 questionnaires to participants, of which 120 were completed and returned, yielding an 80% response rate. According to [23], a response rate of 50% is considered adequate for analysis and reporting, 60% is deemed good, and 70% or higher is classified as excellent. Based on this benchmark, the response rate for this study was outstanding. All individuals within the target group had an opportunity to participate, ensuring a comprehensive assessment of AI-driven cybersecurity measures for safeguarding university networks from emerging threats. The demographic data collected included participants' age, gender, educational background, and roles within the university, providing valuable insights into the cybersecurity landscape in higher education institutions.

3.2 Demographic Information

According to Table 1 below, 55.8% of the respondents were male while 44.2% were female.

Table 1: Gender

What is your gender?					
		Frequency	**Percent**	**Valid percent**	**Cumulative percent**
Valid	Female	53	44.2	44.2	44.2
	Male	67	55.8	55.8	100.0
	Total	120	100.0	100.0	

According to Table 2 below, 66.7% of the respondents had a bachelor's degree, 21.7% had diploma, 9.2% had Master's while 2.5 had a PhD as their highest level of qualification attained.

Table 2: Education

Which is the highest level of education you have attained?					
		Frequency	**Percent**	**Valid percent**	**Cumulative percent**
Valid	Bachelor	80	66.7	66.7	66.7
	Diploma	26	21.7	21.7	88.3
	Masters	11	9.2	9.2	97.5
	PhD	3	2.5	2.5	100.0
	Total	120	100.0	100.0	

According to Table 3 below, 66.7% of the respondents were students, 15.8% were Lecturers, 10.8% were IT staff while 5.8% were administrators.

Table 3: Occupation

What is your role at the university?					
		Frequency	**Percent**	**Valid percent**	**Cumulative percent**
Valid	Administrator	7	5.8	5.8	5.8
	IT Staff	13	10.8	10.8	16.7
	Lecturer	19	15.8	15.8	32.5
	Other	1	0.8	0.8	33.3
	Student	80	66.7	66.7	100.0
	Total	120	100.0	100.0	

According to Table 4 below, 46.7% of the respondents had been in the university for 1–2 years while 32.5% had stayed for 3–5 years.

According to Table 5 below, 44.2% of the respondents used the universities' computer networks daily, 34.2% used it several times in a week while 19.2% rarely used it.

Table 4: Duration

How long have you been in the university?					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	1–2 years	56	46.7	46.7	46.7
	3–5 years	39	32.5	32.5	79.2
	above 5 years	17	14.2	14.2	93.3
	Less than 1 year	8	6.7	6.7	100.0
	Total	120	100.0	100.0	

Table 5: Access to university networks

How frequently do you use the university's network services?					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Daily	53	44.2	44.2	44.2
	Rarely	23	19.2	19.2	63.3
	Several times a week	41	34.2	34.2	97.5
	Weekly	3	2.5	2.5	100.0
	Total	120	100.0	100.0	

According to Table 6 below, 50.8% of the respondents were aware of cyber security threats targeting university networks, 33.3% were not aware while 15.8% were not sure.

Table 6: Awareness of cyber-threats

Are you aware of any cyber security threats targeting university networks?					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	No	40	33.3	33.3	33.3
	Not Sure	19	15.8	15.8	49.2
	Yes	61	50.8	50.8	100.0
	Total	120	100.0	100.0	

According to Table 7 below, 74.2% of the respondents were very concerned about the cyber security threats in the university networks, 10.8% were somehow concerned and neutral while 4.2% were not concerned.

According to Table 8 below, 49.2% of the respondents suggested that the current cyber security measures in the university were moderately effective, 32.5% very effective while 13.3% were slightly effective.

According to Table 9 below, 38.3% of the respondents had encountered phishing attacks, 20% unauthorized access, 17.5% had encountered data breaches while 12.5% had encountered distributed denial of services attacks while 10% encountered other types of attacks.

