Analysis of Digital Ethics and Student Data Security in the Use of Academic Information Systems

Meyti Eka Apriyani[1,2], Hakkun Elmunsyah[1]

[1]Department of Electrical Engineering and Informatics, Universitas Negeri Malang, Indonesia

[2]Department of Informatics Engineering, Politeknik Negeri Malang, Indonesia

DOI: https://dx.doi.org/10.51244/IJRSI.2025.12110085

Received: 01 December 2025; Accepted: 05 December 2025; Published: 09 December 2025

ABSTRACT

The Academic Information System (SIAKAD) is a crucial digital infrastructure used to support academic administration processes in higher education. As technology utilization increases in data management, concerns regarding digital ethics and student information security are becoming increasingly important. This research effort aims to evaluate students' awareness of digital ethics, data security practices, and their level of trust in SIAKAD security. The study used a quantitative approach by distributing questionnaires to students, with analysis including descriptive statistics, validity tests, and reliability tests to map behavioral trends. The results indicate that students have a high level of digital ethics awareness, but this is not fully reflected in their security behaviors. Risky habits are still common, particularly storing passwords in browsers, using shared devices without protection, and not logging out after accessing SIAKAD. Furthermore, students' level of trust in system security is relatively low, particularly related to concerns about internal access and potential academic data leaks. The study recommends improving digital security literacy education, implementing multi-factor authentication, transparency of privacy policies, and adding security features to strengthen data protection and increase student trust in SIAKAD.

Keywords: Data Security, Digital ethics, SIAKAD, Student, Privacy

INTRODUCTION

This group of users is at high risk of digital security breaches. This vulnerability is influenced by weak security practices, including the use of weak passwords, the habit of storing passwords in browsers, and accessing SIAKAD through unsecured public networks (Özkan & Yildirim, 2022; Alzahrani, 2023). In addition to technical aspects, behavioral factors also play a significant role. Many students are not fully aware of the potential long-term security risks or lack discipline in implementing safe usage habits. This situation is closely related to the concept of the privacy paradox, which is a situation where someone expresses a strong concern for privacy, but their actions do not reflect the same level of concern. Recent studies have shown that students have relatively good privacy awareness but still engage in risky behaviors, such as sharing accounts or not logging out of shared devices (Taufik & Juhana, 2025). This illustrates an awareness-behavior gap, the gap between knowledge about the importance of maintaining privacy and actual actions to maintain data security (Mäkelä & Salmela, 2022). Furthermore, students' trust in the security of SIAKAD also influences their behavior when accessing the system. Woodward and Caine (2024) found that low trust in the academic system encourages user caution, but can also lead to maladaptive behaviors such as avoiding access or using inappropriate methods. This emphasizes the importance of an academic system that is not only technically secure but also clearly manages information, thereby increasing user trust. Efforts to improve SIAKAD security do not rely solely on technology. Measures such as digital literacy, security education, and the formation of security habits have proven effective in reducing the likelihood of data breaches. The use of multi-factor authentication (MFA), for example, has been shown to improve account protection, but its effectiveness is largely determined by user acceptance and discipline in using it (Al-Khalifah, 2024). Given these conditions, research on digital ethics and data security in the use of SIAKAD is highly relevant, especially in the context of higher education in Indonesia. This study aims to: (1) analyze the level of digital ethics awareness of students in using SIAKAD, (2) evaluate the data

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

security behavior implemented by students, and (3) identify the level of student trust in the security of the SIAKAD system. The results of the study are expected to provide a more comprehensive empirical understanding and become the basis for recommendations in the preparation of data security policies, increasing digital literacy, and improving the development of SIAKAD in the future.

METHOD

This chapter explains the research methodology steps taken to ensure the analysis aligns with the research objectives regarding student data ethics and security in using the Academic Information System

