Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Implementation of Layered User Verification in Web Applications Using Google Authenticator-Based Two-Factor Authentication

Riski Yanti[1]*, Nurdin[2], Al Khaidar[3]

[1,2,3,] *Master of Information Technology Program, Malikussaleh University, Batam Street, Bukit Indah Campus, Lhokseumawe, Aceh.*
riski15yanti@gmail.com[1], nurdin@unimal.ac.id[2], alkhaidarkutablang@gmail.com[3]*

Abstract

This study discusses the implementation of a layered security system using the Two-Factor Authentication (2FA) method based on the Google Authenticator application on a website login system. The purpose of this study is to improve authentication security without sacrificing user convenience. The methods used include system performance testing by measuring login time and error rate, as well as usability evaluation using the System Usability Scale (SUS). Tests were conducted on 10 users for statistical analysis and 20 respondents for the usability test. The test results show that the average login time without 2FA is 2.11 seconds, increasing to 4.49 seconds after the implementation of 2FA, with the results of the paired t-test producing a t value = -21.8 and p-value = 0.00001, which indicates a statistically significant difference. The average SUS score obtained was 85.1, included in the very good category, which indicates that the system remains easy to use despite the additional authentication process. Blackbox testing results showed that all features functioned as expected, with a system success rate of 92.31% and a non-conformance rate of 7.69%. Risk evaluations and fallback solutions were also developed to address potential issues such as lost devices or forgotten backup keys. Thus, the developed 2FA system proved secure, effective, and user-friendly, and is suitable for enhancing login security in web-based applications.

***Keywords**: Two Factor Authentication, Google Authenticator, Security.*

1. Introduction

The rapid development of information technology has had a significant impact on various aspects of life, particularly in accessing web-based services [1]-[2]-[3]. Technology has made it easier for users to access information, conduct transactions, and even communicate globally. This progress has also opened new opportunities for cybersecurity threats, such as data theft, account hacking, and phishing attacks [4]-[5]. In this regard, protecting user data is crucial to ensure trust and security when using digital services. Traditional permission systems that rely on passwords as the sole security mechanism are still widely used [6]-[7]. Although users can create complex passwords, this method cannot completely prevent brute-force attacks, keyloggers, or theft through social engineering. Reliance on this system has proven to be a major weakness in protecting user data from increasingly complex threats [8].

Two-Factor Authentication (2FA) is a security method that requires two distinct authentication elements to verify a user's identity. The first element is something the user knows, such as a password or PIN. The second element is something the user possesses, such as a physical device or authenticator app that generates a verification code. This verification code is dynamic and changes periodically, making it more difficult to forge [9]-[10]. A current problem is that websites have not yet adopted a multi-layered security system like 2FA. As a result, users often fall victim to detrimental cyberattacks, such as data theft and privacy breaches. Furthermore, many users are unaware of the importance of using additional security technologies, resulting in low adoption rates of advanced security systems.

To address these issues, this research aims to develop a multi-layered security system by implementing a Two-Factor Authentication method based on Google Authenticator. With this method, users are protected not only by a password but also by a dynamic authentication code that is difficult for unauthorized parties to access. It is hoped that implementing this system will significantly improve user data security while providing a sense of security when using web-based services.

2. Literature Review

2.1. State Of The Art

Research into developing a multi-layered security system for website user authentication using Two-Factor Authentication (2FA) based on the Google Authenticator app has become a significant topic in recent years. Cybersecurity, particularly in the authentication process, plays a crucial role in protecting users' personal data and information from the threat of identity theft, hacking, and other attacks.

Although two-factor authentication technology is increasingly used, challenges related to its implementation and effectiveness remain a focus of research. Issues such as dependence on user devices, the possibility of technical issues with the app, and the difficulty of managing authentication at scale are some of the main challenges in optimally implementing this system. Two-Factor Authentication (2FA) based on the Google Authenticator app.

Research conducted by Aprilia, Tantri, et al. (2024) [11] focused on the impact of Two-Factor Authentication (2FA) on preventing data theft or cybercrime on social media. This study demonstrated that vigilance against cybercrime is crucial, especially among Generation Z, who tend to be less concerned about the security of their personal data. Implementing 2FA has been shown to improve account protection from hacking and data theft, making it an effective preventative measure in maintaining the digital security of social media users.

Furthermore, research conducted by Ririn Siti Baiduri, Leonardo Kamajaya, and Fitri (2024) [12] implemented a Two-Factor Authentication (2FA) system on a panel box lock using a combination of Face ID and Radio Frequency Identification (RFID) technology. The results showed that the system was effective in enhancing the security of physical devices, with a success rate reaching 90% under optimal lighting conditions (500–1000 lux). Although this research focused on hardware security, the concept of two-factor authentication remains relevant and adaptable to digital security contexts, such as websites.

