DS Journal of Cyber Security
Volume 3 Issue 1, 1-23, Jan - Mar 2025
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V3I1P101

Original Article

Improved Bring Your Own Device Policy Framework for Mitigation of Malware Threats in Higher Institutions of Learning

Wesimika Andrew[1], Olawale Surajudeen Adebayo[2], Manana Peter[3], Mubuke Faisal[4]

[1,3,4]Marketing and Management Department, Makerere University Business School Mbale Regional campus, Uganda.
[2]Department of Cyber security, Faculty of Computing, National Open University of Nigeria, Abuja.

[1]awesimika@mubs.ac.ug

Received: 04 January 2025; Revised: 07 February 2025; Accepted: 15 March 2025; Published: 31 March 2025

Abstract - This research analyzed the effectiveness of the existing Bring Your Own Device (BYOD) Policy Framework in mitigating Malware attacks in educational institutions and proposed an Improved BYOD Policy Framework (IBYODPF). The IBYODPF was designed specifically for higher institutions of learning to address unique challenges in Malware Mitigation by introducing a new dimension: the application whitelisting policy. This policy includes sub-components such as application breach, audit, and incident response policies, enhancing malware risk management. The study employed a quantitative design, gathering data through an online questionnaire and analyzing it using SPSS v20 and Smart PLS v3. A sample of 404 respondents, drawn from three universities in eastern Uganda, included 264 males and 140 females aged 18-45 and above. Purposive sampling ensured experienced participants. Findings highlighted that the application whitelisting and its sub-policies significantly reduced malware risks in institutional systems. This study contributes to existing knowledge by improving BYOD frameworks for educational institutions, enhancing their resilience against malware attacks.

Keywords - Application whitelisting policy, Bring your own device policy, Cyber security, Higher institutions of learning, Malware mitigation.

1. Introduction

In higher institutions of learning, BYOD is an initiative that allows students, faculty, staff, and others to use Personal Digital Assistants (PDAs) like smartphones, tablets, and laptops to access institutional networks, resources, and learning applications [46, 49]. Over the years, researchers have examined the BYOD policy in organizations, analyzing its effectiveness and the challenges it presents [1]. Studies by [2] highlight an increasing adoption of BYOD policy in organizations as a cost-cutting initiative.

The BYOD is increasingly becoming necessary to manage these personal devices within organizations, ensuring security and compatibility with existing systems. [3, 5, 37] This adoption introduces significant security risks, including data loss and user privacy concerns [8, 11, 43]. Studies conducted by [45] highlight the urgent need to strengthen cyber security policies through improvements due to the global surge in cyber security attacks on higher institutions of learning caused by the evolving and sophisticated nature of cyber threats.

In Uganda, despite having a BYOD policy, many higher institutions of learning face challenges in their enforcement and administration, hence its ineffectiveness [UCC, 2022 report]. This comes from many users, including students, lecturers, and support staff, complicating regulation [44]. This necessitates an examination of the effectiveness of existing cyber security policies to mitigate cyber threats [9, 12]. A preliminary national cyber security policy emphasizes the need for organizations to protect their infrastructure, data, and personal identities. [10].

A study on cyber security awareness in universities indicates that a significant portion of students and academic and administrative staff have limited knowledge regarding cyber security awareness [13, 14]. A study conducted in Uganda investigated the effectiveness of BYOD policies in higher institutions of learning in mitigating malware attacks. While these institutions have implemented BYOD policies, the findings suggest that these policies require further refinement and enhancement, as indicated by [15].

Despite holding the truth that a lot of research has been done on the BYOD framework's ability to reduce malware threats in higher education institutions [39, 55], The BYOD framework for malware threat reduction was suitable and fulfilled its intended functions in the settings of nations such as the United States, India, and Japan [30, 56], it was not replicable in Ugandan settings, according to [31] , there is not a single framework that can be used across the globe; instead, each nation needs a unique framework that can effectively handle its unique needs and tech difficulties.

The usefulness of BYOD strategies in Ugandan universities in preventing malware attacks has not been given theoretical or empirical attention [58]. [59] the current framework is not generally appropriate for emerging nations like Uganda and consequently does not meet Ugandan educational institutions' distinct requirements and challenges in minimizing malware attacks [58]. Made the case that the success of BYOD policies in mitigating malware attacks needs to be given the utmost attention.

In light of this, this study aimed to create a better BYOD framework that would be applied in higher education institutions to reduce attacks caused by malware successfully. The generic BYOD architecture considered general data security measures through device, mobile learning, user, liability, and data security policies, as told by [30]. According to [56], the main elements of the BYOD framework are insufficient to handle malware risks in universities.

With a focus on malware protection, the Application Whitelisting Policy, which includes subcomponents such as application breach, audit, and incident response policies, is introduced by the more robust BYOD framework that this study developed. According to [57], mitigation measures are much strengthened when the BYOD framework is modified with the addition of application whitelisting. By incorporating application whitelisting into the current BYOD framework, this study provides a more thorough enhanced framework to reduce growing malware threats that have continuously affected the business processes in higher education institutions.

In order to combat the present threat of attacks from malware, the created framework will guide the detection of malware and attack projection. Additionally, this will allow the universities BYOD policies to produce alerts and suggestions for potential mitigation measures to handle the risks.

2. Literature Review

2.1. Cyber Security Evaluation Framework for Universities

In the evaluation of any cyber security framework, it is essential to account for both the associated risks and corresponding countermeasures designed to mitigate cyber security threats [16, 17].

Table 1. Cyber security evaluation framework for universities

SN	Framework Components/Description	Proposed Criteria of Analysis and Evaluation	Potential Cyber Security Threats to be Curbed
1	Staff education	The framework proposes cyber security training for all university staff	Phishing attacks
2	Protecting email communication	Indicates the ratio of received mails to the number of spam filters as per the indicator	Mail phishing
3	End user security measures.	The framework highlights the size of unauthorized data transfers as per the indicator.	Data loss
4	Upgrade Equipment	Regular updates of each computer in the organization, depending on the indicator	Equipment loss or theft
5	Establishing and strengthening cyber security	The framework recommends having a comprehensive policy to address cyber security issues.	Entirely at risk
6	Organizational device protection	The framework recommends monitoring networked devices, evaluating their status and ensuring that they receive regular updates.	Risks to interconnected organizational devices
7	Restricted access to organizational devices	Identifying and responding to unauthorized access incidents	Attacks on interconnected gadgets
8	Access to governance policies	Mitigate unauthorized network access	Un authorized access
9	Data backup systems	Regular monitoring of data backups to accommodate growing storage needs	Malicious software attacks and data loss

Source: [15]

2.2. BYOD Policy Framework for Educational Institutions

The policy allows staff and students to use their devices while safeguarding institutional data and fostering a secure, productive, and efficient academic environment [18]. Studies indicate that BYOD policy balances adaptability and ease of using personal devices and institutions' corporate data security [19]. BYOD policy in academia involves selecting and classifying personal devices [20]. Furthermore, the policy aims to make the employee flexible, with the need to protect his data and organizational security at large [21]. The Mobile learning policy dimension provides guidelines on device use for academic purposes [22]. The policy outlines user education and training on BYOD technology [23]. It also addresses cost allocation for mobile usage, defining employer-employee financial responsibilities, liability coverage and procedures for claims related to employee conduct, data breaches and third-party interactions [24]. The Data security policy mandates data segregation, device registration, remote access, encryption, strong passwords and virtual private network usage.

Table 2. BYOD policy framework for educational institutions

SN	Framework Policy Components	Description of the policy framework
1	Policy on devices	The BYOD program defines permissible device types, allowing employees to use personal devices that meet organizational requirements. However, strict restrictions are enforced to regulate device access, ensuring only approved devices are integrated into the workplace to maintain security and efficiency.
2	Policy on mobile learning	The mobile learning policy supports device use of academic learning, seamless communication, application development, inclusivity of disabled students and addressing concerns related to mobile learning.

3	Policy on users	The policy enforces role-based access controls, BYOD training, device reporting, social media policies, data protection, password standards and privacy management.
4	Policy on liability	The policy defines responsibility coverage, liability events, claims procedures, and re-imbursement, with payment terms determined through employer and employee agreements.
5	Policy on data security	Through MDM solutions, organizations enforce data separation, device registration, remote access, encryption, strong passwords and VPNs.

Source: [4]

2.3. Holistic Cyber Security Maturity Assessment Framework (HCMAF) for Higher Education Institutions (HEIs)

According to [6], the assessment framework serves as a tool for self-assessment in Higher Education Institutions (HEIs) to assess their security status, identify vulnerabilities, and outline necessary mitigation strategies to implement [25]. Furthermore, the framework offers security and privacy guidelines that higher institutions of learning must comply with. According to [26], the measurement and assessment of the cyber security performance of higher institutions of learning involve security levels, gap analysis, and the creation of mitigation plans for cyber security threats and attacks.

