 ISSN:2302-8149
e-ISSN:2540-9719

Security of School Financial Transaction Applications with the Implementation of Two-Factor Authentication Method

[1]Novi Hardiansyah*, [2]Rima Aulia, [3]Angelina Hadriani
[1,2]Teknologi Rekayasa Perangkat Lunak, Politeknik Bisnis Digital Indonesia
[3]Sistem Komputer, Universitas Pamulang
[1,2]Jl. Raya Cileungsi No.KM 3, Cileungsi Kidul, Kec. Cileungsi, Kab. Bogor, Jawa Barat 16820
[3]Jl. Suryakencana No.1, Pamulang Bar., Kec. Pamulang, Kota Tangerang Selatan, Banten 15417
*e-mail: nvhardiansyah@gmail.com

(***received*:** 3 December 2024, ***revised*:** 14 March 2025, ***accepted*:** 25 March 2025)

Abstract

Financial transactions over the internet often become targets of cyber attacks that can harm users in conducting transactions due to negligence from both the system and human error. This research will focus on the security level of the SIKOLAH financial application, where every school financial transaction will be conducted online. In this study, the Two-Factor Authentication (2FA) method will be implemented, ensuring that each user has official access with data in the database registered in the application. The results of implementing this method have successfully validated user data through verified email and WhatsApp numbers to send OTP codes to the access holder's smartphone via the official WhatsApp channel of the application manager. Avoiding server phishing actions also limits the OTP code delivery time to no more than 300 seconds to send the OTP code to users, thereby reducing the risk of data interception by cybercrime.

Keywords: two-factor authentication, cyber security, payment system, one-time password (OTP)

1 Introduction

In the rapidly advancing era of digitalization, electronic payment systems have become an integral part of various aspects of life, including in the educational environment. This aligns with the development and implementation of policies to strengthen and expand the use of ICT (Information and Communication Technology) in the field of education [1]. Schools are currently adopting online-based payment systems for various needs, such as tuition fees, extracurricular activity costs, and the purchase of school supplies, which are conducted online to facilitate school financial record-keeping and provide accurate and real-time information to the school's finance department. However, as the reliance on online systems increases, the risk of cyber security also rises. Cyberattacks such as hacking and data theft have become serious threats that can result in financial and reputational losses for educational institutions [2].

One of the main challenges in the security of school payment systems is protecting sensitive data such as personal information of students and parents, as well as financial transaction data. Successful cyberattacks can result in fund misuse, identity theft, and disruption of school operations. Therefore, better efforts are needed to enhance the security of the school payment system.

This research aims to analyze and evaluate the implementation of the Two-Factor Authentication (2FA) method as an effort to enhance the security of the school financial payment system. Specifically, it identifies existing security vulnerabilities in the school financial payment system, designs a 2FA implementation model that meets the school's needs, and evaluates the effectiveness of 2FA in improving the security of the payment system [3].

The results of this research are expected to make a significant contribution to raising awareness about the importance of cybersecurity in designing financial applications that are highly sensitive to hacking, thereby providing room to offer solutions to cybercrime, in order to minimize the theft of sensitive identity data within a system or application [4]. In addition, the findings of this research can serve as a reference for schools and business actors such as PT. Niozone Group, which provides educational application development services, particularly in the school education sector, in designing and implementing a more secure payment system, with application design standards using the implementation[5].

 ISSN:2302-8149
e-ISSN:2540-9719

2 Literature Review

Previous literature on the implementation of Two-Factor Authentication (2FA) often involves sending OTP codes primarily via SMS to users. This practice has led to OTP theft by attackers through physical access to devices, such as mobile malware that steals SMS OTP messages [6]. This attack often occurs by exploiting the micro-USB [7], which also aims to use the interface that is generally common on the micro-USB port used on smartphone devices.

In the previous context, the implementation of 2FA has also been widely applied in finance-based applications as a protection for data and non-cash transaction processes. but also utilizes OTP code delivery services using Telegram. Based on field reviews, the implementation of delivery through Telegram is still not familiar to users, making it difficult for them to understand OTP code verification in this school financial application [8].

In this study, there is an adjustment in the implementation of the 2FA model, specifically one of the variables in the model utilizing the sending of verification codes using an SMS gateway from the database server, which usually incurs costs for the user. However, this time the author will utilize WhatsApp as the medium for sending verification codes or OTP codes through direct authentication applications, which no longer impose verification process costs on the user.