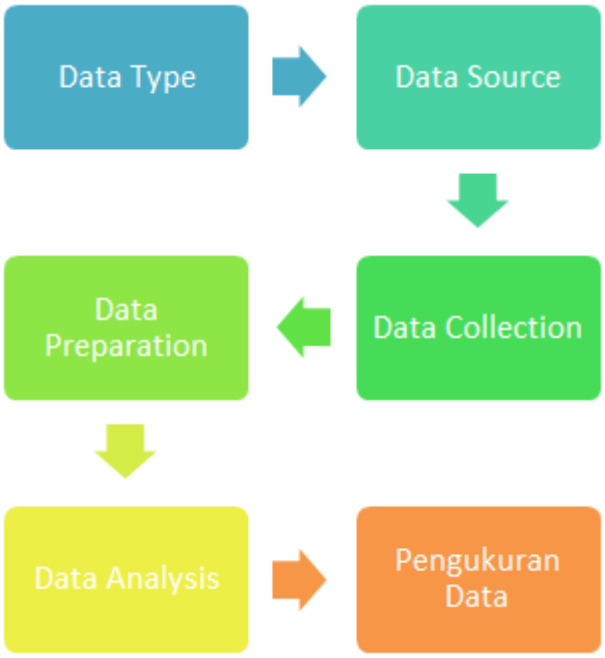

Fig. 1. Research Methodology

Data Type

The initial step in this research was to identify the relationship between the use of the Academic Information System (SIAKAD) and aspects of digital ethics and student data security. To understand this relationship, the study collected data containing student responses regarding their behavior in using SIAKAD, their level of understanding of data privacy and security, and the practices they employ to secure their accounts, such as password use and logging out habits. Furthermore, the data also included student perceptions regarding digital ethics in managing academic information and various risk factors that may arise during the SIAKAD access process, including the use of shared devices or unsecured networks. All data collected was quantitative and obtained through a questionnaire designed to measure student perceptions, knowledge, and behavior in a structured and measurable manner.

Data Source

The data source for this study came from an online questionnaire distributed to active students as the primary respondents. The questionnaire was designed to gather information on various aspects of SIAKAD usage, including the frequency of student access to the system, their level of awareness of ethical academic data management, and data security habits such as strong password usage, logging out habits, and the types of devices used to access the system. Furthermore, the questionnaire included questions regarding student perceptions of the risk of data breaches and their level of compliance with SIAKAD usage regulations. To ensure broad and diverse participation, the questionnaire was distributed through various communication channels, including campus social media, student WhatsApp groups, and academic email.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

Data Collection

The data collection process for this study was conducted online to facilitate participant response and ensure time efficiency and broader engagement. The questionnaire was distributed over a week through digital platforms so that students could complete it according to their schedule. The data collection steps began with creating a questionnaire tool using Google Forms tailored to the research variables. Next, the content was evaluated by lecturers with expertise in information systems and data security to ensure the appropriateness and clarity of the questions. The questionnaire was then distributed to students through various communication channels. After the completion period, all responses were collected and checked for validity, including removing duplicate responses and eliminating incomplete answers. The validated data was then stored and processed as the basis for further analysis.

Data Preparation

After all data was collected, the next step was data preparation to ensure that the data for analysis met research quality standards. This process began with data cleaning, which removed invalid entries, duplicate responses, and incomplete answers to prevent them from interfering with the analysis results. The next stage was data validation, where each response was checked to ensure that respondents met the research criteria, particularly students who had used SIAKAD for at least one semester. Next, data coding was performed, converting qualitative responses into a numerical format so they could be processed using statistical analysis techniques. After the coding process was complete, the data were compiled into a final dataset ready for use in descriptive analysis.

Data Analysis

The data obtained from the questionnaires were analyzed using a descriptive statistical approach to describe SIAKAD usage patterns and student perceptions regarding digital ethics and data security. This analysis was conducted by reviewing several key aspects that reflect the quality of system use by students. First, the frequency of SIAKAD usage was analyzed, including daily access duration, device type, and selected internet connection when accessing the system. Next, the level of understanding of digital ethics was evaluated, including students' awareness of grade confidentiality, prohibitions on accessing other people's accounts, and individual responsibility for maintaining the confidentiality of academic data. The analysis also covered students' data security levels, such as strong password habits, consistent SIAKAD log-out practices, password storage in browsers, and the use of personal or shared devices. Furthermore, students' level of trust in security was assessed.

Measurement Data

The measurement of the variables in Table 1 represents the quality testing of the research instrument. This was conducted in two stages: validity and reliability.

