Ngr. J. Multi. vol-2, issue-7 (July-2026) pp-290-300

ISSN: 3108-2750 (Online)

Nexus Global Research Journal of Multidisciplinary

Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

Research Article

Risk – Based Authentication Enhancement of University Digital Portal Security

Samuel F. Camorongan [1], Diosdado C. Caronongan[2]

[1-2]Graduate School, University of Luzon, Master in Information Technology Program, University of Eastern Pangasinan.

ABSTRACT:

With the rapid advancement of digital systems, academic institutions increasingly utilized centralized digital platforms to support academic services and communication. The University of Eastern Pangasinan currently utilizes a digital portal that has a traditional password-based authentication system, which depends on username and password. This study analyzed user perceptions to the existing authentication method of the digital portal, focusing on three key indicators: (1) accessibility, (2) usability, and (3) security effectiveness. Using a descriptive - developmental research design, data were collected through online surveys and focus group discussion with the administrative staff and students. The findings revealed that while the portal performs well in accessibility and usability, its security effectiveness scored lower, indicating limited user confidence in password – based authentication. Based on data gathered, a prototype for risk – based authentication system was developed. This adaptive system evaluates risk through factors such as device and location trust, IP reputation, login patterns, failed attempts, user behavior, and adjusts verification requirements accordingly. Low risk access uses a single – factor authentication, medium risk triggers one – time code verification via email, and high risk requires one – time pin (OTP) verification and hardware token. By conducting a post – test with the developed prototype, a side-by-side comparison of the weighted means between the existing password - base and the developed risk-based authentication system, the developed system indicates a higher level of satisfaction in terms of accessibility, usability, and security features. The study concludes that the developed prototype for risk – based authentication system significantly shows the security effectiveness of the system without compromising user experience, offering a practical solution for academic institutions.

Keywords: *Risk – Based Authentication, Digital Portal Security, Security Effectiveness, Accessibility, Usability,*

INTRODUCTION

The increasing reliance of higher education institutions on digital technologies has transformed the delivery of academic services, making university portals essential for managing enrollment, grades, student records, and institutional transactions. As these systems store sensitive personal and academic information, ensuring secure user authentication has become a critical concern. The University of Eastern Pangasinan currently employs a traditional password – based login system that relies solely on single – factor authentication. Although convenient, this approach remains vulnerable to unauthorized access, password theft, and other cybersecurity threats, showing the need for stronger authentication mechanism. Recent studies have emphasized the effectiveness of multi-factor authentication (MFA) in enhancing digital security. A systematic literature review by Cahyanto et al. (2025) found that multi – factor authentication significantly reduces the risk of data breaches and unauthorized access while improving user confidence in digital systems. However, the successful implementation of multi – factor authentication depends not only on its security capabilities but also on users' perceptions of its accessibility, usability, and reliability. Authentication models with a multi - factor usually requires the user to confirm their identity by using an additional step, such as a one – time pin (OTP) or mobile device verification. With this added layer of security, it will help to secure the accounts, but its success is not determined by the technology alone. The user acceptance is being shaped by accessibility, ease of use, and perceived of reliability plays a crucial role in its overall effectiveness.

In response to these concerns, this study evaluates users' perceptions of the existing password-based authentication system of the University of Eastern Pangasinan in terms of (1)

Corresponding author: Samuel F. Camorongan,

Received: 16 July 2026; **Accepted:** 20 July 2026; **Published:** 25 July 2026

accessibility, (2) usability, and (3) security effectiveness. Based on the identified issues for each of the aspects, a risk-based authentication prototype incorporating adaptive risk – bases authentication system was developed. This project sought to provide a comprehensive understanding of how user perceive the current authentication system of the university digital portal. After the prototype of the authentication system is developed, the proponent of the study conducted a post – test with the student and administrative staff and gather their feedback to measure the level of satisfaction on the proposed security measure.

STATEMENT OF THE PROBLEM

This study aimed to enhance the digital portal security of the University of Eastern Pangasinan in Binalonan through a risk-based authentication system in order to improve both system security and user experience.

