European Journal of Electrical Engineering and Computer Science
Vol 8 | Issue 2 | March 2024
ISSN 2736-5751

RESEARCH ARTICLE

Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems

Remigius Obinna Okeke[1,*] and Stanislaus Okechukwu Orimadike[2]

ABSTRACT

The objective of this study is to create an advanced cloud computing security system that addresses the security vulnerabilities inherent in existing authentication processes in communication systems. Specifically, the study developed an application-based multi-layer and multi-factor authentication (MFA) program that enhances cloud security measures. The system presented an improved approach to cloud computing security through the implementation of application-based multi-factor authentication (MFA). By leveraging encryption techniques, the system guarantees secure access based on user profiles. These profiles consist of valid usernames, passwords, and token numbers generated by the application. In addition, the system enhances security by integrating the Time-based One-Time Password (TOTP) algorithm (IETF RFC 6238) with location checks, augmenting the overall protection measures. A thorough testing procedure was carried out on the system, with a specific focus on a test web application hosted on the cloud server. The result validated the efficacy of all three authentication factors integrated within the application.

Keywords: Cloud computing, Multi-Factor Authentication (MFA), OTP, security.

Submitted: November 10, 2023

Published: March 07, 2024

10.24018/ejece.2024.8.2.593

[1] *Department of Electrical/Electronic Engineering, University of Port Harcourt, Nigeria.*
[2] *Centre for Information and Telecommunication Engineering, University of Port Harcourt, Nigeria.*

* ***Corresponding Author:***
e-mail: remyokeke17@gmail.com

1. Introduction

Cloud computing simplifies data and program storage and access, replacing reliance on local hard drives with the Internet. The term "cloud" metaphorically represents the vast Internet infrastructure, symbolized as a puffy, white cumulus cloud in earlier depictions. In recent years, cloud computing has become a defining IT trend, revolutionizing businesses and serving as the preferred model for upgrading existing technology infrastructure [1]. It holds a prominent position in the market and enables the integration of advanced technologies such as artificial intelligence, the Internet of Things and others.

Data storage stands out as a prominent service within cloud computing. However, the security and privacy of cloud-stored data have been compromised by various attacks, raising concerns among users [2]. Cloud services alone cannot guarantee crucial security attributes like confidentiality, integrity, identification, and availability [3]. To safeguard against unauthorized data access, user authentication plays a vital role. An effective and trustworthy approach to authentication is essential to avoid issues arising from trust and procedural redundancy. Hence, a suggested MFA (Multi-Factor Authentication) scheme is proposed to strengthen and optimize the authentication process for cloud users [4]. The MFA approach here is based on a secure and user-friendly mechanism using One Time Passwords (OTP) for increased security [5]. MFA offers layered security by requiring users to prove their identities through multiple verification methods, making it harder for attackers to breach the system. Conventional authentication techniques like ID/passwords fall short in the cloud due to frequent attacks, necessitating a well-structured and clearly defined security mechanism.

MFA typically combines knowledge, possession, and inherence factors for authentication. Knowledge factors involve passwords or PINs, possession factors include devices like security tokens or smartphones, and inherence factors comprise biometrics such as fingerprints, facial recognition, or keystroke dynamics. Location and time factors can also be used for additional security measures. While many cloud services have adopted MFA, some systems rely on specialized hardware devices, incurring extra costs for manufacturing and implementation. To address the growing demand for MFA in cloud services,

