KHATULISTIWA SMART : JOURNAL OF ARTIFICIAL INTELLIGENCE
e-ISSN : 3089-9710
p-ISSN : XXXX-XXXX

Khatulistiwa Smart : Journal of Artificial Intelligence
Vol. 1 No. 2 (2025) : 57-66
Available online at : https://journal.literasikhatulistiwa.org/index.php/smart

Siamtek Unuja Security Analysis Using Two-Factor Algorithm Biometric Scan With Fingerprint

Zainal Arifin [1], Fuadz Hasyim [2]
[12] Universitas Nurul jadid
zainal@unuja.ac.id[1] , fuadzhasyim@unuja.ac.id[2]

Doi

Received: 26 Mei 2025 *Accepted: 16 juni 2025* *Published: 30 juni 2025*

Abstract Student data security is a critical priority in academic information systems, particularly at Nurul Jadid University (UNUJA), which utilizes the SIAMTEK platform to manage practicum and final project activities. This study aims to analyze the effectiveness of implementing Two-Factor Authentication (2FA) using biometric fingerprint scanning to enhance the security of the SIAMTEK application. The research employed an experimental approach that included literature review, system analysis, system design, development, and testing. The authentication process consisted of two stages: verification via username and password, followed by a fingerprint scan. System testing was conducted using a Likert scale questionnaire distributed to 4th and 6th semester students, who are active users of the SIAMTEK application. The results indicated a 62% satisfaction index for the user interface and a 65% index for the functionality of the 2FA system. These results suggest that users are moderately satisfied with the added layer of security. Unlike One-Time Password (OTP) methods, which depend on mobile credit or connectivity, fingerprint biometric scanning offers a cost-effective and secure solution without requiring additional user expenses. This study also reviewed previous research on 2FA and Multi-Factor Authentication (MFA), highlighting the vulnerabilities of single-factor systems, particularly to phishing attacks and unauthorized access. The findings confirm that implementing fingerprint-based 2FA in the SIAMTEK system is both feasible and beneficial, significantly reducing risks of data breaches and account misuse. The integration of biometric technology as an additional authentication layer positively contributes to digital academic system security and supports data protection efforts for students' personal and academic information.

Keywords *Two-factor authentication (2FA); biometrics; fingerprint;*

1. INTRODUCTION

Nurul Jadid University (UNUJA) is a higher education institution currently consisting of four faculties with a curriculum that includes Practicum and Final Project courses aimed at strengthening students' mental capacity and knowledge. This is intended to ensure that students are capable of analyzing and contributing to society and the workforce in the future. The current system supporting these two courses is SIAMTEK, an acronym for Sistem Manajemen Praktikum dan Tugas Akhir (Practicum and Final Project Management System). This system handles the registration process for practicums (internships, community service programs) and final projects, including the selection and announcement stages, all of which can be monitored through the platform (Aisyah et al., 2022).

On the other hand, data security has become increasingly important due to the rising number of cyber threats. Many cyberattacks aim to steal data, including confidential information, customer records, financial data, and especially academic information related to students. SIAMTEK, as one of UNUJA's academic applications, still has weaknesses, particularly in its authentication mechanism. It currently uses single-factor authentication with only a username and password, which poses security risks, especially the misuse of access rights. Such issues can have severe consequences, including the leakage of students' personal data or unwanted alterations to practicum, community service, or final project information.

Securing student data has become a key priority for software providers—in this case, UNUJA itself. Up to now, the authentication process has only relied on a username and password, which is considered insufficient in providing a sense of security (Naidu, 2022). Today, security is crucial across all sectors, including banking, government applications, military organizations, educational institutions, and more. The number of digital identities required by each user is increasing due to the rapid expansion of online services. At present, passwords remain the most commonly used security method (Fitriyansyah & Hazri, 2020). Users often choose passwords that are easy to remember—such as their name, common words, birth dates, or simple alphanumeric combinations. These are easily cracked by hackers using basic password-breaking programs.

