Research Article

Design and Development of Information System Security with Authentication Using One-Time Password Identification Based on SMS with MD5 Hash

[1]Irzon Meiditra, [2]Dori Gusti Alex Candra, [3,*] Rizky Rahmansyah, [4]Fitra Yuda, [5]Alifia Restu Selvanda

[1,4,5] Institut Teknologi Rokan Hilir, Tanah Putih, Rokan Hilir Regency, Riau, Indonesia
[2] Institut Teknologi Mitra Gama, Mandau, Bengkalis Regency, Riau, Indonesia
[3] Universitas Prima Indonesia, Medan Petisah, Medan City, North Sumatra

* Corresponding Author: rizkyrahmansyah@unprimdn.ac.id

Abstract: Login security to access WEB-based applications, in the form of security using OTP (One Time Password) which is generated using Hash MD5 and generates a code sent via SMS. The system will take the email field, password, and phone number. The result of the hash function will produce a 32-digit hexadecimal number. Furthermore, four digits of the hexadecimal number are taken. The four numbers are sent as OTP with Zenziva's Cloud SMS Gateway service and the OTP code will be temporarily stored in the database. The OTP sent to the user will be matched with the one stored in the database table to check its validity. If the OTP sent with the one stored in the table matches, then the user can access the WEB-based application. The OTP generated is for security authentication of the WEB user account after logging in by entering the username and password. Users who enter the wrong OTP 3 times will be blocked, the restriction is to narrow the hackers to intercept and infiltrate.

Keywords: Security, MD5, One Time Password, SMS Gateway, Zenziva

Citation: Rahmansyah, R., Lubis, A., & Batubara, S. (2025). Design and development of information system security with authentication using one-time password identification based on SMS with MD5 hash. *Iota*, 5(2). https://doi.org/10.31763/iota.v5i2.926

Academic Editor: Adi, P.D.P

Received: Maret 14, 2025

Accepted: April 22, 2025

Published: May 29, 2025

1. Introduction

Currently, Advances in computer technology allow thousands of people and computers around the world to be connected in a virtual world known as the Internet. Security issues are one of the most important aspects in the world of information technology, as well as hundreds of organizations such as companies, governments, and even individuals, have made information a very valuable asset. This causes data and information to be very important to protect from information manipulation, information theft, and attacks on information directly or indirectly. On the one hand, information systems are profitable and can improve the performance of all components of the organization, but on the other hand, especially in terms of security, web-based information systems are very prone to being tapped by unauthorized parties. Many methods are often used by hackers to find out the username and password of an account. One of the ways hackers use to find out someone's account information is sniffing. By using this Time Password method the message is sent by means of Multi-channel authentication, which is the process of utilizing more than one communication channel to secure the user's identity. It is now possible to use a connection between a mobile phone and a computer, which can communicate with an authentication server on the Internet for example to initiate the authentication process.

The authentication process. The response to the authentication request can be sent to the user using a Short Message Service (SMS). Sending messages with SMS is easier to implement than receiving messages using 3rd party applications such as Google Authenticator, and Email services. Because users no longer need to install the application to receive the authentication code.

From these problems, this research is focused on designing a login security application for information systems using SMS-based Time Password authentication with MD5 cryptography, which is integrated into a website-based information system. Cryptography aims to provide security services, including security to protect passwords. A good information system is an information system that can be assessed for its level of security, so as to provide comfort for users (Umar, Riadi, & Handoyo, 2019).

The MD5 cryptographic function is used to generate OTP by taking email fields, passwords, user cellphone numbers taken from the user database, and user access time. This web login security design uses PHP programming: Hypertext PreProcessor (PHP) programming, and data storage using MySQL. Based on the description above, the author conducts more in-depth research by taking the title concept, namely "Designing Information System Security with Authentification Using SMS-Based One Time Password Identification with MD5 Hash". The objectives of this research are: [1] Apply the MD5 cryptographic algorithm to design and build the website login page security. [2] To implement an encryption system (Bairwa, A.K & Joshi, S.2021, Shekhawat, H., & Gupta, D.S. 2024, Adeniyi, A.E., et.al.2024) using the One Time Password method into an information system that is built.

2. Theory

2.1 Information System Security and its components

According to G. J. Simons, information system security is how we can prevent fraud (cheating) or, at least, detect fraud in an information-based system, where the information itself has no physical meaning. In addition, information system security can be defined as policies, procedures, and technical measures used to prevent unauthorized access, program changes, theft, or physical damage to information systems. Security systems for information technology can be improved by using techniques and equipment to secure computer hardware and software, communication networks, and data. The security system is also known as authentication. Authentication is a method of certifying that the information is genuine, or that the person accessing or providing the information is the person in question.

Moreover, Passwords can be used for authentication services, which are services related to identification, both identifying the correctness of the communicating parties (user authentication or entity authentication) and identifying the correctness of the message source. Two communicating parties must be able to authenticate each other so that they can confirm the source of the message. Message source authentication also implicitly assures data integrity, because if the message has been modified, it means that the source of the message is incorrect. One one-time password (OTP) is a password that is only valid for a single login session or a single transaction. Unlike the use of static passwords, OTP does not use the same password for each login or transaction, so if an unauthorized party manages to record the OTP password that has been used then he will not be able to misuse the password because it is no longer valid. To be able to create an OTP password, one of the cryptographic methods is used, namely the hash function, and the character selection is randomly selected with a Pseudo Random Number Generator. (Sakti, Agani, & Hardjianto, 2016)

Furthermore, Cryptography is the science of encryption techniques where data is scrambled using an encryption key into something difficult to read by someone who does not have the decryption key. Decryption using the decryption key gets back the original data. The encryption process is done using an algorithm with several parameters. Usually, the algorithm is not kept secret encryption that relies on the secrecy of the algorithm is considered a bad thing. The secret lies in some of the parameters used, so the key is determined by the parameters. The parameters that determine the decryption key are what should be kept secret. (Agung & Prasta, 2018)

In cryptography, you will often find various terms or terminology. Some terms that must be known are: [a] Encryption and Decryption, The process of encoding plaintext into ciphertext is called encryption or enciphering. The process of returning ciphertext to plaintext is called decryption or deciphering. [b] Cipher and Key, Cryptographic algorithms are also called ciphers, which are rules for encryption and decryption, or mathematical functions used for encryption and decryption. Some ciphers require different algorithms for enciphering and deciphering, as can be seen in Figure 1.

Figure 1. Encryption and Decryption Scheme Using Keys

Moreover, MD5 is one of the most widely used hash functions. MD5 is an improved version of MD4 designed by Ron Rivest in 1991. MD5 is commonly used as a checksum to verify the integrity of files downloaded from the internet. MD5 processes the input text into blocks of 512 bits, which are then divided into 16 sub-blocks of 32 bits. The output of the MD5 algorithm is a set of 4 blocks of 32 bits each, which then produces a hash value of 128 bits (Agung & Linda, 2016). SMS Gateway is a communication using SMS that contains information in the form of the sender's cell phone number, recipient, time, and message. This information can be processed and can activate transactions depending on the agreed codes. To be able to manage all incoming transactions, a system is needed that is able to receive a certain number of SMS codes, process the information contained in SMS messages, and carry out the required transactions (Afrina & Ibrahim, 2015). The author will use Zenziva as a Cloud SMS gateway service provider.