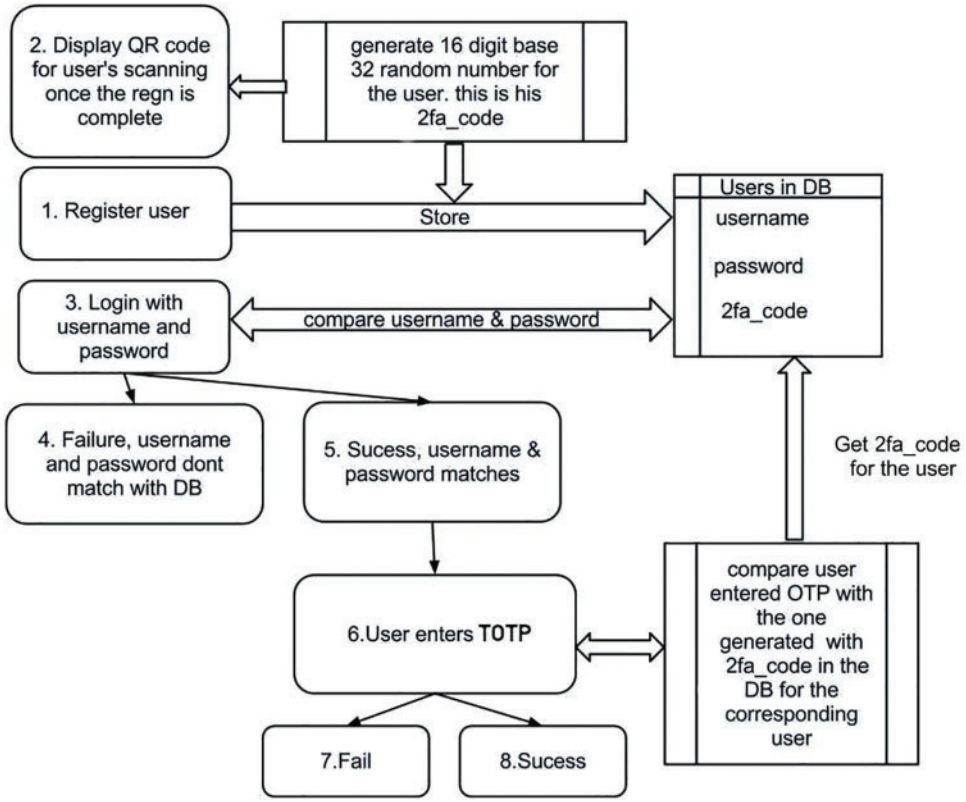

Fig. 1. The proposed system architecture.

a flexible yet robust authentication process is crucial to combat data breaches and thefts by intruders. Existing Two Factor Authentication (2FA) systems from companies like Google and Microsoft have shown vulnerabilities if any of the factors are compromised, leaving users exposed to attackers. This study aims to evaluate and resolve such issues by proposing an MFA system with an added security layer. By doing so, the research strives to enhance the overall security of cloud computing, providing users with increased protection and peace of mind.

2. Design Methodology

The Proposed system introduces an enhanced cloud computing security approach by implementing application-based multi-factor authentication (MFA). The system employs encryption to ensure secure access based on user profiles, which are created using valid usernames, passwords, and token numbers generated by the application. It actively monitors and detects any unauthorized activities, such as incorrect usernames, passwords, or token numbers that could potentially compromise the cloud resources of other users in the environment. To safeguard user credentials, the system incorporates credential hashing technology, preventing even administrators from accessing user credentials.

Moreover, as an added security measure, the system integrates the Time-based One-Time Password (TOTP) algorithm (IETF RFC 6238) along with location verification. It promptly alerts users about security breaches and attempts to bypass security protocols, including unauthorized access from unknown locations not registered in the system's database. In cases where intruders employ brute force attack tools to automatically generate random credentials for unauthorized access, the system can detect and track the IP address associated with such attempts. It keeps users informed about the number of intrusion attempts within a specific time frame. In the event of a potential compromise and unauthorized access to a user's cloud files, the system promptly notifies the user through the application, enabling them to revoke the intruder's access remotely.

2.1. System Design Process and Architecture

This section provides an overview of the design process employed to construct the proposed Multi-Factor Authentication (MFA) system, utilizing Java for implementation and SQLite for storing user information. The mobile application environment is Android Studio, while the server incorporates NodeJS, MySQL, and Redis DB. The frontend user interface is developed using AngularJS 8, and the backend of the service is implemented with NodeJS. Both the web application and the mobile application connect to a RESTful API, as depicted in Fig. 1. MySQL serves as the central database for storing user information and generating authentication keys (tokens). The proposed system architecture, which outlines the process flow, is presented in Fig. 1, while the flow chart is captured in Fig. 2.

2.2. Application Build

This section provides a comprehensive overview of the functioning of the application and outlines the results that users can expect from the proposed solution. The software was developed utilizing programming tools, as elaborated in the preceding section. Both the front end and back end