Table 7: Level of concerns on cyber-threats affecting university networks

How concerned are you about cyber security threats affecting university networks?					
		Frequency	**Percent**	**Valid percent**	**Cumulative percent**
Valid	Neutral	13	10.8	10.8	10.8
	Not concerned	5	4.2	4.2	15.0
	Somewhat concerned	13	10.8	10.8	25.8
	Very concerned	89	74.2	74.2	100.0
	Total	120	100.0	100.0	

Table 8: Effectiveness of university cyber security measures

How effective do you think the university's current cyber security measures are?					
		Frequency	**Percent**	**Valid percent**	**Cumulative percent**
Valid	Moderately effective	59	49.2	49.2	49.2
	Not effective a	6	5.0	5.0	54.2
	Slightly effect	16	13.3	13.3	67.5
	Very effective	39	32.5	32.5	100.0
	Total	120	100.0	100.0	

Table 9: Types of cyber security threats encountered

What types of cyber security threats have you encountered or heard about in your university?					
		Frequency	**Percent**	**Valid percent**	**Cumulative percent**
Valid		1	0.8	0.8	0.8
	Data breaches	21	17.5	17.5	18.3
	Distributed denial of service	15	12.5	12.5	30.8
	Others	12	10.0	10.0	40.8
	Phishing attack	46	38.3	38.3	79.2
	Ransom ware	1	0.8	0.8	80.0
	Unauthorized access	24	20.0	20.0	100.0
	Total	120	100.0	100.0	

According to Table 10 below, 34.2% of the respondents suggested that multi-factor authentication strategies were currently being used in the university, 30% suggested firewalls and IDS, 13.3% suggested AI-based threat detection while 10% suggested that there was regular cyber security training awareness.

According to Table 11 below, 40% of the respondents suggested that all the AI-driven cyber security solutions listed above would be effective for universities, 24.2% suggested AI-driven IDS and response systems while 6.7% suggested AI-based user behavior analytics to detect threats.

According to Table 12 below, 90.8% of the respondents support the integration of AI-driven cyber security in the universities' security framework, 5.8% were not sure while 2.5% rejected the integration.

Table 10: Cyber security & strategies currently being used

What cyber security tools or strategies are currently in use at the university?					
		Frequency	Percent	Valid percent	Cumulative percent
Valid		2	1.7	1.7	1.7
	AI-based threat detection	16	13.3	13.3	15.0
	Firewall and IDS	36	30.0	30.0	45.0
	Multi-factor authentication	41	34.2	34.2	79.2
	Others	12	10.0	10.0	89.2
	Regular cybersecurity awareness training	13	10.8	10.8	100.0
	Total	120	100.0	100.0	

Table 11: AI-driven cyber security solutions

What AI-driven cyber security solutions do you think would be most effective for universities					
		Frequency	Percent	Valid percent	Cumulative percent
Valid		1	0.8	0.8	0.8
	AI-based user behavior analytics to detect threats	8	6.7	6.7	7.5
	AI-driven phishing and scam detection	7	5.8	5.8	13.3
	AI-driven intrusion detection and response systems	29	24.2	24.2	37.5
	All	48	40.0	40.0	77.5
	Automated malware detection and prevention	27	22.5	22.5	100.0
	Total	120	100.0	100.0	

Table 12: Level of support for the integration of AI-driven cyber security in your university's network security framework

Would you support the integration of AI-driven cyber security in your university's network security framework?					
		Frequency	Percent	Valid percent	Cumulative percent
Valid		1	0.8	0.8	0.8
	Maybe	7	5.8	5.8	6.7
	No	3	2.5	2.5	9.2
	Yes	109	90.8	90.8	100.0
	Total	120	100.0	100.0	

According to Table 13 below, a significant majority (84.2%) of respondents are aware of common cyber threats like phishing, malware, and data breaches, indicating strong general awareness. Only 65.8% agree that the university provides regular cybersecurity training, while 19.2% are neutral and 15% disagree. This suggests that training efforts are present but could be more consistent or better communicated. A mixed response 61.7% feel confident in recognizing and reporting suspicious activities, but a notable 24.2% either disagree or strongly disagree, indicating a need for more training or clarity on reporting procedures. With regards to understanding of Strong Passwords and Multi-Factor Authentication, the area shows the highest awareness, with 96.7% understanding its importance, reflecting strong personal knowledge of security best practices. Concerning personal Cybersecurity Measures, a high percentage (94.2%) actively take steps to protect their data, suggesting strong personal responsibility among respondents.