Table 3. Summary of the Holistic Cyber security Maturity Assessment Framework (HCMAF) for Higher Education Institutions (HEIs)

HCMAF **Sections**	**Component Description**
Introduction	The framework highlighted higher education institutions' increasing cyber security threats and the need for a comprehensive assessment framework.
Objective	Specifically designed for higher education institutions.
Framework Components	The key components of the framework included identity, protect, detect, response and recovery. These guided governance, risk management and security practices. Security Operations, Incident Response, and Continuous Improvement.
Governance	Emphasized the role of leadership and policies in establishing a secure environment.
Risk Management	Focused on identifying, assessing, and mitigating institutional data and systems risks.
Security Operations	Covered the implementation and management of security controls and technologies.
Response to incidents	Outline procedures for detecting, addressing, and recovering from cyber security incidents.
Continuous Improvement	Stresses the importance of regular reviews and updates to the cyber security strategy.
Methodology	Describe the research methods used, including literature review and expert consultations.
Framework Validation	Explored the validation process through case studies and feedback from cyber security experts in academia.
Findings	The validation of results demonstrates the framework's efficacy in evaluating cyber security maturity.
Recommendations	Provided practical recommendations for implementing the framework within academia.
Conclusion	Summarized the importance of a holistic approach to cyber security and the benefits of the proposed framework.
Future Work	Suggested areas for further research included adapting the framework for different types of institutions and evolving cyber security threats.

Source: [6]

2.4. Current State of Cyber Security in Higher Education Institutions in Uganda

Higher education institutions of learning in Uganda do not have systematic approaches to cyber security threats [UCC, 2022 report]. This highlights a critical gap in the readiness of these institutions to tackle the evolving landscape of cyber threats. Additionally, the study revealed a limited investment in cyber security infrastructure, highlighting threats that cybercriminals can exploit.

Furthermore, with limited security designs within organizations across the globe, malware detection has become a unique challenge [27]. The (2019 NITA-U statistics report) highlights the importance of enhancing cyber security awareness initiatives, advocating for structured training and certification programs, integrating cyber security education into the curriculum at all levels of education, and addressing budget constraints for research and development in Uganda.

Higher Education Institutions in Uganda are vulnerable to cyber security threats [28]. It is, therefore, imperative to establish robust policies for effectively managing malware to bolster the security of both data and the underlying infrastructure [29].

2.5. Cyber Security Education

The increase in malware attacks targeting higher education stems from insufficient cyber security education, deficient security policies, and inadequate leadership abilities [30, 31]. A study highlights that these breaches are caused by insufficient security awareness, causing between 50% to 80% of incidents [32]. Security gaps affect policy compliance and effectiveness [33]. Organizations must implement regulatory requirements when creating robust cyber security guidelines [34].

2.6. Research Gap

Institutions increasingly adopt BYOD policies as a cost-cutting initiative [35, 36]. However, this shift introduces significant security risks, including data loss and user privacy concerns [42]. Research highlights that organizations permitting diverse users to connect personal devices to institutional networks must be regulated to mitigate cyber security threats [37].

Despite having BYOD policies, many higher institutions of learning find them less effective due to challenges in their enforcement and administration, making the policy ineffective [UCC, 2022 report]. This is due to the varied user base, including students, lecturers, and support staff, making it even more complicated to regulate and increasing security vulnerabilities.

Research by [38] reveals that malware threats can undermine the existing BYOD policies intended to enhance security, compromising institutional networks, data integrity, and user privacy. This necessitates improving the existing cyber security policy frameworks to safeguard institutional networks [39].

Studies by [40] highlight the urgent need to analyze and refine existing BYOD policies in higher institutions of learning to address malware threats and create a secure academic environment [40]. In response, the researcher has modified the BYOD policy framework for educational institutions by introducing an additional policy dimension, the Application Whitelisting Policy, which comprises three key components:

Application Breach Policy, Application Audit Policy, and Incident Response Policy. These enhancements aim to strengthen BYOD policy effectiveness, ensuring a more secure and resilient institutional network while mitigating cyber security risks in higher education settings.

2.7. Existing Bring Your Own Device Policy Framework

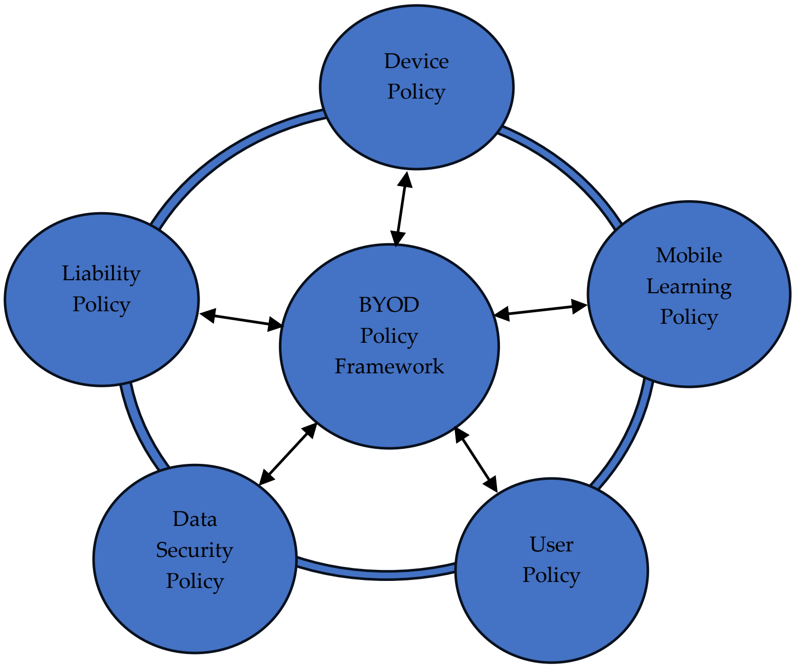

Fig. 1 BYOD policy framework for educational institutions

Table 4. Description of the existing BYOD policy framework

SN	Policy / Regulation	Description
1	Policy on regulations of devices	It explains the devices allowed under the BYOD program. The policy allows employees to come with their devices to work as long as they can serve the purpose; however, there is an emphasis on restricting the devices that come into the organization.
2	Policy on mobile learning	Explains the acceptance of mobile devices to be used for academic purposes anywhere and anytime
3	Policy for users	It highlights assigning different responsibilities and roles to users in the organization that are deemed important for policy compliance.
4	Liability Policy	The policy establishes definitions for BYOD liability protection and explains employer and employee reimbursement procedures when claims arise and the extent of cost-sharing for each party.
5	Data Security Policy	The security policy includes Separate data storage, device registration features, remote access capabilities, encryption systems, and requirements for strong passwords and Virtual Private Network (VPN) implementation. Organizations merge security protocols into Mobile Device Management (MDM) third-party solutions for security enhancement.

Source: [4]

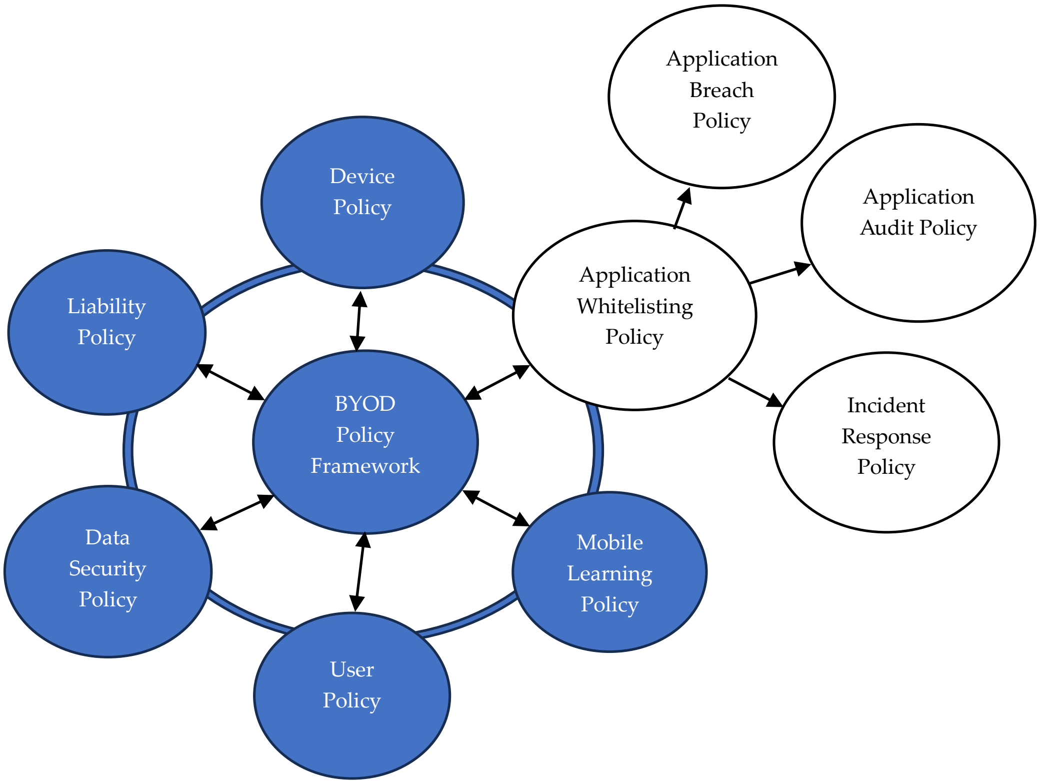

Fig. 2 The IBYODPF for mitigation of malware attacks in higher institutions of learning