Important user information becomes highly vulnerable to various forms of attacks, such as phishing. Phishing is commonly used to obtain email addresses or phone numbers by sending messages from what appear to be trustworthy sources. Cybercriminals craft these messages to appear legitimate, tricking victims into responding. Through social engineering techniques, they manipulate victims into trusting and engaging with malicious communications.

In response to this, software vendors have been racing to adopt stronger authentication mechanisms, moving beyond the traditional username-password approach to methods such as Two-Factor Authentication (2FA). 2FA acts as an additional layer of protection to secure system access. It requires users to go through two authentication steps: initially by entering their username and password, and then by using a unique code, biometric scan, software authenticator, one-time passcode (OTP), or a hardware token (Wang et al., 2020).

Several studies have been conducted to address authentication-related security issues. A number of them implement 2FA as a solution. Below are some of the relevant studies:

In a study titled "Two-Factor Authentication for Effective Information Security", the author discusses the vulnerabilities of single-password verification, which is now considered insecure and prone to being hacked. The study proposes multiple methods of two-factor authentication. It compares seven methods based on primary authentication, secondary authentication, and overall security level. These methods are ranked from highest to lowest security as follows: Microsoft Authentication App, FIDO2 Security Key, OATH hardware tokens, OATH software tokens, SMS, Voice Call, and lastly, Password as the least secure. The integration of two-factor verification offers users both convenience and better protection (Naidu, 2022).

Another study by Ibrokhimov et al. (2019) focuses on the challenges users face with multi-factor authentication (MFA). The sequence of authentication steps—requiring not only passwords but also special key numbers—demonstrates a higher level of cybersecurity. The study describes several types of MFA. The first involves fingerprint scanning combined with user-specific random projections. Another involves threshold cryptography, which generates OTPs by randomly splitting a code and reconstructing it when the OTP is required. The study also mentions multimodal biometrics-based MFA (MFA-MB) for cloud computing applications.

The final study by Wang et al. (2020) discusses security failures in multi-factor authentication systems. Most of the failed schemes were designed for single-server architectures using 2FA. Designing 2FA schemes for multi-user architectures is more complex. The study suggests that Three-Factor Authentication (3FA) could be built upon 2FA by adding biometric verification to achieve enhanced security.

2. RESEARCH METHODS

2.1. System Development Method

The author employs an experimental method with the aim of understanding the structure of information presentation and processing that involves decision-making and result delivery. The first stage begins with data collection and continues through to drawing conclusions. The stages of the research are illustrated in Figure 1.

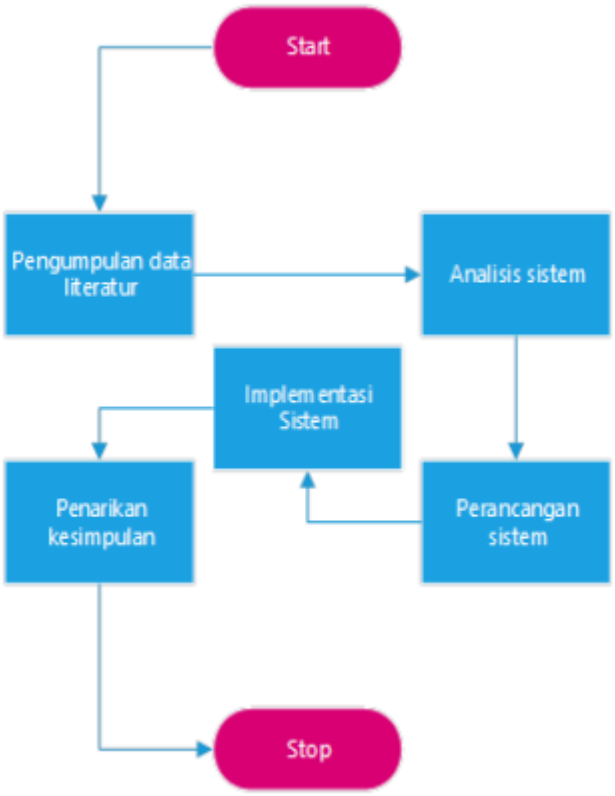

Figure 1. Stages of Research

2.2. Literature Data Collection

In this stage, the researcher gathers references relevant to the research topic. All references related to cybersecurity, particularly the use of two-factor authentication, are collected, including journals, books, research reports, or other credible sources concerning biometric scanning, especially fingerprint authentication. A decision study is then conducted to draw conclusions from the references and to propose a better system design by the researcher.