Specifically, the study sought to answer the following questions:

1. What is the extent of user perception of the current authentication mechanism of the University of Eastern Pangasinan digital portal in terms of:

a.) Accessibility;

b.) Usability; and

c.) Security Effectiveness?

2. What authentication system can be designed based on the user perceptions to enhance both user experience and system security?

3. What is the level of user satisfaction on the proposes authentication system?

SIGNIFICANCE OF THE STUDY

This study is significant as it provides a deeper understanding on how user perceived the security authentication mechanism of a digital portal within a local university. By focusing on accessibility, usability, and security effectiveness, the project identifies both the capabilities of the current authentication mechanism of the system. The finding aimed to broaden knowledge on user – centered security, as it offers insights into how protective measures are received and experienced. The findings can serve as a guide for better practices and policies, contributing to a safer digital environment.

MATERIALS AND METHODS

The study employed a descriptive–developmental research design to systematically gather and analyze essential data for the development of an authentication method developed to the institution digital portal. This approach was deemed appropriate as it enabled a comprehensive examination of the existing authentication system, including current conditions, user experiences, and operational challenges. Through this design, the proponent was able to identify security vulnerabilities, evaluate the effectiveness of the current authentication mechanisms, and capture the perceptions of users involved in the system. To strengthen the investigation, an extensive review of related literature was conducted, drawn from books, peer reviewed journal articles, technical reports, and credible online sources. The review focused on contemporary authentication practices and emerging risk-based technologies, particularly their application within academic institutions. Furthermore, qualitative data were collected through focus group discussions (FGDs) involving administrative personnel responsible for managing the university digital portal. These discussions offered in depth insights into their experiences, challenges encountered with existing authentication methods, and recommendations for system improvement. The integration of findings from the literature review and FGDs enabled the development of a well-informed and context-sensitive understanding of the institution's current digital security framework. Descriptive–developmental design played a critical role in ensuring that the proposed authentication model is both technically robust and aligned with the specific needs of the institution. As a research approach, descriptive–developmental design is widely recognized for its effectiveness in systematically describing phenomena without manipulation, particularly in areas with limited prior studies. It facilitates the identification of patterns, trends, and classifications using both qualitative and

quantitative methods, such as surveys, observations, and case analyses. In this study, its developmental component further guided the structured design and creation of an authentication solution grounded in empirical evidence and user centered insights.

In a study, the Technology Acceptance Model (TAM) is utilized to examined the perceived usefulness and ease of use affect students' intention to use portal. Additionally, the research incorporated elements such as accessibility, collaboration, and document exchanged as it provides broader understanding of portal adoption in academic setting. The findings showed that both Technology Acceptance Model (TAM) and contextual factors significantly developed the user acceptance, as it offers insights in terms of designing more effective and secure digital portals in higher education, (Gura and Chen, 2010). Moreover, the figure shown to the subsequent page is the Technology Acceptance Model (TAM) diagram of the study. It included the Accessibility, Security Effectiveness, and Usability of the implemented authentication mechanism of the digital portal. After it is the perceived usefulness, and to come up with the perception of risk – based authentication system in a local university portal.

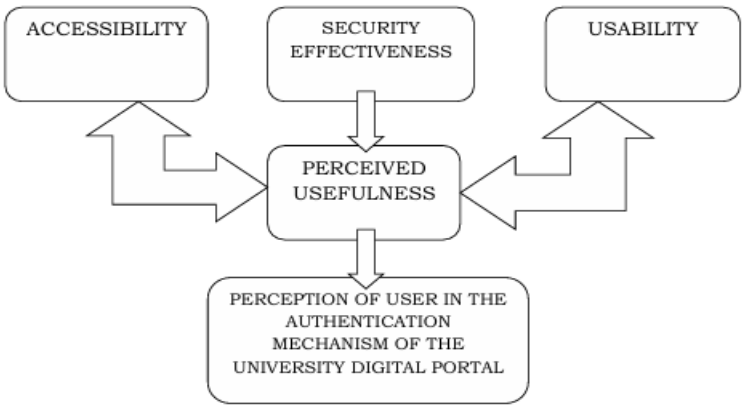

Figure 1. Technology Acceptance Model of the Study

The proponent of this study incorporated the Technology Acceptance Model (TAM) to examines how users perceive authentication mechanism in a local university portal. Technology Acceptance Model (TAM) provided a framework to understand the influences of usability, accessibility, and security effectiveness aspects to user behavior. By applying Technology Acceptance Model (TAM) the proponent identified the factors, and ultimately it served as the guide in the development of the authentication methods.