Table I Variable Measurement

Variable	Operational Definition	Indicators	Scale
Digital Ethics (ETIK)	The level of students' understanding and compliance with ethical principles in the use of academic data within the Academic Information System (SIAKAD)	• Data confidentiality• Account access• Digital responsibility• Compliance with regulations	Likert 1–5
Data Security (SEC)	Students' behaviors in maintaining the security of their SIAKAD accounts	• Secure password• Logout practices• Network security• Use of personal devices	Likert 1–5
SIAKAD Usage Behavior (USE)	Students' habitual patterns in using SIAKAD	• Usage frequency• Duration• Device used• Access location	Likert 1–5

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

Validity testing was used to ensure that each question item measures the intended variable, while reliability testing was used to determine the level of consistency of respondents' responses to the instrument. Validity testing was conducted using the Pearson Product Moment technique, which aims to measure the relationship between each item's score and the total score of the variable. The formula used is:

$$r = \frac{N\sum XY - (\sum X)(\sum Y)}{\sqrt{[N\sum X^2 - (\sum X)^2][N\sum Y^2 - (\sum Y)^2]}} \quad (1)$$

Each item is declared valid if the calculated r-value is greater than the r-table at a significance level of α = 0.05. Thus, the greater the calculated r-value compared to the r-table, the stronger the relationship between the item and the measured variable. The calculation results show that all items have calculated r-values above the r-table, so all items are declared valid and suitable for use in subsequent analyses. Reliability testing was conducted using the Cronbach's Alpha method, which functions to assess the internal consistency of all items in each variable. The formula used is:

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum \sigma_i^2}{\sigma_t^2}\right) \quad (2)$$

where k is the number of items, $\sigma_i^2$is the variance of each item, and $\sigma_t^2$is the total variance. The reliability assessment criteria are as follows:

α ≥ 0.90: Very Good

0.70–0.89: Good

0.60–0.69: Adequate

< 0.60: Poor

The test results indicate that the Cronbach's Alpha value for each variable is in the good to excellent category, indicating that the instrument has a high level of internal consistency and can be used reliably in this study.

RESULT

This research was conducted by distributing an online questionnaire via Google Forms to students. A total of 120 students participated. The survey results are presented in tabular form, similar to the structure of a reference paper, with detailed discussions of each section.

Table II SIAKAD Access Duration

No	SIAKAD Access Duration	Frequency	Percentage
1	< 10 minutes/day	28	23.3%
2	10–30 minutes/day	67	55.8%
3	> 30 minutes/day	25	20.8%

Table 2 above shows that the majority of students (55.8%) access SIAKAD for 10–30 minutes per day, primarily to view class schedules, KRS (Student Plan Plan), KHS (Student Plan Program), and attendance. This indicates that SIAKAD is used routinely, but does not include applications with long usage times like social media. This duration is quite consistent with the pattern of academic platform access, which is primarily for necessity, not entertainment.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

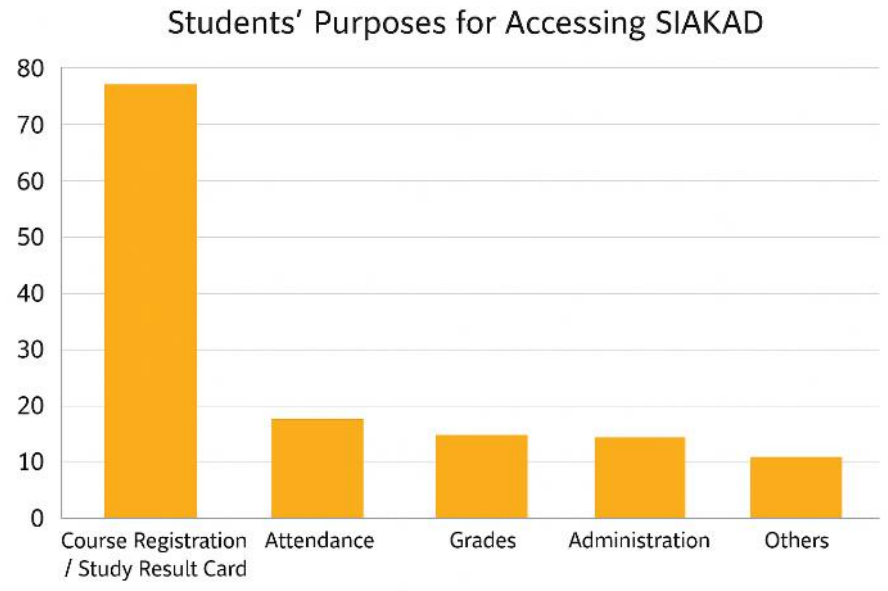

Fig. 2. Student Access SIAKAD

Figure 2 above shows that students' primary purpose for accessing SIAKAD is for their KRS/KHS (67.5%), indicating that SIAKAD functions as a primary academic portal. Administrative and other uses are relatively minor. This confirms that students perceive SIAKAD as a medium, not a platform with social or interactive features.