Table 13: Cyber security awareness

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I am aware of common cyber security threats such as phishing, malware, and data breaches.	62.5%	21.7%	12.5%	0.8%	2.5%
The university provides regular cyber security training and awareness programs.	25.8%	40.0%	19.2%	12.5%	2.5%
I know how to recognize and report suspicious online activities within the university network.	39.2%	22.5%	14.2%	21.7%	2.5%
I understand the importance of strong passwords and multi-factor authentication for online security.	75.0%	21.7%	1.7%	0.0%	1.7%
I actively take measures to protect my personal and academic data from cyber threats.	61.7%	32.5%	4.2%	0.0%	1.7%

According to Table 14 below, a strong majority (95.9%) agree that AI-based systems enhance network security by identifying cyber threats in real time, showing high confidence in AI's capability for proactive threat detection. 93.3% of respondents believe AI-driven solutions help reduce unauthorized access to sensitive university data, indicating widespread trust in AI's protective role. 84.2% agree that automated AI monitoring is more effective than traditional security methods. However, 10% disagree, reflecting some skepticism or preference for conventional systems. 93.3% of participants feel that AI enhances response times to security incidents, suggesting appreciation for AI's efficiency and speed in incident handling. A clear majority (95%) support prioritizing AI integration in cybersecurity strategies to strengthen university network security.

The Model Summary Table 15 below, provides key statistics from a linear regression analysis where Cybersecurity Awareness is used as a predictor variable. The R value of 0.466 indicates a moderate positive correlation between cybersecurity awareness and the dependent variable cybersecurity effectiveness. The R Square value of 0.217 means that approximately 21.7% of the variance in the dependent variable can be explained by cybersecurity awareness. The Adjusted R Square of 0.210 slightly adjusts this value to account for the number of predictors in the model, making it a more accurate reflection of model performance in a population. Lastly, the Standard Error of the Estimate (0.67405) indicates the average distance that the observed values fall from the regression line, with lower values suggesting a better model fit. Overall, the model shows a moderate predictive strength, explaining about one-fifth of the variability in the outcome based on cybersecurity awareness.

Table 14: Effectiveness of AI-driven cybersecurity solutions

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
AI-based threat detection systems improve network security by identifying cyber threats in real time.	69.2%	26.7%	3.3%	0.8%	0.0%
AI-driven security solutions reduce the risk of unauthorized access to sensitive university data.	57.5%	35.8%	5.8%	0.8%	0.0%
Automated AI monitoring helps detect and prevent cyber-attacks more effectively than traditional security measures	47.5%	36.7%	5.8%	10.0%	0.0%
AI-driven cyber security solutions enhance the response time to security incidents within the university.	47.5%	45.8%	5.8%	0.8%	0.0%
The integration of AI in cyber security should be prioritized to strengthen university network security.	57.5%	37.5%	4.2%	0.8%	0.0%

Table 15: Model summary

Model summary				
Model	R	R square	Adjusted R square	Std. error of the estimate
1	0.466[a]	0.217	0.210	0.67405

Note: [a]Predictors: (Constant), Cyber security awareness.