System Development and Methodology

Figure 2. Rapid Application Development Model

Figure 1 shows the phases of the adopted system development methodology. Rapid Application Development (RAD) specifically have five (5) phases:

Requirements Planning. The first phase is analogous to project scoping meeting. Under planning phase, though shorter than in other project management techniques, it is still vital to the project's success. In order to clarify the project objectives and expected results, as well as any existing or potential issues that would need to resolved during development, the developer must communicate to its beneficiary at this stage. This phase is very fundamental elements are investigating the issue at hand, outlining the project requirements, and finalizing the requirements with the agreement of all parties. The proponent of the study gathered the requirements in the area related to the topic, review relevant studies and scholarly journals, analyzed some related planned systems, and focus group discussion to analyzed with the administrative staff. The development of the beta parts of the system, the proponent also conducted interviews with administrative staff and subject matter experts to aid in formulating an authentication model suited to the digital portal.

In gathering the requirements for the software project helped the developer and the organization to have an effective analyzation for the software requirements, avoid misunderstandings and achieve the target output. In requirements planning it is beneficial to the client and developer as it serves as the blueprint that guided and help them in tracking the progress of the project (Severn, 2022). The proponent of the study gathered the requirements in the area related to the topic, review relevant studies and scholarly journals, analyzed some related planned systems, and focus group discussion to analyzed with the administrative staff. The development of the beta parts of the system, the proponent also conducted interviews with administrative staff and subject matter experts to aid in formulating an authentication model suited to the digital portal.

System Testing. Once the project's scope has been established, the user design developed through numerous iterative testing. In this stage, the proponent created models and components that accurately represent all system operations, inputs, and outputs. Through this ongoing interactive process, users can evaluate, alter, and ultimately accept a functional system model that satisfies the requirements. As being defined, system testing is the presentation of the base product for which it closely resembles the outward presentation and functionality of the target output. In addition, the development of the beta parts gave a better idea as it provides a better visual model of the target project. In this phase the project manager can also check the beta parts if it matches to the expected functionality and features.

As being defined, system testing is the presentation of the base product for which it closely resembles the outward presentation and functionality of the target output. In addition, the development of the beta parts gave a better idea as it provides a better visual model of the target project. In this phase the project manager can also check the beta parts if it matches to the expected functionality and features. The iterative testing can help the developer in tracking the progress of the project while it is under the development. Moreover, all of the malfunctions and problems are identified and fix (Lal, 2022).

Evaluation / Analysis. At this stage of the study, the developer conducted a survey to collect feedback from the users regarding their experienced in using the digital portal. The main purpose of this stage is to identify the strengths and weaknesses of the current system, particularly in terms of usability, accessibility, and the overall satisfaction. Through the responses gathered, the developer understands the needs, concerns, and expectations of the users, as it served as an important basis for improving the system's features and performance. Moreover, a conducted a survey supports the application of a human centered approach, as it encouraged user participation in the development process. It allows the developer to design and implement system improvements based on real user input, ensuring that the final output is more effective, user-friendly, and

responsive to the needs of the institution's community.

System evaluation refers to the process of assessment whether a computing system, software, or algorithm meets its intended objectives by comparing actual performance against predefined specifications and user requirements. It helps determine if project goals were achieved and identifies areas for improvement and modification. Evaluation includes a range of methods—experimental, analytical, and empirical and involves criteria such as consistency, completeness, precision, usability, security, and reliability. These assessments not only validate system design but also guide future enhancements. Depending on the context, evaluation can occur at different stages of development and supports ongoing optimization and trustworthiness in complex computing environments.