Meanwhile, research by Mahnida Zahra Siregar, Nabilla Fairus, et al. (2024) [13] discussed the implementation of two-factor authentication for personal data security on the Instagram platform from the perspective of UINSU Stambuk 2021 students. The results revealed that although students understand the importance of 2FA, their usage rate is still low because it is considered complicated and impractical. However, those who activate 2FA feel an increased sense of security against the threat of personal data leaks. This research provides an important basis for further research that will implement Google Authenticator-based Two-Factor Authentication (2FA) in website security systems, to strengthen the digital protection of user data.

The novelty of this research lies in the development of a custom-built web application using the Laravel framework, integrated with a Two-Factor Authentication (2FA) system. Unlike previous studies that focused on implementing 2FA on existing platforms such as social media or physical security systems, this research introduces an innovative approach by integrating Google Authenticator-based 2FA directly into a self-developed web environment. By constructing the website from scratch, this study not only evaluates the effectiveness of 2FA in enhancing user authentication security but also demonstrates how this mechanism can be optimally embedded within a modern Laravel-based web architecture. Consequently, the research contributes to advancing web security development by providing a practical and adaptive solution to mitigate cyber threats.

2.2. Two Factor Aunthentication (2FA)

Two-Factor Authentication (2FA) is a method used to verify the legitimacy of an account by requiring two steps of verification in addition to a password. This second process typically involves a unique code generated specifically or sent via text message. This method provides a reasonable level of protection for certain services, such as financial services [14]. Understanding 2FA is crucial for young people, especially students, so they can protect their accounts from hacking and hacking threats. Therefore, efforts are needed to educate users about the importance of using two-factor authentication, especially on social media platforms.

Two-factor authentication security systems require users to provide two different forms of identification, increasing the security of their online accounts [15]. Typically, users only need an email address and password to log in, but with 2FA, they must go a step further. Sites that implement 2FA are often linked to the user's mobile phone number. A common example of authentication is using a smartphone, which receives an OTP code or link from the system. The purpose of this process is to ensure that the person accessing the account is the true owner. This second factor can be obtained through a code on the device being used or the CVV number on a credit card, not just through a smartphone.

Two-factor authentication (2FA) requires users to go through two separate verification steps to prove their identity. Typically, these systems combine two elements from different categories to ensure that the user attempting access is truly legitimate. In general, this form of authentication can be divided into five types:

1. Personal knowledge, such as a PIN, password, or passcode known only to the user;
2. Possession, such as an ID card, security token, or smartphone;
3. Biometrics, such as facial, voice, fingerprint, or iris recognition;
4. Geographic location, as determined by IP address or GPS data;
5. Access time, such as the device's local time or the user's login time.

One-Time Passcodes (OTPs) are a widely used authentication method in 2FA systems. OTPs are a series of alphanumeric characters or numbers that are automatically generated and valid only once. The advantage of OTPs is their resistance to replay attacks because the code cannot be reused. This means that if an OTP is intercepted or discovered by an unauthorized party, it will no longer be valid if reused. OTPs can be used as a single authentication method, in conjunction with a static password, or as an additional layer in a security system.

Users can receive their OTPs through various means, including strong tokens, weak tokens, or short message service (SMS). The illustration can be seen in Figure 1.

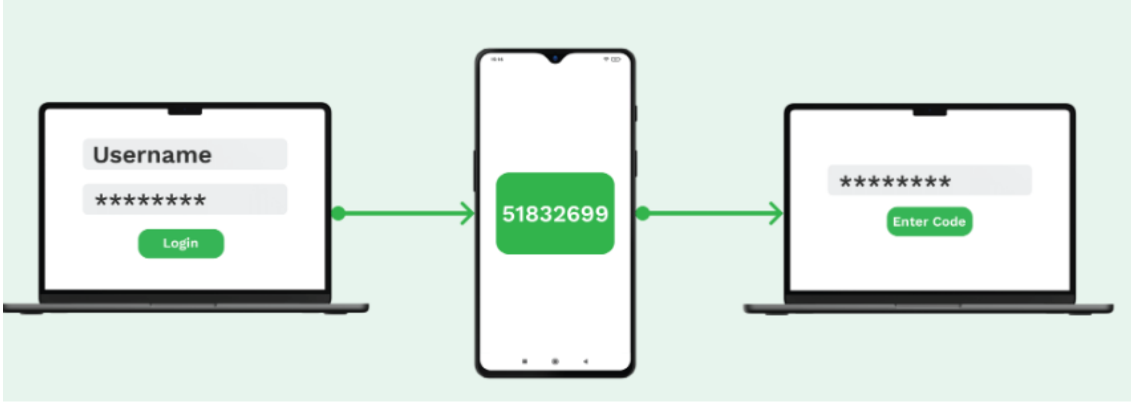


Figure 1 Two-Factor Authentication Illustration

3. Research Methodology

3.1. Research Method/Framework

This research uses an applied quantitative approach with a focus on system development. The primary objective is to design, implement, and test a network security system. To ensure the research runs smoothly and produces relevant findings, the research framework stages are shown in Figure 2.