Source: Bring your own Device Policy framework [4]

Table 5. Description of the new improved policy dimensions introduced to the framework

Policy Name	Policy Description
Application Whitelisting Policy	A security measure that allows only approved or whitelisted applications to run on the universities systems. All applications that are not on the whitelist are blocked to prevent potential malware attacks or unauthorized software execution.
Application Breach Policy	The policy details procedures and guidelines to follow in the event of any security breach caused by an application. This policy outlines steps for identifying, containing, and mitigating the breach and post-incident review.
Application Audit Policy	Defines the process for regularly reviewing and auditing applications to ensure they comply with security and organizational policies. This policy aims to identify vulnerabilities, unauthorized software, and compliance issues.
Incident Response Plan Policy	A structured approach for handling and managing cyber security incidents such as malware infections or breaches. The policy outlines the steps to detect, respond, recover, and document incidents to minimize damage and prevent recurrence.

Source: New improved policy dimensions introduced to the framework (Figure 2)

3. Materials and Methods

A quantitative Method of data collection was adopted with the intent of gathering data in numerical form. The method of collecting data stated in numerical form was embraced as quantitative research. [41] The study population comprised 3 universities, namely Islamic University, Makerere University Business School and Busitema University, because they represent a perfect mix of both public and private universities, ensuring a broader perspective on how different universities permit their staff to bring their own devices for access of university resources and whether the devices are regulated to mitigate persistent malware threats. The target population consisted of 404 respondents. The study utilized a sample of approximately 135 participants from a total population of 404, drawn from 3 universities in eastern Uganda. The sample size was determined using the Survey Monkey calculator. The three universities were selected through purposive sampling. The choice of these institutions was justified by their full accreditation from the National Council for Higher Education, meeting minimum required standards, including robust IT infrastructure.

This technological environment, where students, faculty, and staff frequently use personal devices to access university networks, exposes them to cyber security risks, making them suitable for examining the impact of malware threats. The researcher used a questionnaire (Google Forms) to collect primary data for this study. The data gathered through Google Forms helped the researcher analyze the weaknesses, suggest mitigation strategies for the existing bring-your-own-device Policy Framework in Educational Institutions and evaluate the IBYODPF to mitigate malware attacks in higher institutions of learning. To ensure data quality, the google form was validated using the platform's built-in validation rules to regulate the response entries.

3.1. Analysis of Data

Quantitative data analysis was carried out using SPSS version 20 and smart PLS 3.0. A five-point Likert scale was utilized to capture respondents' views, providing five response choices to indicate their degree of agreement and disagreement with different statements. SPSS v20 was used to generate descriptive statistics that delved deep into gender and their role in generating insights on malware mitigation, age, education, weaknesses of the existing BYOD policy framework, and recommendations on the existing BYOD policy framework for malware mitigation. The Smart PLS version 3 generated the SEM model of the IBYODPF for mitigating malware threats in higher institutions of learning.

The SEM model explains the item reliability basing on the indicator variance, indicator loading, internal consistency reliability, structural model using R square results from the extended BYOD endogenous variables, path coefficient and significance test results, Descriptive statistics for Evaluation of the IBYODPF and results on path coefficient and T-statistics of the improved BYOD policy framework. The analysis results depict the relationships between the existing BYOD and IBYODPF and how the new component of application whitelisting and its subcomponents can help mitigate malware threats in higher institutions of learning.

3.2. Validity and Reliability of the Research Tools

The google validation rule was applied to the google form before it was deployed online. The validation rule function was established to confirm that survey participants enter data in compliance with researcher-imposed regulations. The specified format and response types controlled the data entries to maintain accurate and consistent records. The reliability of the research instrument was evaluated using Cronbach's Alpha Coefficient [53], and Composite Reliability and Average Variance extracted [54] were assessed using Smart PLS version 3.0.

3.3. Ethical Considerations

3.3.1. Plagiarism

The researcher credited all sources, materials, and any other support received during the study.

3.3.2. Confidentiality

All the information collected during the study was confidential and only used for academic purposes. Participants' identities remained anonymous.

3.3.3. Informed Consent

The study was carried out exclusively for academic reasons, without any commercial intentions of personal benefit, and participation was completely voluntary in nature.

4. Results and Discussion

4.1. Demographic Profile of Respondents

The study achieved a 100% response rate of 404 out of 404 respondents from the three universities, which contributed 100% of the unit of analysis. The response rate for IT experts was 20 out of 20 respondents.

Table 6. Frequency of respondent's gender

Respondents Gender	Frequency	%	Valid Percent	Accumulated %
Male	264	65.3	65.3	65.3
Female	140	34.7	34.7	100.0
Total	404	100.0	100.0	

Source: Author's Primary Data (2024)

The results are presented in Table 6. Illustrate the key findings from the analysis, which present the majority of the respondents as Male at 65.3%, followed by female at 34.7%. Although a majority of them were Male, it implies that there is no gender discrimination in higher institutions of learning.

Table 7. Respondents age bracket

Respondents Age	Frequency	%	Valid Percent	Accumulated %
18-25	60	14.9	14.9	14.9
25-35	221	54.7	54.7	69.6
35-45	105	26.0	26.0	95.5
Above 45	18	4.5	4.5	100.0
Total	**404**	**100.0**	**100.0**	

Source: Author's Primary Data (2024)

The findings presented in Table 7 reveal the majority of respondents falling within the 25-35 age range at a frequency of 60, followed by those in the 35-45 at a frequency of 105, followed by 18-25 at a frequency of 60, and those above 45 age brackets with a frequency of 18. This implied that most Respondents were in their most productive and reasonably experienced age brackets and could give feedback based on their long-term experiences.

Table 8. Descriptive statistics on the educational attainment of the respondents

Educational Attainment	Freq	%	Valid Percentage	Accumulated %
Certificate	1	.2	.2	.2
Diploma	14	3.5	3.5	3.7
Bachelor	225	55.7	55.7	59.4
Masters	130	32.2	32.2	91.6
PHD	34	8.4	8.4	100.0
Total	404	100.0	100.0	

Source: Author's Primary Data (2024)

Regarding education, findings in Table 8 show that the majority of the respondents had bachelor's degrees at 55.7%, followed by master's holders at 32.2%, followed by 8.4% by PHD, followed by 3.5% Diploma holders and 0.3% Certificate level. This implied that most of the participants had an advanced level of education.

Table 9. Descriptive statistics of different respondents categories

Category	Frequency	Percent	Valid Percent	Cumulative Percent
IT expert	20	5.0	5.0	5.0
Administrator	262	64.9	64.9	69.8
Student	40	9.9	9.9	79.7
Academic staff	82	20.3	20.3	100.0
Total	404	100.0	100.0	

Source: Author's Primary Data (2024)

Results from Table 9 reveal that 5.0% represented IT experts, 64.9% administrators, 9.9% students and academic staff represented 20.3%. This implies that respondents are directly or indirectly affected by the bring your own device policy at various institutions.