Conclusion. During this phase, the approved system design is transformed into a functional prototype that demonstrates the core features and functionalities of the proposed system. The prototype serves as a working model used to validate the system's design, authentication workflow, and user interactions. Development focuses on implementing the essential modules, integrating the required technologies, and refining the prototype based on testing, evaluation, and user feedback. Identified issues, errors, and necessary improvements are addressed iteratively to enhance the prototype's functionality, usability, and security before proceeding to the final evaluation.

As being pointed out that in this phase it plays as the crucial part as it makes sure that the software project works exactly the same with plan. Moreover, the user undergoes in testing. Uncover bugs and other problems, or security issues that is not being found during the iterative testing is already fixed before the development of the software. The development of programs and applications, coding, unit, integration, and system testing are some of the smaller processes that make up the phase (Adam, 2023).

Cutover. The final stage involves the prototype testing and evaluation. At this stage, the completed prototype is deployed in a controlled environment for demonstration and assessment rather than full-scale operational use. The prototype undergoes functional testing to verify that its core features perform as intended, while selected users evaluate its accessibility, usability, and security effectiveness. Feedback and evaluation results are collected to identify strengths, limitations, and areas for improvement, providing the basis for further refinement and future system development.

As being mentioned, after all of the iterative testing, fixing all of the bugs, and the system functionalities are working correctly and it is now ready to release. Besides, after the deployment the developer manage and check the bugs of the software. All the final adjustments have been made, (Watts, 2023).

According to the methodologies employed by the proponent, tools involved identifying the following: (1) issues or problems; (2) user needs; and (3) the project's requirement – related necessity. It sought to ascertain how to completely finish the project using the methods that the proponent utilize. The proponent has a variety of options after gathering data. The suggested methods include sources of data, questionnaires, surveys, and any additional methods that might be appropriate.

Sources of Data. Focus group discussion method (FGDs) is the first method that the proponent utilized. To get a sense of the respondents' perspectives, the proponent of the study conducted an in – person focus group discussion (FGDs) with the administrative staff of the institution. Additionally, by utilizing this method, the proponent examined the respondents' actual issues and experience. It is critical to used sources of data in research because they offer an explanation for any queries pertaining to the proponents' study. According to its definition, data is a type of information provided by the respondent. Resources must be present in every piece of data. It assesses and measures the given study's primary goal. In addition, data is used to choose the outcomes that with the provided research questions with answers (Medin, 2022). When selecting the data collection

techniques to be employed in the study, it is crucial to take these factors into account. Since it provides an answer to the research question, data must be gathered from the appropriate sources and according to the proper methodology. On the other hand, when the proponents chose an unsuitable data collection technique, the study came to the wrong conclusion, (Mwita, 2022).

Survey Questionnaire. A survey is one of the most distinctive methods to gather data from a big group of people. Surveys have some benefits, such as the fact that they don't take much time since the proponent only gives the respondents questionnaires. Additionally, a survey questionnaire can gather a ton of data that the proponents can use as a foundation for the development of the authentication method. However, using a survey questionnaire cost more money, and the accuracy of the data depend on the respondents' counter-response rates.

In comparison with the two types of survey questionnaire. As being characterize, in online – based survey it is easy to implement since the interviewee can access and answer it thru email, or social media. One advantage of online – based survey, it is not time consuming in tallying the response of the interviewee as it is automatically stored in the database. While in paper – based survey, the quickness of collecting data is the gradual factor as it takes a lot of time for the respondent to answer the survey form. However, in paper – based survey get better responses as the proponents can guide those respondents that experiences a difficulty in reading. In addition, online – based survey and paper - based survey is suitable for question types such as grid and list questions (DeFranzo, 2019).

