IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13901

Assessing Security Vulnerabilities in University Student Management Information Systems (SMIS) and Their Impact on Student Data Security

Kosgey Festus Kipchirchir[1], Dr. Roselida Maroko Ongare[2], Dr. Patrick Oduor Owoche[3]

Registrar Assistant (Records Officer), UEAB. P.O.BOX 2500-30100. Eldoret, Kenya[1]

Lecturer, Kibabii University, P.O.BOX 1699-50200 Bungoma, Kenya[2]

Lecturer, Kibabii University, P.O.BOX 1699-50200 Bungoma, Kenya[3]

Abstract: The rapid integration of technology in educational institutions has led to the widespread adoption of Student Management Information Systems (SMIS) to streamline administrative processes and enhance student experiences. However, these systems are increasingly becoming targets for cyber-attacks due to the sensitive nature of the data they store, such as personal information, academic records, and financial details. This study evaluates the existing vulnerabilities in university SMIS implementations, focusing on their potential impact on student data security. Through a comprehensive analysis of various university SMIS across different institutions, this research identifies common security flaws, including inadequate access controls, outdated software, lack of encryption, and improper data handling practices. Additionally, the study highlights the implications of these vulnerabilities, such as unauthorized data access, data breaches, identity theft, and potential reputational damage to institutions. By examining these risks, the study provides a framework for understanding the critical areas that require immediate attention and offers recommendations for enhancing the security posture of university SMIS. The findings aim to guide universities in developing robust security measures to protect student data, ensuring the privacy and integrity of their academic environments.

Keywords: Cybersecurity, Vulnerabilities, Student Data Security, SMIS (Student Management Information Systems), Encryption, Access Controls, Data Breaches

I. INTRODUCTION

The integration of information technology in educational institutions has greatly changed how universities manage their administrative functions, especially with the use of Student Management Information Systems (SMIS). These systems play a key role in handling various aspects of student information, such as enrollment, attendance, academic records, and financial transactions [1] [2]. By centralizing these functions, SMIS have improved the efficiency and effectiveness of university operations, making data management processes more streamlined and supporting both administrative and academic activities [3] [4].

Despite the benefits offered by Student Management Information Systems (SMIS), their extensive use has brought significant security challenges. These systems hold a large amount of sensitive information, including personal identification details, academic records, and financial data, making them attractive targets for cyberattacks [5]. The study's findings highlight a rising number of reported cyber incidents in higher education, indicating the need to carefully assess the security vulnerabilities within these systems and their potential impact on the confidentiality, integrity, and availability of student data [6].

The research identified several vulnerabilities in university SMIS, including outdated software, inadequate data encryption, weak authentication protocols, and insufficient access controls. These weaknesses can be exploited by cybercriminals to gain unauthorized access to sensitive information, potentially leading to data breaches, identity theft, and other cybercrimes [4]. The study also pointed out that a lack of awareness and training among university staff and students about cybersecurity best practices worsens these vulnerabilities, increasing the risk of successful cyberattacks [7] [8].

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024
DOI: 10.17148/IJARCCE.2024.13901

In the context of Kenyan universities, the study highlighted a balanced view towards the adoption of Student Management Information Systems (SMIS). While these systems offer notable operational advantages, there are also considerable concerns regarding security risks [9]. Cybersecurity threats, such as malware attacks, phishing, and data breaches, have been particularly common, making universities attractive targets. Research findings and a report by [10] indicate that Kenya faced a significant number of malware attacks, emphasizing the need for effective security measures to safeguard sensitive student data within university SMIS.

The study carried out a detailed analysis of the security status of Student Management Information Systems (SMIS) in selected Kenyan universities, identifying common security weaknesses and evaluating their effects on student data protection. This assessment offered valuable insights into the vulnerabilities within these systems and their potential impact on student data security, which is important for creating effective strategies to protect sensitive information and maintain the integrity of educational institutions.

The insights from this research are highly valuable for university administrators, IT professionals, and policymakers, helping them to address the specific security requirements of Student Management Information Systems (SMIS) in academic environments. Additionally, the study adds to the wider field of cybersecurity by bringing attention to the unique challenges that higher education institutions encounter in safeguarding their digital assets against evolving cyber threats. As universities increasingly adopt digital technologies, securing SMIS is essential to protect the privacy and security of student data.