2.3. System Analysis

System analysis is the initial stage of system implementation, serving as the foundation for determining the success of the system. In this phase, an assessment of initial requirements and analysis of ideas and concepts must be conducted to gather information on system needs. The analysis is carried out through interviews and literature studies. The researcher's analysis focuses on how two-factor authentication is implemented within the SIAMTEK application.

2.4. System Design

System design translates system requirements into a software design plan that can be estimated prior to the coding phase. This process focuses on data structures, software architecture, and procedural algorithm details. The output is a software requirement document, which will be used by developers during the system development phase.

2.5. System Development

System development involves converting the previously created design into a programming language—in this research, Java is used. The code must be written according to the specifications defined during the design stage and must be properly

documented. After coding is completed, the system undergoes a testing process to draw conclusions about its performance and functionality.

3. RESULTS AND DISCUSSION

In the results and discussion stage, the implementation of each phase described in the methodology section is discussed in detail. The outcomes that can be concluded are as follows:

3.1. Literature Data Collection

As previously mentioned, this study identified three journals discussing two-factor authentication. It can be concluded that the implementation of two-factor authentication methods has a positive effect on enhancing system security. This is because system access requires users to go through two stages: first, using an identifier such as a password or username, and second, through a fingerprint scanner.

3.2. System Analysis

A comprehensive system analysis ensures that the two-factor authentication method is implemented properly, in accordance with both the system's functional requirements and the security needs of SIAMTEK. In this study, the system analysis is presented using a Software Requirement Specification (SRS). The following are the identified system requirements: The system accepts user identifiers (username, password, phone number, and email), The system identifies the user credentials, The system captures the user's fingerprint, The system verifies the user's fingerprint, and The system grants access to the user.

This will assist UNUJA, as the provider of the SIAMTEK application, in enhancing data access security, protecting sensitive information, and reducing potential security risks.

3.3. System Design

System design is carried out after the analysis stage is completed. This stage aims to provide a blueprint for the users, specifying system and software requirements and defining the overall system architecture. The login process and user management are illustrated in Figure 4. There are two actors involved: the User and the Admin. The Admin is responsible for managing user accounts, while the User performs registration (sign-up) and login operations.