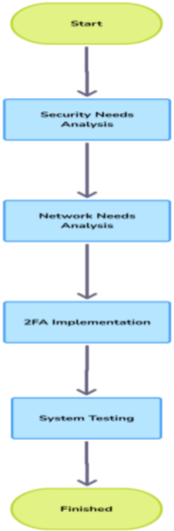


Fig. 2: Research Method/Framework

Based on the research process framework, the stages can be described as follows:

1. Starting
   This is the initial stage of the research and system development process. At this stage, the researcher determines the topic, formulates the problem, and establishes the research objective, namely implementing Google Authenticator-based two-factor authentication (2FA) to improve login security on web systems.
2. Security Requirements Analysis
   This stage aims to identify system security requirements, such as double authentication, user data encryption, an OTP verification mechanism, and a fallback system if a user loses access. This analysis also considers information security principles such as confidentiality, integrity, and availability.
3. Network Requirements Analysis
   This examines the technical network aspects required to support the implementation of 2FA. These include a stable internet connection, secure data transmission between the client and server, and anticipation of network threats such as man-in-the-middle attacks or phishing.
4. 2FA Implementation
   At this stage, the two-factor authentication system is integrated into the existing login system using the Laravel framework. 2FA features include secret key generation, QR code generation for Google Authenticator, and dynamic, time-based One-Time Password (OTP) verification.
5. System Testing

The testing phase is conducted to evaluate the system's performance and effectiveness. Testing includes login times with and without 2FA, OTP input error rates, and blackbox testing to verify system functionality. A usability evaluation is also conducted using the System Usability Scale (SUS) questionnaire.

6. Finish
   This is the final stage, which includes conclusions from the testing results and recommendations for further system development. A system is considered successful if it improves login security without significantly reducing user experience.

3.2. System Topology

The following is a system topology that illustrates the process of connecting various devices within a system. This can be seen in Figure 3.

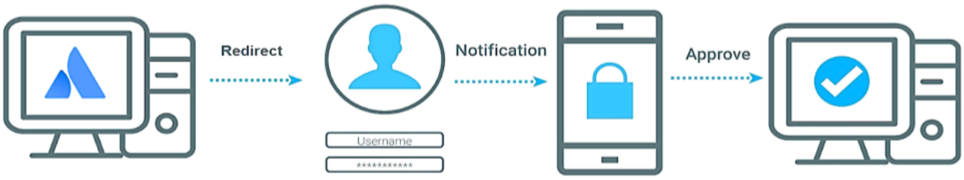


Fig. 3: System Topology

Figure 3 shows the Two-Factor Authentication process, which begins with a user accessing a website and being prompted to authenticate using valid credentials. After the first step is successful, the system sends a One-Time Password (OTP) to the email address registered to the user's account as an additional verification method. The user then opens the email, receives the OTP, and enters the OTP code on the page provided by the system. Once the system verifies the OTP matches, access to the user's account is granted, allowing the user to continue using the service with a higher level of security. This process is designed to enhance account security by adding a second layer of protection through verification that relies on a factor the user possesses, namely access to a personal email address.

3.3. Block Diagram

A block diagram is a visual representation that serves to show the important elements in a system and how they are related to each other. The block diagram for this system can be seen in Figure 4.