II. METHODOLOGY

The study adopted a **descriptive cross-sectional research design** to evaluate the current state of security vulnerabilities within university SMIS implementations and their impact on student data security. This design was chosen because it allows for the collection and analysis of data at a specific point in time, providing a snapshot of the existing conditions. A descriptive design is particularly useful in identifying and describing the nature and extent of vulnerabilities in SMIS, while a cross-sectional approach facilitates the examination of multiple variables simultaneously, such as different types of vulnerabilities and their effects on data security.

The study employed a **quantitative research approach**, focusing on numerical data to identify patterns and measure the extent of vulnerabilities within university SMIS. This approach was selected to provide a systematic and objective method for analyzing data, allowing for the quantification of the relationships between identified vulnerabilities and their potential impact on student data security. The quantitative approach enabled the researcher to generalize findings to a larger population and draw conclusions based on statistical analysis.

A **survey strategy** was utilized to collect data from respondents at selected universities. This strategy was chosen due to its effectiveness in gathering large amounts of data from a diverse group of respondents. Surveys, in the form of structured questionnaires, were used to collect information on the perceptions and experiences of university staff and students regarding SMIS vulnerabilities and data security. The use of questionnaires allowed for standardized data collection, facilitating the comparison of responses across different groups within the universities.

The study was conducted at two universities in Kenya: **Kibabii University** and the **University of Eastern Africa, Baraton**. These universities were chosen to represent both public and private institutions, providing a comprehensive view of SMIS vulnerabilities across different types of educational settings. The target population included **IT staff, administrative staff (Registrar Academics and Student Finance Office), faculty members, and students** within the selected universities who interact with or manage the SMIS.

To ensure a representative sample, a **stratified sampling technique** was employed. This method involved dividing the population into distinct subgroups based on their roles and levels of interaction with the SMIS, ensuring that all relevant perspectives were adequately represented. A sample size of **120 respondents** was determined, comprising 20 IT staff, 10 administrative staff (5 each from the Registrar Academics Office and Student Finance Office), 20 faculty members, and 70 students. This sample size was selected based on the guidelines provided by Mugenda and Mugenda (2003), who suggest a minimum sample size of 10% of the total population for research purposes.

Data were collected using a **structured questionnaire** designed specifically for this study. The questionnaire consisted of **closed-ended questions** to facilitate quantitative analysis and ensure consistency in responses. The questions were developed to align with the study's objectives, focusing on identifying the types of vulnerabilities present in university SMIS, their potential impact on student data security, and the effectiveness of current security measures.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024
DOI: 10.17148/IJARCCE.2024.13901

The questionnaires were distributed to respondents at Kibabii University and the University of Eastern Africa, Baraton, both in paper form and online, to accommodate different preferences and schedules. Prior to distribution, the questionnaire was reviewed by experts in the field to ensure its validity and relevance to the study's objectives.

The collected data were analyzed using both **descriptive and inferential statistical methods**. Descriptive statistics, such as frequencies, percentages, mean, and standard deviation, were used to summarize and present the data, providing an overview of the identified vulnerabilities and their perceived impact on data security. These statistics helped in understanding the general trends and patterns within the data related to SMIS security in universities.

Inferential statistics, particularly **correlation analysis**, were employed to examine the relationships between different types of vulnerabilities and their impact on student data security. This analysis aimed to identify significant associations between variables, such as the presence of specific security weaknesses (e.g., lack of encryption, outdated software) and the likelihood of data breaches. The findings from the inferential analysis provided deeper insights into the factors contributing to SMIS vulnerabilities and their potential impact on data security.

To ensure the validity and reliability of the research instruments, the questionnaire underwent a **rigorous pre-testing process**. The content validity of the questionnaire was established through expert review, involving feedback from IT professionals and academic staff knowledgeable in SMIS security. This process ensured that the questions were relevant, clear, and aligned with the study's objectives.

Reliability was assessed using **Cronbach's Alpha**, a measure of internal consistency that indicates how closely related the items in a questionnaire are as a group. A Cronbach's Alpha value of 0.70 or higher was considered acceptable for this study (Nunnally & Bernstein, 1994). The pre-test results yielded an average Cronbach's Alpha of 0.726, indicating a satisfactory level of reliability.