Zenziva is an online SMS Center & SMS Masking service. To use Zenziva services, users must register first. There are several SMS package options provided by Zenziva and can be selected by the user depending on the needs of each user. By calling the web service from Zenziva, the system can already use the Zenziva SMS gateway service. API is a software interface that consists of a collection of instructions stored in the form of a library and describes how software can interact with other software. According to (Rama & Kak, 2015) "*In general, the API is a focused expression of the overall functionality in a software module that can be accessed by people who need it in a service-defined way*". An overview of the API and its components is shown in Figure 2. The API categories can be seen in Table 1.

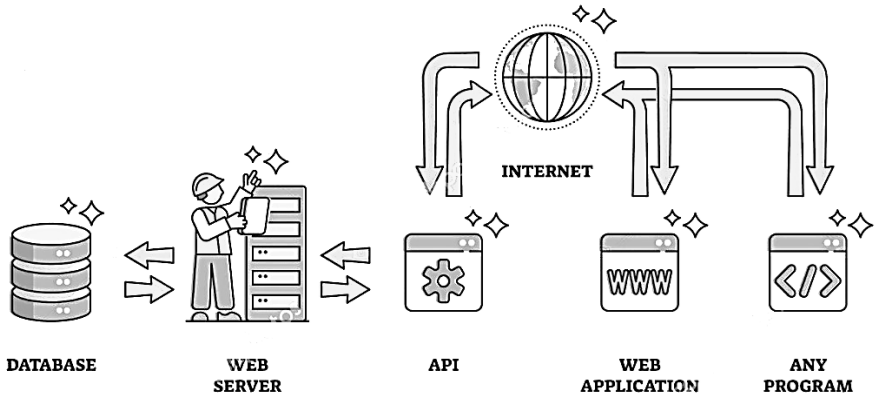

Figure 2. API and connected components

Table 1. API Category

API Category	Descriptions	Example
Operating System	A fire is used for basic functions that can be performed by a computer. Such as I/O processing, and program execution.	API for MS Windows
Programming Languages	An API is used to extend the execution capabilities of a programming language.	Java API
Application Service	APIs that are used to access data and services provided by an application.	API for mySAP (BAPI/Business Application Programming Interfaces)
Infrastructure Service	Used to access the infrastructure of a computer. Infrastructure here is a computer along with peripherals such as storage, applications, and others.	Amazon EC2 (Elastic Compute Cloud) for access to virtual computing and Amazon S3 (Simple Storage Service) for storing large amounts of data.
Web Services	API is used to access content and services provided by a web application.	Facebook Graph API is used to access shareable information.

3. Method

The research stages include the steps of conducting the research from beginning to end. Each research step is described in detail as following Figure 3, There are 3 main components, i.e., Literature Study, Problem Analysis, System Analysis, Need Analysis, Design, and Implementation.

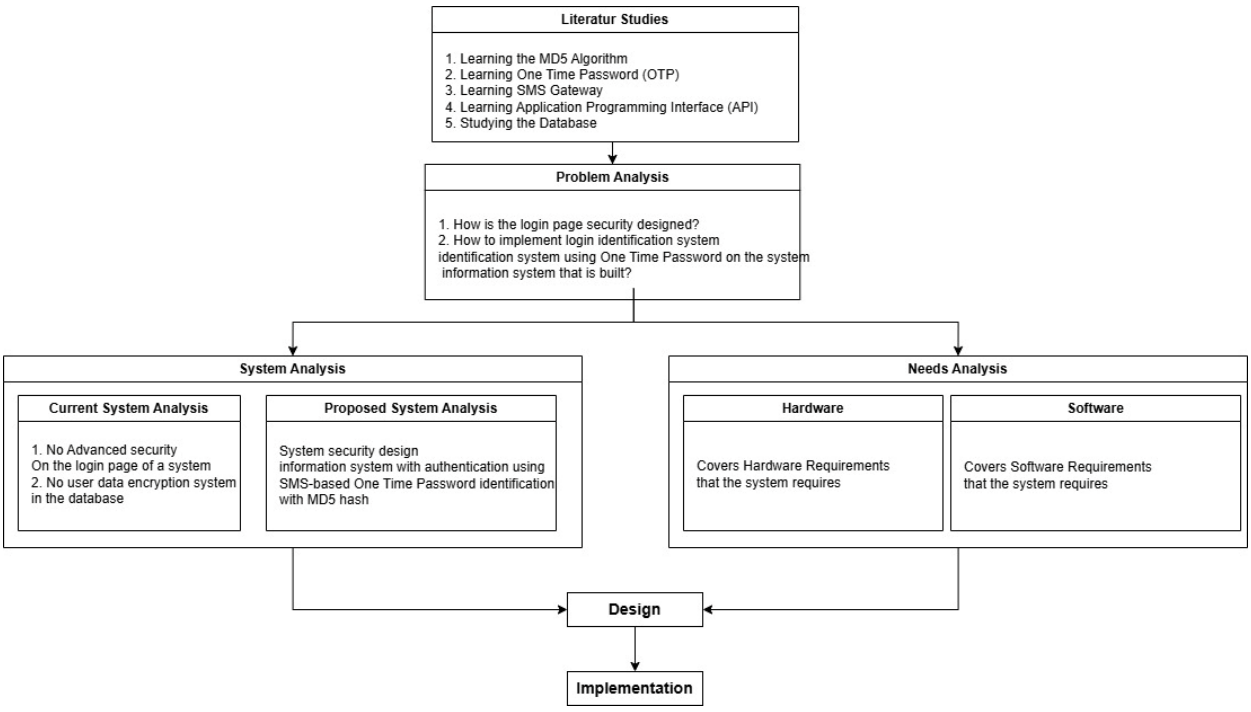

Figure 3. Research Stages

Furthermore, at the Literature Study stage, the author collects all the information needed to build the system. This information can be obtained by the author from various sources by reading the literature contained in journals, articles, books, and theses. At this stage several studies will be carried out, such as studying the MD5 algorithm, One Time Password (OTP), SMS Gateway, Application Programming Interfaces (API), and databases. Moreover, At the problem analysis stage, the author will analyze the problem and collect existing data on the previous system, and then the author will propose several methods to improve the previous system, the method proposed by the author is expected to reduce hacker intrusion into the system, several methods that the author proposes such as, how to design login page security? How to implement a login identification system using One Time Password on the information system being built?

Furthermore, at the stage of analyzing the current system, the author will analyze the security of the current information system and collect existing problems in the previous system. The author conducts experiments on the current system so that the author can collect what weaknesses are found in the current system. At the stage of analyzing the proposed system, the author will propose a better security system than before which only relies on username and password to enter the information system. The author's proposed system is an information system security design with authentication using SMS-based one-time password identification with MD5 hash. At the system requirements analysis stage, the author will analyze the needs of the hardware and software that will be used to build the system. The ongoing flow map can be seen in Figure 4 and the Proposed flowchart in Figure 5.