Table III Overview Student Frequency

No	Frequency of Data Input	Frequency	Percentage
1	Often (weekly)	14	11.7%
2	Monthly	22	18.3%
3	Per semester	72	60.0%
4	Never	12	10.0%

Table 3 presents the frequency data of students, showing that most students (60%) only input their personal data when there are academic activities such as course registration (KRS) or profile updates. This indicates a low level of personal data input activity; however, it still carries risks if students do not fully understand the security of their personal data during these processes

Table IV Student Confidence

No	**Confidence Level**	**Frequency**	**Percentage**
1	Confident	42	35.0%
2	Not Confident	71	59.2%
3	Others	7	5.8%

Table 4 shows that 59.2% of students are not confident that their academic data is completely secure in SIAKAD. This lack of confidence stems from concerns about grade leaks, personal data leaks, or data use by third parties.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

Table V Student Understanding Data Security

No	Understanding	Frequency	Percentage
1	Understand & Aware	107	89.2%
2	Do Not Understand	13	10.8%

Table 5 shows that students' understanding of data security is very high (89.2%). Other indicators are shown in Figure 2 below:

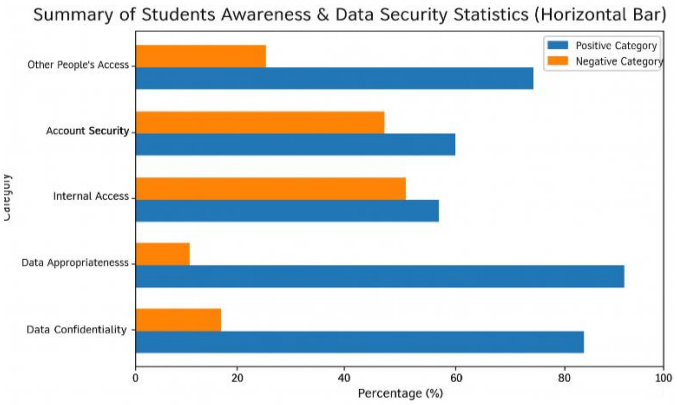

Fig. 3. Student Indicator

Figure 3 presents a summary of five key indicators related to student data awareness and security in using SIAKAD. The graph is a horizontal bar chart with two categories for each indicator: Positive and Negative, facilitating visual comparison. The Data Confidentiality indicator shows that 85% of students are always careful when inputting or accessing data in SIAKAD, while 15% are careless, for example by using public Wi-Fi or saving passwords in their browsers. The second indicator, Data Conformity, shows that the majority of students (90.8%) input data according to actual conditions, while 9.2% have been inconsistent due to concerns about personal data security. The Internal Access indicator reveals that 54.2% of students are aware that some of their data can be accessed by lecturers or administrators, while 45.8% feel that the data cannot be accessed by others. This illustrates internal privacy concerns (internal data exposure). The Account Security indicator shows that 60.8% of students implement security settings such as strong passwords, but 39.2% still ignore basic security practices. Finally, the Account Access by Others indicator shows that 78.3% of students keep their accounts private, while 21.7% still lend access or allow others to access SIAKAD on their devices. Overall, this graph indicates that student awareness is quite high, but there is still room for improvement, especially in account security practices and protection from unauthorized access. 21.7% of students allow others to access their SIAKAD accounts (e.g., borrowing a cell phone without logging out). This graph indicates a serious risk for misuse of academic data.