Online – based survey approach is being utilized in this study. In order to give the respondents an access to the prepared survey form of the proponent. In addition, online – based survey is suited in collecting information as it can be read and answer by the respondents on time. The survey questionnaire form is being provided by the proponent of this study. Before the questionnaire administer to the respondents it is first checked by the statistician for the validity of the content. The questions presented in the survey form is being utilized to collect response from the respondents. The given response of the respondents is being utilized to determine the capabilities, experiences, and problems that associated with the main of the study. Before distributing survey questionnaires, the total number of respondents must be taken into account. The proponent of the study utilized Cochran formula to calculate the sample size needed for a survey, particularly for a large or infinite populations, and below is the given formula.

$$n_0 = \frac{Z^2 \cdot p(1-p)}{e^2}$$

n0: initial sample size

Z: the Z – score corresponds to the desired confidence level.

p: the estimated proportion of an attribute in the population (if unknown, 0.5 is often uses for maximum variability)

q: 1 – p (used as 0.5 x 0.5 if p = 0.5)

e: the desired margin of error expressed as a decimal)

The formula requires the confidence level to find the Z value, the margin of error, and the estimated proportion of the attribute. If the population is small and finite, a modified formula can be used that incorporates the population size. By using the formula, mentioned above the appropriate sample size given the specified combination of precision, confidence, and variability is 375.

RESULTS:

This section presents the results, analysis, and interpretation of the data gathered to address the objectives of the study. Specifically, it discusses: (1) the user perception to the existing university digital portal's authentication system across three aspects — accessibility, usability, and security effectiveness; (2) the development and key features of the proposed risk-based authentication system; (3) the satisfaction level of the respondents on the developed authentication system; and (4) a synthesis of the findings drawn from the data analysis.

In order to obtain a comprehensive insight, the proponent of the project administered a structured survey to 375 respondents, aimed at evaluating how users perceive the effectiveness of the university's current digital portal authentication mechanism. The survey measured user perception across three aspects: (1) accessibility, (2) usability, and (3) security effectiveness. Responses were measured using a five-point Likert scale where 1.00 - 1.80 = Strongly Disagree, 1.81 - 2.60 = Disagree, 2.61 - 3.40 = Neutral, 3.41 - 4.20 = Agree, and 4.21 - 5.00 = Strongly Agree.

User Perception to the Current Authentication System

Table 1. User Perception Result for the Current Digital Portal

Indicator	Weighted Mean	Description
Accessibility	3.65	Agree
Usability	3.26	Neutral
Security Effectiveness	2.35	Disagree

The results provide an overall evaluation of the existing authentication mechanism and serve as the basis for identifying areas requiring improvement and for justifying the implementation of a risk-based multi-factor authentication system.

A.) Accessibility

The results indicate that the existing digital portal is generally perceived as accessible, obtaining an overall weighted mean of 3.65 (Agree). Respondents strongly agreed that the portal can be accessed directly without third-party applications and that it accommodates user preferences. However, they expressed concerns regarding the system's performance in areas with limited internet connectivity and the delayed delivery of password-related notifications. These findings suggest that while the portal provides convenient access under normal conditions, improvements in connectivity support and notification reliability are necessary to enhance overall accessibility.

B.) Usability

The findings show that the existing digital portal's authentication usability received an overall weighted mean of 3.26 (Neutral), indicating mixed user perceptions. Respondents positively assessed the ease of navigation, accessibility of the login process, and general understanding of the interface. However, concerns were identified regarding authentication errors, insufficient feedback during login, and the simplicity of the overall login experience. These results suggest that while users can perform basic authentication tasks, improvements are needed in system reliability, user guidance, and interface design to achieve a more efficient and satisfactory authentication experience.

C.) Security Effectiveness

The results indicate that the existing digital portal's security effectiveness received an overall weighted mean of 2.35 (Disagree), reflecting users' low confidence in the current authentication mechanism. Respondents expressed concerns regarding the adequacy of password-based authentication, protection of login credentials, detection of suspicious activities, and prevention of unauthorized access. Although some users acknowledged that security measures can function alongside accessibility, the findings suggest that the existing system requires stronger authentication

controls and improved security mechanisms to enhance user trust and protect sensitive information.