3 Research Method

McCabe explains that Two-Factor Authentication (2FA) is a process that strengthens the authentication system, playing a crucial role in providing a higher level of protection by extending security levels, making it more difficult for attackers to successfully authenticate unless they have legitimate access to directly connect in the authentication process on devices or applications. This way, the application can respond in the user database, where users are already registered in the system as individuals who are indeed entitled to access and manage data in the system according to their access level [9].

This research conducts an analysis by referring to issues found during the implementation of the school financial payment application. The researchers observed indications where each user, especially those managing academic data in this application, sometimes considers passwords to be very simple and easy to remember, believing that this does not endanger the financial data in the application, which may eventually experience a financial data breach. Some of the causes of this are the lack of double authentication in an application, so only accounts that have access can perform and manage data in the application [10].

3. 1 The process of implementing Two-Factor Authentication

The analysis was conducted by referring to the issues found during the implementation of the school financial payment application. The researchers observed indications where each user, especially those managing academic data in this application, sometimes consider passwords to be very simple and easy to remember, believing this does not endanger the financial data in the application, which may eventually experience a financial data breach [11]. Several causes of this issue include the lack of two-factor authentication in an application, so only accounts with access can perform and manage data within the application [12].

Before implementing Two-Factor Authentication (2FA) on this school financial recording application, the researcher needs to develop the flow of the 2FA implementation. In this process, the researcher utilizes 3 important records in the database and ensures that this data has been verified by the application beforehand, namely email or tokenID as the primary account identity, password, and active WhatsApp number of the user [13]. The researcher also limits user parameters to superusers and parents of students, with the aim of securing the Authentication process, which is at risk of being hacked by cyber disturbances. The flow of the implementation process can be seen in the diagram in Figure 1 below.

 ISSN:2302-8149
e-ISSN:2540-9719

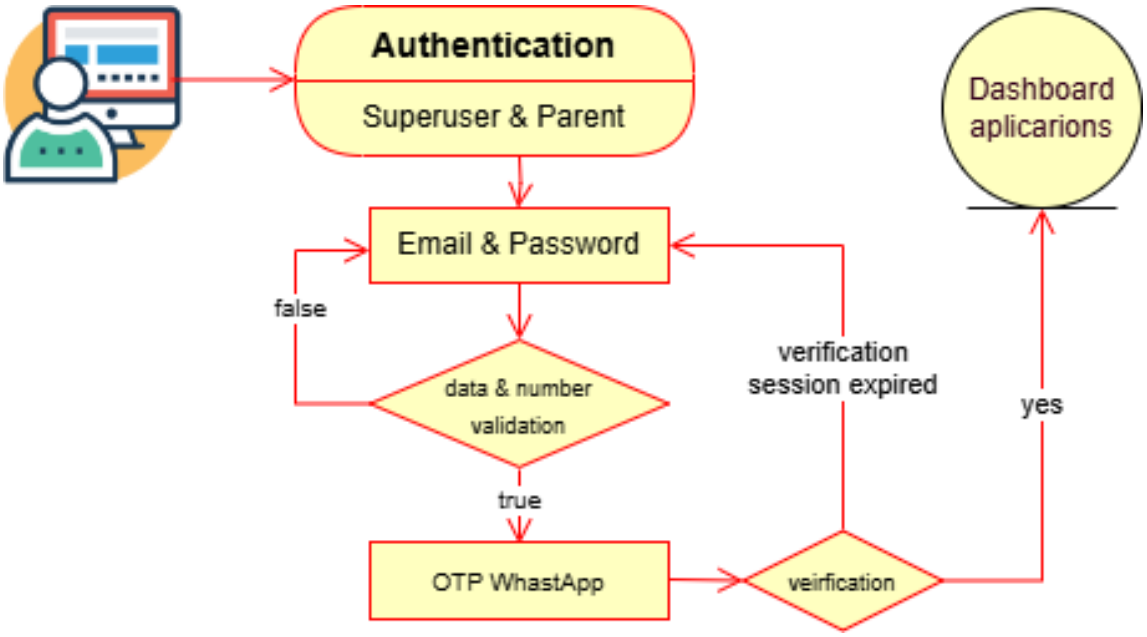

Figure 1. Diagram proses authentication

3. 2TOTP Server Management

To avoid delays in the delivery of OTP codes sent via WhatsApp, the researchers implemented and secured a cloud server that will reduce delays and improve the accuracy of the time it takes for users to receive the Time-Based One-Time Password (TOTP) code. In this study, the server requires approximately 5–10 seconds, so the system will continue to run and will not experience prolonged downtime [14]. The results of the server testing show that this application essentially has 2 active and passive servers to avoid issues in the application's continuous operation. The measurement results can be seen in Table 1 below.