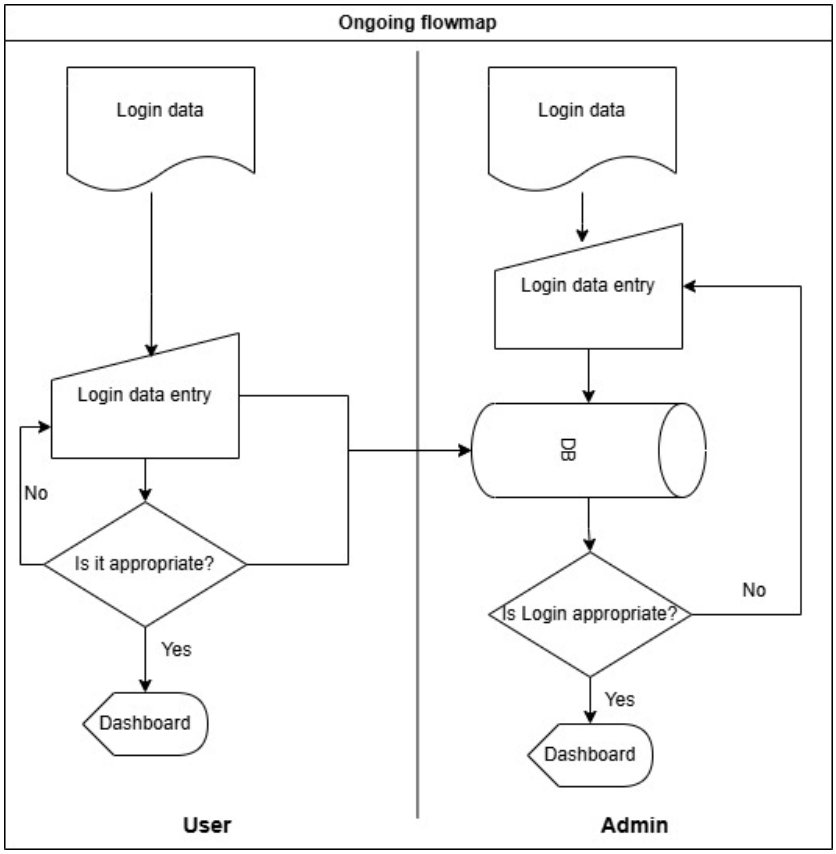

Figure 4. Ongoing flow map

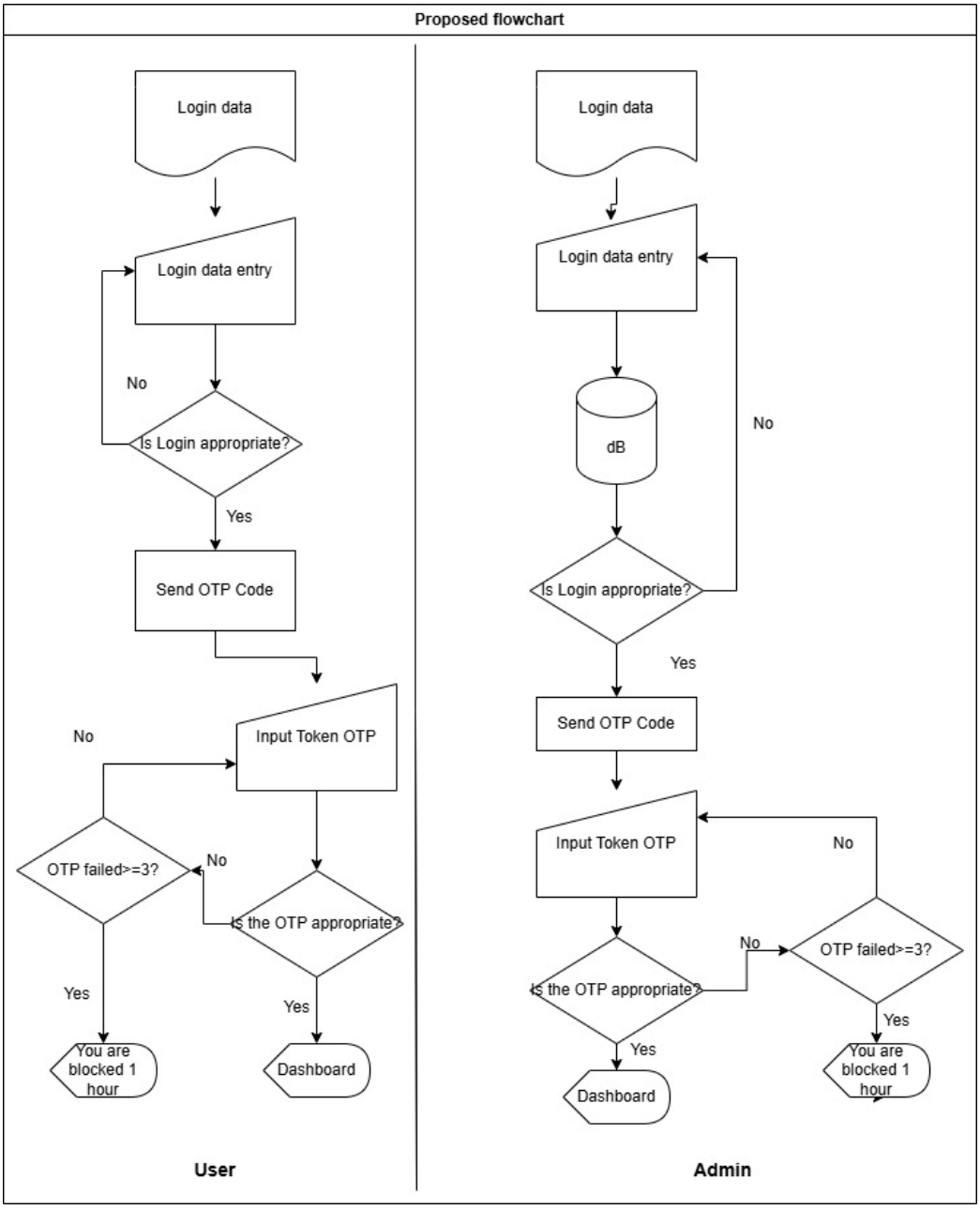

Figure 5. Proposed Flowchart

In the Proposed System Analysis, there are the following steps: [a] The password entered by the user will be encrypted using MD5 hash. [b] The password stored in the database will be encrypted using MD5 hash. [c] In addition to the username and password the user will be asked for a token code that will be sent to the cell phone as a security. and [d] Before entering the main page (dashboard) the user will be directed to the Two Factor Authentication form to be asked to enter the OTP code sent to the user's cell phone via SMS, in detail shown in the Proposed Flowchart in Figure 5.