4.2. Descriptive Statistics of Weaknesses of the Existing BYOD Policy Framework

Results from the descriptive analysis reveal a (mean: 4.20, stde: .894, bootstrap- lower: 3.75, upper 4.55) indicates agreement that there is limited control of mobile devices more than the looming threat of malware attacks at the campus. This is supported by the bootstrap analysis, which indicates that a positive lower and upper bound of the mean is statistically significant in relation to the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.65, stde: .489, bootstrap- lower: 4.45, upper 4.85) reflects the respondent's agreement that there is limited training of stakeholders on risks associated with malware mitigation. This is supported by the bootstrap analysis, which indicates that a positive lower and upper bound of the mean is statistically significant in relation to the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.95, stde: 1.099, bootstrap- lower: 3.45, upper 4.45). This means that respondents agreed that there is more effort to control devices owned by the institution than devices that come with the employees. This is supported by the bootstrap analysis, which indicates that a positive lower and upper bound of the mean is statistically significant in relation to the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.05, stde: .999, bootstrap- lower: 3.65, upper 4.45), which shows that respondents concurred that no policy at your institution restricts the use of personal devices in accessing the institution's network, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean is statistically significant in relation the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.90, stde: .718, bootstrap- lower: 3.55, upper 4.20), which shows that respondents agreed that all the employees of the institution are not familiar with bring your own device policy at the institution, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean is statistically significant in relation the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.10, stde: .852, bootstrap- lower: 3.70, upper 4.45), which shows that respondents agreed that no training had been organized to sensitize stakeholders on how to mitigate malware attacks on personal devices at work, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean is statistically significant in relation the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.00, stde: .795, bootstrap- lower: 3.60, upper 4.30), which shows that respondents agreed that there is no clear definition of employee roles, compliance, and guidelines for third-party interactions at the institution, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean is statistically significant in relation the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.90, stde: .718, bootstrap- lower: 3.55, upper 4.20), which shows that respondents agreed that there is no regular security audit policy for mitigation of malware attacks at the institution. This is supported by the bootstrap analysis, which indicates that a positive lower and upper bound of the mean is statistically significant in relation to the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.10, stde: .852, bootstrap- lower: 3.70, upper 4.45), which shows that respondents agreed that application whitelisting is not often used on applications that are recommended for use by the IT staff at the institution, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean is statistically significant in relation the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 1.95, stde: .224, bootstrap- lower: 1.85, upper 2.00), which shows that respondents disagreed that the staff at the institution are held liable for data breaches and are served punishments for breach of responsibility and data breach policy, whereas the bootstrap analysis indicates a positive lower and upper bound of the mean and is statistically significant in relation to the weaknesses of the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.05, stde: .999, bootstrap- lower: 3.60, upper 4.45), which shows that respondents agreed that clear incident response plans are not established at the institution in case of malware attacks. This is supported by the bootstrap analysis, which indicates that a positive lower and upper bound of the mean is statistically significant in relation to the weaknesses of the existing BYOD policy.

4.3. Descriptive Statistics of Recommendations to the Existing BYOD Policy Framework

Results from the descriptive analysis reveal a (mean: 3.85, stde: .933, bootstrap- lower: 3.45, upper 4.20), which shows that respondents agreed and recommended the development of a comprehensive policy framework for the Mitigation of malware attacks at the institution, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.45, stde: 1.276, bootstrap- lower: 2.90, upper 3.95) which shows that respondents agreed and recommended an improvement on control of mobile devices more than the looming threat of malware attacks on non-mobile devices at the campus, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.00, stde: .973, bootstrap- lower: 3.55, upper 4.35), which shows that respondents agreed and recommended analysis of the effectiveness of the existing malware mitigation policies at the institution should be conducted regularly in order to improve the existing policies., this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.45, stde: 1.276, bootstrap- lower: 2.90, upper 3.95), which shows that respondents agreed and recommended that staff and students at the institution be held liable for application breaches and are served punishments for breach, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.00, stde: .973, bootstrap- lower: 3.55, upper 4.35), which shows that respondents agreed and recommended that there should be well defined incident response plans at the institution for handling malware attacks, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.85, stde: .933, bootstrap- lower: 3.45, upper 4.20), which shows that respondents agreed and recommended restriction of devices that come to the organization by the IT staff. This is supported by the bootstrap analysis, which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.45, stde: 1.276, bootstrap- lower: 2.90, upper 3.95), which shows that respondents agreed and recommended that the application and whitelisting policy would significantly reduce the risk of malware infiltration in the institution, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.00, stde: .973, bootstrap- lower: 3.55, upper 4.35) which shows that respondents agreed and recommended that the application and whitelisting policy should allow approved applications to run on devices of staff in the institution, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.45, stde: 1.276, bootstrap- lower: 2.90, upper 3.95) which shows that respondents agreed and recommended that to minimize the use of the unauthorized Application, an application breach policy should be put in place, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 4.00, stde: .973, bootstrap- lower: 3.55, upper 4.35), which shows that respondents agreed and recommended that regular application audit policy is a proactive approach that will minimize the likelihood of successful malware attacks by using unauthorized applications, it enhances the institutions' overall security posture. This is supported by the bootstrap analysis, which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

Results from the descriptive analysis reveal a (mean: 3.85, stde: .933, bootstrap- lower: 3.45, upper 4.20), which shows that respondents agreed and recommended that Incident Response Plan policy would help in containment, eradication, recovery, and reporting procedures on malware attacks in the institution, this is supported by the bootstrap analysis which in dictates a positive lower and upper bound of the mean and is statistically significant in relation to the existing BYOD policy.

4.3.1. Observation of Extreme Collinearity on the IBYODPF (Figure 3)

The 3 latent variables that were dropped include mobile learning policy, user policy and liability policy using the partial list squares algorithm under the singular matrix problem because they were identical, showed cases of extreme perfect collinearity, and correlated 1. The 3 latent variables also showed similar values for each observation and had a zero variance. However, the model accepted only 2 variables on the existing BYOD, namely data security policy and device policy, during analysis in addition to the extended IBYODPF as the latent variables on the IBYODPF had no extreme collinearity implying that the IBYODPF was suitable for Mitigation of malware threats.

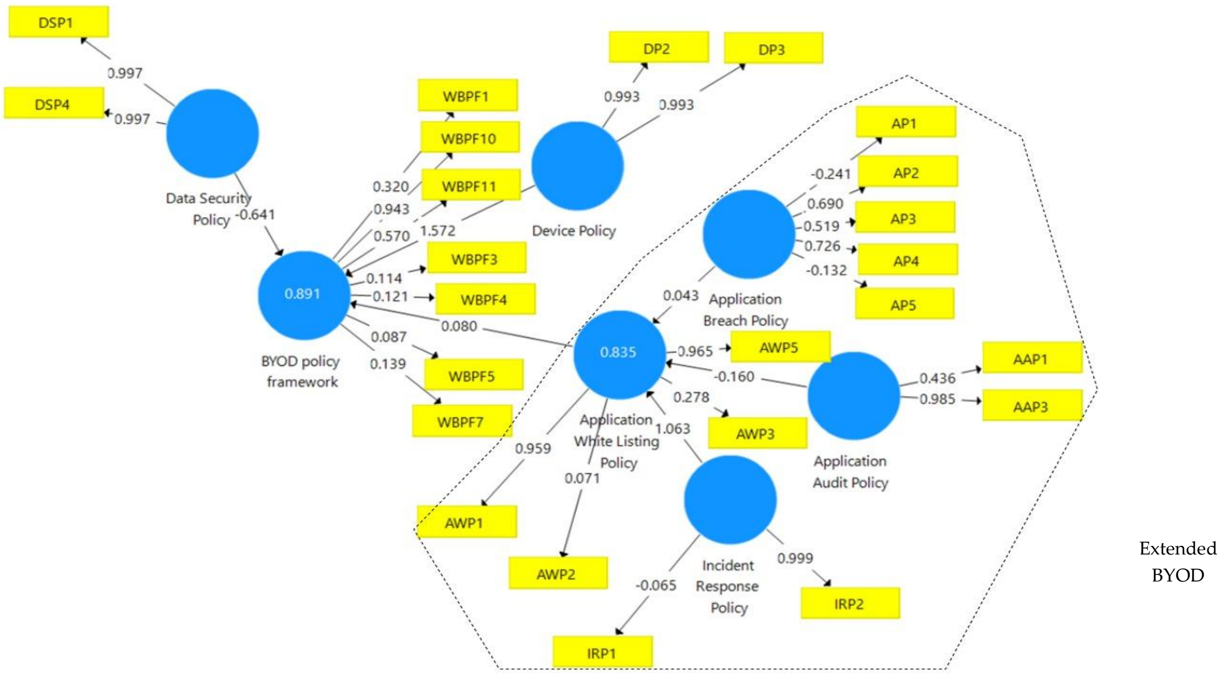

Fig. 3 Final improved BYOD policy framework

Source: Author and primary data Smart PLS 3.0 (2024)

4.3.2. Observation of Extreme Collinearity on the IBYODPF (Figure 3)

The 3 latent variables that were dropped include mobile learning policy, user policy and liability policy using the partial list squares algorithm under the singular matrix problem because they were identical, showed cases of extreme perfect collinearity, and correlated 1. The 3 latent variables also showed similar values for each observation and had a zero variance. However, the model accepted only 2 variables on the existing BYOD, namely data security policy and device policy, during analysis in addition to the extended IBYODPF as the latent variables on the IBYODPF had no extreme collinearity implying that the IBYODPF was suitable for Mitigation of malware threats.