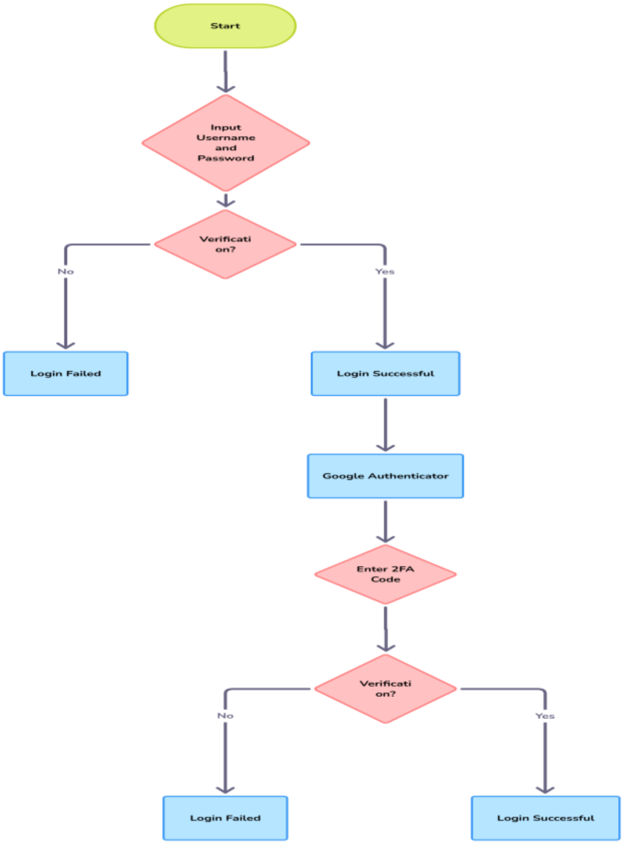


Fig. 4: Block Diagram

Figure 4 represents the authentication process with two-factor authentication (2FA) implementation. The process begins with the user entering a username and password. The next step is the initial verification of these credentials. If verification fails, the program flow ends with a "Login Failed" status. However, if the username and password verification are successful, the program flow continues to the stage of sending a 2FA code to the user's registered email. After the 2FA code is sent, the user is prompted to enter it. This stage is followed by verification of the entered 2FA code. If the entered code is invalid or does not match the code sent to the email, the "Login Failed" status is displayed and the authentication process ends. Conversely, if the entered 2FA code is valid, the authentication process is considered successful and the user is granted access (the "Login Successful" status). Overall, this flowchart illustrates the implementation of 2FA as an additional layer of security. After verifying the basic credentials (username and password), the system performs a second verification via a unique code sent to the user's email.

4. Result and Discussion

This chapter discusses the implementation of a multi-layered security system for website user authentication using the Google Authenticator application-based two-factor authentication (2FA) method, as well as the results and testing of the system. The results of this research and testing will be explained in more detail below.

4.1. Register Page

The Register page on this system displays an interface for users registering a new account as the first step in implementing a multi-layered security system using Two-Factor Authentication (2FA). On this page, users enter information such as their full name, email address, and password. The resulting Register page display can be seen in Figure 5.

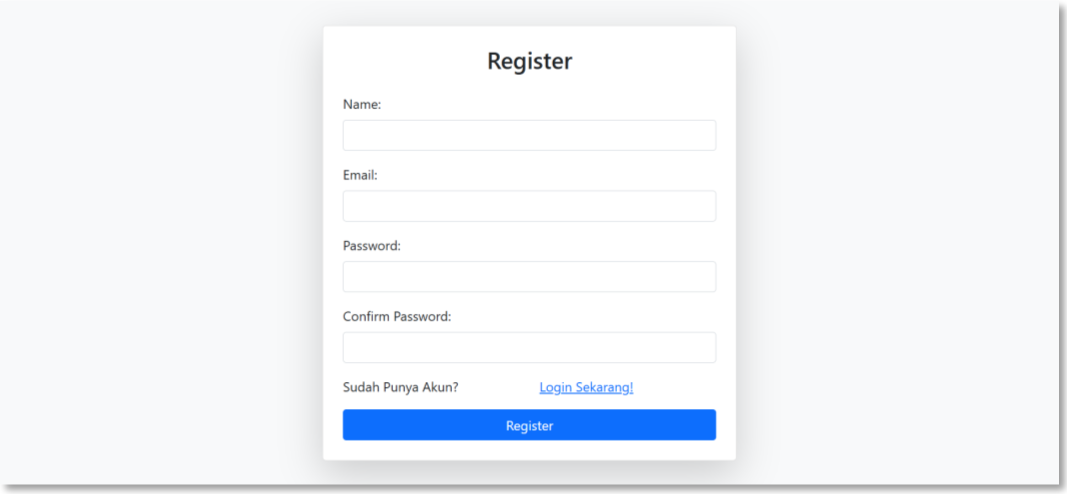


Fig. 5: Register Page

4.2. Login Page

The login page is a crucial element of the system, allowing registered users to securely access their accounts. On this page, users must enter the email address and password they created during the registration process. The login page display can be seen in Figure 6.

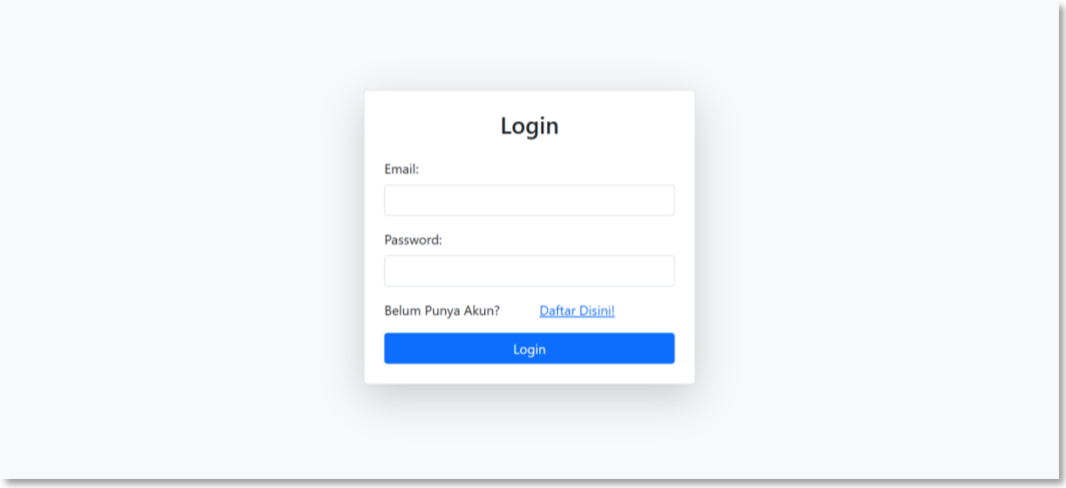
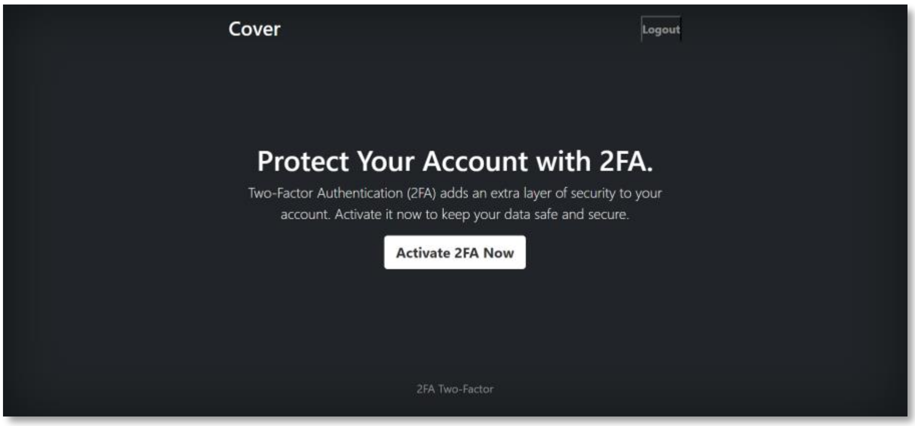