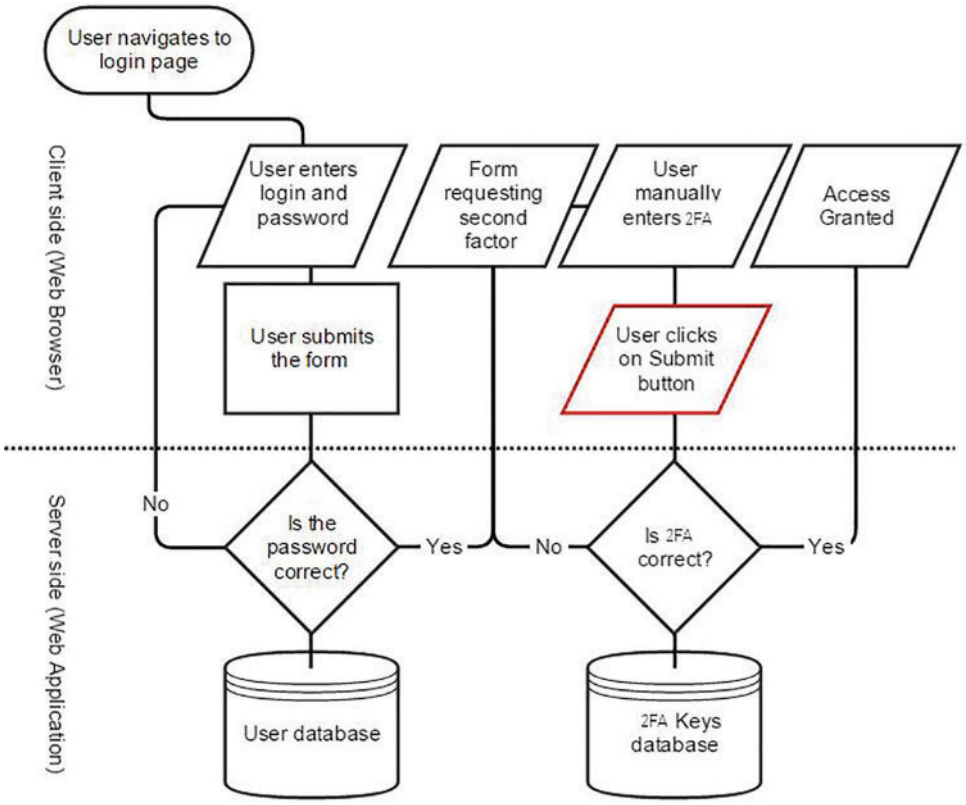

Fig. 2. Proposed system flowchart.

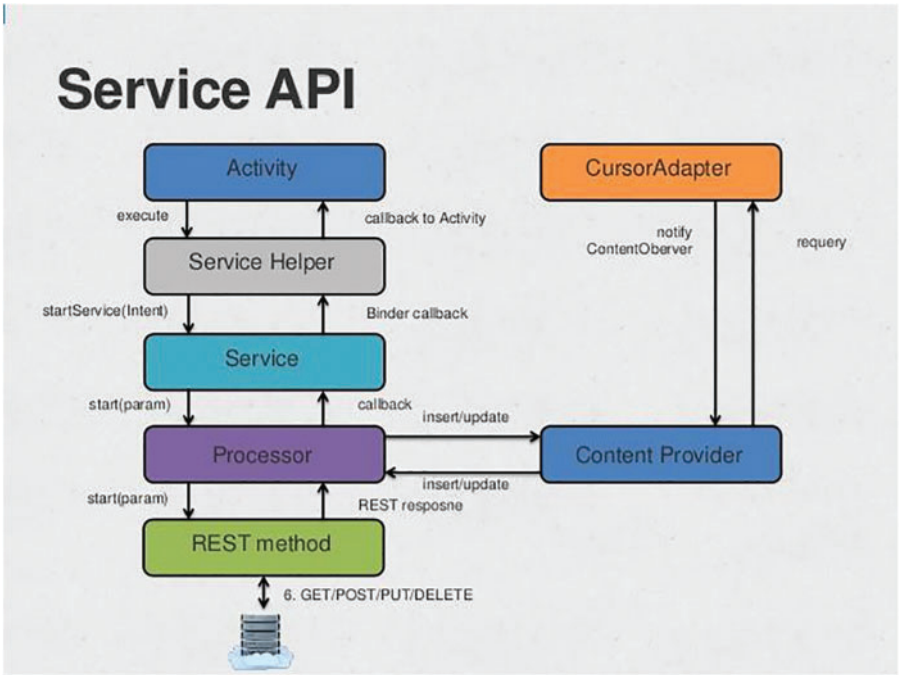

Fig. 3. Mobile interaction with web server RESTFUL API.

of the software were constructed using Angular8, NodeJS, and RESTful API. Mobile Interaction with web server RESTFUL API is established from this configuration as shown in Fig. 3. The database of the system was designed using MySQL, while the mobile application environment was exclusively developed on the Android Studio platform.

The server-side functionality of the system was implemented using NodeJS and Angular J8, which are JavaScript programming tools. When users log into the system, they provide the required information, which is then stored in the server's database. The mainframe database of the application is built using MySQL and SQLite. Additionally, it is important to mention that the system incorporates Redis DB, which works alongside the data structure and memory storage of the application. To utilize the system, the following components are required: a Personal Computer with a 64-bit Windows Operating System,

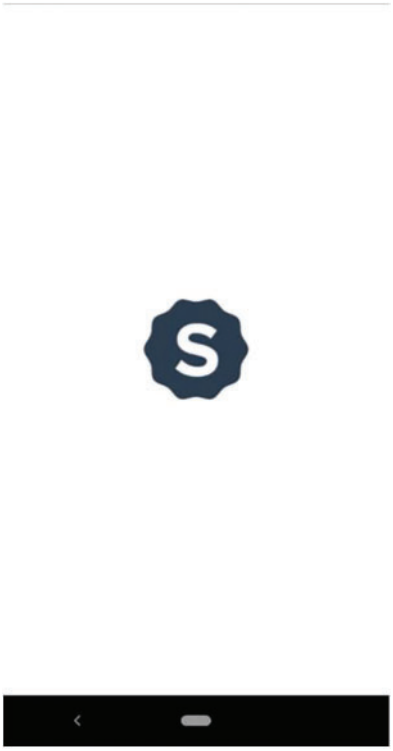

Fig. 4. Loader image of the proposed system.