Table 1. Pengukuran Availability Server

Server Up	Up Time (s)	Down Time	Availability
1. Stand Alone	15:18:00	08:42:00	63,75%
2. Dual Storage Cluster	23:59:55	080:00:05	99,99%

Based on the measurement results above, the researcher can conclude that the login process performed by users will be placed on the Dual Storage Cluster server to send the Time-Based One-time [15] Password (TOTP) code faster, as it experiences a downtime of 5 seconds, resulting in an uptime of 23 hours, 59 minutes, and 55 seconds [16].

4 Results and Analysis

From the results of the Two-Factor Authentication (2FA) implementation testing on the SIKOLA School Financial Payments Application, the next step is to analyze the process of implementing this method directly on the application, and several stages that need to be re-evaluated based on the findings of this research.

In the testing process, which needs to be limited in this study, the implementation of 2FA only includes a few access rules, namely the accounts of student parents and superusers or school operators only. The process of sending the OTP code will involve a third party using the RestAPI OneSender, which is an unofficial WhatsApp sender service.

In the blueprint for the design of this application, there are 3 forms of 2FA processes used, but the researcher only focuses on OTP notifications using WhatsApp and does not implement Biometric and Student ID Card designs as shown in this figure.

 ISSN:2302-8149
e-ISSN:2540-9719

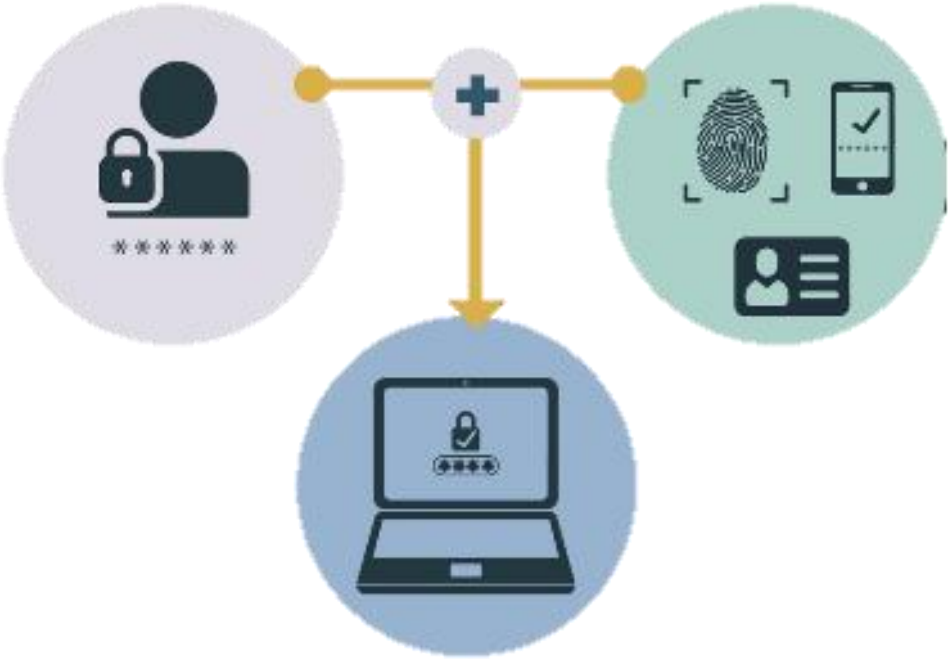

Figure 2. Design authentication proccess

4. 1Data presentation

Based on the figure above, the data that will be loaded in the implementation of 2FA is in the first stage of inputting the username or email data and the account password according to the user's data, and verifying the user's WhatsApp number to send the OTP code to the registered user's number, which is the second stage of the login process in the SIKOLAH application system. In the implementation or security testing process of the application, the author has limited the testing parameters only to the data needed as shown in the table of authentication process requirements for the SIKOLAH application.