4.3.3. Comparison of Research Findings with Existing Literature

Unlike prior research emphasizing general data security measures through device, mobile learning, user, liability, and data security policies [4], this study introduces the Application Whitelisting Policy, encompassing subcomponents like application breach, audit, and incident response policies, specifically targeting malware mitigation. Findings demonstrate that general data security measures are insufficient to address malware threats, whereas applying whitelisting significantly strengthens mitigation strategies [47]. This contrasts with [48], which focuses solely on data privacy and security. This study advances cyber security research by addressing the critical gap identified in [4], offering a more comprehensive framework (IBYODPF Figure 3) to mitigate evolving malware risks in higher education institutions.

4.4. Measurement Model

The minimum percentage of the indicator variance should be 50%, demonstrating item reliability at 0.708. The latent variables' outer or indicator loading results show that 15 indicators have values below 0.708. These indicators are: AAP1, AP1, AP2, AP3, AP5, AWP2, AWP3, IRP1, WBPF1, WBPF10, WBPF11, WBPF3, WBPF4, WBPF5, and WBPF7.

Table 10. Indicator loading

Indicators	Application Audit Policy	Application Breach Policy	Application White Listing Policy	BYOD Model	Data Security Policy	Device Policy	Incident Response Policy
AAP1	0.436						
AAP3	0.985						
AP1		-0.241					
AP2		0.690					
AP3		0.519					
AP4		0.726					
AP5		-0.132					
AWP1			0.959				
AWP2			0.071				
AWP3			0.278				
AWP5			0.965				
DP2						0.993	
DP3						0.993	
DSP1					0.997		
DSP4					0.997		
EV1							
EV2							
IRP1							-0.065
IRP2							0.999
LP4							
MLP4							
R4							
UP5							
WBPF1				0.320			
WBPF10				0.943			
WBPF11				0.570			
WBPF3				0.114			
WBPF4				0.121			
WBPF5				0.087			
WBPF7				0.139			

Source: Author's Primary Data (2024)

Table 11. Indicator of internal consistency and reliability

	Cronbach's Alpha Results	Composite Reliability Results	Average Variance Extracted (AVE) Results
Application Audit Policy	0.431	0.707	0.580
Application Breach Policy	0.245	0.401	0.270
Application White Listing Policy	0.527	0.714	0.483
BYOD Model	0.454	0.483	0.196
Data Security Policy	0.994	0.997	0.994
Device Policy	0.986	0.993	0.987
Incident Response Policy	-0.055	0.467	0.501

Source: Author's Primary Data (2024)

The research evaluated its parameters using Cronbach's Alpha measure of internal consistency (CA) [53]. Composite Reliability measure of reliability (CR) and Average Variance Extracted measure of convergent validity (AVE) [54]., through Smart PLS 3.0. CA and CR function through parallel evaluation criterion because high numbers show better reliability. The validity of underlying constructs could be compromised when variables exceed the proposed reliability range of 0.70 to 0.90 since it implies variable redundancy. The SEM assessment process includes establishing reliability and validating convergent and discriminant aspects of the models.

The results from Table 11 show that five variables from CC failed to meet minimum standards while another two variables satisfied the norms. Three CR variables did not meet the recommended values, and four others fulfilled the requirements. The researcher utilized AVE analysis to check convergent validity by assessing constructs that must demonstrate at least 50% (0.5) variance in their items. This model's results showed that three latent variables failed to achieve the threshold, whereas four variables exceeded the necessary level, thus validating their worth.

4.5. Structural Model

Table 12. R square result from the extended BYOD endogenous variables

	R Square	R Square Adjusted
Application White Listing Policy	0.835	0.834
BYOD Framework	0.891	0.890

Source: Author's Primary Data (2024)

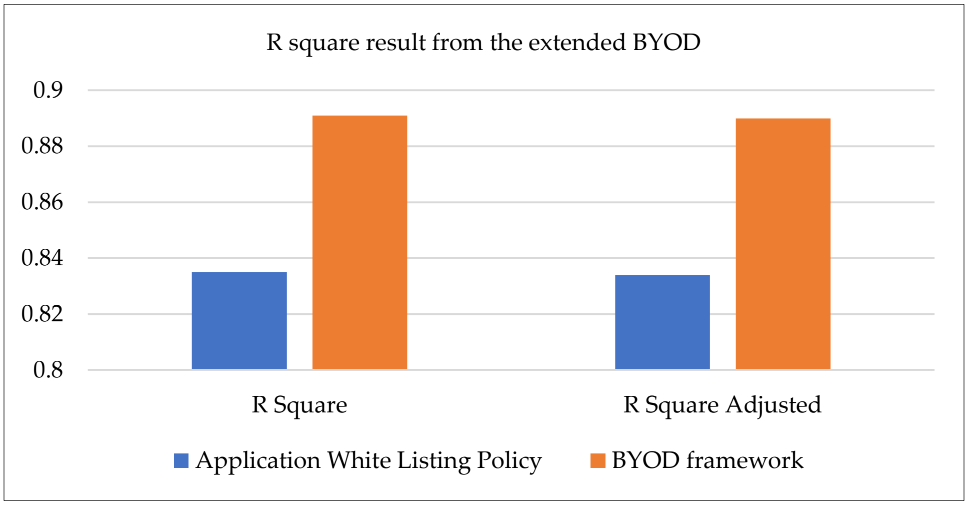

Fig. 4 R square result from the extended BYOD endogenous variables

The Variance Inflation Factor (VIF) results showed that two latent variables have VIF values below 5, an indicator that they are not collinear, whereas four latent variables had VIF values greater than five, indicating that they are collinear. Research shows that the predictive power is also known as R^2 and is an explanatory strength indicator ranging from 0 to 1, where higher values suggest a greater ability to explain the phenomenon.

Results from Table 12 indicate that the R^2 values from every endogenous variable vary. The BYOD framework, the pure endogenous variable, has an R^2 value of 0.891. it shows that the variables involved explain 89.1% of the BYOD framework. The same interpretation can be done with the Application whitelisting policy, whose R^2 value is 0.835. This implies that the Application whitelisting policy has an 83.5% predictive power over the existing BYOD policy framework; therefore, we suffice to say that the application whitelisting policy greatly enhances the implementation of the improved BYOD policy framework for malware mitigation.

Table 13. Showing path coefficient and significance test results

	Path Coefficients	T Statistics (|O/STDEV|)	Decision
Application Audit Policy -> Application White Listing Policy	-0.160	0.894	Not supported
Application Breach Policy -> Application White Listing Policy	0.043	0.803	Not supported
Application White Listing Policy -> BYOD Model	0.080	3.189	Supported
Data Security Policy -> BYOD Model	-0.641	2.257	Supported
Device Policy -> BYOD Model	1.572	5.694	Supported
Incident Response Policy -> Application White Listing Policy	1.063	6.859	Supported

Source: Author's Primary Data (2024)