The ANOVA Table 16 below provides a statistical test of the overall significance of the regression model. In this case, the dependent variable is the Effectiveness of AI-Driven Cybersecurity Solutions, and the predictor is Cybersecurity Awareness. The F-value of 32.653 is relatively high, indicating that the model significantly predicts the outcome variable better than a model with no predictors. The associated significance value (Sig.) of 0.000 (which is less than 0.05) confirms that the relationship between cybersecurity awareness and the effectiveness of AI-driven cybersecurity solutions is statistically significant. The Regression Sum of Squares (14.836) shows the amount of variation explained by the model, while the Residual Sum of Squares (53.612) represents the unexplained variation. Overall, the ANOVA results support the conclusion that cybersecurity awareness significantly contributes to the perceived effectiveness of AI-driven cybersecurity solutions.

Table 16: Analysis of variance (ANOVA)

ANOVA[a]						
Model		Sum of squares	df	Mean square	F	Sig.
1	Regression	14.836	1	14.836	32.653	0.000[b]
	Residual	53.612	118	0.454		
	Total	68.448	119			

Note: [a]Dependent variable: effectiveness of AI driven cyber security solutions. [b]Predictors (Constant), cyber security awareness.

The Coefficients Table 17 below provides insight into how Cybersecurity Awareness influences the Effectiveness of AI-Driven Cybersecurity Solutions, which is the dependent variable. The unstandardized coefficient (B) for Cybersecurity Awareness is 0.443, meaning that for every one-unit increase in cybersecurity awareness, the effectiveness of AI-driven cybersecurity solutions increases by 0.443 units, assuming other factors remain constant. The standardized coefficient (Beta) is 0.466, indicating a moderate positive impact of cybersecurity awareness on the dependent variable when both are measured in standardized units. The t-value of 5.714 and the significance level (Sig.) of 0.000 confirm that this relationship is statistically significant. The constant (intercept) value of 1.566 suggests that when cybersecurity awareness is zero, the predicted baseline level of perceived effectiveness is 1.566. Overall, the results indicate a strong and significant positive relationship between cybersecurity awareness and the effectiveness of AI-driven cybersecurity solutions.

Table 17: Coefficients

Coefficients[a]						
Model		Unstandardized coefficients		Standardized coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.566	0.282		5.551	0.000
	Cyber security awareness	0.443	0.077	0.466	5.714	0.000

Note: [a]Dependent variable: effectiveness of AI driven cyber security solutions.

4 Discussions

The survey shows that 44.2% of respondents use the university's computer networks, while 50.8% are aware of cyber threats targeting these systems. Over 74.2% expressed serious concern about such threats, and 49.2% rated current cybersecurity measures as moderately effective. Common threats experienced include phishing (38.3%), unauthorized access (20%), data breaches (17.5%), and distributed denial of service attacks (DDoS) attacks (12.5%). Recent studies highlight significant concerns regarding cybersecurity among university students. A 2023 study by Bottyan assessed the security awareness of university students, emphasizing the necessity of implementing adequate protective measures to safeguard personal data and ensure uninterrupted education. Similarly, research [24] evaluated the extent of cybersecurity awareness among college students and proposed measures to protect them from cyber-attacks, underscoring the importance of understanding threats like phishing, malware, and ransomware. These findings align with the survey results, indicating prevalent concerns and highlighting the need for enhanced cybersecurity measures within university settings.

A study by [25] which discusses the role of multi-factor authentication (MFA) in mitigating cyber threats. Their research highlights how MFA significantly strengthens security by adding an extra layer of verification, reducing the likelihood of unauthorized access. This aligns with the 34.2% of respondents who reported using MFA as a security measure. Additionally, 40% believe all listed AI-driven cybersecurity solutions would be effective, with 24.2% favoring AI-driven intrusion detection systems (IDS) and response systems specifically. The findings indicate strong support (90.8%) for integrating AI-driven cybersecurity into university systems, alongside high awareness (84.2%) of common cyber threats like phishing and malware. According to a study by [26], which explores the effectiveness of AI-and data-driven cybersecurity techniques in enhancing threat identification and response. The study underscores how AI-driven systems improve the detection of cyber threats and enable faster, more effective responses, aligning with the high level of support for AI integration in university cybersecurity systems which supports the researchers' findings. While most respondents understand and practice strong password use and multi-factor authentication (96.7%), only 65.8% feel the university provides regular cybersecurity training, suggesting room for improvement in institutional efforts. Ref. [27] examined the effectiveness of cybersecurity training in higher education institutions. The study found that while many universities offer training, it is often inconsistent or inadequate, leading to gaps in awareness and security behavior among students. This highlights the need for more comprehensive and regularly updated cybersecurity training programs in university settings to address emerging threats effectively. Notably, 94.2% actively take personal measures to protect their data, reflecting a high level of individual responsibility toward cybersecurity.