III. RESULTS AND DISCUSSION

The primary objective of this analysis was to evaluate the existing vulnerabilities in university Student Management Information Systems (SMIS) and assess their potential impact on student data security.

A. *Key Vulnerabilities Identified*

The research identified several significant cybersecurity vulnerabilities within university Student Management Information Systems (SMIS). These vulnerabilities range from basic security oversights to more sophisticated issues, posing substantial risks to student data security. Below is a detailed summary of the key vulnerabilities identified, severity of vulnerabilities and non-parametric test outcomes.

- **Weak or Default Passwords**: The study revealed that 83.8% of respondents identified weak or default passwords as a prevalent issue. This vulnerability is critical as it allows unauthorized access to sensitive student data. Aloul (2012) supports these findings, indicating that password-related vulnerabilities are a common problem in various organizations, including universities.

- **Lack of Encryption for Sensitive Data**: A significant vulnerability identified by 59.0% of respondents was the lack of robust encryption for sensitive data. Without adequate encryption measures, sensitive information, such as student records and financial data, is exposed to risks during both transmission and storage. Olatunji (2019) emphasized the importance of comprehensive encryption strategies to protect such data in educational settings.

- **Unpatched Software or Outdated Systems**: Unpatched software and outdated systems were highlighted as critical vulnerabilities by 54.3% of respondents. These vulnerabilities serve as common entry points for cyber attackers and could lead to significant data breaches and loss. EDUCAUSE (2020) noted that outdated software greatly increases the risk of cyber-attacks in higher education institutions.

- **Insufficient Access Controls**: The study found that 45.7% of respondents identified insufficient access controls as a significant risk factor, potentially leading to unauthorized data access and breaches. Balozian and Leidner (2017) stressed the importance of strict access controls to enhance the security of SMIS effectively.

- **Vulnerable Third-Party Plugins or Integrations**: About 40.0% of respondents pointed out the risks associated with vulnerable third-party plugins or integrations. If not properly vetted, these plugins can introduce security vulnerabilities. Mitropoulos et al. (2015) advocated for thorough vetting processes for third-party components to ensure robust security.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024
DOI: 10.17148/IJARCCE.2024.13901

- **Lack of Robust Authentication Mechanisms**: The absence of strong authentication mechanisms was noted by 52.4% of respondents, highlighting a significant vulnerability. Alotaibi (2020) recommended the implementation of multi-factor authentication to enhance security.

- **Inadequate Logging and Monitoring Capabilities**: Reported by 42.9% of respondents, inadequate logging and monitoring capabilities were identified as a vulnerability that could delay the detection and response to security incidents. Miller (2018) underscored the need for robust monitoring systems to quickly identify and mitigate security threats.

- **Lack of Regular Security Audits or Assessments**: The absence of regular security audits or assessments was noted by 52.4% of respondents. Tuttle (2017) emphasized that regular security assessments are crucial to identify and address potential vulnerabilities timely.

- **Improperly Configured Security Settings**: Improperly configured security settings, identified by 27.6% of respondents, can lead to severe security breaches. Tsai et al. (2016) highlighted the necessity of proper configuration management to prevent such issues.

- **Lack of User Awareness Regarding Security Best Practices**: A lack of user awareness regarding security best practices was reported by 57.1% of respondents, indicating that human error remains a significant risk. Alqahtani (2018) emphasized the importance of user education in mitigating security risks.

Table 1 below summarizes the key vulnerabilities identified, including the percentage of respondents who indicated each issue and supporting references from the literature.

TABLE 1 KEY VULNERABILITIES IDENTIFIED

Vulnerability	Prevalence (%)	Impact	Supporting Research
Weak or Default Passwords	83.8	Allows unauthorized access to sensitive student data.	Aloul (2012)
Lack of Encryption for Sensitive Data	59.0	Exposes sensitive data (e.g., student records, financial data) to risks during transmission and storage.	Olatunji (2019)
Unpatched Software or Outdated Systems	54.3	Serves as entry points for attackers, potentially leading to data breaches and loss.	EDUCAUSE (2020)
Insufficient Access Controls	45.7	Could lead to unauthorized data access and breaches.	Balozian and Leidner (2017)
Vulnerable Third-Party Plugins or Integrations	40.0	Introduces security vulnerabilities if not properly vetted.	Mitropoulos et al. (2015)
Lack of Robust Authentication Mechanisms	52.4	Increases the risk of unauthorized access.	Alotaibi (2020)
Inadequate Logging and Monitoring Capabilities	42.9	Delays the detection and response to security incidents.	Miller (2018)
Lack of Regular Security Audits or Assessments	52.4	Prevents timely identification and addressing of potential vulnerabilities.	Tuttle (2017)
Improperly Configured Security Settings	27.6	Can lead to severe security breaches.	Tsai et al. (2016)
Lack of User Awareness Regarding Security Best Practices	57.1	Human error remains a significant risk due to lack of user education.	Alqahtani (2018)