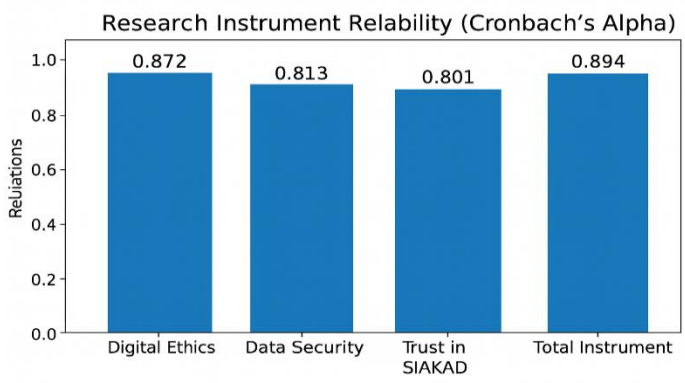

Fig. 4. Visualization Cronbach's Alpha

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

Figure 4 shows a visualization of the research instrument's reliability based on Cronbach's Alpha values for four groups of variables: Digital Ethics, Data Security, SIAKAD Trust, and Total Instrument. The graph uses a bar chart to facilitate comparison of the level of internal consistency between variables. In general, the Cronbach's Alpha values in the graph are above 0.80, indicating that the instrument has a very good level of reliability. The Digital Ethics variable shows a reliability value of 0.872, indicating that the items in this variable are consistent in measuring aspects of students' digital ethics. The Data Security variable has a value of 0.813, indicating that questions in this aspect are able to provide consistent and stable answers from respondents. For the SIAKAD Trust variable, the reliability value is recorded at 0.801, which also indicates a reliable category and can be relied upon in measuring students' perceptions of academic system security. Meanwhile, the highest value is found in the Total Instrument with a Cronbach's Alpha of 0.894, confirming that the entire research instrument has very strong internal consistency. With a value well above the minimum reliability threshold (0.70), this graph confirms that all items in the questionnaire are suitable for further analysis. These findings provide a strong basis for the data obtained to have high stability, consistency, and reliability in describing the state of digital ethics, data security, and student trust in SIAKAD. Overall, the results of the study indicate several important phenomena related to digital ethics and student data security in the use of the Academic Information System (SIAKAD). These findings indicate a significant gap between students' knowledge, perceptions, and actual behavior regarding academic information security. While students' digital ethics awareness is very high (89.2%), their security behavior still shows substantial weaknesses. Many students understand the importance of data confidentiality and ethical principles in academic systems, but in practice they still engage in risky actions, such as saving passwords (39.2%) or not logging out of shared devices. This phenomenon aligns with the concept of the privacy paradox, which is a condition where individuals have high privacy awareness but not accompanied by consistent protective behavior. Furthermore, this condition also indicates an awareness-behavior gap, namely the gap between what is known as correct behavior and the actual actions taken in using SIAKAD. Furthermore, concerns about data security in SIAKAD remain relatively high. As many as 59.2% of students stated they were unsure that SIAKAD was capable of maintaining the confidentiality and integrity of their data. This doubt was primarily triggered by three main factors: the potential for excessive access by internal parties, concerns about grade and personal data leaks, and uncertainty about user account protection mechanisms. This distrust can impact the quality of student interactions with the system, as high risk perceptions can affect the comfort and frequency of using campus digital services. Furthermore, student security is still heavily influenced by external factors. Students tend to be cautious only when facing compelling situations, for example, when using a public device after experiencing a data loss incident. This indicates that students' security orientation is more reactive than proactive. In other words, high awareness does not automatically result in safe behavior, unless there are experiences or conditions that exert direct pressure. This study is consistent with various previous literature and research, including studies of digital ethics among Instagram users in higher education settings. In both contexts, students demonstrated a high level of privacy awareness, yet still exhibited a tendency toward less secure behavior and continued distrust of digital systems. These results reinforce the idea that digital security issues among students are not solely caused by a lack of knowledge, but rather by weak internalization of security habits (security habit formation) and a low perception of long-term risks. Overall, these results underscore the need to strengthen digital security literacy, emphasizing not only knowledge but also building secure habits and behaviors in the use of academic systems. Furthermore, transparency in data management and enhancement of security features in SIAKAD are important steps to increase student trust in educational institutions' information systems.

CONCLUSION

This study shows that although students have a high level of digital ethics awareness, their data security behavior remains inconsistent. Students understand the importance of maintaining confidentiality and ethical use of technology, yet they still engage in risky habits such as storing passwords in browsers, using public devices without protection, and not logging out after using SIAKAD. These findings confirm the existence of a privacy paradox and an awareness–behavior gap, a situation where the level of knowledge is not accompanied by adequate security behavior. Furthermore, student confidence in SIAKAD security remains low, particularly regarding the potential for internal access and concerns about academic data leaks. This situation indicates the need to strengthen technical and non-technical security aspects in the implementation of academic systems. Going forward, universities are advised to improve digital security education through regular training, digital

literacy campaigns, and the provision of easily accessible learning materials for students. The implementation of multi-factor authentication (MFA) and the addition of security nudges such as password change reminders, suspicious login notifications, and logout warnings can help strengthen student security behavior. Furthermore, institutions need to increase transparency regarding privacy policies and data protection mechanisms to increase student confidence in system security. SIAKAD developers also need to conduct regular security audits and integrate digital ethics education modules into the system. These efforts are expected to create a safer, more trustworthy digital academic environment and support the development of a culture of security literacy among students.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia (Kemendikbudristek) for the financial support provided through the PDDI Scholarship 2025. The authors also express their gratitude to the supervisors, reviewers, and colleagues who provided valuable feedback throughout the development of this paper. Appreciation is also extended to all technicians and students who assisted in the preparation of equipment and data collection during the research process.