A thorough examination of improving data privacy through multi-layer encoding, robust cryptographic methods, One time Password (OTP) authentication, and multi-cloud storage architectures can be found in the reviewed article, Advancing Data Privacy in Cloud Storage: A Novel Multi-Layer Encoding Framework [28], Although it focuses on cloud storage, the strategies covered layered encryption, key management, threat management, auditing procedures, and compliance validation apply just as well to protecting university networks. Universities are depending more and more on cloud-integrated systems for administrative records, research outputs, and student data all of which are susceptible to security breaches. University networks would be better protected against unwanted access, support regulatory compliance (such as General Data Protection Regulation (GDPR) for international students), and guarantee trust in digital services if the paper's multi-layer encoding framework and privacy-preserving features were implemented. As a result, the framework can be modified to provide comprehensive cybersecurity for educational institutions outside of commercial cloud environments.

Important cybersecurity tactics like intrusion detection, anomaly monitoring, resilient architectures, and cutting-edge cryptographic techniques are highlighted in the reviewed article, A Comprehensive Review of Cybersecurity in Energy Systems: Threats, Challenges, and Emerging Solutions [29]. Despite being focused on energy systems, many of the strategies it suggests can be applied to university networks, which are susceptible to similar risks of illegal access, system outages, and data breaches. For example, sensitive student data, research outputs, and administrative records can be secured by implementing layered security architectures, machine learning-driven anomaly detection, and intrusion detection systems. Similarly, the focus on energy systems' resilience planning, real-time monitoring, and regulatory compliance can guide tactics for defending university digital infrastructure against insider threats as well as external cyberattacks. As a result, this article's insights go beyond energy systems and provide a strong basis for enhancing cybersecurity in educational settings.

The findings reveal strong support for AI in enhancing cybersecurity, with 95.9% of respondents agreeing that AI-driven systems effectively detect threats in real time and 93.3% trusting AI to reduce unauthorized data access. Additionally, 84.2% believe AI monitoring outperforms traditional methods, and 93.3% recognize its efficiency in responding to incidents. Overall, 95% advocate for prioritizing AI integration to strengthen university network security. Ref. [30] explores the role of AI-driven security mechanisms in improving cybersecurity. Their research highlights how AI systems provide real-time detection of cyber threats, enhance the identification of unauthorized access attempts, and optimize the response to security incidents, mirroring the survey findings on AI's effectiveness in securing university networks which supports the findings.

The Model Summary shows a moderate positive correlation (R = 0.466) between cybersecurity awareness and cybersecurity effectiveness. About 21.7% of the variation in effectiveness is explained by awareness (R^2 = 0.217). The model has a reasonable fit, with a standard error of 0.67405. The ANOVA results show that cybersecurity awareness significantly predicts the effectiveness of AI-driven cybersecurity solutions, with a high F-value of 32.653 and a significance value of 0.000. This indicates that the model is statistically significant, explaining a notable portion of the variation in the effectiveness of AI-driven solutions. The Coefficients table shows that cybersecurity awareness significantly influences the effectiveness of AI-driven cybersecurity solutions, with a positive unstandardized coefficient of 0.443 and a standardized Beta of 0.466. The relationship is statistically significant, as indicated by a t-value of 5.714 and a significance of 0.000, suggesting a strong positive impact. The intercept value of 1.566 represents the baseline effectiveness when awareness is zero.