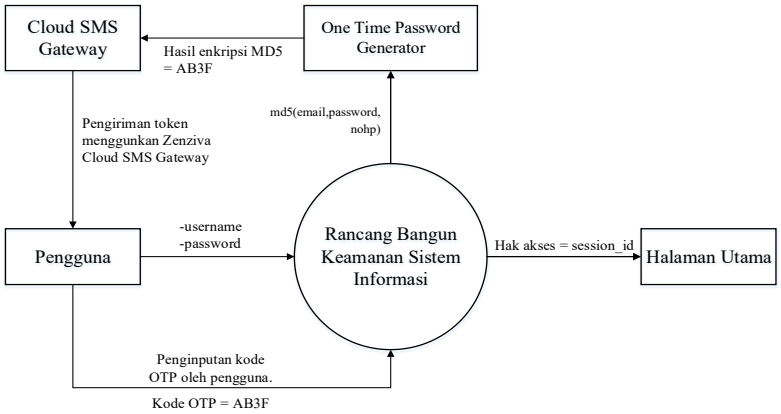

Figure 6. Diagram Context

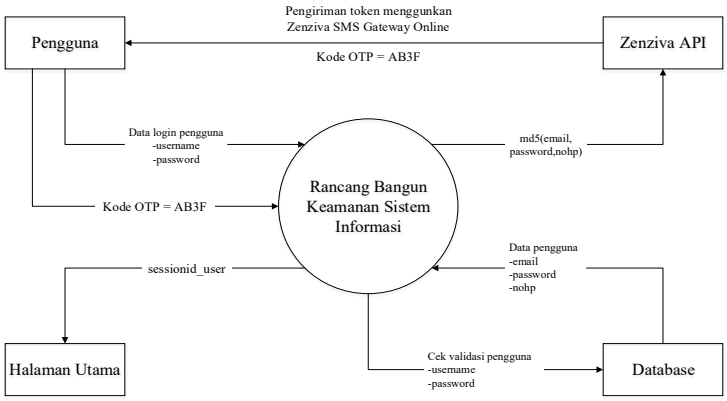

Figure 7. Data Flow Diagram Level 1

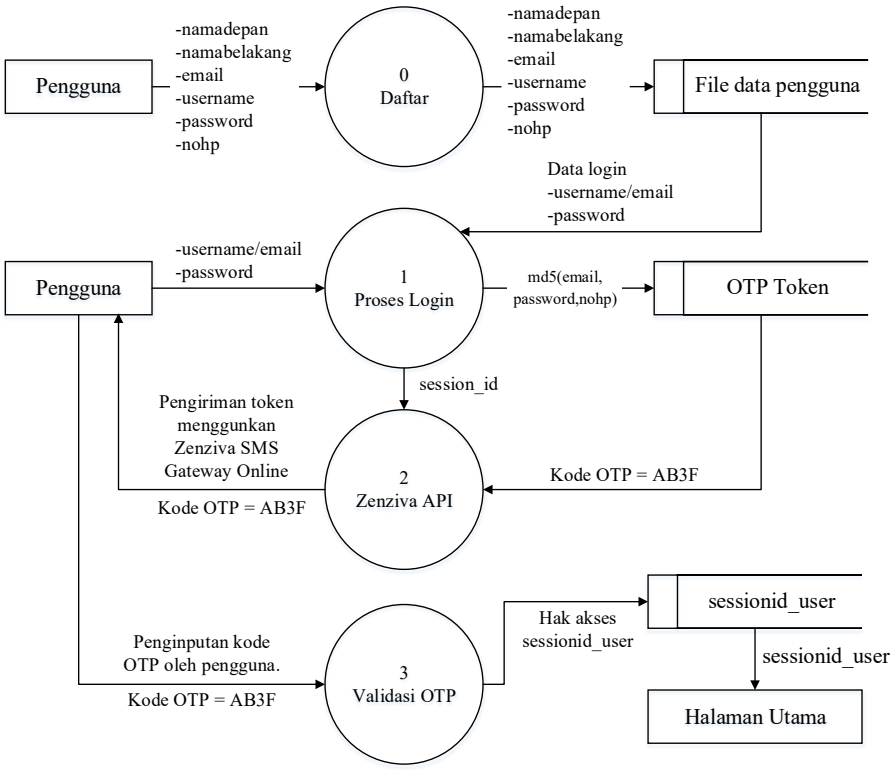

Figure 8. Data Flow Diagram Level 2

Furthermore, A context diagram is a diagram that consists of a process and describes the scope of a system. A context diagram is the highest level of DFD that describes all inputs into the system or outputs from the system and gives an overview of the entire system, This Context Diagram is shown in Figure 6. Next, this level 1 diagram [Figure 7] describes the data fragments from the context diagram. The explanation of the level 1 data flow diagram above is as follows:

a) Users input login data such as username and password.
b) Then the system will validate the data entered by the user. The system will match the data in the database.
c) When validation is complete and the login data is declared suitable, then the system generates an OTP code from a combination of email, password, and user cellphone number.
d) The output of the generated results will be stored in the database and then sent to the Zenziva API Server to be sent to the user's cellphone number.
e) After the OTP code is received, the Zenziva API Server will send the OTP code to the user's cellphone number.
f) The user will receive an incoming SMS in the form of an OTP code.
g) The user will be directed to the OTP code verification form to be asked to input the OTP code received from the SMS.
h) The OTP code sent by the user will be matched with the OTP code in the database.
i) If the OTP code is matched, the user will be directed to the main page (dashboard).

Moreover, this level 2 diagram [Figure 8] describes the data fragments of the level 1 data flow diagram where the processes carried out are the list, login process, zenziva API, and OTP validation. The explanation of the level 2 data flow diagram above is as follows:

a) Users input the data needed for registration such as first name, last name, email, username, password, and cellphone number.
b) The system will input user registration data into the MySQL database.
c) After the registration is declared successful, the user will be directed to the login page.
d) Users input login data such as username and password, users can also use email as a substitute for username at login.
e) The system will validate the username and password entered by the user at the time of login and will match the data in the database.
f) After the validation is complete and the login data matches the one in the database, the system will generate an OTP code using the MD5 algorithm by combining the user's email, password, and cellphone number.
g) The system will send the encrypted OTP to the Zenziva server via API (Application Programming Interfaces) technology.
h) OTP is received by Zenziva and after that, the OTP code will be sent to the user via SMS.
i) i. The user receives an incoming SMS containing the OTP code.
j) j. The user will be directed to the OTP code verification form to be asked to input the OTP code received from the SMS.
k) k. The OTP code sent by the user will be matched with the OTP code in the database.
l) l. If the OTP code matches, the user will be directed to the dashboard.

Furthermore, The initial message or Plaintext will be encrypted using the One-Time Password (OTP) algorithm to produce ciphertext. This ciphertext is generated from a combination of email, password, and cellphone numbers taken from the database. The email, password, and cellphone number are then combined into one string and then MD5 encryption is performed on the string which then produces an output in the form of an

MD5 hash. From the hash obtained, 6 characters are taken which will later be used as a token code or One Time Password (OTP) which will be sent via SMS to the account owner's cellphone number. Here is an overview of the encryption procedure shown in Flowchart Figure 9.

Moreover, the login system procedure is that the user inputs a username/email and password then the system will match the username/email and password recorded in the MySQL database, after the user is verified by the system, a token will be sent to the registered account's cellphone number, then the token is used as a second password to enter the system. Here is the flowchart of the system procedure shown in Figure 10.

The registration system procedure is that the user inputs the first name, last name, username, email and password, and cellphone number then after the user clicks the submit button, the system will check the availability of the username, if the username is entered by the user has been registered, the user will be shown the registration form again, but if the username is available and can be used, the data entered by the user will be inputted into the database with a password that is processed first into an MD5 hash for security purposes. The following is a flow map of the registration system procedure shown in Figure 11.