B. ***Severity of Vulnerabilities***

The severity of these vulnerabilities was assessed, revealing varying levels of concern among respondents. As shown in Table 2, 34.3% of respondents rated the vulnerabilities as severe, and 21.9% considered them very severe, indicating an urgent need for immediate attention. Meanwhile, 25.7% rated the vulnerabilities as moderate, suggesting that while threats are present, they could be managed with appropriate measures. A smaller portion, 11.4%, perceived the vulnerabilities as negligible, and 6.7% were unsure about the severity.

The table 2 below shows the distribution of respondents' ratings on the severity of the vulnerabilities.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13901

TABLE 2 THE DISTRIBUTION OF RESPONDENTS' RATINGS ON THE SEVERITY OF THE VULNERABILITIES

Severity Level	Percentage of Respondents (%)
Very Severe	21.9
Severe	34.3
Moderate	25.7
Negligible	11.4
Unsure	6.7

C. ***Further Analysis of Vulnerabilities in University Student Management Information Systems***

To further analyse the vulnerabilities and their impact, four non-parametric tests were conducted. Results are as summarized in Table 3 below.

TABLE 3 CYBERSECURITY VULNERABILITIES

Test	Findings
Chi-Square Tests	Found a significant association between different types of cybersecurity vulnerabilities ($p < 0.001$), indicating that some vulnerabilities are more prevalent than others.
Mann-Whitney U Test	Identified a significant difference between IT staff and students regarding the frequency of security incidents ($p = 0.034$), suggesting varying experiences based on roles.
Kruskal-Wallis H Test	Found a significant difference in the frequency of security incidents across various departments ($p = 0.008$), highlighting that some departments experience higher frequencies of incidents.
Spearman's Rank Correlation	Revealed a moderate positive correlation (rho = 0.402, $p = 0.002$) between the frequency and severity of incidents, indicating that as the frequency of incidents increases, so does their perceived severity.

D. ***Key Findings***

The research identified critical vulnerabilities in university SMIS that pose significant risks to student data security. The severity of these vulnerabilities ranged from moderate to very severe, highlighting the urgent need for comprehensive security strategies. These findings underscore the importance of implementing stronger policies, conducting regular updates, enhancing user education, and adopting comprehensive security measures to protect sensitive student data effectively.

These research findings emphasize the need for continuous assessment and enhancement of security protocols within university SMIS. Addressing these vulnerabilities requires coordinated efforts from university administrators, IT staff, and users to establish more stringent security measures and increase awareness about cybersecurity best practices.

IV. SUMMARY

The evaluation of existing vulnerabilities within university Student Management Information Systems (SMIS) highlighted several significant risks to student data security. Key vulnerabilities identified include weak or default passwords, lack of encryption for sensitive data, unpatched software or outdated systems, and insufficient access controls. These vulnerabilities were rated as severe or very severe by a substantial proportion of respondents, indicating high concern over the security of student data within SMIS.

Weak or default passwords emerged as the most prevalent vulnerability, posing a critical risk due to potential unauthorized access. The lack of encryption for sensitive data was also a major concern, exposing student records and financial information to potential breaches during transmission and storage. Unpatched software and outdated systems were found to be common entry points for attackers, increasing the risk of data breaches. The findings underscored the need for stronger security practices and enhanced protocols to protect sensitive student information from potential threats.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024
DOI: 10.17148/IJARCCE.2024.13901

V. CONCLUSION

The analysis concluded that existing vulnerabilities within university SMIS pose significant risks to the security of student data. The prevalence of weak or default passwords, inadequate encryption measures, and unpatched software represents major security gaps that could lead to unauthorized access, data breaches, and loss of sensitive information. The high severity ratings associated with these vulnerabilities reflect a widespread awareness of the potential impact of these security weaknesses on student data security. The study's findings suggest that while some security measures are in place, they are insufficient to address the critical vulnerabilities identified. This indicates a pressing need for universities to adopt more robust security protocols and practices to effectively mitigate these risks and enhance the overall security posture of their SMIS.