Development of the Risk – Based Authentication System

The system evaluates potential threats by assigning risk scores based on several factors, including the user's location, device characteristics, and IP address. Through this scoring method, the system can intelligently detect unusual activity and apply stronger verification when needed. Risk evaluation factors consist of device and location trust, time patterns, IP reputation, failed attempts, and behavior patterns. The authentication levels consist of three tiers: (1) Low Risk — single-factor authentication (password only); (2) Medium Risk — one-time pin (OTP) via email; and (3) High Risk — hardware token combined with OTP authentication. Presented below is the diagram illustrating how the risk -based authentication system operates. Presented to the succeeding page is the flowchart of the developed risk – based authentication system prototype.

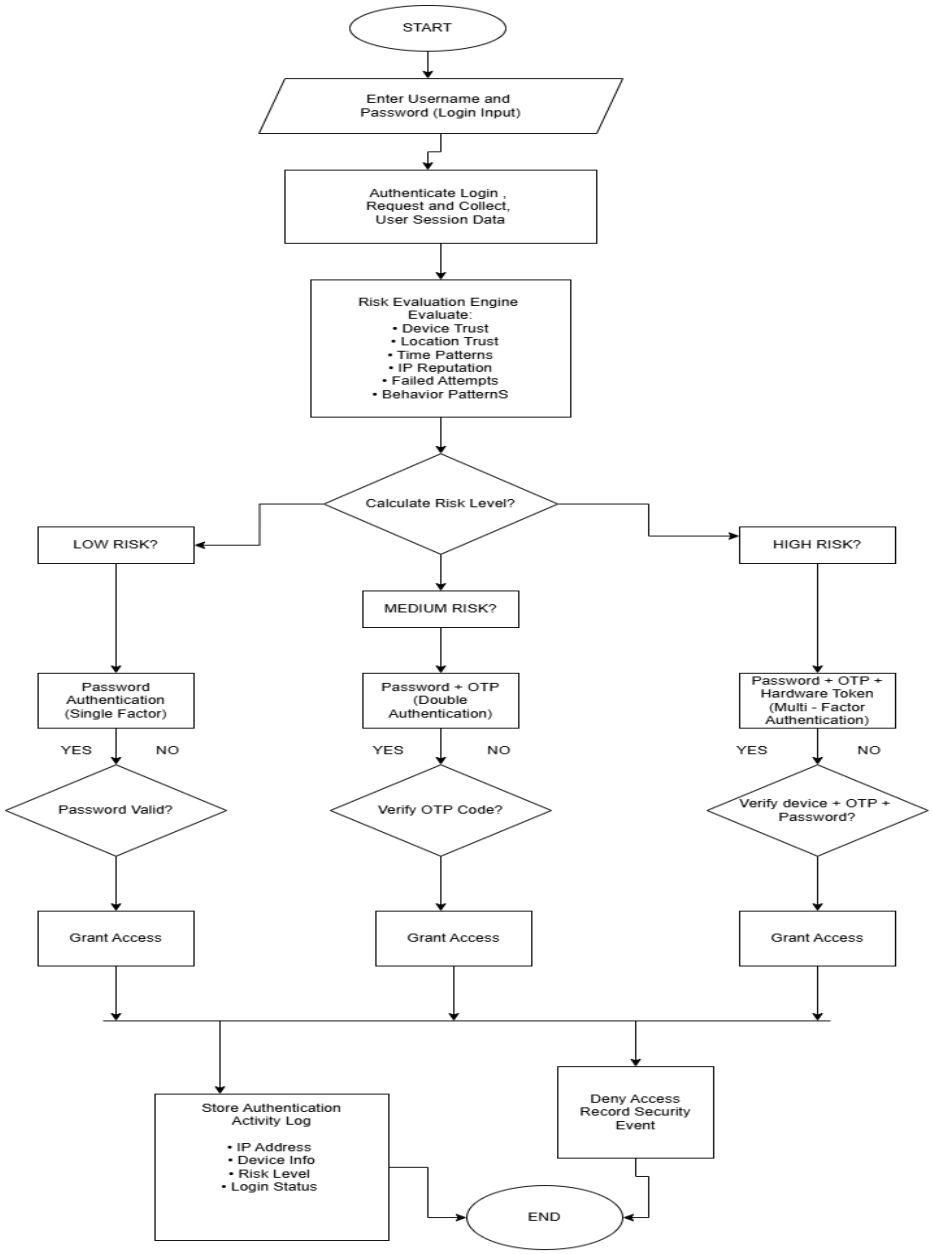

Figure 3. Risk – Based Authentication System Flowchart

For the (1) low-risk level, users are required to enter their student ID and password for verification. When the assessed risk level is low, the digital portal applies single-factor authentication, relying solely on password-based verification. This tier applies to users accessing from known devices and familiar locations with no history of failed login attempts. The (2) medium-risk tier is activated when the system detects suspicious patterns such as multiple recent failed logins attempts or a newly created account. Under this condition, the authentication system prompts the user to confirm access through a one-time verification code sent via email, adding a second layer of verification beyond the standard password. In (3) high-risk situations such as when a login attempt originates from an unrecognized device, an unusual or unfamiliar location, repeated failed authentication attempts, or activity associated with a newly created account, the system automatically activates its highest level of security control. These scenarios are treated as potentially suspicious, prompting the implementation of stricter verification measures to safeguard user data and system integrity.

User Satisfaction Level on the Developed Risk-Based Authentication System

After the development of the risk-based authentication method, the proponent prepared fifteen (15) survey items answered by a total of forty (40) respondents, composed of five (5) questions per aspect — accessibility, usability, and security effectiveness — as stated in the study. Satisfaction was measured using a five-point scale where 1.00 1.80 = Very Dissatisfied, 1.81–2.60 = Dissatisfied, 2.61–3.40 = Neutral, 3.41–4.20 = Satisfied, and 4.21–5.00 = Very Satisfied. Table 4. User Satisfaction Level on the Developed Risk – Based Authentication System.

Table 2. User Satisfaction Level on the Developed Risk – Based Authentication System