Fig. 6: Login Page

4.3. Protect Account Page

The Protect Account page on this system displays a notification to users about the importance of enabling Two-Factor Authentication (2FA) as an additional layer of security. On this page, there is an "Activate 2FA Now" button to initiate the two-factor authentication activation process. This feature is designed to ensure that only users with an authentication device can access their accounts. The resulting Protect Account page can be seen in Figure 7.



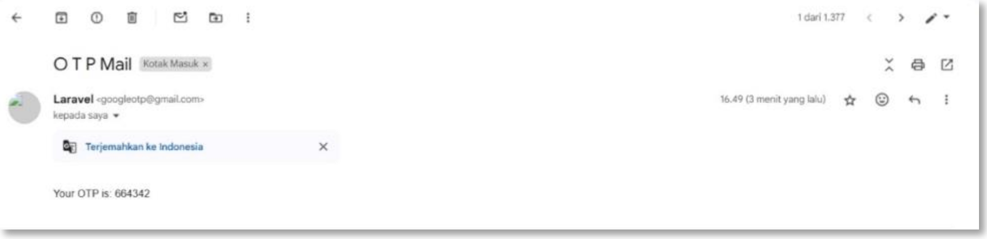
Protect Your Account with 2FA.

Two-Factor Authentication (2FA) adds an extra layer of security to your account. Activate it now to keep your data safe and secure.

Fig. 7: Protect Account Page

4.4. Email Code Delivery

The system will send a verification code to the user's registered email address. After the user successfully enters their username and password, the system will automatically generate a unique verification code and send it to the user's email address. This code is dynamic and has a limited validity period to ensure the security of the authentication process. Users are advised to check their email inbox, including their spam folder, for the verification code. After receiving the code, they can enter it into the field provided on the verification page to complete the Two-Factor Authentication (2FA) process. The results of the verification code sent via email can be seen in Figure 8.



O T P Mail

Laravel <googleotp@gmail.com>
kepada saya

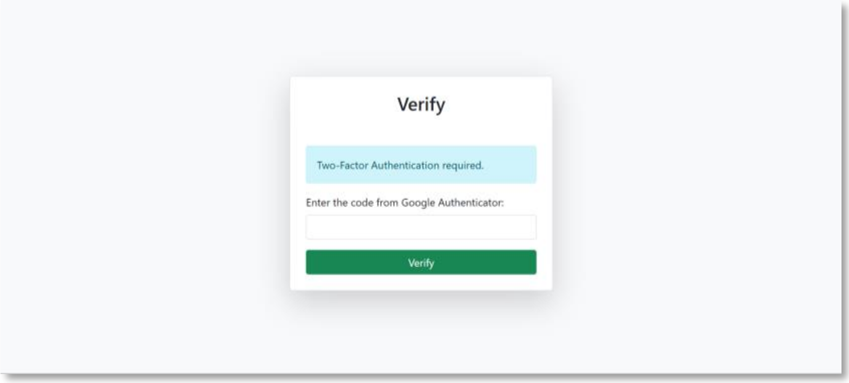
16.49 (3 menit yang lalu)

Your OTP is: 664342

Fig. 8: Email Code Delivery

4.5. Two-Factor Authentication Verification

The Two-Factor Authentication Verification page is the final stage in the user authentication process. After successfully entering a username and password, the user will be asked to enter a verification code dynamically generated by the Google Authenticator application. On this page, there is an input field where the user must enter the appropriate verification code. This code has a limited validity period to ensure system security from unauthorized access attempts. This verification process is a crucial step in implementing the Two-Factor Authentication (2FA) method to ensure that only users with physical access to the authentication device can log in to the system. The results of the two-factor authentication verification page can be seen in Figure 9.