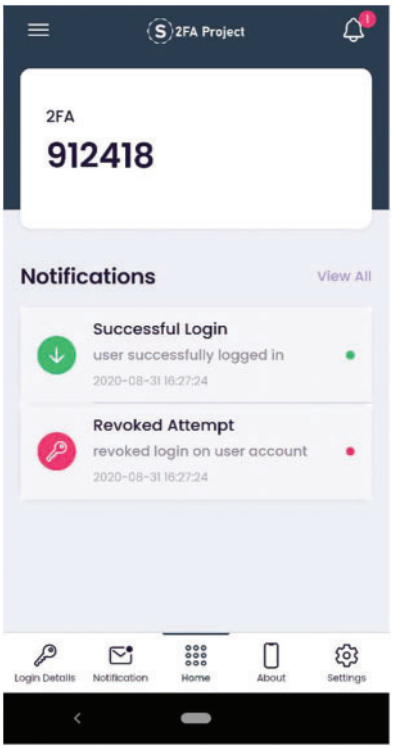

Fig. 5. Home page of the proposed system.

8 GB RAM, and a 500 GB HDD; a mobile device capable of hosting the application; and a cloud server that runs the designated cloud service.

The loader image of the system is depicted in Fig. 4, serving as the initial page upon launching the application. This display has been thoughtfully designed using HTML, Cascading Style Sheet (CSS), Node JS, and Angular J8 to ensure an ergonomic and visually appealing structure.

Displayed in Fig. 5, the home page of the software application presents the generated authentication key number and provides real-time activity notifications on the user's system. This page is presented following a successful login using the user's pre-registered login credentials. It includes details such as the precise time and date of the user's access to the MFA app. As an added functionality, users who have installed the proposed software can utilize this feature to revoke authorized access for intruders on a specific device in the event of a compromised attempt.

Fig. 6 showcases the Settings Menu, which grants users the ability to enable sound notifications by toggling the corresponding option. Additionally, it provides a feature that allows users to update their login password. The 2-step verification toggle switch enables users to activate or disable the MFA app for login access on the web server. When the toggle switch is turned off, users can access the web server simply by logging in with their username and password, without requiring the MFA authentication.

Fig. 7 showcases our test web page's landing page, developed with HTML, CSS, Bootstrap, and JavaScript. The official welcome page for cloud users features clearly labelled and brightly coloured interactive links. The test web page's link is https://2fa.jobychat.com/login. Existing users must provide login details and the OTP (authentication keys) from Fig. 6 before access to their accounts is

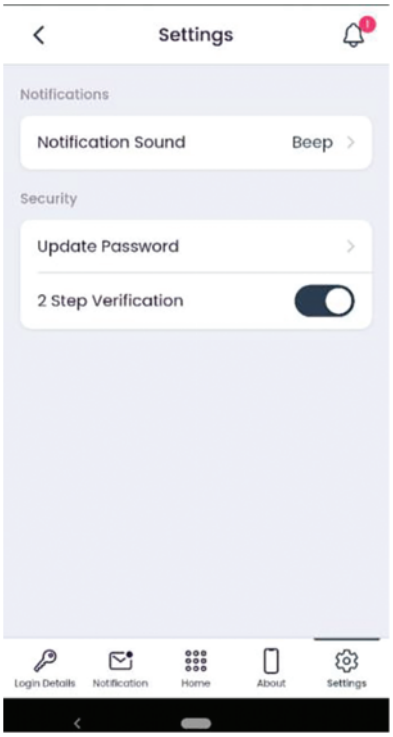

Fig. 6. Settings menu.

granted. New users can register by clicking "Signup now". Clicking the "Signup now" link opens a registration window where users enter their email ID, full name, password, and confirm password as shown in Fig. 8. After inputting the required information and clicking "Register," the email