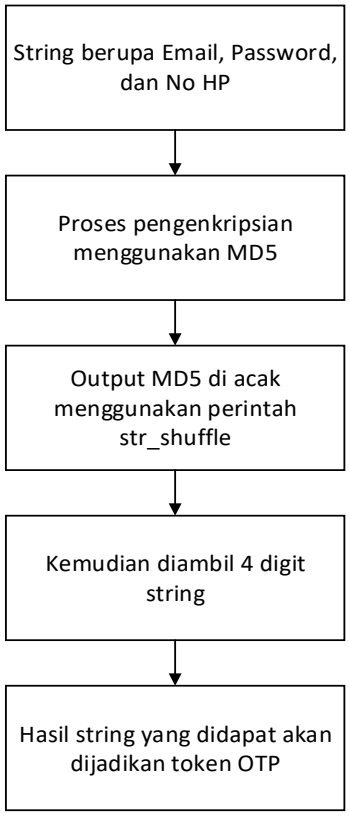

Figure 9. Encryption Procedure Flowchart

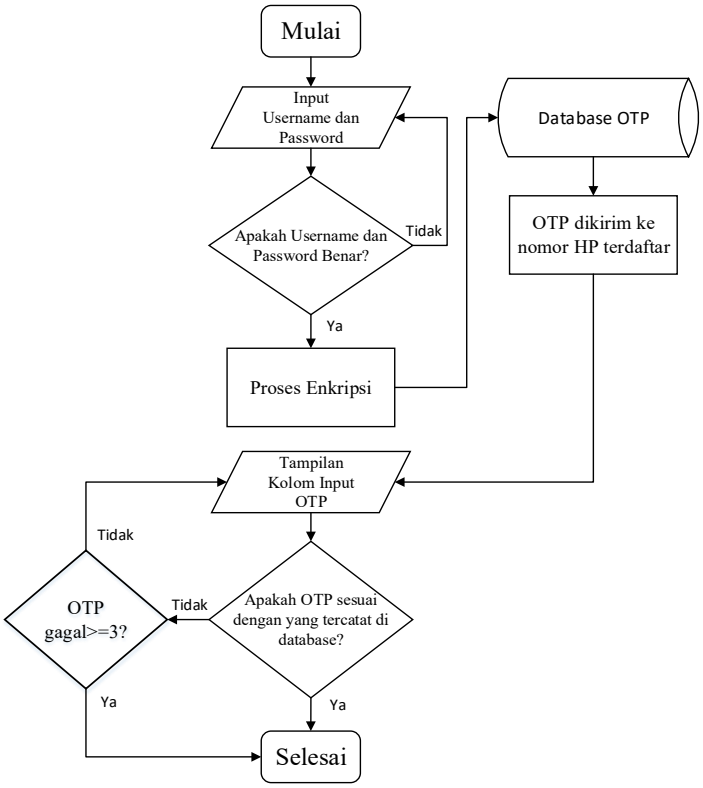

Figure 10. Login Procedure Flowchart

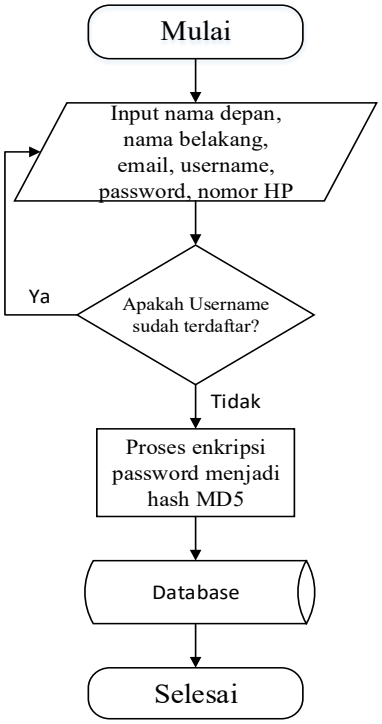

Figure 11. Flowchart of Registration Procedure

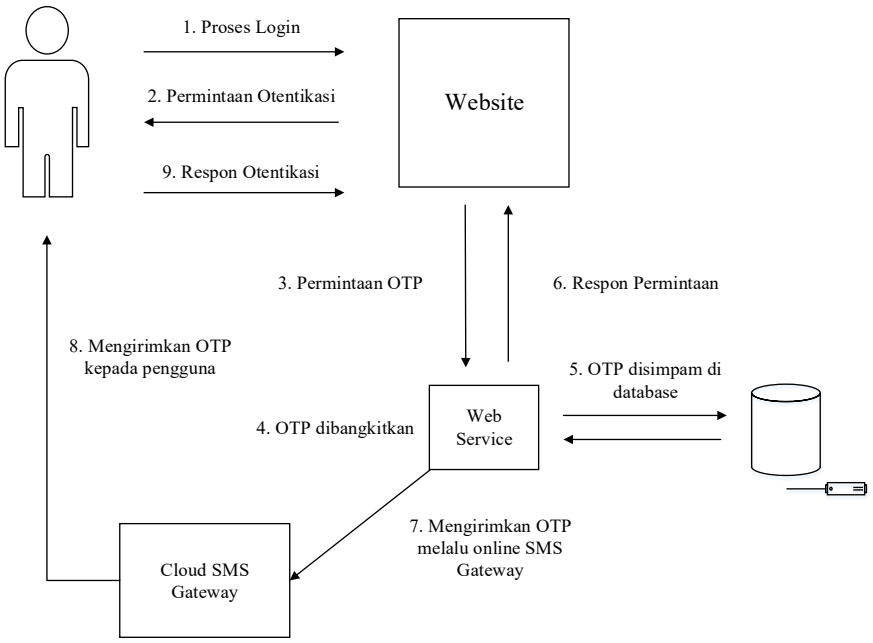

Figure 12. Architectural Design

The design architecture is carried out with the aim of defining the main objectives of the built security system needed to support applications in handling data. This design architecture will explain in general how a security system using One Time Password runs. The following is the design architecture of a security system using a one-time password token as shown in Figure 12.

4. Result and Discussion

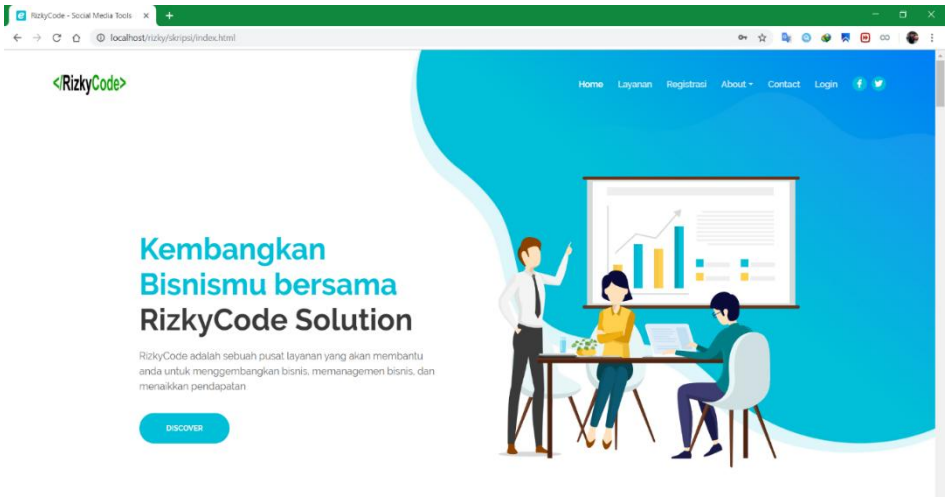

Figure 13. Home Page Display

The implementation of the interface of the information system security design with authentication using SMS-based one-time password identification with md5 hash is an implementation of the interface design described in the previous chapter where the implementation can be seen in Figure 13. The home page display is the display that first appears when a user opens a website. On this display, the author will promote the services and features of the website created.

The registration page view [Figure 14] is a view where users can register themselves as members of a website. Description:

1. Is a text area column where users are required to enter their first name.
2. Is a text area column where users are required to enter their last name.
3. Is a text area column where users are required to enter an active email address, this email will later be used as an identity to log into the system.
4. Is a text area column where users are required to enter an active cellphone number, this cellphone number will later be used by the system to send a one-time password (OTP) code.
5. Is a text area column where in this column users are required to enter a username or username.
6. Is a text area column where users can input a password as an identity when logging into the system.
7. Not much different from text area number 6, in text area number 7, users are also required to enter a password as in number 6. This column only aims to ensure whether the user has entered the password correctly.
8. If all the data is required for registration then the user is asked to press the registration button.