VI. RECOMMENDATIONS

To address the identified vulnerabilities in university SMIS and improve student data security, the following recommendations are proposed:

- **Implement Stronger Password Policies**: Universities should enforce stronger password policies, including the use of complex passwords, regular password changes, and the elimination of default passwords. User education programs should be developed to raise awareness about the importance of strong passwords and the risks associated with weak ones.

- **Adopt Robust Encryption Protocols**: It is crucial to implement robust encryption measures for sensitive data, both at rest and during transmission. This will protect student records, financial information, and other sensitive data from unauthorized access and potential breaches.

- **Regular Updates and Patch Management**: Universities must establish a rigorous schedule for regular software updates and patch management to address vulnerabilities associated with unpatched software and outdated systems. This will help mitigate the risks of exploitation by cyber attackers.

- **Enhance Access Controls**: Strengthening access control mechanisms is essential to prevent unauthorized access to sensitive data. Universities should implement multi-factor authentication (MFA) and role-based access controls (RBAC) to limit data access to authorized personnel only.

- **Conduct Comprehensive Security Audits**: Regular security audits and assessments should be conducted to identify and address existing vulnerabilities within the SMIS. These audits will help ensure that security measures are up to date and effective in protecting student data.

- **Increase Cybersecurity Awareness and Training**: Universities should invest in comprehensive cybersecurity training programs for all staff and students. These programs should focus on best practices for data security, recognizing phishing attempts, and understanding the importance of regular updates and secure configurations.

By implementing these recommendations, universities can significantly reduce the risks associated with the identified vulnerabilities and strengthen the security of their Student Management Information Systems, ultimately protecting student data more effectively.

REFERENCES

[1] Iwhiwhu, E. B. (2005). Management of records in Nigerian universities: Problems and prospects. *The Journal of Electronic Library, 23*(3), 345-355.
[2] Arora, S. P. (2006). *Office organization and management*. Vikas Publishing House London Pvt. Ltd.
[3] Baharun, H. (2019, March). Management information systems in education: The significance of e-public relation for enhancing competitiveness of higher education. In *Journal of Physics: Conference Series* (Vol. 1175, No. 1, p. 012151). IOP Publishing.
[4] Ampofo, J. A. (2020). Challenges of student management information system (MIS) in Ghana: A case study of University for Development Studies, Wa Campus. *International Journal of Management & Entrepreneurship Research, 2*(5), 332-343.
[5] Polyvyanyy, A., van der Werf, J. M. E., Overbeek, S., & Brouwers, R. (2019). Information systems modeling: Language, verification, and tool support. In *International Conference on Advanced Information Systems Engineering* (pp. 194-212). Springer.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13901

[6] Hameed, M. A., & Arachchilage, N. A. G. (2021). The role of self-efficacy on the adoption of information systems security innovations: A meta-analysis assessment. *Personal and Ubiquitous Computing, 25*(5), 911-925.

[7] Martins, J., Branco, F., Gonçalves, R., Au-Yong-Oliveira, M., Oliveira, T., Naranjo-Zolotov, M., & Cruz-Jesus, F. (2019). Assessing the success behind the use of education management information systems in higher education. *Telematics and Informatics, 38*, 182-193.

[8] Soegoto, E. S., & Jayaswara, M. R. (2018). Web and android programming course information system. In *IOP Conference Series: Materials Science and Engineering* (Vol. 407, No. 1, p. 012063). IOP Publishing.

[9] Macharia Njoroge, M. P. (2021). An examination of threats facing assets in use in Kenyan public universities. *International Journal of Scientific and Research Publications (IJSRP), 11*(5), 687–695. https://doi.org/10.29322/ijsrp.11.05.2021.p11372

[10] Africa Newsroom. (2022, February 24). Kaspersky reports the anomalous decline of mobile malware in Africa in 2021. *Africa Newsroom*. https://kaspersky.africa-newsroom.com/press