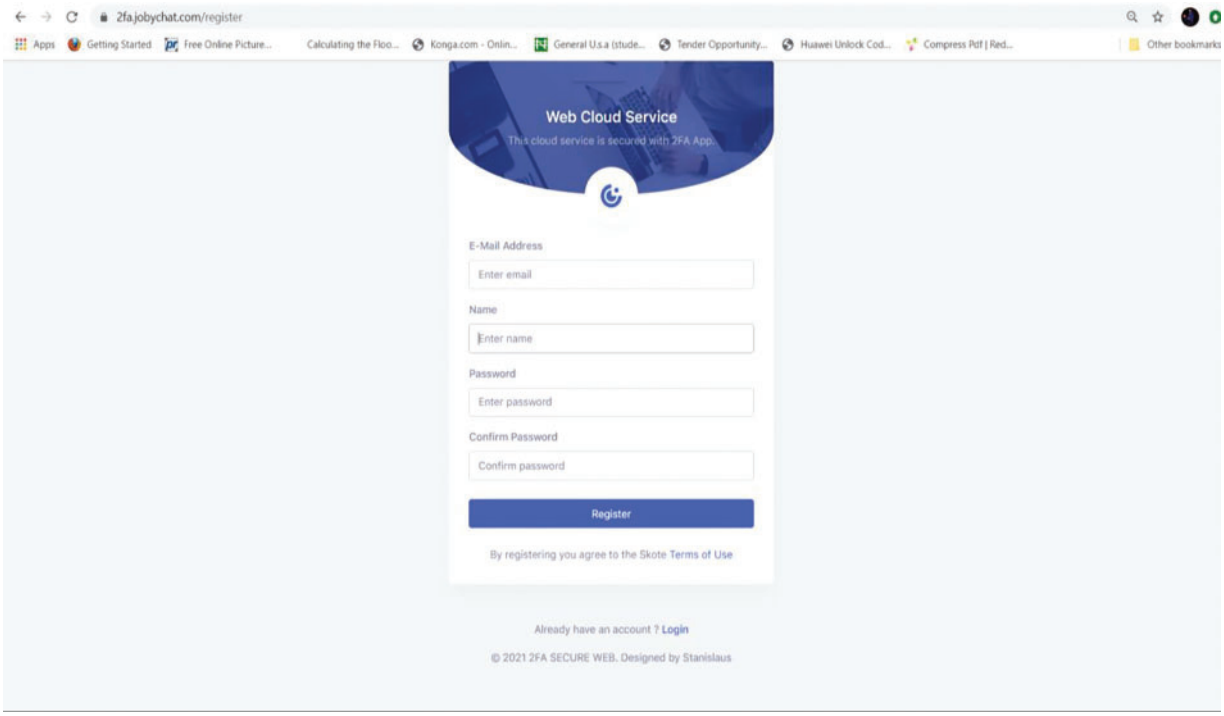

Fig. 7. Sign up page of the test web app.

undergoes validation using a regular expression. Valid emails allow users to log in with their new credentials. The password is encrypted using BlowFish 128-bit encryption for security. Users enter their registered email ID and password. Incorrect credentials trigger an alert prompt as seen in Fig. 9. Upon successful authentication, a session token is assigned to the user's browser as a cookie. Users then enter the OTP (Fig. 10) generated from the MFA system for access to the test web app (cloud server). The home page of the test web app contains a user profile section and a menu button as shown in Fig. 11. The application notification section (Fig. 12) displays login history, including successful logins, unauthorized access attempts, and IP address mismatches. Users can log out by clicking the logout button in the top-right dropdown menu (Fig. 12). After a successful logout, a page as shown in Fig. 13 is displayed.

3. Results & Discussion

A rigorous evaluation of the existing systems was conducted to perform a comparative analysis of authentication ease and the rate of false notifications generated by these systems. The rate of false notifications is a crucial parameter to consider, as it significantly affects the system's ability to differentiate between the behavior of an intruder and that of a registered user, thereby enabling an appropriate response or action. This application is based on three authentication verification factors-knowledge (passwords), possession (OTP token), and the unique location factor (IP address matching). It has demonstrated a highly secure authentication process when compared to the works of Liou and Bhashyam [6] and Yoo *et al*. [7], who only employed two authentication factors (knowledge and possession).

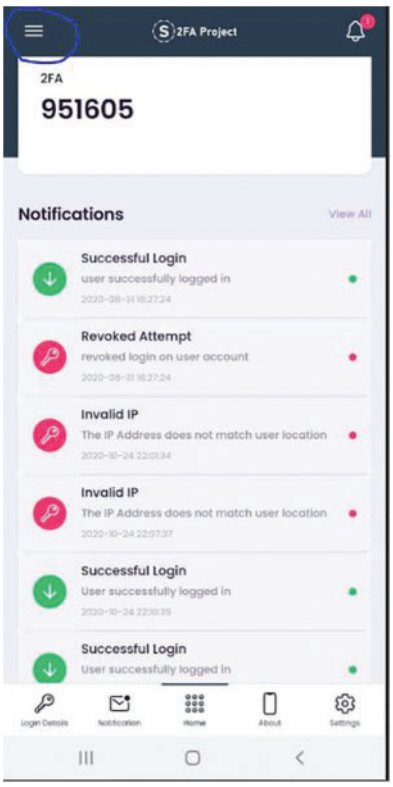

Fig. 8. Menu bar showing both a successful login and a revoked attempt.