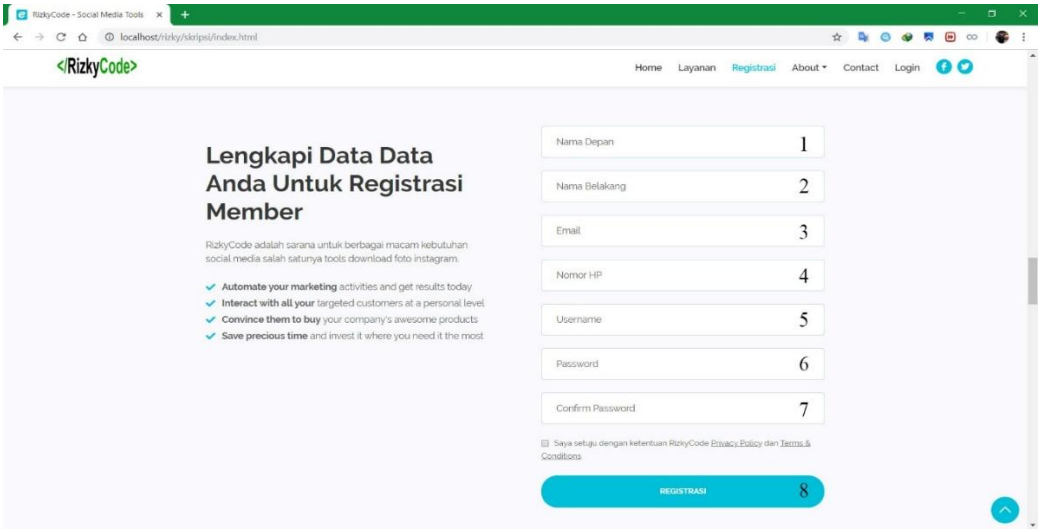

Figure 14. Registration Page Display

Furthermore, The login page can be likened to the gateway into the system. The login page [Figure 15] is a display where users can enter the data needed to enter the system such as email and password. Description: [1] This is a text area where users input the email that has been registered previously. [2] Is a text area where users input the password that has been registered before. and [3] Is a login button that functions when the user has entered an email and password.

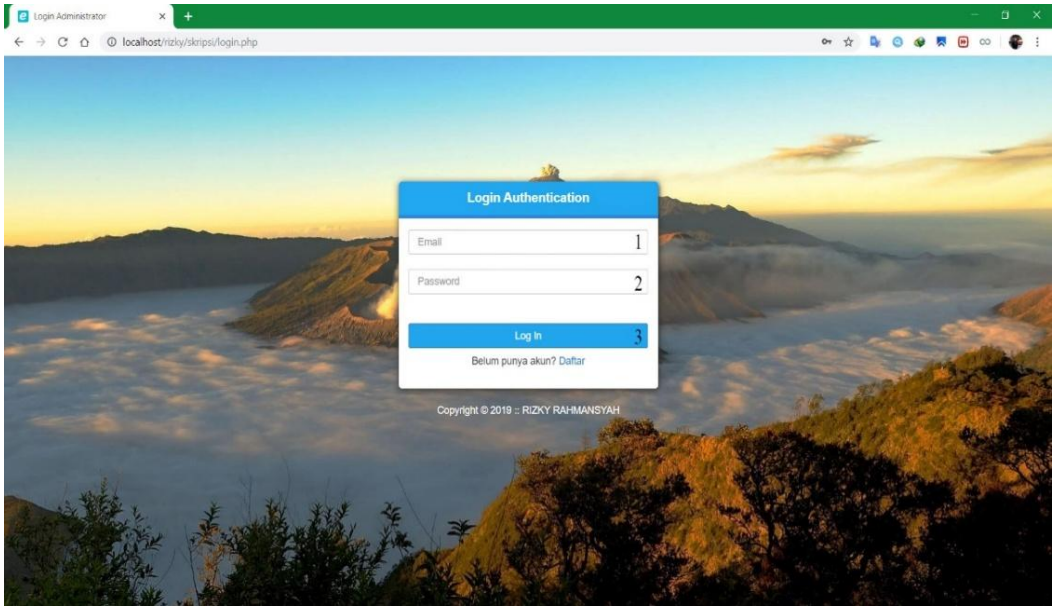

Figure 15. Login Page Display

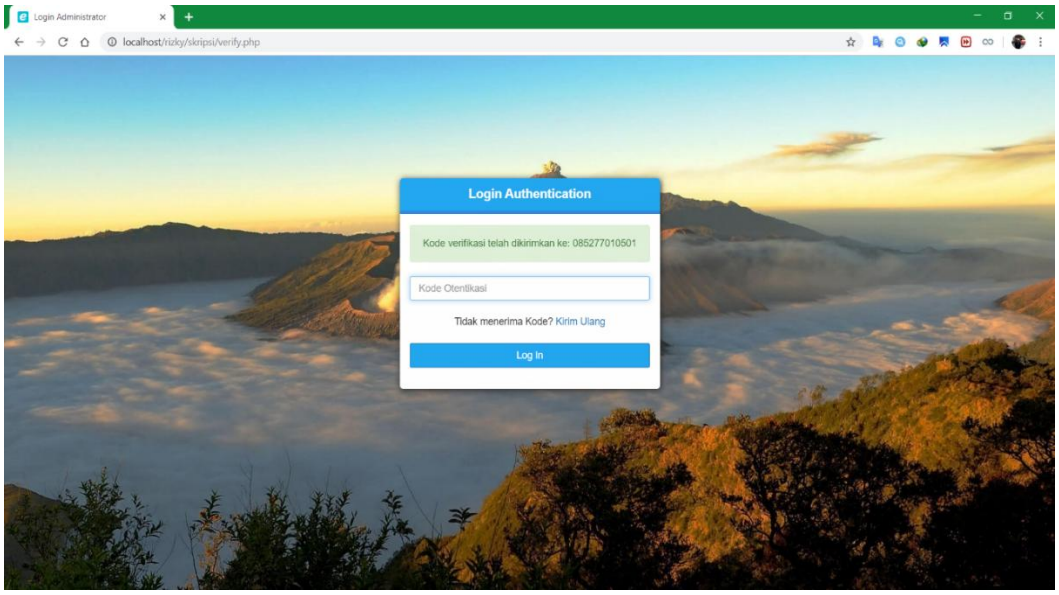

Figure 16. OTP Verification Display

Figure 16 is an OTP Verification Display, The OTP verification page display is the display that appears when the user has passed the login page, at this time the user is asked to input the OTP code sent to the cellphone number. The main page display [Figure 17] is a page where the user has successfully passed the OTP verification page. This page contains the features of the system built, at this time the author provides Instagram photo downloader features and several other menus.