Indicator	Weighted Mean	Description
Accessibility	4.24	Very Satisfied
Usability	4.66	Very Satisfied
Security Effectiveness	4.70	Very Satisfied

Table 2 presents the detailed post – test evaluation ratings across the three aspects of the developed risk-based authentication method. The weighted mean per indicator — 4.24 for Accessibility, 4.66 for Usability, and 4.70 for Security Effectiveness— all fall under the Very Satisfied range, demonstrating that the developed authentication mechanism is consistently met or exceeded the respondents' expectations across all three dimensions.

Discussion of Findings

This section summarizes the study's findings by combining the user perception results of the existing portal and user level satisfaction results of the developed risk-based authentication system.

In terms of accessibility, the university digital portal obtained an overall weighted mean of 3.65 (Agree), indicating that the existing system is generally accessible. Most indicators received positive ratings, the proponent noted that users can log in independently, use different email addresses, and access recovery features conveniently. However, the system performs poorly in areas with limited internet connectivity (1.27, Strongly Disagree), revealing a critical accessibility gap. The low rating on timely password-change notifications (2.05, Disagree) further indicates communication weaknesses in the current system. In contrast, the

user level satisfaction results on the developed system showed a weighted mean of 4.24 (Very Satisfied) for accessibility, reflecting a meaningful improvement. The risk-based authentication system addressed the existing accessibility concerns by providing a clearer, more responsive login experience that operates across different devices and conditions.)

Regarding usability, the portal's authentication process obtained an overall weighted mean of 3.26 (Neutral), reflecting mixed user experiences. While users find navigating from the login page straightforward (4.70, Strongly Agree) and can access accounts quickly (4.49, Strongly Agree), there are serious usability concerns: the portal fails to provide adequate feedback during login (1.84, Strongly Disagree), and the login experience is considered poorly designed in terms of simplicity (1.37, Strongly Disagree). These critical gaps indicate that the current system fails to communicate meaningfully with users during the authentication process. The user satisfaction level results for usability registered a weighted mean of 4.66 (Very Satisfied), representing an improvement of 1.40 points. The proponent attributes this significant gain to the clarity of the step-by-step authentication process and the usefulness of verification messages incorporated. In terms of security effectiveness, the portal received the lowest overall weighted mean of 2.34 (Disagree), reflecting significant user distrust in the current password-based system.