On addressing the limitations of the study it's difficult to deploy the AI-driven cyber security model since its very expensive and there is limited infrastructure that can be used to support the model. There are very few AI professionals. The study may be limited in terms generalizability in other universities worldwide due to different architectures used and also the AI digital literacy levels.

The study focused more on the modern AI-based solutions as compared to the traditional Cyber security methods. AI-based solutions in other sectors, such as, healthcare and finance have demonstrated high detection accuracy according to a study by [31]. Rapid integration of AI technology in banking improves trade, threat operation, and customer service, but non-supervisory fabric compliance presents challenges. AI-driven innovations in healthcare improve patient problems and diagnostics, but ethical dilemmas including data privacy and algorithmic impulses need to be handled.

In terms of ethical and privacy considerations, federated learning would be an excellent option to use when trying to increase privacy in university networks because this would enable building AI models locally on the user devices without having to send raw user data over central servers. A decentralized solution cuts down the possibility of data breach and other malicious access significantly due to the sensitive nature of the data involved which in this case are academic and personal data. Ethical considerations, however, such as concerns related to informed consent, ownership of data, potential misuse or overreach, are brought up by the integration of AI-driven surveillance and data collection systems. Whether we are in the academic setting or an enterprise, it is essential to guarantee the transparent and responsible use of such technologies without damaging the principles of academic freedom, privacy, and trust, which are bases of the learning environment.

5 Conclusion

In conclusion, the survey results and supporting studies indicate a growing awareness and concern among university students regarding cybersecurity threats, with significant support for integrating advanced

AI-driven solutions into university systems. The findings highlight the importance of multi-factor authentication and firewalls/IDS in mitigating cyber risks, while demonstrating strong support for AI's role in real-time threat detection and improving incident response. However, despite high awareness of common cyber threats, there is a notable gap in regular cybersecurity training within universities, emphasizing the need for more consistent and comprehensive educational efforts. The statistical analysis confirms a moderate positive relationship between cybersecurity awareness and the perceived effectiveness of AI-driven cybersecurity solutions, underscoring the critical role of awareness in enhancing overall security measures. Results suggest that there is potential for enhancement in the application of international standards, given the ongoing prevalence of cyberattacks, which often stem from insufficient resources and inadequate technological investment. To effectively mitigate these threats, it is essential to fully implement the policy and enhance organizational, human, physical, and technological controls. This research offers valuable insights for policymakers, administrators, and cybersecurity professionals aiming to improve security practices within the academic sector. A major difficulty encountered throughout the research was guaranteeing that respondents remained anonymous while obtaining authentic responses. To conclude, the rise in cyber threats underscores the need for a strong, tailored cybersecurity framework designed for Kenyan universities to effectively protect their digital assets.

According to the study's findings, Kenyan universities should focus on fully implementing cybersecurity policies, boosting investment in information technologies to tackle resource shortages and outdated systems, and improving organizational controls via regular risk assessments and cybersecurity awareness initiatives. It is also important to enhance physical security measures and implement a thorough cybersecurity framework. While there are strong personal awareness and proactive behavior in cybersecurity among respondents, institutional support in the form of regular training and clear reporting procedures appears to be an area for improvement. There is overwhelming support for the use of AI in enhancing cybersecurity within the university. Respondents recognize the effectiveness of AI in threat detection, prevention, and response, and strongly advocate for its integration into existing security frameworks. A small percentage remain cautious, especially when comparing AI to traditional methods.

6 Recommendations

Based on the survey findings and supporting studies, it is recommended that universities prioritize the integration of advanced cybersecurity measures, particularly AI-driven systems, to enhance threat detection, incident response, and overall network security. Given the high level of support for AI solutions and multi-factor authentication, universities should implement these technologies more broadly to mitigate cyber risks. Additionally, it is essential to provide consistent, comprehensive, and regularly updated cybersecurity training programs to address emerging threats and bridge the gap in awareness, as a significant portion of respondents felt that current training efforts were inadequate. Furthermore, fostering a culture of individual responsibility toward cybersecurity should be encouraged by continuing to raise awareness and promoting best practices such as strong passwords and multi-factor authentication. By aligning institutional efforts with these recommendations, universities can effectively strengthen their cybersecurity posture and better protect sensitive data from evolving cyber threats.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Conceptualization, Boniface Wambui; methodology, Boniface Wambui, Margaret Mwinji, Hellen Nyambura; formal analysis, Boniface Wambui, Margaret Mwinji; writing—original draft preparation, Boniface