Verify

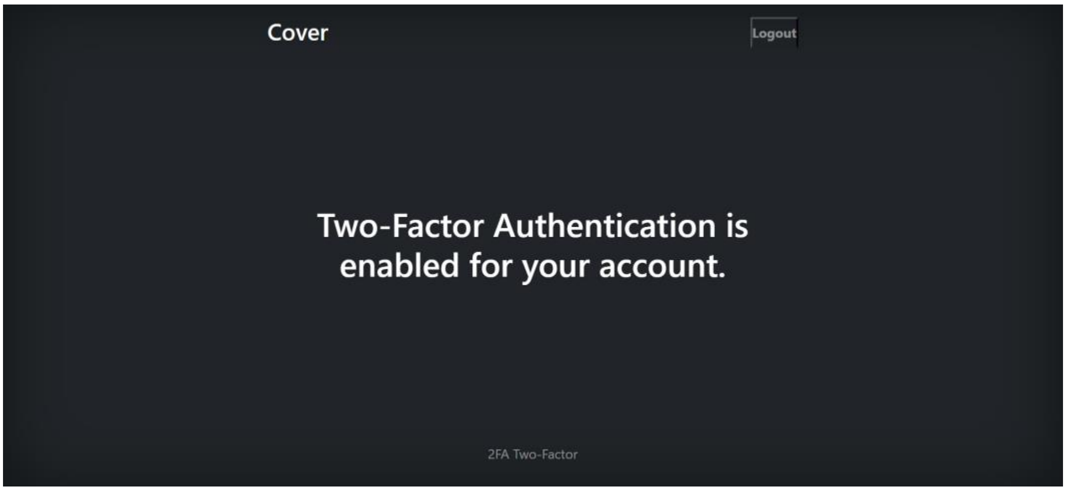
Two-Factor Authentication required.

Enter the code from Google Authenticator:

Fig. 9: Two-Factor Authentication Verification

4.6. Verification Results Page

The verification results page displays an interface informing you that Two-Factor Authentication (2FA) has been enabled for the user account. Two-Factor Authentication is a security method that requires two steps of verification to ensure that only authorized users can access the system. By enabling 2FA, users must enter a dynamic verification code generated by an application such as Google Authenticator, in addition to their email and password. The displayed message confirms that the 2FA activation process was successful, so the user account is now protected by an additional layer of security. The results of the two-factor authentication verification results page can be seen in Figure 10.

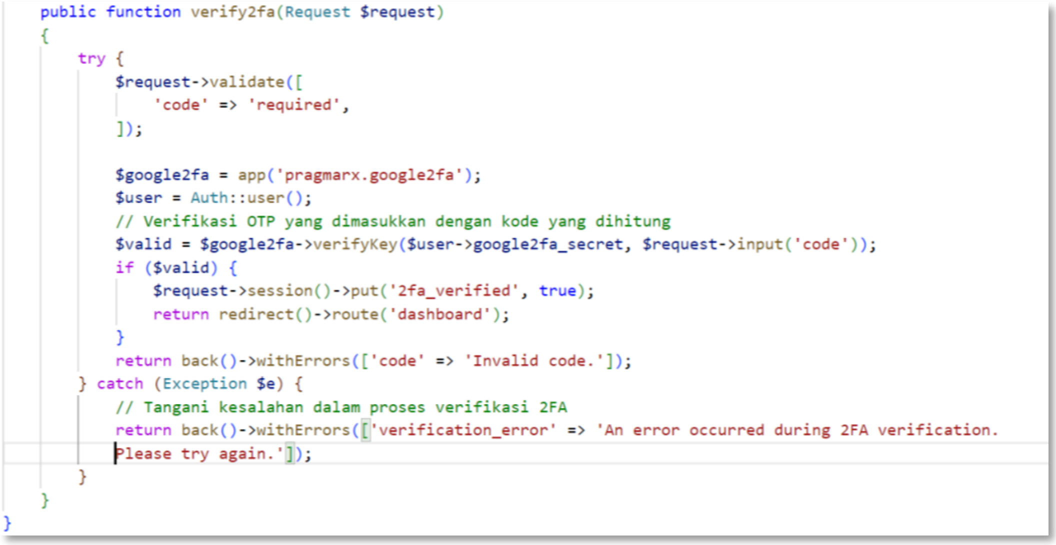


Two-Factor Authentication is enabled for your account.