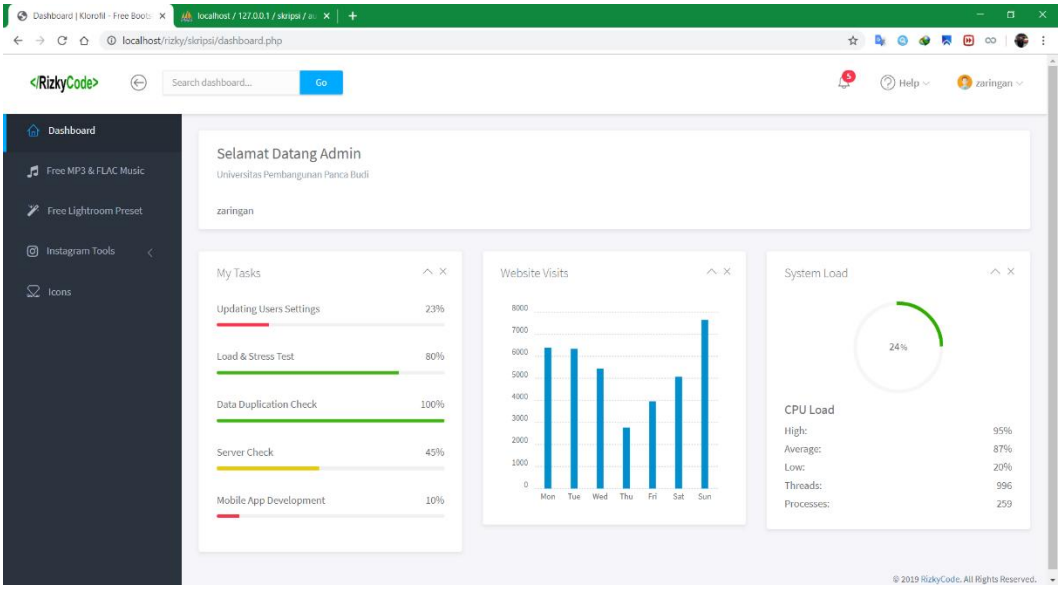

Figure 17. Main Page Display

Furthermore, At this stage will describe the login access test using the email address rizkyrahman2015@gmail.com and password pancabudi as shown in Figure 18. In this test, the email address and password entered by the user to the login page match the email and password listed in the database. Login is declared successful and users will be redirected to the OTP verification form.

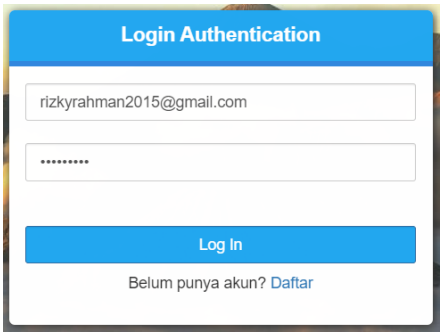

Figure 18. Login Authentication

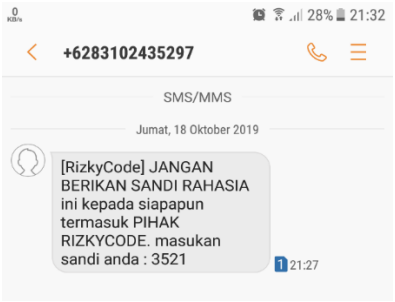

Figure 19. Display of SMS Message Contents

This test will describe the display of SMS contents containing the OTP code. This code will be entered into the OTP input form described in Figure 19. This test shows that the email and password are available and valid in the database and the user will be redirected to the OTP input form. In Figure 20 there is an OTP input form, the user will be asked to enter the OTP code sent to the cellphone number. In this test, the OTP code is: 3521. Figure 21 proves that the OTP code sent via SMS synchronizes with the OTP code in the website database.

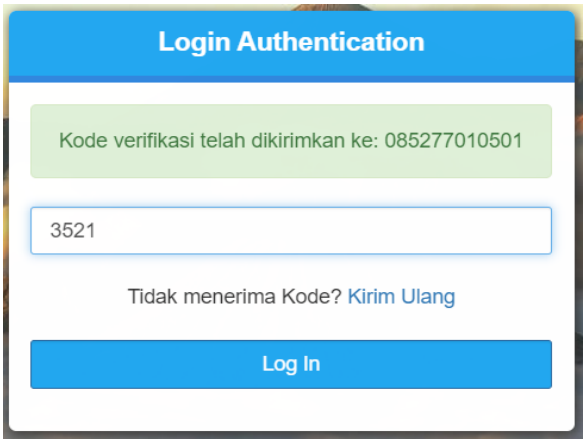

Figure 20. OTP Verification Page Display

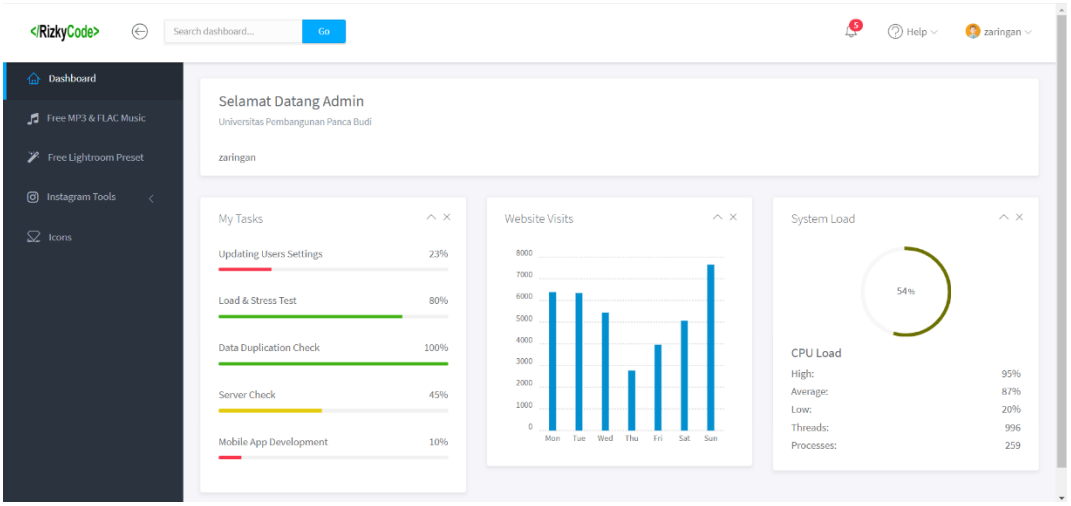

Figure 21. Website display after successful login with OTP code

Moreover, in Figure 22, the "Wrong Email or Password!" popup will appear when the user enters the wrong email or password on the website login page. In Figure 23, a red notification text will appear that reads "Incorrect Verification Code!". This notification appears if the user enters the wrong OTP code. Then Figure 24, At this stage, it will be tested to enter the wrong OTP code 3 times, and a red notification text will appear that says "You are blocked for the next 1 hour!". The user will be blocked and cannot log in during the specified time.