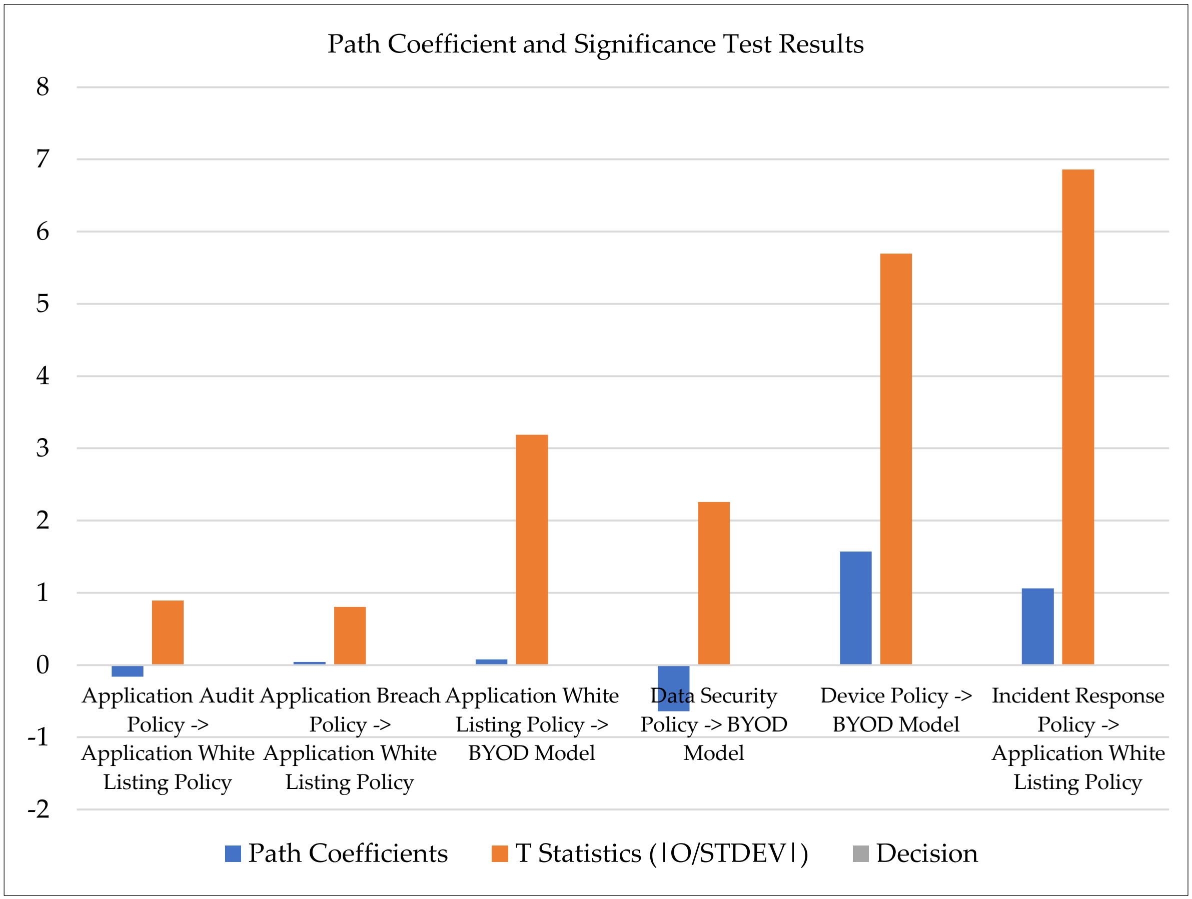

Fig. 5 Path coefficient and significance test results

4.6. Descriptive Statistics for Evaluation of the IBYODPF

Results from the descriptive analysis reveal a (mean: 3.85, stde: .933, bootstrap- lower: 3.40, upper 4.25), which shows that respondents who were IT experts agreed that the improved BYOD policy framework Uses Clear and simple explanations for its components, this is supported by the bootstrap analysis which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the improved BYOD policy framework for malware mitigation. This implies that stakeholders at high institutions of learning can easily implement the improved BYOD policy framework.

Results from the descriptive analysis reveal a (mean: 3.45, stde: 1.276, bootstrap- lower: 2.85, upper 4.00), which shows that respondents who were IT experts agreed that the improved BYOD policy framework requires little training to be used. This is supported by the bootstrap analysis, which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the improved BYOD policy framework for malware mitigation. This implies that stakeholders at high institutions of learning can easily implement the improved BYOD policy framework.

Results from the descriptive analysis reveal a (mean: 4.00, stde: .973, bootstrap- lower: 3.55, upper 4.40), which shows that respondents who were IT experts agreed that the improved BYOD policy framework is easy to use. This is supported by the bootstrap analysis, which indicates a positive lower and upper bound of the mean and is statistically significant in relation to the improved BYOD policy framework for malware mitigation. This implies that the improved BYOD policy framework can easily be used by stakeholders at higher institutions of learning compared to the original BYOD policy framework.

4.7. Discussion of Results on Path Coefficient and T-Statistics of the Improved BYOD Policy Framework

1. Application Audit Policy -> Application White Listing Policy: The path coefficient between the two variables above indicates a negative value, which means the correlation is negative. This means the application audit policy may not affect the Application whitelisting policy implementation on the improved BYOD policy framework. For t-statistics, the framework provided a value below the critical value of 1.96. This aligns with studies by [46]. Since the relationship is not significant, it is important to pay attention to this relationship for further improvement.
2. Application Breach Policy -> Application White Listing Policy: The path coefficient between the two variables shows a positive value, indicating a direct positive correlation. This means the application breach policy will significantly influence the application whitelisting policy implementation on the improved BYOD policy framework. For t-statistics, the framework provided a value below the critical value of 1.96. Since the relationship is not significant, it is important to pay attention to this relationship for further improvement.
3. Application White Listing Policy -> BYOD Model: The path coefficient between the two variables shows a positive value, indicating a direct positive correlation. This means the application whitelisting policy significantly influences the implementation of the improved BYOD policy framework. For t-statistics, the framework provided a value above the critical value of 1.96. Since the relationship is significant, the Application whitelisting policy greatly enhances the implementation of the improved BYOD policy framework for malware mitigation.
4. Data Security Policy -> BYOD Model: The path coefficient between the two variables shows a positive value, indicating a direct positive correlation. This means the data security policy significantly influences the implementation of the improved BYOD policy framework. For t-statistics, the framework provided a value above the critical value of 1.96. Since the relationship is significant, the data security policy enhances the implementation of the improved BYOD policy framework for malware mitigation.
5. Device Policy -> BYOD Model: The path coefficient between the two variables shows a positive value, indicating a direct positive correlation. This means the device policy significantly influences the implementation of the improved BYOD policy framework. For t-statistics, the framework provided a value above the critical value of 1.96. Since the relationship is significant, the device policy enhances the implementation of the improved BYOD policy framework for malware mitigation.
6. Incident Response Policy -> Application White Listing Policy The path coefficient between the two variables shows a positive value, indicating a direct positive correlation. This means the incident response policy significantly influences the implementation of the improved BYOD policy framework. For t-statistics, the framework provided a value above the critical value of 1.96. This implies that the relationship is significant; therefore, the incident response policy enhances the implementation of the improved BYOD policy framework for malware mitigation.

4.7.1. Assessment of the IBYODPF using Path Coefficient and T-statistics

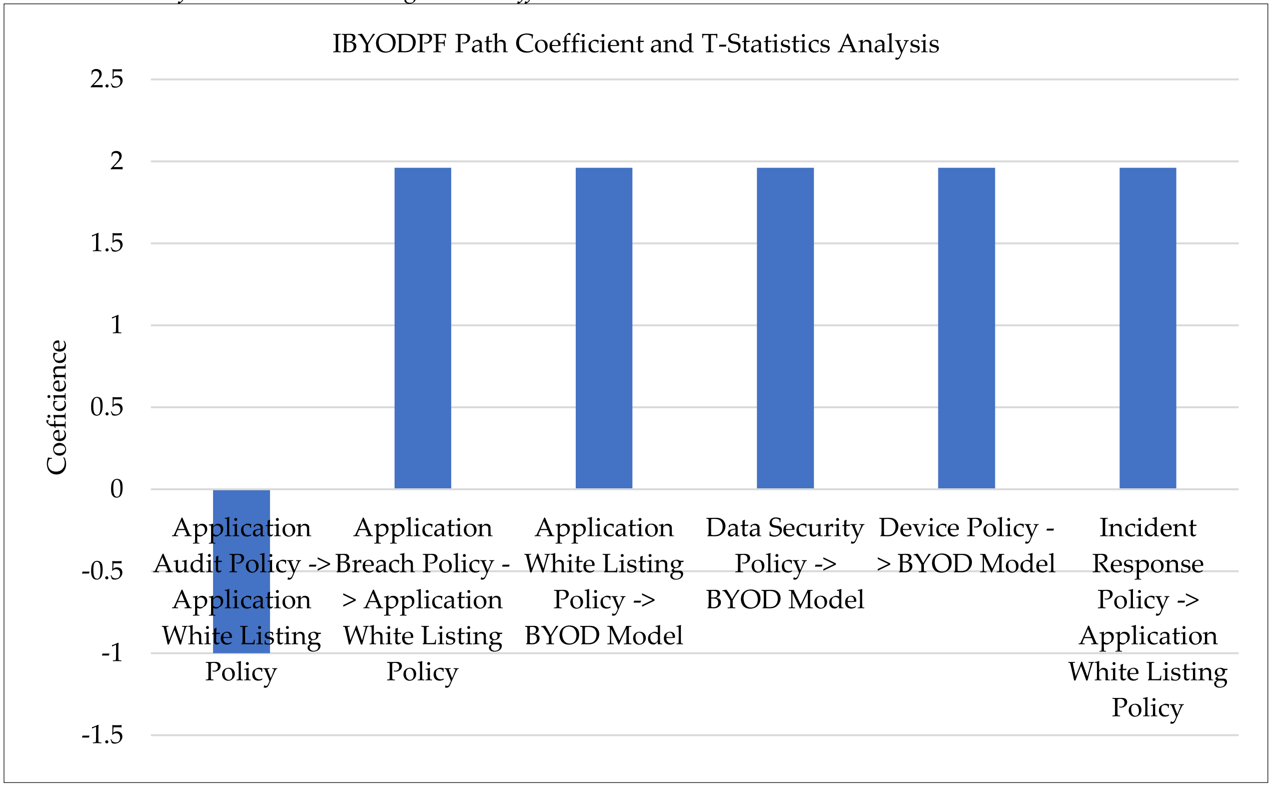

Fig. 6 Path coefficient and T-statistics of the IBYODPF

The bar graph represents relationships between different policies and their impact on IBYODPF for malware mitigation. The negative values indicate a negative correlation, implying that the policy is ineffective in malware mitigation, whereas the majority of positive values represent a positive correlation, implying effectiveness in malware mitigation efforts.