Wambui; writing—review and editing, Margaret Mwinji, Hellen Nyambura. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are openly available in https://www.kaggle.com/datasets/bcccdatasets/large-scale-ids-dataset-bccc-cse-cic-ids2018, accessed on 23 September 2025.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Shahana A, Hasan R, Farabi SF, Akter J, Al Mahmud MA, Johora FT, et al. AI-driven cybersecurity: balancing advancements and safeguards. J Comput Sci Technol Stud. 2024;6(2):76–85. doi:10.32996/jcsts.2024.6.2.9.
2. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: literature review and future research directions. Inf Fusion. 2023;97(6):101804. doi:10.1016/j.inffus.2023.101804.
3. Singh A, Gupta BB. Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms. Int J Semant Web Inf Syst. 2022;18(1):1–43. doi:10.4018/ijswis.297143.
4. Alom MZ, Taha TM, Yakopcic C, Westberg S, Sidike P, Nasrin MS, et al. The history began from alexnet: a comprehensive survey on deep learning approaches. arXiv:1803.01164. 2018. doi:10.48550/arxiv.1803.01164.
5. Bottyan Z. Assessing the security awareness of university students: protecting personal data and ensuring uninterrupted education. J Cybersecur Educ. 2023;13(3):363. doi:10.24368/jates363.
6. Shokri R, Shmatikov V. Privacy-preserving deep learning. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security; 2015 Oct 12–16; Denver, CO, USA. doi:10.1145/2810103.2813687.
7. Talal H, Zagrouba R. MADS based on DL techniques on the Internet of Things (IoT): survey. Electronics. 2021;10(21):2598. doi:10.3390/electronics10212598.
8. Vudathala NR. AI-driven risk-adaptive app architecture: a dynamic approach to authentication and security in mobile applications. J Eng Comput Sci. 2025;4(7):911–6. doi:10.5281/zenodo.16225319.
9. Alshajahey R. The role of artificial intelligence in predicting and preventing cyber attacks: opportunities and risks for industry. SSRN. 2025. doi:10.2139/ssrn.5420494.
10. Adeyeye OJ, Akanbi I, Emeteveke I, Emehin O. Leveraging secured ai-driven data analytics for cybersecurity: safeguarding information and enhancing threat detection. Int J Res Publ Rev. 2024;5(10):3208–23. doi:10.55248/gengpi.5.1024.2911.
11. Gichubi PM, Maake B, Chweya R. Cybersecurity framework for Kenyan universities in conformity with ISO/IEC 27001: 2022 standard. OALib. 2024;11(8):1–15. doi:10.4236/oalib.1110810.
12. Islam MZ, Chowdhury MMH, Sarker MM. The impact of big data analytics on stock price prediction in the Bangladesh stock market: a machine learning approach. Int J Sci Bus. 2023;28(1):219–28. doi:10.58970/ijsb.2216.
13. Zaman S, Alhazmi K, Aseeri MA, Ahmed MR, Khan RT, Kaiser MS, et al. Security threats and artificial intelligence based countermeasures for Internet of Things networks: a comprehensive survey. IEEE Access. 2021;9:94668–90. doi:10.1109/access.2021.3089681.
14. Sindiramutty SR. Autonomous threat hunting: a future paradigm for AI-driven threat intelligence. arXiv:2401.00286. 2023.
15. Prince NU, Faheem MA, Khan OU, Hossain K, Alkhayyat A, Hamdache A, et al. AI-powered data-driven cybersecurity techniques: boosting threat identification and reaction. Nanotechnol Percept. 2024;20(S10):332–53. doi:10.13140/RG.2.2.22975.52644.
16. Lee J, Kim J, Kim I, Han K. Cyber threat detection based on artificial neural networks using event profiles. IEEE Access. 2019;7:165607–26. doi:10.1109/access.2019.2953095.
17. Kamaruddin NHC, Zolkipli MF. The role of multi-factor authentication in mitigating cyber threats. Borneo Int J. 2024;7(4):35–42.
18. Dwork C, Roth A. The algorithmic foundations of differential privacy. Found Trends® Theor Comput Sci. 2014;9(3–4):211–407. doi:10.1561/0400000042.