The unique location factor feature in this software verifies a user's location by comparing the IP address of the current user with the IP addresses stored in the system database. If the IP address of the initiating user differs from the addresses in the database, it will trigger an alert in the system, notifying the user of a potential unauthorized

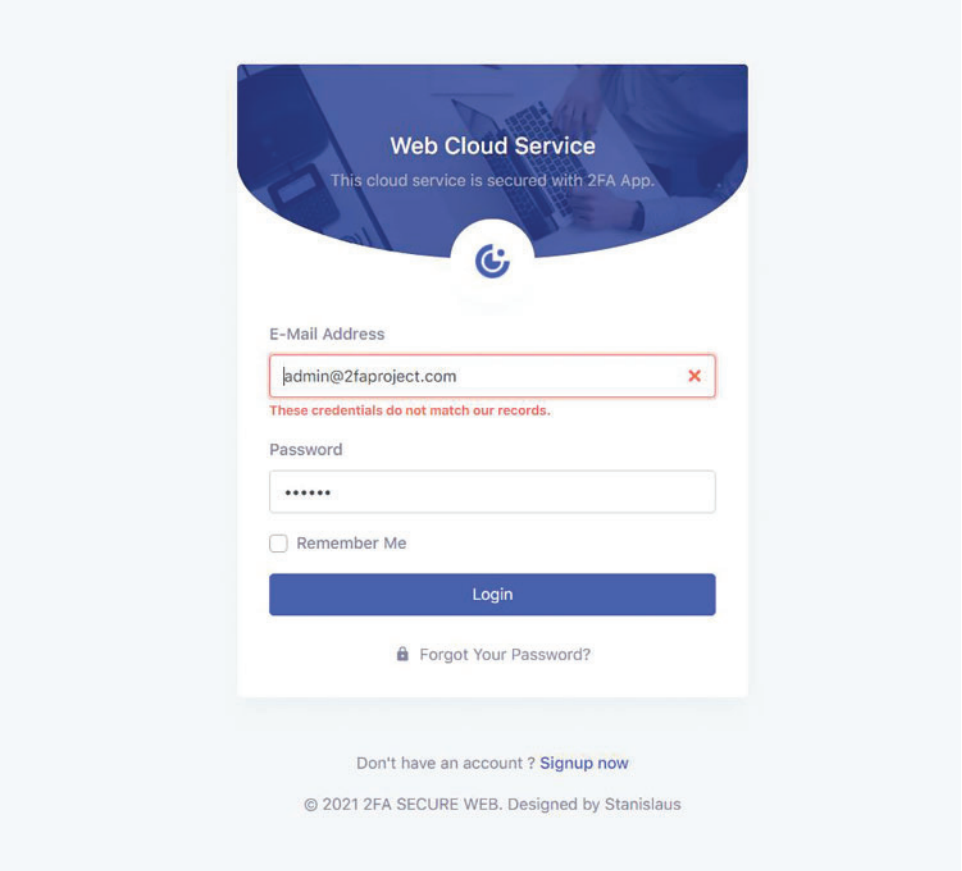

Fig. 9. Failed login error page.

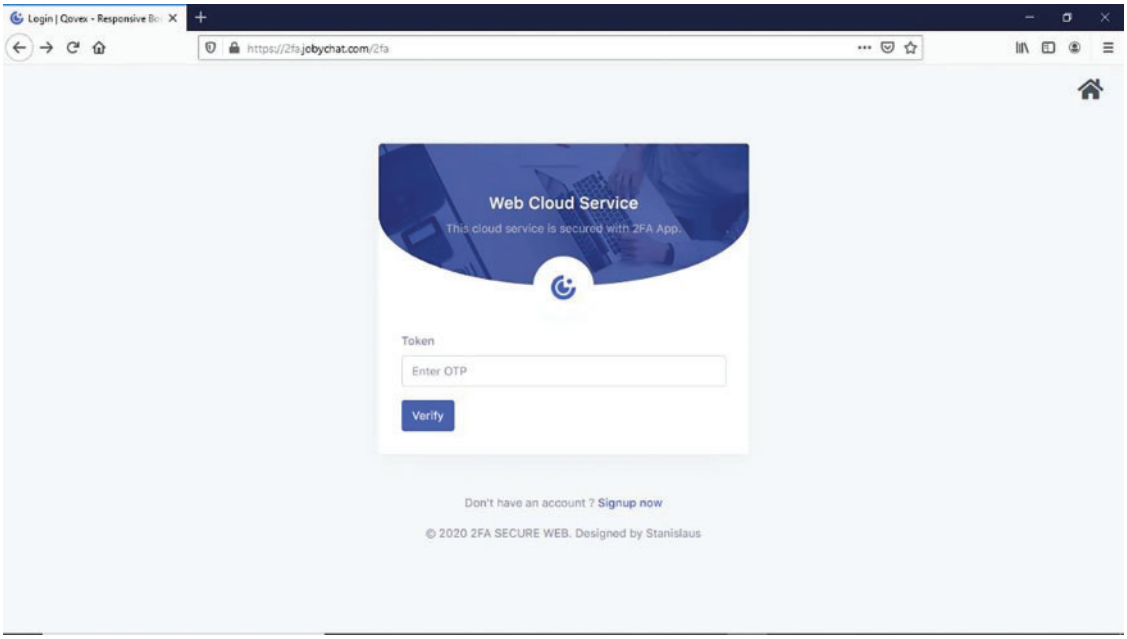

Fig. 10. OTP login page to linked test web app.