Fig. 10: Verification Results Page

4.7. Two-Factor Authentication Implementation

Implementation of the Two-Factor Authentication (2FA) verification process using Google Authenticator in a web-based application. This function receives input in the form of a verification code from the user via the Request object. First, the system validates the code input to ensure that the code has been filled in. Next, the system uses the pragmarx/google2fa library to verify the code entered by the user with a secret code (secret key) stored in the database and associated with the currently logged in user. If the verification code is valid, the system will save the 2FA verification status in the session and redirect the user to the dashboard page. However, if the code is invalid or an error occurs during the verification process, the system will return an appropriate error message. This implementation demonstrates that the Google Authenticator-based 2FA method can be well integrated into the system to improve user access security. The results of the implementation can be seen in Figure 11.



```php
public function verify2fa(Request $request)
{
    try {
        $request->validate([
            'code' => 'required',
        ]);

        $google2fa = app('pragmarx.google2fa');
        $user = Auth::user();
        // Verifikasi OTP yang dimasukkan dengan kode yang dihitung
        $valid = $google2fa->verifyKey($user->google2fa_secret, $request->input('code'));
        if ($valid) {
            $request->session()->put('2fa_verified', true);
            return redirect()->route('dashboard');
        }
        return back()->withErrors(['code' => 'Invalid code.']);
    } catch (Exception $e) {
        // Tangani kesalahan dalam proses verifikasi 2FA
        return back()->withErrors(['verification_error' => 'An error occurred during 2FA verification.
        Please try again.']);
    }
}
}
```

Fig. 11: Two-Factor Authentication Implementation

4.8. Login Time and Error Rate Statistical Testing

To determine whether there was a significant difference between login times before and after the implementation of the Two-Factor Authentication (2FA) system, a statistical test was conducted using the paired t-test method. This test was used because the measurements were conducted on the same subjects under two different conditions: logging in without 2FA and logging in with 2FA. The results of this statistical test can be seen in Table 1.

Table 1: Login Time and Error Rate Statistical Testing

Condition	Average	Std Dev	Number of Tests
Without 2FA	2.11 detik	0.13	10
With 2FA	4.49 detik	0.22	10
	Hasil Paired t-Test	**t= -21.8**	**p = 0.00001**

Table 1 the test results using the paired t-test statistical test, obtained a t value = -21.8 with a p-value = 0.00001. The p value is much smaller than the significance limit of 0.05 indicates that there is a statistically significant difference between login times before and after the implementation of Two-Factor Authentication (2FA). A negative t value indicates that login times increased after the implementation of 2FA, because the reduction was carried out in the order "without 2FA minus with 2FA". This result shows that although the implementation of 2FA increases login duration, the increase is a natural impact of the additional security process required in the two-step authentication system, and is statistically significant.

4.9. Usability Evaluation

To assess the usability of the system built with the implementation of Two-Factor Authentication (2FA) based on Google Authenticator, a test was conducted using the System Usability Scale (SUS) method. This method consists of 10 statements assessed by users using a Likert scale of 1–5, which is then calculated into a usability score ranging from 0 to 100. This test involved 20 respondents who were students from the Department of Information and Computer Technology, who had previously tried the login system directly with 2FA. The results of the SUS score calculation can be seen in Table 2.

Table 2. Usability Evaluation

Respondents	SUS Score
20	85.1

Based on the SUS test results, an average usability score of 85.1 was obtained. According to SUS interpretation standards, a score above 85 is included in the "very good" category, indicating that the system is very easy to use and provides a positive user experience. Although the implementation of Two-Factor Authentication (2FA) slightly increases the login process time, it does not reduce the overall user experience. Thus, it can be concluded that from a usability perspective, the implemented application-based two-factor authentication system is not only user-friendly but also very suitable for use as an additional layer of security.

4.10. Risk Evaluation and Fallback Solutions

The implementation of a Two-Factor Authentication (2FA) security system, in addition to the benefits offered in increased account protection, also presents several technical and non-technical risks that need to be evaluated. These risks include the possibility of users losing access to the authenticator device, the device being damaged, or the user forgetting to back up their key. Therefore, it is important to design a fallback solution or recovery mechanism so that users can still access the system securely if they encounter these obstacles. The risk evaluation and proposed fallback solution can be seen in Table 3.

Table 3: Risk Evaluation and Fallback Solutions

No	Risk	Impact	Fallback Solution
1	User loses smartphone containing Authenticator	Can't login	Use the backup codes provided initially
2	Authenticator app deleted or factory reset	OTP data loss	Account synchronization via Google account (if available)
3	Didn't save backup key when first registering	Can't recover account	Educate users to save and print backup keys
4	OTP code from the application has expired	Temporary login failure	Wait for new code (new OTP appears every 30 seconds)
5	Dual devices, OTP not synced between devices	Validation failed	Use one primary device or resynchronize time

Table 3 risks in implementing 2FA include lost devices, deleted apps, and forgetting to save backup keys, which can result in user login failures. Fallback solutions such as backup codes, account synchronization, and user education are in place to ensure access remains secure and available in the event of issues.

5. Conclusion

The conclusions drawn after going through the design and testing stages are as follows.

1. The website security system implementation using the Google Authenticator-based Two-Factor Authentication (2FA) method was successfully implemented effectively in the user login process. This system provides an additional layer of security through dynamic, time-based validation of One-Time Password (OTP) codes. Although it increased the average login time from 2.11 seconds to 4.49 seconds, the usability test results using the System Usability Scale (SUS) method showed an average score of 85.1, which falls into the very good category, ensuring the system remains easy to use for users.