Table 1. Pengukuran availability server

Server Up	Up Time (s)
User Data Verification	Yes
validate whatsapp user number	Yes
OTP Code delivery accuracy time	Yes
OTP Code Verification Limit 5 OTP	Yes
Code Verification Limit	Yes

4. 2Two-Factor Authentication process testing

At this stage, the author will present the results of testing the Two-Factor Authentication method for this application, by conducting tests on the school operator user account, under the Superuser access rule.

First, perform the Access data verification process on the database to ensure that the Superuser account at IBS Utsmani Cileungsi school is correctly registered in the application database. This will require validating the email and password data registered in the application and in the database. By entering the email and password on the application login page as shown in figure 3 below.

 ISSN:2302-8149
e-ISSN:2540-9719

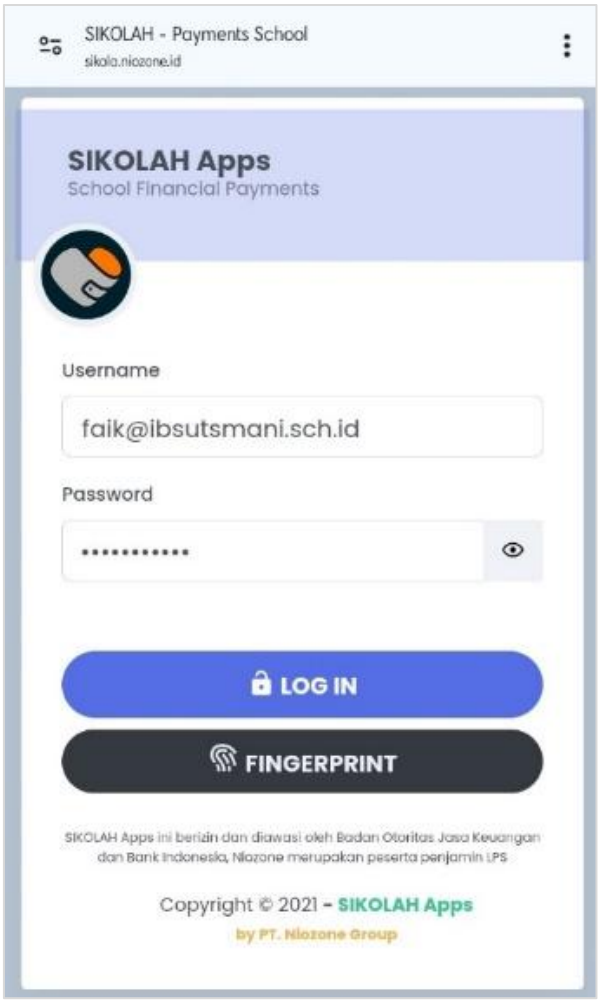

Figure 3. Logins superuse school

After the application validates the data to verify that the data is registered in the application database, the application will automatically check the WhatsApp number associated with this Superuser account, allowing it to proceed to the next step of sending the OTP code to the WhatsApp number registered as the user. The measure of success of this process can be seen in figure 4 below.

Figure 4. OTP code sent to whatsapp

 ISSN:2302-8149
e-ISSN:2540-9719

The next process is to input the OTP code that has been received in the user's WhatsApp into the application. Automatically, the verified account will be redirected to the OTP verification page as shown in figure 5 below