access attempt on their account. For instance, consider a scenario where the designed software is implemented in the Centre for Information and Telecommunication Engineering (CITE), University of Port Harcourt (Uniport), Nigeria, hosted on a local IP address. If an intruder located in Canada or the USA, despite possessing the passwords (knowledge factor) and MFA app for the OTP token (possession factor), attempts to gain entry using a foreign IP address, they will be completely denied access to the system due to the disparity in IP addresses. Upon reviewing the proposed software, it has been demonstrated this developed application successfully passed multiple functionality tests, aligning with the anticipated performance of the proposed system. All authentication methods were thoroughly tested and executed on the designated web test platform, demonstrating their effectiveness and efficiency.

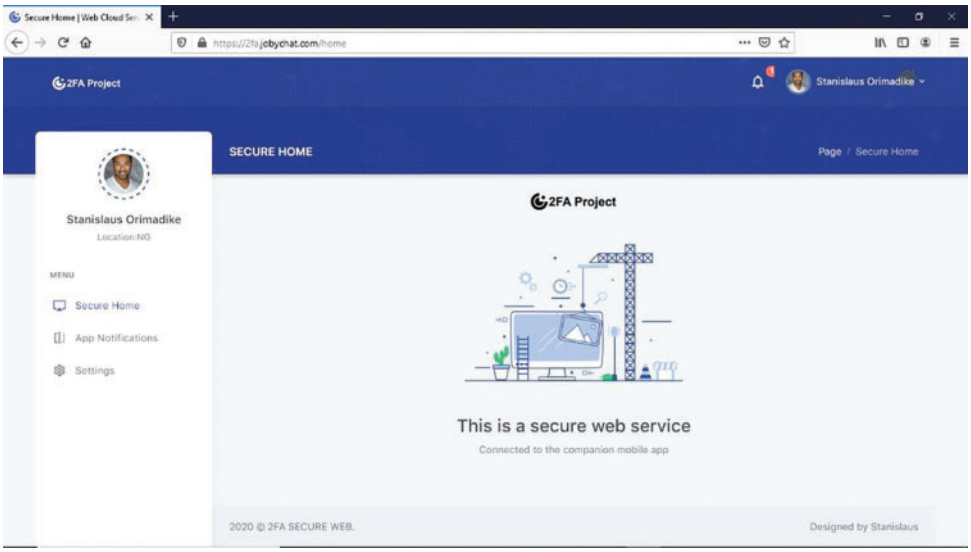

Fig. 11. Home page to the link test app.

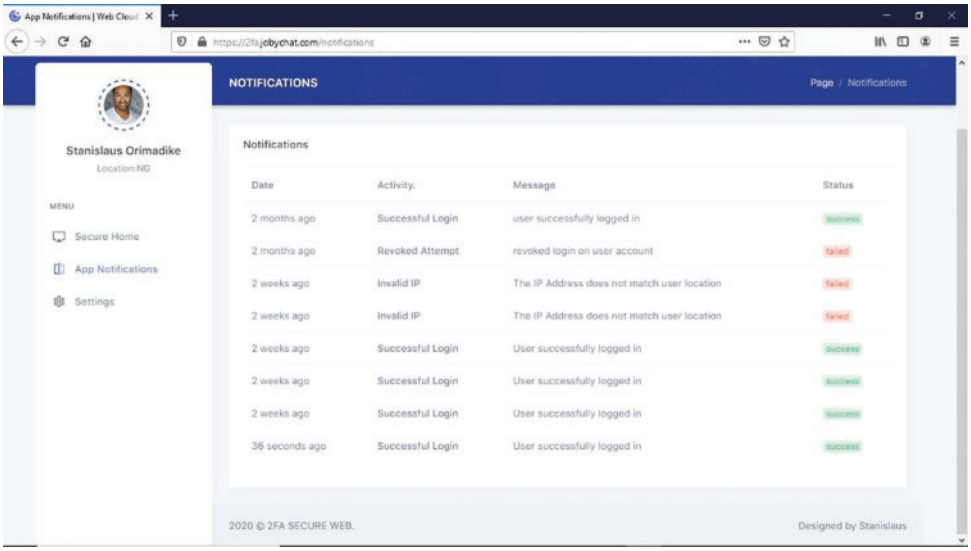

Fig. 12. Application notification of the web test app.