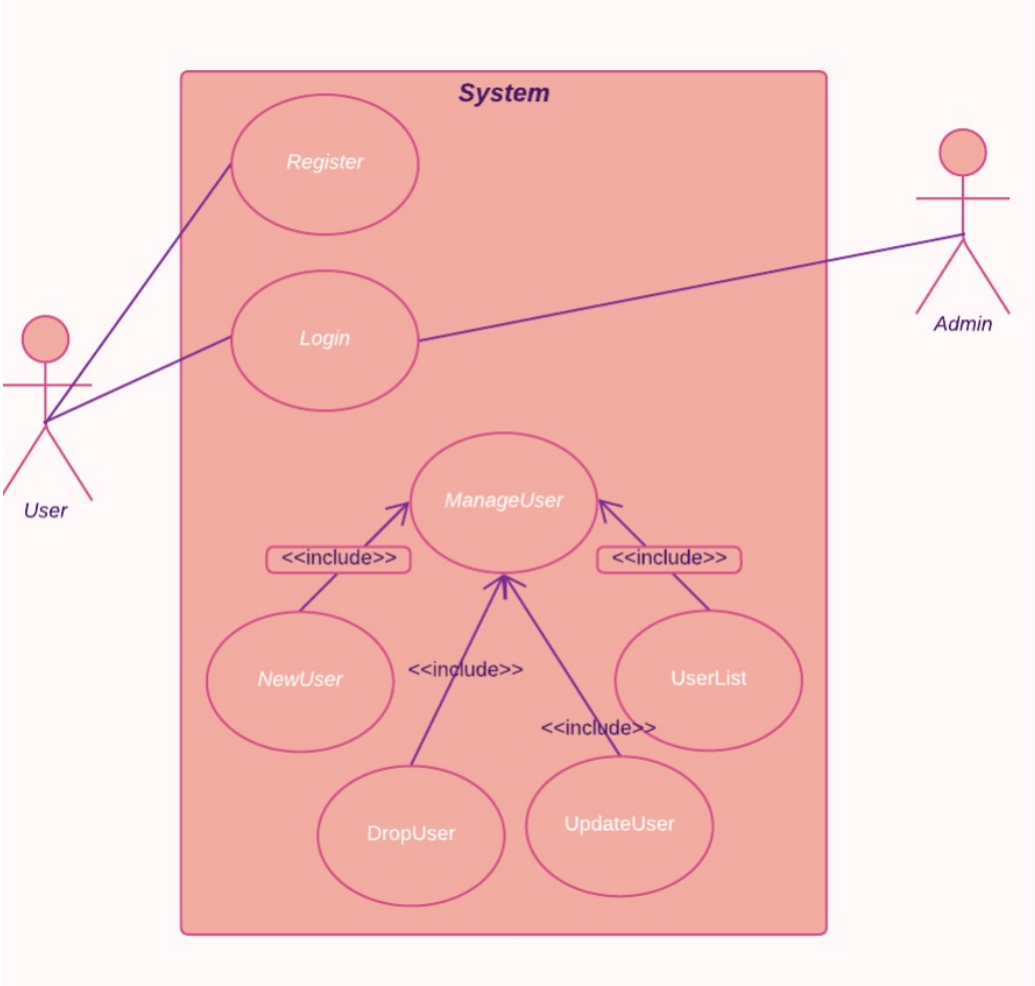

Figure 2. Login process use case diagram

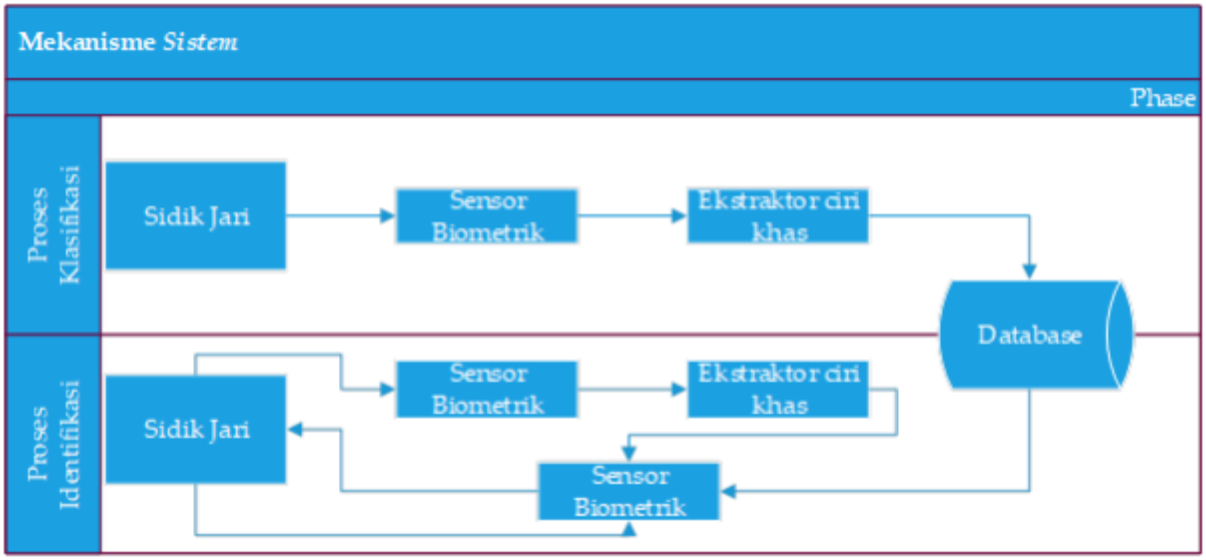

Figure 3. System Mechanism

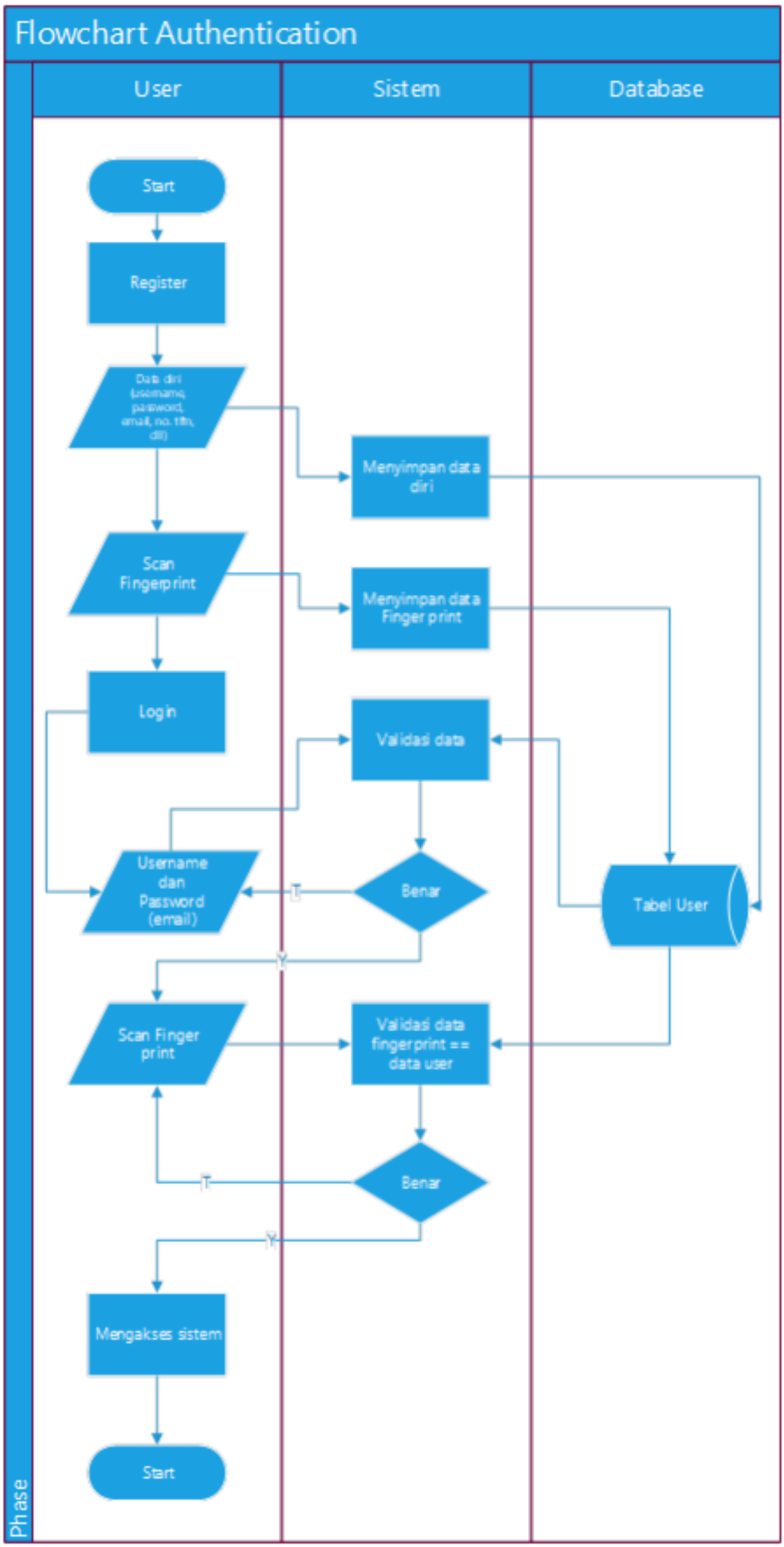

Figure 4. System Flowchart

3.4. System Implementation

After the system design stage, the system is then developed according to the previously created design. Following development, the system is tested to obtain conclusions. The testing is conducted using a Likert scale, with data collected through questionnaires distributed to respondents. The following presents the results of the system implementation and system testing.