REFERENCES

1. Ahmed, A., & Thomas, R. (2022). Security awareness and behavioral inconsistency in academic information systems: A systematic review. IEEE Access, 10, 125233–125247.
2. Al-Khalifah, F. (2024). Multi-factor authentication adoption in higher education: Challenges and effectiveness. International Journal of Information Security Science, 13(1), 17–29.
3. Alzahrani, S. O. (2023). Factors influencing cybersecurity behavior of students in online academic systems. Heliyon, 9(2), e13122.
4. Andersen, P., & Davies, G. (2023). Ethical use of academic platforms: An integrative review. Education Digital Ethics Review.
5. Chen, H., & Zhao, Q. (2023). User authentication risks in web-based academic portals: A behavioral analysis. IEEE Transactions on Learning Technologies, 15(3), 360–372.
6. Cruickshank, M. (2024). Long-term effectiveness of security nudges in digital learning platforms. Computers & Security, 132, 103838.
7. Duggan, M., & Smith, P. (2023). Student privacy and the digital learning paradox: Behavioral gaps in higher education security practices. Computers & Security, 124, 103013.
8. Evans, R. (2024). Security habit formation in digital platforms: A behavioral perspective. Cyberpsychology, Behavior, and Social Networking, 14(2), 122–133.
9. Huang, L. (2023). Trust and avoidance behaviors in academic information systems. Journal of Educational Technology, 44(3), 215–229.
10. Islam, S. R., Hansen, T., & Karyda, M. (2022). Ethical considerations in learning analytics: Transparency, data minimization, and student trust. Computers in Human Behavior Reports, 6, 100205.
11. Karyda, M., Hansen, T., & Islam, S. (2022). Risk perceptions and behavioral inconsistency in young digital users. Computers in Human Behavior Reports, 6, 100214.
12. Mäkelä, P., & Salmela, T. (2022). The privacy paradox among university students using e-learning platforms. Information & Computer Security, 30(2), 295–312.
13. Molino, L., & Bennett, N. (2024). Digital ethics and privacy in higher education information systems. Journal of Higher Education Policy and Management, 46(1), 98–115.
14. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). U.S. Department of Commerce.
15. Olvera, M. D. (2023). Human factor vulnerabilities in academic data systems: A behavioral risk assessment. Journal of Information Security and Applications, 70, 103548.
16. Özkan, Ç. A., & Yildirim, B. (2022). Investigating password hygiene among university students: An empirical assessment. Journal of Cybersecurity Education, 9(2), 45–60.
17. Pour, K. L., & Lee, A. J. (2024). Security nudges and habit formation in educational platforms. Computers & Education: Artificial Intelligence, 5, 100315.
18. Pratama, R. K. (2021). Information quality and system usability in university academic information

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue XI November 2025

systems. Journal of Information Education, 12(2), 44–56.
19. Shibata, N., & Sato, Y. (2024). Password reuse and authentication fatigue among college students. ACM Transactions on Privacy and Security, 27(1), 1–22.
20. Taufik, C. I. N., & Juhana, A. (2025). The privacy paradox of students' personal data security in the digital age. SATESI: Jurnal Sains Teknologi dan Sistem Informasi, 5(1), 1–6.
21. Torres, E. M., & Miller, J. (2023). The role of institutional communication in improving student trust in academic information systems. Information Systems Education Journal, 22(4), 45–57.
22. Watini, S., Davies, G., & Andersen, N. (2024). Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments. International Transactions on Education Technology, 4(1), 112–128.
23. White, B., & Tan, G. (2023). Understanding student data exposure risks in university information systems. IEEE Security & Privacy, 21(6), 67–75.
24. Woodward, J., & Caine, A. (2024). Student trust in educational data systems: A cross-institutional analysis. Education and Information Technologies, 29(3), 3555–3572.