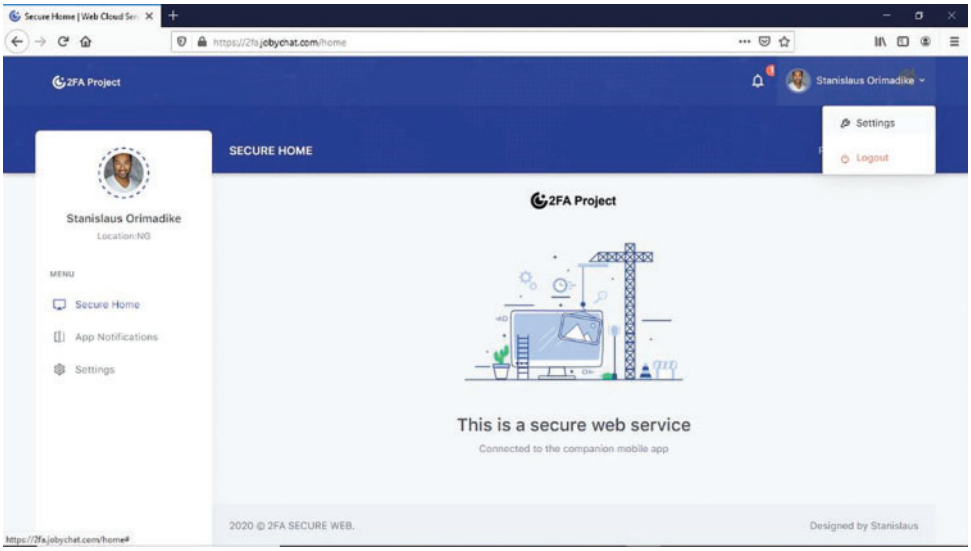

Fig. 13. Logout menu from test web app.

TABLE I: Client Review Table

Client review	No of client's response
Extremely satisfactory	90
Satisfactory	111
Somewhat satisfactory	67
Indifferent	40
Dissatisfied	32
Extremely dissatisfied	10

Furthermore, the developed application is easily implementable and can be integrated into existing systems. Analysis of the developed system has confirmed the flawless operation of both the User Login session and Authentication sessions, achieving a 100% success rate. A comprehensive evaluation was carried out to determine the suitability of this application, involving the participation of 350 sample users. The findings from this assessment are presented in Table I, depicting the responses received from clients regarding the utilization of this application. A significant proportion of these clients, approximately 77%, rated it favorably.

4. Conclusion

The demand for a secure cloud computing environment is experiencing substantial growth. Numerous organizations are adopting cloud services to conduct and expand their businesses, leading to a surge in individual users creating and owning accounts on these servers. To enhance security for these organizations and their users' data, an application-based multi-factor authentication (MFA) system is recommended. This system significantly improves protection against threats that could result in data unavailability, compromised data integrity, or breach of data confidentiality due to unauthorized intrusions.

The developed MFA system implements multi-layered security measures by employing more than two factors of authentication, earning it the title of *an application for the future*. A comprehensive testing process was conducted on the system, specifically on a test web app (cloud server), to verify the effectiveness of all three authentication factors incorporated within the application.

It should be emphasized that achieving 100% efficiency is not attainable in any system, as is typical in the design, development, and implementation of software. Hence, considering this fact, the developed system may underperform under certain conditions. For instance, it may not be compatible with newer operating systems on mobile and desktop devices due to the lack of self-updating capability. Additionally, users may encounter login challenges if their network is unavailable or if they are using a virtual private network (VPN), as conflicting IP addresses could hinder their access to the system when utilizing the software.

Conflict of Interest

Authors declare that they do not have any conflict of interest.

References

[1] Sadiku MNO, Musa SM, Momoh OD. Cloud computing: opportunities and challenges. *IEEE Potentials*. 2014;33(1):34–6.
[2] Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem. 2016. *arXiv preprint arXiv:160901107*.
[3] Khalil IM, Khreishah A, Azeem M. Cloud computing security: a survey. *Comput*. 2014;3(1):1–35.
[4] Nagaraju S, Parthiban L. SecAuthn: provably secure multi-factor authentication for the cloud computing systems. *Indian J Sci Technol*. 2016;9(9):1–18.
[5] Mohsin JK, Han L, Hammoudeh M, Hegarty R. Two factor vs multi-factor, an authentication battle in mobile cloud computing environments. *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017.
[6] Liou JC, Bhashyam S. A feasible and cost effective two-factor authentication for online transactions. *The 2nd International Conference on Software Engineering and Data Mining 2010*, IEEE, 2010.
[7] Yoo S, Shin SJ, Ryu DH. An innovative two factor authentication method: the qrlogin system. *Int J Secur Its Appl*. 2013;7(3):293–302.