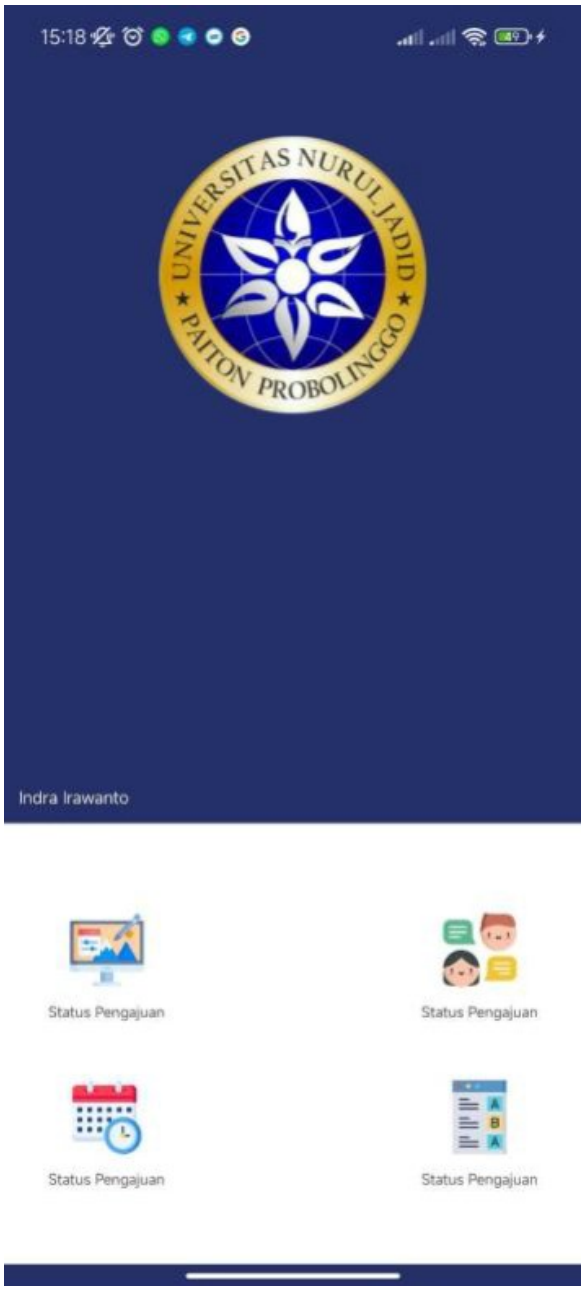

Figure 5. SIAMTEK Home Page View

Figure 5 shows the main page of the SIAMTEK application. The application will automatically log out if it is inactive for 10 minutes and will return to the login page. Users will then need to log in again to continue using the system.

3.5. System Testing

The SIAMTEK application was then tested using the Likert scale method. Respondents in this test were UNUJA students in the 4th and 6th semesters, as they are required to take practicum courses. Respondents were first shown how to use the application, particularly the login process. After that, they performed independent trials to gain hands-on experience with the login feature. The assessment standards used in this testing are presented in Table 1 as follows.