4.7.2. Justification of the IBYODPF in Malware Mitigation

The improved bring your own device policy framework is intended to enhance malware mitigation in higher institutions of learning by integrating application whitelisting with application breach policy, application audit policy, and incident response policy. This structured approach improves malware mitigation beyond traditional BYOD security frameworks through proactive security measures, a layered defence strategy, and adaptability to evolving threats. Studies conducted by [50] explain how application whitelisting prevents unauthorized or malicious software from being executed on networked devices, unlike traditional cyber security mechanisms.

Research conducted by [51] reveals that once adopted, Application audit and breach policies can enhance threat detection and response because audit policies ensure continuous monitoring of applications, identifying vulnerabilities before exploitation. Furthermore, Incident response policies provide a structured approach to security breaches, ensuring rapid containment and reduction of threats over the conventional approaches [52].

5. Conclusion

The original BYOD policy framework contained multiple latent variables, as illustrated in Figure 2. However, the Partial Least Square (PLS) analysis of the BYOD policy framework only validated two variables, as shown in Figure 2. These variables had a significant relationship with the Application whitelisting policy, with its subcomponents forming a new dimension in the IBYODPF for malware mitigation. The results emphasize the role of the IBYODPF in strengthening cyber security measures in higher education institutions.

By incorporating the application whitelisting policy and its subcomponents of application breach policy, application audit policy and incident response policy, the IBYODPF provides a more robust defense against malware threats and ensures a secure digital environment for students, faculty, and all administrative systems. Consequently, higher education institutions can leverage the IBYODPF to enhance data security, protect sensitive information, and promote safer BYOD practices.

Furthermore, researchers could investigate the integration of artificial intelligence in bring your own device policy frameworks to enhance malware threat detection in higher institutions of learning. Comparative studies can also be carried out across other regions, and institutional settings could provide more insights into the improved bring your own device policy framework's applicability and potential refinements.

5.1. Recommendations

The study identified several weaknesses in existing BYOD policy frameworks aimed at mitigating malware in Higher Institutions of Learning. Policy development and implementation stakeholders highlighted these challenges to pinpoint factors undermining current malware mitigation strategies. Therefore, it is imperative for university management to address these challenges effectively to adopt more robust malware mitigation strategies, as outlined below:

Regular security audits are crucial as a proactive measure to reduce the likelihood of successful malware attacks and enhance overall institutional security. University management and stakeholders should prioritize scheduling security audits for devices and networks to detect and mitigate potential vulnerabilities before they are exploited. Adopting an Incident Response Plan policy encompassing containment, eradication, recovery, and reporting procedures is essential to effectively mitigate malware attacks within the institution.

Enforcing a data security policy that mandates device registration by users is necessary. Additionally, implementing an application and whitelisting policy can significantly decrease the risk of malware infiltration in the institution. These recommendations underscore the need for university management to implement robust strategies for mitigating malware attacks in higher educational institutions.

5.2. Areas of Further Research

Even though the newly improved BYOD policy was evaluated and found fit to guide the Mitigation of malware attacks in higher institutions of learning, the researcher recommends further studies on the Mitigation of malware attacks in higher institutions of learning.

Contributions of the Authors

Author 1 wrote the introduction and developed the materials and methods section. Author 2 prepared tables and data presentation. Author 3 analyzed the data and wrote results and discussion section, and 4 contributed by drafting the conclusion and recommendations

Acknowledgements

The authors dearly express their gratitude to the participating universities in eastern Uganda for their cooperation and support during the study. Special thanks go to the respondents who provided valuable data and insights. The authors also acknowledge the technical support and guidance provided by colleagues and mentors throughout the research process.

References

[1] Ben Scott, Raina Mason, and Patryk Szewczyk, "A Snapshot Analysis of Publicly Available BYOD Policies," *Proceedings of the 2021 Australasian Computer Science Week Multiconference*, Dunedin New Zealand, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ntwari Richard, Annabella E. Habinka, and Fred Kaggwa, "BYOD Systematic Literature Review: A Layered Approach," *European Journal of Technology*, vol. 6, no. 1, pp. 69-85, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Melina Seedoyal Doargajudhur, and Peter Dell "The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation," *Journal of Computer Information Systems*, vol. 60, no. 6, pp. 518-529, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Oluranti Jonathan, and Sanjay Misra, "Policy Framework for Adoption of Bring your Own Device (BYOD) by Institutions in Nigeria," *International Journal of Control Theory and Applications*, vol. 9, no. 23, pp. 377-385, 2016. [Google Scholar]

[5] Kibreab Adane, "Threats Introduced by Bring Your Own Devices (BYOD) Adoption in an Ethiopian Higher Educational Institution: Solutions to Security and Privacy," *IUP Journal of Information Technology*, vol. 16, no. 2, pp. 7-29, 2020. [Google Scholar] [Publisher Link]

[6] Aliyu Aliyu et al., "A Holistic Cyber Security Maturity Assessment Framework for Higher Education Institutions in the United Kingdom," *Applied Sciences*, vol. 10, no. 10, pp. 1-15, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Alexei Arina, and Alexei Anatolie, "Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning," *International Journal of Scientific and Technology Research*, vol. 10, no. 3, pp. 128-133, 2021. [Google Scholar] [Publisher Link]

[8] Joachim Bjørge Ulven, and Gaute Wangen, "A Systematic Review of Cyber Security Risks in Higher Education," *Future Internet*, vol. 13, no. 2, pp. 1-40, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Oonge S. Omboga, Muhambe T. Mukisa, and Ratemo M. Cyprian, "A Bring Your Own Device Risk Assessment Model," *International Journal of Security*, vol. 12, no. 2, pp. 15-34, 2021. [Google Scholar] [Publisher Link]

[10] Scott N. Romaniuk, and David Andrew Omona, "Uganda's Cyber Security Capacities and Challenges," *Companion to Global Cyber-Security Strategy*, pp. 573-632, 2021. [Google Scholar]

[11] Eric C.K. Cheng, and Tianchong Wang, "Institutional Strategies for Cyber Security in Higher Education Institutions," *Information*, vol. 13, no. 4, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Diptiben Ghelani, "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," *Authorea Preprints*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Kanos Matyokurehwa et al., "Cyber Security Awareness in Zimbabwean Universities: Perspectives from the Students," *Security and Privacy*, vol. 4, no. 2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Richard Ntwari, Annabella E. Habinka, and Fred Kaggwa, "Enhancing Bring Your Own Device Security in Education," *Journal of Science & Technology*, vol. 2, no. 4, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Md Alimul Haque et al., "Cyber Security in Universities: An Evaluation Framework," *SN Computer Science*, vol. 4, no. 5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Simon Kramer, and Julian C. Bradfield, "A General Definition of Malware," *Journal in Computer Virology*, vol. 6, no. 2, pp. 105-114, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[17] Antonina Pavlovna Sokolova et al., "Influence of BYOD Concept on Development of the Learning Process in Universities," *Propositus Representations*, vol. 9, no. 2, pp. 1-10, 2021. [Google Scholar] [Publisher Link]

[18] Stanford Musarurwa, Attlee M. Gamundani, and Fungai Bhunu Shava, "An Assessment of BYOD Control in Higher Institution of Learning: A Namibian Perspective," *1st Africa Week Conference (IST-Africa)*, Nairobi, Kenya, pp. 1-9, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Eric B. Blancaflor, and Joel R. Hernandez, "A Compliance Based and Security Assessment of Bring Your Own Device (BYOD) in Organizations," *International Conference on Computer and Communication Engineering*, Switzerland, pp. 116-127, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nida AL-Sous et al., "Integrated E-Learning for Knowledge Management and its Impact on Innovation Performance Among Jordanian Manufacturing Sector Companies," *International Journal of Data and Network Science*, vol. 7, no. 1, pp. 495-504, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Bashayer Alotaibi, and Haya Almagwashi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," *1st International Conference on Computer Applications & Information Security*, Riyadh, Saudi Arabia, pp. 1-6, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Faizal Dine, "Cyber Threat Analysis and the Development of Proactive Security Strategies for Risk Mitigation," 2024. [Google Scholar]