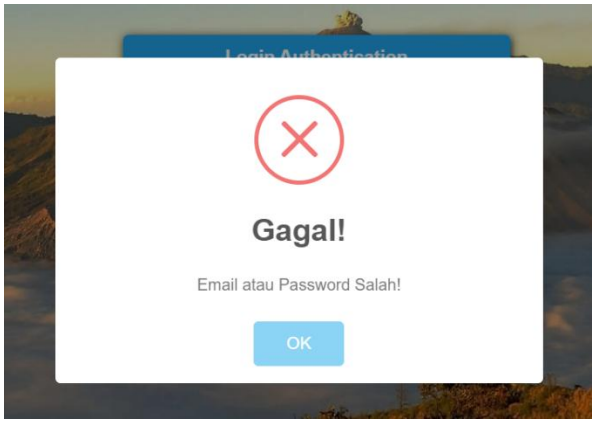

Figure 22. Display when Email or Password is Incorrect

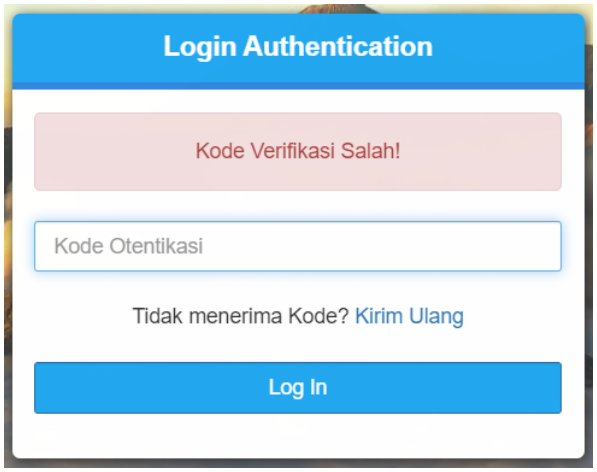

Figure 23. Display When the Verification Code is Incorrect

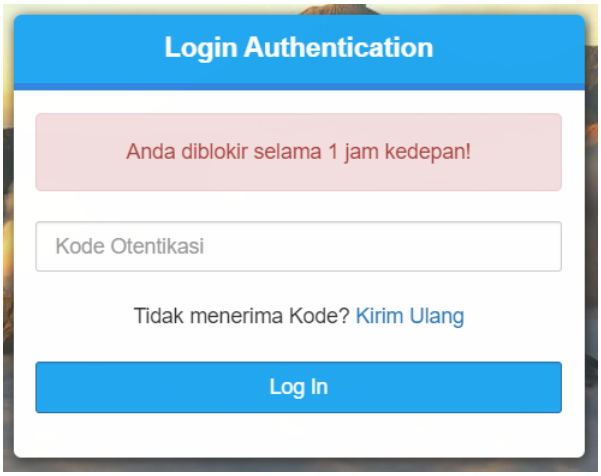

Figure 24. Display when a user is blocked

5. Conclusions

The conclusions obtained from the design of this software are [1] The concept of One Time Password using SMS Gateway can be applied to banks, payment accounts, and online stores where security is vital in that field. [2] This concept is more secure than the usual login system because the password is always changing and the password is sent via another network directly to the user. The disadvantage of this concept is that the delivery time is highly dependent on the network. [3] The thing that needs to be considered in implementing this concept is the delay between when the user requests a password and when the user gets the password via SMS (Short Message Service). Suggestions and improvements from this software development are that this concept can be applied using other tools or media to speed up delivery time (For example: email, special tools such as pagers, etc.).

Acknowledgments: Thanks to all parties in the Department of Computer Systems, Universitas Pembangunan Panca Budi Medan who have helped the author with all the resources provided, hopefully, this research can continue to develop well, especially the discipline of Computer Science which focuses on the field of information system security.

Author contributions: The authors are responsible for building Conceptualization, Methodology, analysis, investigation, data curation, writing—original draft preparation, writing—review and editing, visualization, supervision of project administration, funding acquisition, and have read and agreed to the published version of the manuscript.

Funding: The study was conducted without any financial support from external sources.

Availability of data and Materials: All data are available from the authors.

Conflicts of Interest: The authors declare no conflict of interest.

Additional Information: No Additional Information from the authors.

References

[1] Afrina, M., & Ibrahim, A. (2015). Pengembangan Sistem Informasi SMS Gateway Dalam Meningkatkan Layanan Komunikasi Sekitar Akademika Fakultas Ilmu Komputer Unsri. Jurnal Sistem Informasi, 7(2), 852–864.

[2] Agung, H., & Linda. (2016). Aplikasi Laporan Keuangan Akuntansi Bulog-Jakarta Menggunakan Algoritma MD5 dan RSA.

[3] Agung, H., & Prasta, I. (2018). Implementasi Algoritma Rivest , Shamir , Adleman Untuk File Sharing Pada PT . Sumber Makmur Pangan Sejahtera Berbasis Web. 5(2), 96–102.

[4] Ariawan, J., & Wahyuni, S. (2015). Aplikasi Pengajuan Lembur Karyawan Berbasis Web. Jurnal Algoritma Sekolah Tinggi Teknologi Garut, 5(1), 62–66.

[5] Djahir, Y., & Pratita, D. (2014). Bahan Ajar Sistem Informasi Manajemen. In Bahan Ajar Sistem Informasi Manajemen. Bandung: Informatika.

[6] Hutahaean, J. (2017). Konsep Sistem Informasi. Jurnal Administrasi Pendidikan.

[7] Madcoms. (2016a). Pemrograman PHP dan MySQL untuk pemula. Yogyakarta: Andi.

[8] Madcoms. (2016b). Sukses Membangun Toko Online dengan PHP & MySQL. Yogyakarta: Andi.

[9] Marshall B. Romney, & Steinbart, P. J. (2015). Accounting Information Systems 9th Edition. In African Journal of Microbiology, Research. https://doi.org/10.5897/AJMR12.475

[10] Mulyani, S. (2017). Metode Analisis dan Perancangan Sistem. Bandung: Abdi Sistematika.

[11] Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer, 10(1), 20. https://doi.org/10.30872/jim.v10i1.23

[12] Raharjo, B., Heryanto, I., & Rosdiana. (2015). Modul Pemrograman Web HTML, PHP & MySQL Revisi Kedua. Bandung: Modula.

[13] Rahman, F., & Santoso. (2015). Aplikasi pemesanan undangan online. Aplikasi Pemesanan Undangan Online, 1(2), 78–87.

[14] Rama, G. M., & Kak, A. (2015). Some structural measures of API usability. Software - Practice and Experience. https://doi.org/10.1002/spe.2215

[15] Sakti, D. V. S. Y., Agani, N., & Hardjianto, M. (2016). Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android. Conference: Budi Luhur Information Technology, At Budi Luhur University, Volume: 13 No. 1, 13(1), 1–3.

[16] Shalahuddin, M., & Sukamto, R. A. (2018). Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek Edisi Revisi. In Jurnal Pilar Nusa Mandiri.

[17] Suharyanto, C. E., Chandra, J. E., & Gunawan, F. E. (2017). Perancangan Sistem Informasi Penggajian Terintegrasi Berbasis Web (Studi Kasus di Rumah Sakit St. Elisabeth). Jurnal Nasional Teknologi Dan Sistem Informasi, 3(2), 225–232. https://doi.org/10.25077/teknosi.v3i2.2017.225-232

[18] Sukmaindrayana, A., & Sidik, R. (2017). Aplikasi Grosir Pada Toko Rsidik Bungursari Tasikmalaya. Jurnal Manajemen Informatika, 4(2), 1–158. https://doi.org/10.1017/CBO9781107415324.004

[19] Swara, G. Y., & Pebriadi, Y. (2016). Rekayasa Perangkat Lunak Pemesanan Tiket Bioskop Berbasis WEB. Jurnal TEKNOIF, 4(2), 27–39.

[20] Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). Jurnal Sistem Informasi Bisnis. https://doi.org/10.21456/vol9iss1pp47-54

[21] Bairwa, A.K & Joshi, S.2021. Mutual authentication of nodes using session token with fingerprint and MAC address validation. Egyptian Informatics Journal, Volume 22, Issue 4, December 2021, Pages 479-491. doi. 10.1016/j.eij.2021.03.003

[22] Shekhawat, H., & Gupta, D.S. 2024. Quantum-resistance blockchain-assisted certificateless data authentication and key exchange scheme for the smart grid metering infrastructure. Pervasive and Mobile Computing. Volume 100, May 2024, 101919. doi. 10.1016/j.pmcj.2024.101919

[23] Adeniyi, A.E., et.al.2024.A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. Computers and Electrical Engineering. Volume 118, Part A, August 2024, 109330. 10.1016/j.compeleceng.2024.109330