2. Based on the black box test results, the system performed according to its expected functionality without any significant bugs or system errors. Across all tested scenarios, the system's functional success rate reached 92.31%, while the non-conformity rate was only 7.69%. This demonstrates that the implementation of Google Authenticator-based two-factor authentication not only improves security but also operates stably and reliably within the operational context of the website login system.

Reference

[1] A. Khaidar, M. Azzanna, R. Rahmad, A. Hasibuan, M. Daud, and N. Nurdin, "Information Systems and Information Technology Strategies in the EMIS (Education Management Information System)," *Journal of Artificial Intelligence and Software Engineering*, vol. 5, no. 3, 2025.

[2] A. A. Fauzi, S. Kom, M. Kom, B. Harto, I. M. Dulame, P. Pramuditha, and S. T. ST, *Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0*. Indonesia: PT. Sonpedia Publishing, 2023.

[3] A. Fricticarani, A. Hayati, I. Hoirunisa, and G. M. Rosdalina, "Strategi pendidikan untuk sukses di era teknologi 5.0," *Jurnal Inovasi Pendidikan dan Teknologi Informasi (JIPTI)*, vol. 4, no. 1, pp. 56–68, 2023.

[4] S. Azizah, Z. N. Ula, D. Mutiara, and M. P. Prameswari, "Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya," Akuntansi dan Teknologi Informasi, vol. 17, no. 2, pp. 221–237, 2024.

[5] R. D. N. I. Sari, M. Istan, and H. Hendrianto, "Pengaruh Transformasi Sistem Keamanan dan Penggunaan Teknologi Baru Terhadap Serangan Siber pada Data Nasabah," Doctoral dissertation, Institut Agama Islam Negeri (IAIN) Curup, 2025.

[6] L. Judijanto, Y. P. Pasrun, T. B. Rohman, I. G. I. Sudipa, R. Selviana, I. D. G. A. Pandawana, and N. G. Permata, *Sistem Informasi: Teori dan Penerapannya di Berbagai Bidang*. Indonesia: PT. Sonpedia Publishing, 2025.

[7] Z. K. Kadir, "Kejahatan berbasis identitas digital: Menggagas kebijakan kriminal untuk dunia metaverse," *Jurnal Litigasi Amsir*, vol. 12, no. 2, pp. 124–137, 2025.

[8] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-layered multi-factor authentication using decentralized blockchain in an IoT environment," *Sensors*, vol. 24, no. 11, p. 3575, 2024, doi: 10.3390/s24113575.

[9] V. Papaspirou, M. Papathanasaki, L. Maglaras, I. Kantzavelou, C. Douligeris, M. A. Ferrag, and H. Janicke, "A novel authentication method that combines honeytokens and Google Authenticator," *Information*, vol. 14, no. 7, p. 386, 2023, doi: 10.3390/info14070386.

[10] P. T. Tran-Truong, M. Q. Pham, H. X. Son, D. L. T. Nguyen, M. B. Nguyen, K. L. Tran, L. C. P. Van, K. T. Le, K. H. Vo, N. N. T. Kim, T. M. Nguyen, and A. T. Nguyen, "A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis," *Journal of Systems Architecture*, vol. 162, p. 103402, 2025, doi: 10.1016/j.sysarc.2025.103402.

[11] T. Aprilia, B. S. Pitoyo, A. Fauzi, R. G. Ramadhanti, R. D. Nurazizah, E. T. Wanti, and A. R. Prasetyo, "Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial," *Madani: Jurnal Ilmiah Multidisiplin*, vol. 2, no. 5, 2024.

[12] R. S. Baidury, L. Kamajaya, and Fitri, "Two Factor Authentication (2FA) pada Pengunci Panel Box Menggunakan Face ID & Radio Frequency Identification (RFID)," *Kohesi: Jurnal Sains dan Teknologi*, vol. 3, no. 4, pp. 57–67, 2024.

[13] M. Z. Siregar, N. F. I. E. Trisna, R. Alya, Z. Z. Nasution, M. Yusuf, and N. Harahap, "Penerapan Autentikasi Dua Faktor untuk Keamanan Data Pribadi di Instagram: Perspektif Mahasiswa UINSU Stambuk 21," *Triwikrama: Jurnal Multidisiplin Ilmu Sosial*, vol. 6, no. 7, pp. 41–50, 2025, doi: 10.6578/triwikrama.v6i7.9683.

[14] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," *Digital Health*, vol. 9, May 2023, Art. no. 20552076231177144, doi: 10.1177/20552076231177144.

[15] A. Hannan, F. Hussain, N. Ali, M. Ehatisham-Ul-Haq, M. U. Ashraf, A. Mohammad Alghamdi, and A. Saeed Alfakeeh, "A decentralized hybrid computing consumer authentication framework for a reliable drone delivery as a service," *PLoS One*, vol. 16, no. 4, p. e0250737, Apr. 2021, doi: 10.1371/journal.pone.0250737.