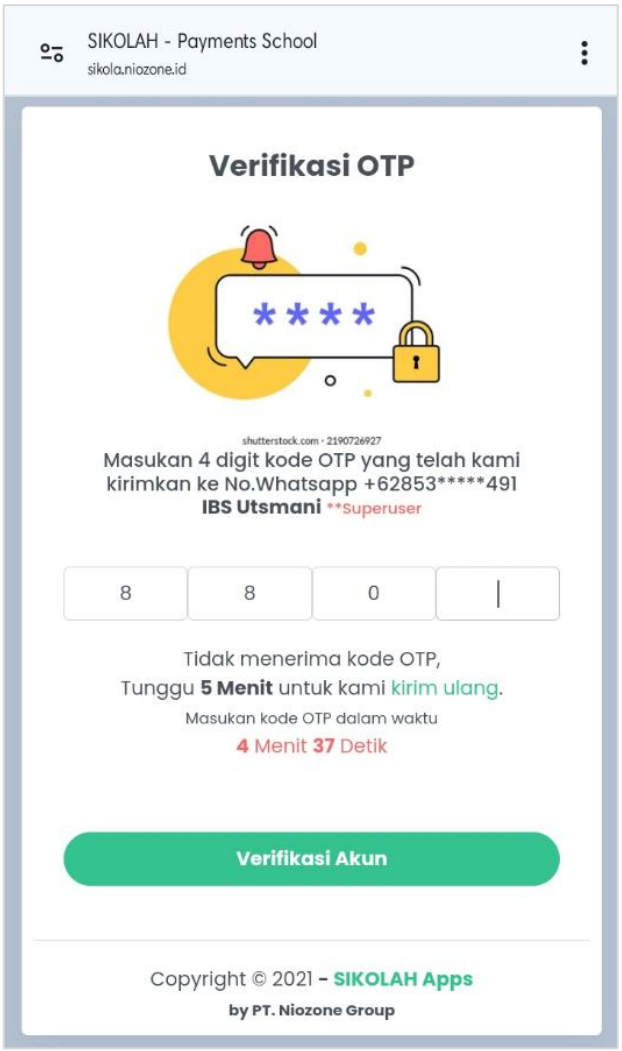

Figure 5. Verify OTP code on the application

Note for users: The input time should not exceed 300 seconds or 5 minutes. This duration is considered because there are sometimes delays in the OTP code delivery process due to weak user networks, and the Rest API process for reading and sending data. Therefore, the author has set a longer duration. This process can be expedited for security considerations to avoid phishing by users with malicious intent

4. 3TOTP Server Management

Reducing the failure rate at this testing stage, the author also established several rules for validating failures in the login process. This stage aims to avoid the issues previously described that are caused by external service providers, such as slow network connections, user negligence due to taking too long to respond to the OTP verification code, exceeding the verification session time of 300 seconds or 5 minutes.

a) If the OTP code verification process fails or the input session times out, the user will be redirected back to the login page to start the login process from the beginning.
b) Provide a new OTP code if the login process fails or is delayed.

The initial login process aims to inform the application users that they are required to re-enter the first and second processes, as shown in Figure 6 below.

 ISSN:2302-8149
e-ISSN:2540-9719

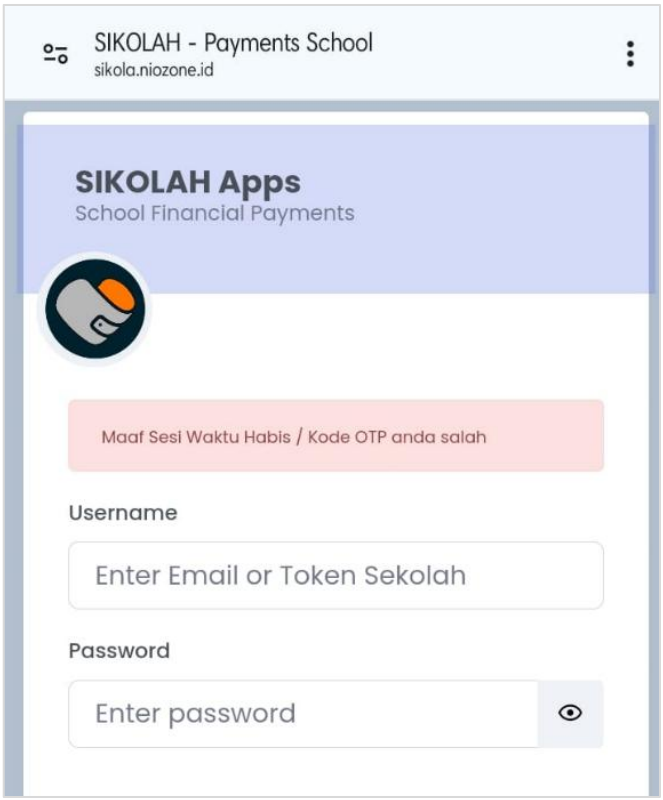

Figure 6. Repetition process and login failure information

This is the user interface when the login process fails or there is a disruption in the application. At this stage, it is categorized as successful in the implementation of the looping flow. The author also experienced that a session timeout that is too long would endanger the failure process and risk hackers taking advantage of this extended time for SQL Injection on this SCHOOL application.

5 Conclusion

The implementation of Two-Factor Authentication (2FA) in applications has proven to provide a significant additional layer of security in protecting user data from various cyber threats. By requiring users to provide two forms of identity verification, 2FA effectively reduces the risk of unauthorized account breaches.