The proponent found that respondents expressed strong concern that traditional authentication does not adequately guarantee data security (1.32, Strongly Disagree) and that the system lacks sufficient security coverage (1.78, Strongly Disagree). The system also received low ratings for detecting suspicious login attempts (2.48, Disagree) and logging out inactive sessions (2.33, Disagree), further highlighting critical vulnerabilities. The user level satisfaction results for security yielded the highest aspect mean among all three dimensions at 4.70 (Very Satisfied), an increase of 2.36 points — the largest improvement observed. This finding confirms that the adaptive, multi-layered verification mechanism of the risk-based authentication mechanism directly and effectively resolved the most critical weakness of the existing system.

Overall, the findings reveal a consistent and significant improvement across all three aspects after the adoption of the risk-based system. The proponent concluded that the existing digital portal, while moderately accessible, falls critically short in usability feedback and security effectiveness. The developed system successfully addressed each identified gap, resulting in an overall satisfaction mean of 4.54 (Very Satisfied). These results affirm that the risk-based authentication is a viable, effective, and user-accepted solution for improving the university digital portal's authentication system.

CONCLUSION

The proponent of the study draws upon the accumulated findings and insights from this research project to present a comprehensive and meaningful conclusion that addresses the effectively and incorporation of risk – based authentication model. Mentioned below are the following conclusions drawn from the project:

The findings show that the university digital portal performs well in terms of accessibility and usability, as reflected by a positive weighted mean rating. Additionally, study identified weaknesses in the security effectiveness of the existing password – based authentication system. Disagree to negative user perceptions indicate low confidence in its ability to prevent unauthorized access and comply with modern cybersecurity standards.

In view of the findings presented, the proponents concluded that the development of a risk-based authentication system for the digital portal is essential. The proposed system incorporates three (3) distinct risk categories, namely: (1) low risk, (2) medium risk, and (3) high risk. Through this approach, the system is capable of assessing the user’s corresponding risk level before permitting access to the digital portal, thereby enhancing the overall security of the platform.

The primary users and subject matter experts of the digital portal rated the developed risk – based authentication system as “Very Satisfied”. They provide excellent feedback confirming this is

a reliable, secure, and improved alternative to traditional password – only authentication model.

Recommendations

Based on the abovementioned findings and conclusions in this study, mentioned below are the following recommendations from the researchers:

Future researchers and institutions are encouraged to adopt and integrate the developed risk-based authentication prototype into their digital portal security systems. Implementing the prototype in real-world environments will enable further evaluation of its effectiveness in detecting and mitigating potential cybersecurity threats while providing valuable insights for future enhancements and broader institutional adoption.

It is recommended that future researchers explore integrating additional adaptive verification mechanisms, such as biometric authentication (fingerprint) or app – based authentication tools. These methods can further strengthen the security of the digital portal without compromising usability.

To the future researcher, it should focus on expanding the accessibility testing to ensure the portal accommodates users with diverse needs, including those with disabilities. This involves evaluating compatibility with assistive tools, screen readers, and various devices while considering different user preferences.

REFERENCES

- Cahyanto, I., Madihah, H., Budiarso, I., Sutrisno, A., & Hidayat, T. (2025). Effectiveness of multifactor authentication technology for protecting student privacy: A systematic literature review
- Gura, M., & Chen, Q. (2010). Factors affecting adoption of a student portal
- Severn, L. (March, 2021). The Process of Gathering Requirements for Software Development.
- Lal, R. (February, 2023). What Is Software Prototyping and Why Do You Need It? Medin, D. (2022). Using Data Sources in Research. Research Square
- Adam, J. (March, 2023). What is the software development life cycle (SDLC) and why is it important? A brief introduction to SDLC phases, methodologies.
- Watts, S. (October, 2023). Software Development Lifecycle (SDLC): An Introduction
- DeFranzo, S. (2019). Which is More Effective: Paper-Based Surveys or Online Surveys?
- Mwita, K. (2022). Factors to consider when choosing data collections methods.researchgate.net
- Medin, D. (2022). Using Data Sources in Research. Research Square