p–ISSN: 2723 – 6609 e-ISSN: 2745-5254
Vol. 6, No. 1, January 2025 http://jist.publikasiindonesia.id/

Designing a Two-Factor Authentication (2FA) System in E-Commerce Applications

Daffa Sholah Islamey[1]*, Joko Sutopo[2]
Universitas Teknologi Yogyakarta, Indonesia
Email: daffasholah26@gmail.com, jksutopo@uty.ac.id
*Correspondence

ABSTRACT

Keywords: system design; two-factor authentication (2fa); android application.

The development of digital technology has given significant changes to human life, especially in the Internet world, the Internet makes it easier for humans to carry out daily activities and work. However, this convenience can also increase the threat of cybercrime. This research aims to implement a security system based on Two-Factor Authentication (2FA) with a One-Time Password (OTP) on Android applications, to protect data from cybercrimes such as Phishing data theft and ransomware. The research method used is the waterfall model, which contains system analysis discussing what is needed in building applications with 2FA and OTP security, system design discusses the system flow that will be applied and created, coding discusses how the backend can run the system flow created, and implementation discusses the application of previous results. The result of the research obtained is that the implementation of Two-Factor Authentication (2FA) using a One-Time Password (OTP) can improve the security of user data by providing an additional layer of security that reduces unauthorized access rights, this also provides a safer experience for application users who implement it.

Introduction

The development of digital technology has flourished in recent years, affecting almost every aspect of human life, from information to the economy, and the latest is the integration of artificial intelligence (AI). The need for internet access today is huge, with almost everyone using the internet for various daily activities, both for social purposes and work that depends on a network connection. (Wiyono & Susilowati, 2018). One of the positive impacts of technology is the ease of access to search for things and knowledge, especially through smartphones, which is increasingly becoming a necessity in daily activities in Indonesia. However, behind these advances, threats to the security of personal data are increasing, especially through cybercrime. (Akhuai et al., 2022).

Cybercrime is a criminal act committed using digital technology, such as the internet and computer devices. One clear example of its impact in Indonesia is the theft of 6 million Taxpayer Identification Number (NPWP) data, including data belonging to the President of Indonesia, which was illegally sold on forums. Cases like this show how important it is to protect personal data in today's digital era (Ilmi et al., 2023).

The security of personal data is not only about the privacy of each person but also their right to control sensitive information, such as names, addresses, phone numbers, and financial data. (Romansky, 2022). Misuse of this data can be detrimental to users, such as fraud, fake account opening, or identity misuse. Therefore, maintaining the security of personal data is very important to minimize the occurrence of data theft.

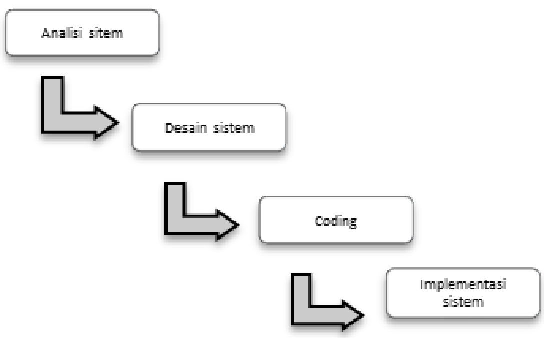
In the face of this challenge, the Two-Factor Authentication (2FA) method with One-Time Password (OTP) is one of the security options that is increasingly adopted. 2FA adds an extra layer of protection by relying not only on passwords but also on unique codes sent via text messages or authentication apps. The combination of 2FA and OTP has been proven to reduce the risk of unauthorized access and improve data security in modern applications. (Alfaruqi et al., 2022).

Previous research has shown the success of 2FA implementation in improving application security. (Taqwim et al., 2021) Implemented the SPECK 128/128 algorithm to encrypt OTPs, so that only authorized users can access the app via OTP sent via SMS. Similarly, another study by (Aprilia et al., 2024). Shows that the combination of 2FA and firewall policies can improve the security of website administrators' page access.

This research aims to design and implement a 2FA-based security system with OTP on Android applications. The system is expected to run smoothly and improve the security of user data by adding a significant layer of protection against data theft or leakage. (Mahardhika & David, 2020). The use of OTPs, which are unique and can only be used once, provides stronger security assurance. (Cahyadi et al., n.d.). Thus, this research seeks to contribute to the protection of personal data in the increasingly evolving digital era.

Method

This researcher uses the waterfall method. The waterfall SDLC software development method is often referred to as a linear sequential model or classic life flow. The waterfall model provides a sequential approach to software life starting from system analysis, system design, coding, and system implementation. (Xu et al., 2017).



Picture 1
Waterfall Groove

Research using this waterfall has several stages, namely the following and its implementation:

1. System analysis, at this stage we analyze the needs that need to be applied to the application.
2. System design, after knowing the needs needed, we make a system design such as the application flow using use cases and activity diagrams.
3. coding, at this coding stage we make a flow like the system flow that has been designed beforehand.
4. implementation, i.e. applying everything that has been done previously from the stage of system analysis, system design, and coding

Results and Discussion

System Analysis

In this stage of system analysis, we examined previous findings to design this 2FA security. Next, we identified weaknesses in the findings. Once all of this is found, the researcher makes a scope of the system to be developed. This involves detailing functional needs, such as the design of the login button, and non-functional needs, such as the ability of the Android chipset to be adequate for downloading apps. This process aims to ensure that system development focuses on measurable and relevant needs.