19. Amarasinghe AMSN, Wijesinghe WACH, Nirmana DLA, Jayakody A, Priyankara AMS. AI based cyber threats and vulnerability detection, prevention and prediction system. In: 2019 International Conference on Advancements in Computing (ICAC); 2019 Dec 5–7; Malabe, Sri Lanka. doi:10.1109/ICAC49085.2019.9103372.
20. Crumpler W, Lewis JA. Cybersecurity workforce gap. Washington, DC, USA: Center for Strategic and International Studies (CSIS); 2022.
21. Akhtar ZB, Tajbiul Rawol A. Enhancing cybersecurity through AI-powered security mechanisms. J Res Dev. 2024;9(1):50–67. doi:10.25299/itjrd.2024.16852.
22. van den Akker J. Principles and methods of development research. In: Design approaches and tools in education and training. Dordrecht, The Netherlands: Springer; 1999. p. 1–14. doi:10.1007/978-94-011-4255-7_1.
23. Mugenda OM, Mugenda AG. Research methods: quantitative and qualitative approaches. Nairobi, Kenya: Acts Press; 2003.
24. Verma V, Pawar J. Assessment of students cybersecurity awareness and strategies to safeguard against cyber threats. J Adv Zool. 2024;2024:82–9. doi:10.53555/jaz.v45is4.4156.
25. Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Nitin Bhagoji A, et al. Advances and open problems in federated learning. Found Trends® Mach Learn. 2021;14(1–2):1–210. doi:10.1561/2200000083.
26. Kim J, Kim J, Le Thi Thu H, Kim H. Long short term memory recurrent neural network classifier for intrusion detection. In: 2016 International Conference on Platform Technology and Service (PlatCon); 2016 Feb 15–17; Jeju, Republic of Korea. doi:10.1109/PlatCon.2016.7456805.
27. Borode A, Olubambi P. Optimisation of artificial intelligence models and response surface methodology for predicting viscosity and relative viscosity of GNP-alumina hybrid nanofluid: incorporating the effects of mixing ratio and temperature. J Supercomput. 2024;80(4):4841–69. doi:10.1007/s11227-023-05652-y.
28. Mishra KN, Lal RK, Barwal PN, Mishra A. Advancing data privacy in cloud storage: a novel multi-layer encoding framework. Appl Sci. 2025;15(13):7485. doi:10.3390/app15137485.
29. Mai VT, Mohammadzadeh A, Alattas KA, Taghavifar H, Ghaderpour E. Cybersecurity in maritime power systems: a comprehensive review of cyber threats and mitigation techniques. Electr Power Syst Res. 2025;247(2):111797. doi:10.1016/j.epsr.2025.111797.
30. Zhang F, Wang H, Zhou L, Xu D, Liu L. A blockchain-based security and trust mechanism for AI-enabled IIoT systems. Future Gener Comput Syst. 2023;146:78–85. doi:10.1016/j.future.2023.03.011.
31. Khan N, Rehman A, Jabeen R, Siraj M, Ahmed I, Iftikhar A. The intersection of AI in finance and healthcare: comparative analysis of adoption trends, challenges, and economic impact. In: Generative AI techniques for sustainability in healthcare security. Hershey, PA, USA: IGI Global; 2024. p. 301–12. doi:10.4018/979-8-3693-6577-9.ch016.