In this trial, it successfully reduced the phishing process by cybercrime, where the server with a short time span sends OTP codes via users' WhatsApp in no more than 300 seconds. and successfully performed initial validation for identifying emails that have been verified in the database, making it easier for the application to recognize legitimate users on this application.

Dependence on the performance infrastructure of 2FA is highly reliant on the stability of the infrastructure, application servers, and the cellular networks of application users. Future development is recommended to upgrade to Multi-Factor Authentication (MFA) so that fingerprint biometrics can be applied as a second login option for users.

Reference

[1] Tim Kemdikbudristek, “Rencana Strategis Kementrian Pendidikan dan Kebudayaan 2020-2024,”Kementeri. Pendidikan, Kebudayaan, Ris. dan Teknol., pp. 1–129, 2020, [Online]. Available: https://dikti.kemdikbud.go.id

[2] N. N. K. Sari, S. Geges, N. Hasanah, “Penerapan Sistem Notifikasi Chat dan Payment Gateway pada Sistem Informasi Pembayaran SPP berbasis Website,” Jurnal Teknologi Informasi, vol. 17, no. 1, Jan, pp. 2656-0321, 2023.

[3] G. C. Mahardhika and F. David, “Implementasi Two Factor Authentication (2FA) pada Sistem Keamanan Otentikasi User di Aplikasi Kasir Legends Barbershop,” Jurnal Sistem dan Teknologi

 ISSN:2302-8149
e-ISSN:2540-9719

Informasi (Justin), vol. 8, no. 4, p. 357, 2020, doi: 10.26418/justin.v8i4.42247
[4] Hardiansyah, Novi. "Penggunaan Metode Extreme Programming pada Perancangan Sistem MYDOSEN." Jurnal Edik Informatika Penelitian Bidang Komputer Sains dan Pendidikan Informatika 10.2 (2024): 67-77.
[5] V. D. Slavov and S. A. Jalil, “Smart Financial Management for Cooperatives: A Web and Payment Gateway Integration Approach,” vol. 3, no. 1, pp. 16–36, 2025
[6] Setiawan, A., & Kamajaya, R. M. A. (2024). Implementasi SMS-based One-Time Password Stealing Attack pada Akun Aplikasi Android menggunakan Digispark Atitiny85. Info Kripto, 18(1), 15-23.
[7] Sunaringtyas, S. Ulfa, D. F. Priambodo, and A. Setiawan. "Implementasi Sms-Based One-Time Password Stealing Attack pada Akun Aplikasi Android menggunakan Digispark Atitiny85." (2023).
[8] Ramdhon, M. (2019). Implementasi Two Factor Authentication sebagai Otentikasi Transaksi Non Tunai (Doctoral dissertation, Universitas Muhammadiyah Sukabumi).
[9] McCabe, Charlotte, Althaff Irfan Cader Mohideen, and Raman Singh. "A Blockchain-based Authentication Mechanism for Enhanced Security." Sensors 24.17 (2024): 5830.
[10] Gilsenan, C., Shakir, F., Alomar, N., & Egelman, S. (2023). Security and Privacy Failures in Popular {2FA} Apps. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2079-2096).
[11] Heriyanto, Y., Qalban, A. A., & Mukaromah, I. A. (2022). Pengembangan Metode Login Two Factor Authentication (2fa) untuk Keamanan Sistem Informasi Akademik. Journal of Innovation Information Technology and Application (JINITA), 4(2), 142-150.
[12] R. S. Pressman and B. R. Maxim, Software Engineering A Practitioner’s Approach. McGraw-Hill, 2020
[13] Amsyah, Novri, A. Asmar, and R. Kurniawan. "Monitoring System for Electrical Energy use and Charging Electricity Tokens based on Website and Whatsapp Application." Jurnal Ecotipe (Electronic, Control, Telecommunication, Information, and Power Engineering) 11.1 (2024): 97-106.
[14] Yamkhin, Jambaljav, et al. "Spatial Distribution Mapping of Permafrost in Mongolia using TTOP." Permafrost and Periglacial Processes 33.4 (2022): 386-405.
[15] Mayanda, Deara, et al. "Load Balancing Techniques for Server Clustering in Cloud Environment: Systematic Literature Review." Journal of Renewable Energy, Electrical, and Computer Engineering 4.2 (2024): 173-179.
[16] Supendar, H., & Handrianto, Y. (2019). Teknik Availability Manajemen Server berbasis Clustering. Bina Insani ICT Journal, 6(1), 1-10.