System Design

System design is the process of planning and determining the structure, components, modules, interfaces, and other features of a system. This design includes the technical and functional aspects necessary to implement the needs that have been identified during the analysis stage. The system design used is a use case diagram and an activity diagram as follows.

Use Case Diagram

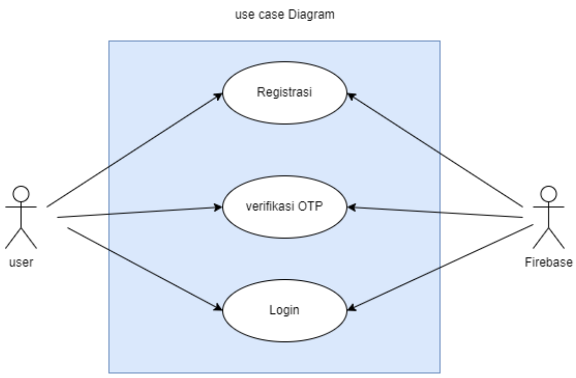
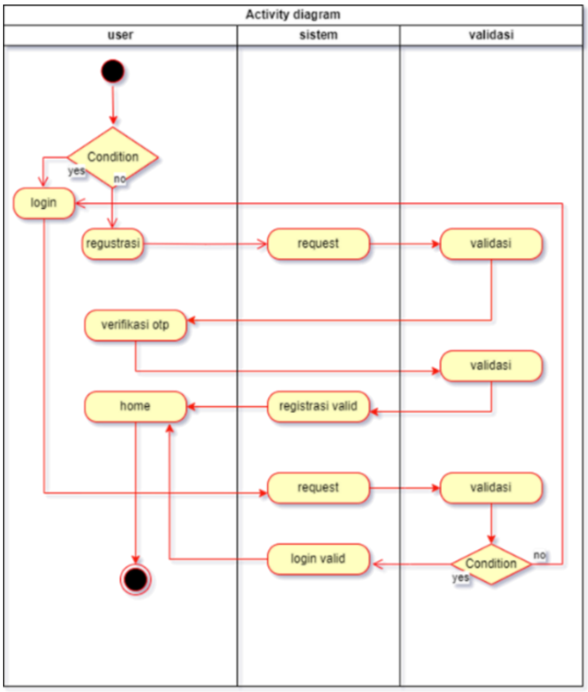


Figure 2 Use Case Diagram

The explanation of Figure 2 use case is the implementation process on the application, the first is that the user registers then Firebase saves the data and then the user is in the command to verify the OTP to add to the security system after successfully registering, while the login takes data from firebase if the data is available or has been registered in the firebase data then the user can log in to the application.

Activity Diagram



Picture 2 Activity Diagram

The explanation from Figure 3 shows that after opening the app, the user will face two conditions. The first condition is that if the user already has an account, they can go directly to the login page. If the user does not have an account yet, then they are required to register first.

At the registration stage, users are asked to fill in data such as email addresses and passwords. Next, the system will ask for approval and send an OTP code via the previously registered email. The user is then asked to verify the OTP code. If the verification is successful, the process will proceed to the main page (home).

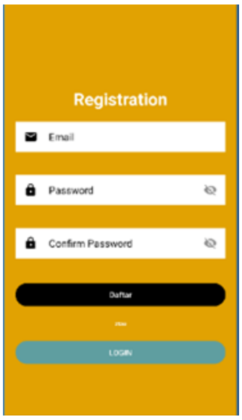
Meanwhile, at the login stage, if the user already has an account, they are allowed to fill in the data that has been registered. If the data entered is incorrect, the user will be prompted to re-enter the data that has already been registered. However, if the data is valid, the user will be immediately redirected to the home page.

Coding

In this coding stage, the researcher is responsible for developing a backend that can execute commands from the application according to the predetermined system design. In addition, it is necessary to create a user-friendly and responsive user interface. The result of this coding process includes the implementation of several features and functionalities that are organized in the system design. By detailing each step and component, researchers can ensure that the results of these coding stages are in line with pre-set needs and expectations. As follows

Registration UI Display

The display on this UI contains an email bar, password, and password confirmation, the user is expected to fill in all the bars correctly, and there is also a signup and login button.