Table 1. Parameter Value

Skor Nilai	Skor Nilai
1 Sangat Tidak Setuju	1 Sangat Tidak Setuju
2 Tidak Setuju	2 Tidak Setuju
3 Netral	3 Netral
4 Setuju	4 Setuju
5 Sangat Setuju	5 Sangat Setuju

Table 2. System Testing

No	Pertanyaan	Respon					Jumlah	Index %
		1	2	3	4	5		
User Interface								
1.	Apakah tampilan login dalam aplikasi	1	0	0	6	7	60	61
2.	Apakah proses login dalam aplikasi mudah diaplikasikan?	1	0	0	7	5	54	64
Total		2	0	0	13	12	114	**62 %**
Fungsionalitas								
3	Apakah proses login dalam aplikasi dapat dilakukan?	1	0	0	5	8	61	54%
4	Apakah user menerima request fingerprint dari sistem?	1	2	1	4	8	64	57%
5	Apakah fitur login sesuai dengan kebutuhan?	1	0	0	7	6	59	60%
6	Apakah proses login berjalan dengan cepat?	1	0	2	4	7	58	59%
7	Apakah dengan adanya proses login dengan fingerprint, aplikasi lebih aman?	0	1	0	7	6	59	60%
8	Apakah aplikasi komunikatif?	1	0	0	7	6	59	60%
Total		5	3	3	34	41	360	**65%**

Based on the results of system testing using the Likert scale, the outcomes are presented in Table 2. The index score for the user interface is 62%, while the functionality scores 65%.

4. CONCLUSIONS

Based on the results presented in the previous section, this study found that securing the SIAMTEK application at UNUJA using two-factor authentication (2FA) based on biometric fingerprint scanning can effectively reduce the risk of fraud and the theft of personal data. By relying on a fingerprint scan that must belong to the actual user, every login attempt to access the SIAMTEK application must genuinely be performed by the

account owner, in this case, a UNUJA student. This is intended to ensure that personal information, particularly academic data, is protected from unauthorized access or leakage, whether by known or unknown parties, thereby preventing harm to the application users. It is concluded that the implementation of two-factor authentication (2FA) in the SIAMTEK application at UNUJA is feasible. The 2FA mechanism requires users to perform a fingerprint scan. Through testing using the Likert scale, the results showed a 62% score for the user interface and a 65% score for the functionality of the implemented two-factor authentication. These scores indicate that the 2FA implementation in SIAMTEK sufficiently meets user needs. Unlike the use of OTP delivery, which relies on the availability of user phone credit, biometric scanning, particularly fingerprint authentication, is more cost-effective for users, as it does not require additional costs to perform authentication.

5. REFERENCES

Aisyah, S., Furqan, M., & Sudriyanto. (2022). Analisa prototype sistem manajemen praktikum dan tugas akhir (siamtek) pada perangkat android. NJCA, 7, 76–83.

Fitriyansyah, A. Y., & Hazri, M. (2020). Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password. Sainstech: Jurnal Penelitian Dan Pengkajian Sains Dan Teknologi, 30(1), 1–14. https://doi.org/10.37277/stch.v30i1.725

Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. Journal of Intelligent Manufacturing, 25(2), 217–230. https://doi.org/10.1007/s10845-012-0669-y

Haryadi, S., Indonesia, U. I., & Campus, S. (2021). Implementasi dan Analisis Performansi Autentikasi Sistem Biometrik Sidik Jari. 2021(January 2005).

Ibrokhimov, S., Hui, K. L., Abdulhakim Al-Absi, A., Lee, H. J., & Sain, M. (2019). Multi- Factor Authentication in Cyber Physical System: A State of Art Survey. International Conference on Advanced Communication Technology, ICACT, 2019-Febru, 279–284. https://doi.org/10.23919/ICACT.2019.8701960

Naidu, D. (2022). TWO-FACTOR AUTHENTICATION FOR EFFECTIVE INFORMATION SECURITY. 04(06), 4307–4312.

Sumijan, M. S., Purnama, P. A. W. S. K. M. K., & Arlis, S. S. K. M. K. (2021). Teknologi Biometrik Impementasi pada Bidang Medis Menggunakan Matlabs. In Teknologi Biometrik. http://www.adityarizki.net/teknologi-biometrik/

Wang, D., Zhang, X., Zhang, Z., & Wang, P. (2020). Understanding security failures of multi-factor authentication schemes for multi-server environments. Computers and Security, 88, 101619. https://doi.org/10.1016/j.cose.2019.101619