[23] Selma Şenel, and Hüseyin Can Şenel, "Remote Assessment in Higher Education during The COVID-19 Pandemic," *International Journal of Assessment Tools in Education*, vol. 8, no. 2, pp. 181-199, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] V. Joseph Raymond, and R. Jeberson Retna Raj, "Investigation of Android Malware with Machine Learning Classifiers using Enhanced PCA Algorithm," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2147-2163, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Francis Ssekitto, "Staying Safe While Teaching and Learning Online in Library and Information Science Training Schools in Uganda: The Case of Makerere University," *Library Philosophy and Practice*, vol. 7085, pp. 1-13, 2022. [Google Scholar] [Publisher Link]

[26] Sadaf Hina, and P. Dhanapal Durai Dominic, "Information Security Policies' Compliance: A Perspective for Higher Education Institutions," *Journal of Computer Information Systems*, vol. 60, no. 3, pp. 201-211, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] James Chester Hyatt, "*External, Internal, and Inherent Factors Affecting End-User Security Awareness within Institutions of Higher Learning*," Walden University, 2015. [Google Scholar] [Publisher Link]

[28] Norshima Humaidi, and Vimala Balakrishnan, "Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness," *International Journal of Information and Education Technology*, vol. 5, no. 4, pp. 311-318, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[29] Eric C.K. Cheng, and Tianchong Wang, "Editorial for the Special Issue 'Information Technologies in Education, Research, and Innovation," *Information*, vol. 15, no. 1, pp. 1-3, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Ieda M. Santos, "BYOD in the Classroom, Opportunities, Issues, and Policies," *Encyclopedia of Education and Information Technologies*, pp. 267-272, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Katherine A. Clark et al., "Do Educators Realize the Value of Bring Your Own Device (BYOD) in Fieldwork Learning?," *Journal of Geography in Higher Education*, vol. 45, no. 2, pp. 255-278, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Melva Ratchford et al., "BYOD Security Issues: A Systematic Literature Review," *Information Security Journal: A Global Perspective*, vol. 31, no. 3, pp. 253-273, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[33] Rathika Palanisamy et al., "BYOD Policy Compliance: Risks and Strategies in Organizations," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 61-72, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Judith Schoonenboom, "The Fundamental Difference Between Qualitative and Quantitative Data in Mixed Methods Research," *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, vol. 24, no. 1, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[35] Rayyan Aqila Praditya, and Agus Purwanto, "Linking The Influence of Dynamic Capabilities and Innovation Capabilities on Competitive Advantage: PLS-SEM Analysis," *Professor: Professional Education Studies and Operations Research*, vol. 1, no. 2, pp. 6-10, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[36] Julio Cabero-Almenara et al., "Development of the Teacher Digital Competence Validation of DigCompEdu Check-In Questionnaire in the University Context of Andalusia (Spain)," *Sustainability*, vol. 12 no. 15, pp. 1-14, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[37] Gordon W. Cheung et al., "Reporting Reliability, Convergent and Discriminant Validity with Structural Equation Modelling: A Review and Best-Practice Recommendations," *Asia Pacific Journal of Management*, vol. 41, no. 2, pp. 745-783, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[38] Noora Shrestha, "Factor Analysis as a Tool for Survey Analysis," *American Journal of Applied Mathematics and Statistics*, vol. 9, no. 1, pp. 4-11, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[39] Dong Kyu Lee et al., "Data Transformation: A Focus on the Interpretation," *Korean Journal of Anesthesiology*, vol. 73, no. 6, pp. 503-508, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] Kathleen Downer, and Maumita Bhattacharya, "BYOD Security: A Study of Human Dimensions," *Informatics*, vol. 9, no. 1, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[41] Khalid A. Almarhabi, "An Improved Smart Contract-Based Bring-Your-Own-Device (BYOD) Security Control Framework," *Alexandria Engineering Journal*, vol. 105, pp. 598-612, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[42] Izzah Inani Abdul Halim et al., "BYOD Security Policy Model: A Systematic Literature Review," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 60, no. 4, pp. 170-186, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[43] Indunil Karunarathna et al., "Comprehensive Data Collection: Methods, Challenges, and the Importance of Accuracy," 2024. [Google Scholar]

[44] A.N. Datta, Shinu Abhi, and Nishanth Kumar, "Enhancing BYOD Security: A Risk Assessment Framework for Corporate Resources," *International Conference on Computing and Machine Learning*, Singapore, pp. 483-496, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[45] Harjinder Singh Lallie et al., "Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector," *Computers*, vol. 14, no. 2, pp. 1-28, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[46] Noor Rahmawati Alias et al., "Investigating Factors Affecting the Adoption of BYOD in Educational Sectors: A Structured Literature Review Approach," *Journal of Islamic*, vol. 9, no. 66, pp. 682-697, 2024. [Google Scholar] [Publisher Link]

[47] Christian Odo et al., "Strengthening Cyber Security Resilience: the Importance of Education, Training, and Risk Management," *Training and Risk Management*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[48] Rebecca Fioravanti et al., "Bring Your Own Device (BYOD) Student Experiences and Policy Considerations for Nontraditional Colleges," *The International Journal of Adult, Community and Professional Learning*, vol. 31, no. 2, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[49] Mohammed Althamir et al., "Enhancing Malware Detection Efficacy: A Comparative Analysis of Endpoint Security and Application Whitelisting," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 6, pp. 2451-2465, 2024. [Google Scholar] [Publisher Link]

[50] Oluwatoyin Ajoke Farayola, Oluwabukunmi Latifat Olorunfemi, and Philip Olaseni Shoetan, "Data Privacy and Security In It: A Review Of Techniques and Challenges," *Computer Science & IT Research Journal*, vol. 5, no. 3, pp. 606-615, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[51] Dina Moloja, Tembisa Ngqondi, and Noluntu Mpekoa, "BYODelving: Unmasking Security Risks in Higher Education Learning Management Systems South African Perspective," 1st *Africa Conference (IST-Africa)*, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[52] Mohammed Althamir et al., "Enhancing Malware Detection Efficacy: A Comparative Analysis of Endpoint Security and Application Whitelisting," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 6, pp. 2451-2465, 2024. [Google Scholar] [Publisher Link]

[53] Anirudh Khanna, *Ransomware Prevention*, Securing an Enterprise, Apress, Berkeley, CA, pp. 119-138, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[54] Dipo Dunsin et al., "Reinforcement Learning for an Efficient and Effective Malware Investigation during Cyber Incident Response," *High-Confidence Computing*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[55] Muhammad Amirrudin, Khoirunnisa Nasution, and Supahar Supahar, "Effect of Variability on Cronbach Alpha Reliability in Research Practice," *Journal of Mathematics, Statistics and Computation*, vol. 17, no. 2, pp. 223-230, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[56] Meltem Yalin-Uçar et al., "Development of the Reasoning Ways Scale: Validity and Reliability Study," *Kalem Education Human Science Journal*, vol. 14, no. 1, pp. 129-153, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[57] V.T. Jimshith, and V. Mary Amala Bai, "Evaluation of Security Framework for BYOD Device in Cloud Environment," *Automatika,* vol. 65, no. 3, pp. 803-814, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[58] Tafheem Ahmad Wani et al., "Status of Bring-Your-Own-Device (BYOD) Security Practices in Australian Hospitals-A National Survey," *Health Policy and Technology,* vol. 11, no. 3, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[59] Aljuaid Turkea Ayedh M et al., "Systematic Literature Review on Security Access Control Policies and techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions," *Applied Sciences*, vol. 13, no. 14, pp. 1-37, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[60] National Council for Higher Education, Guidelines for Acceptable and Responsible Access and Use of Digital Materials in Higher Education, 2024. [Online]. Available: https://unche.or.ug/wp-content/uploads/2024/05/Guidelines-for-acceptable-and-responsible-access-and-use-of-digital-materials-in-Higher-Education_2024-1.pdf

[61] Gema Howell et al., "Mobile Device Security: Bring Your Own Device (BYOD)," *National Institute of Standards and Technology*, 2023. [CrossRef] [Google Scholar] [Publisher Link]