Picture 3
Registration View

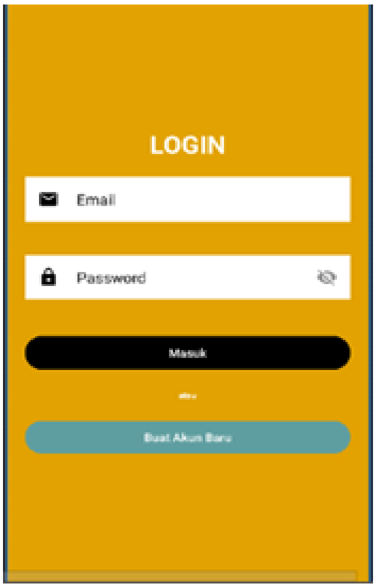
OTP Verification UI Display

The verification user interface includes a verification button and several fields to enter the OTP code that has been sent via email. Users are expected to fill in these fields; If it is not filled in, access to the app will not be available. The importance of filling out this OTP code is to ensure user security and authentication before accessing the application. By filling in the code, users can proceed to the next screen and use the application more safely and verified.

Picture 4
OTP Verification UI Display

Login UI Display

The display in the login section displays a bar similar to the registration process. There is only a difference in the password confirmation section, where the login process does not require login confirmation and OTP code verification anymore. As such, the login process is designed to be simpler and more efficient, minimizing the steps that users must take to access their accounts. By reducing the elements of confirmation and verification, it is hoped that it can increase the convenience and speed of the login process.



Picture 5 Login UI Display

Implementation

In the implementation stage, the application that is made can run in line with what is desired as the registration process functions well from filling in emails, and passwords, then confirming passwords are successfully applied and providing an OTP verification code in the form of 6 digits to continue the otp verification stage, then in the OTP verification process the system succeeds to run the command, namely to enter 6 digits of numbers sent to the email, And during the login session after the registration process and OTP verification was successful, we conducted a trial on the login session, in this login session we entered the email and password to successfully enter the main page of the application, so in this research process we succeeded in implementing 2FA OTP security well, and can prevent data theft because only the account owner or registered email owner can only enter the application.

The results of the research that has been carried out show several successes. First, this application provides a simpler and safer user experience, especially with 2FA OTP protection. This feature not only improves the ease of use of the app but also provides an additional layer of security, thus protecting personal data from the risk of theft. With 2FA OTP, users can feel more confident in the security and integrity of their data when using this application.

Conclusion

This research can successfully implement two-factor authentication with a one-time password. The waterfall method has provided a structured system flow design. Starting from needs analysis to implementation, the results of the research conducted successfully show that the use of 2fa with OTP effectively succeeds in reducing unauthorized access rights. With the application of this technology, users can have a safer experience in using applications, and also keep sensitive information safe, this study, emphasizes the importance of implementing sophisticated security systems to protect data from unwanted things in the ever-evolving digital era and provide a foundation for future researchers in the field of data security and privacy protection. The next suggestion for researchers is to simulate cyber attacks directly so that the use of 2FA with OTP can be structured and proven in dealing with various types of cyber attacks.

Bibliography

Akhuai, W., Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Al Romadhona, R. A. (2022). Social capital of Pancasila education in smart education with social media in cybercrime prevention in the industrial revolution era 4.0. *Jurnal Panjar: Pengabdian Bidang Pembelajaran*, *4*(2), 283–442.

Alfaruqi, R., Alfarisi, S., & Afrizal, T. (2022). Implementasi firebase cloud storage pada aplikasi e-commerce toko ktoys berbasis android. *JRKT (Jurnal Rekayasa Komputasi Terapan)*, *2*(03).

Aprilia, T., Pitoyo, B. S., Fauzi, A., Ramadhanti, R. G., Nurazizah, R. D., Wanti, E. T., Nugroho, M. Y., Shawa, B. N. P., & Prasetyo, A. R. (2024). Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial. *Madani: Jurnal Ilmiah Multidisiplin*, *2*(5).

Cahyadi, I. H., Hidayatullah, M. A., & Ramdan, S. N. (n.d.). *Perancangan Sistem Otentikasi Berbasis One Time Passworsd (Otp) Dengan Algoritma Rsa Sebagai Metode Autentikasi: Implementasi Menggunakan Bahasa Pemrograman Phyton*.

Ilmi, R., Mawarni, I., & Irawan, F. (2023). Peran E-Commerce Pada Ekonomi Syariah Di Era 5.0. *AL-BAYAN: JURNAL HUKUM DAN EKONOMI ISLAM*, *3*(2), 178–189.

Mahardhika, G. C., & David, F. (2020). Implementasi Two Factor Authentication (2FA) pada Sistem Keamanan Otentikasi User di Aplikasi Kasir Legends Barbershop. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, *8*(4), 357–361.

Romansky, R. (2022). Digital age and personal data protection. *International Journal on Information Technologies & Security*, *14*(3), 89–100.

Taqwim, M. A., Kusyanti, A., & Siregar, R. A. (2021). Implementasi Algoritme Speck Untuk Enkripsi One-Time Password Pada Two-Factor Authentication. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *5*(7), 3103–3111.

Wiyono, G., & Susilowati, F. (2018). The Community Perception To Good Governance Implementation Of Village Funds In Bantul Regency. *Journal of Governance and Public Policy*, *5*(2).

Xu, R., Zhang, L., Zhao, H., & Peng, Y. (2017). Design of network media's digital rights management scheme based on blockchain technology. *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, 128–133.