International Conference on Sciences, Engineering & Environmental Technology (ICONSEET), 7(15): 118 – 124, 2022

ISSN 0794-9650

www.repcomseet.org

DEVELOPMENT OF A SECURE MOBILE TEXT MESSAGING, FORUM, AND ONLINE TEST APPLICATION (APP) (A Case Study of Federal Polytechnic Ede, Osun State)

Ekuewa Jacob. B., Oyetunji Olumayowa.O, Adigun, Olajide. I., and Afolabi Olajide, J.

Department of Computer Science, Federal Polytechnic, Ede, Osun State
Author's Corresponding Email: oludmayor1@gmail.com

Abstract: A secure mobile application for text messaging, forums, and online tests is a smartphone app that enables students to study and work with their friends in real time at different languages and interact with people they didn't know were on campus while also giving them the opportunity to practice for their tertiary institutions' exams for free. The manual and defunct electronic systems have a number of drawbacks because they are susceptible to data redundancy, inconsistency, and difficulty updating and maintaining data, poor security, and difficulty imposing constraints on different data files and backing up data. It is necessary to use a secured database Advanced Encryption Standard (AES) to monitor the performance of the secure mobile application for text messaging, discussion forums, and online tests over time. Because it was carefully developed, the system is error-free, highly effective, and time-saving. The entire software development cycle is used, and it is important to note that the system is quite reliable. Future system development is accommodated for. In conclusion, the new system is created using Android SDK (System Development Kit), Transport Layer Security (TLS), so that the old system could be used alongside it in parallel implantation formalism rather than being abruptly discarded. This would assist in upgrading and updating the new system in terms of any issues that may have gone unsolved owing to a time constraint during the design phase.

Keywords: ***Mobile Application, Network, TLS, Android SDK, AES,***

1.0 Introduction

Recent years have shown a significant increase in the popularity and ubiquity of mobile devices among users all around the globe. These devices, based on a specific operating system, enable users to install a vast variety of applications, commonly referred to as "apps," from online sources called markets: Apple App Store and Google Play *(Guo et al., 2019).* The aforementioned apps are the essence of smartphones, enriching their functionality and enhancing the everyday lives of their users. -e app markets allow users to perform a quick search and installation of new apps, but at the same time, they are also a source of different kinds of malware disguised as normal apps. Nowadays, mobile devices are subjected to a wide range of security challenges and malicious threats *(Mavoungou et al., 2016).*

The mobile revolution has empowered and influenced users to move almost all of their everyday operations into the mobile environment and so-called mobile applications. Hence, we can observe rapid growth in the domains of both mobile developers and users. Mobile devices are treated by their users as very personal tools, mainly used to facilitate everyday operations, but they also serve to store very sensitive personal information *(Papageorgiou et al., 2018).*

Contemporary mobile applications are ubiquitous and very easy to install on almost every mobile operating system: iOS, Android, Windows phone, etc. As a result of aggressive competition among application providers, we can observe more and more advanced and customized applications appearing on the market, resolving complex problems. These applications profoundly change a user's behavior by facilitating their day-to-day transactions *(Chen et al., 2019).* A secure mobile application for text messaging, forums, and online tests is a smartphone app that enables students to study and work with their friends in real time at different languages and interact with people they didn't know were on campus while also giving them the opportunity to practice for their tertiary institutions' exams for free. Apps and platforms that offer instant messaging are known as messaging apps (sometimes known as social messaging or chat applications), and many of these apps have grown into large platforms that include conversational commerce (online shopping through chat), payments, and status updates *(Ling et al, 2016).* A growing number of authors who have researched the development of secure mobile applications are being discussed as a result of the demand for such applications for text messaging.

Patel (2020), Update mobile operating systems and on-board applications with security patches: keeping the operating system (Android and iOS) and the installed applications up to date is a must. Both Google and Apple provide regular updates to users, which resolve recent vulnerabilities or other threats, as well as sharing additional performance and security features. However, updating an app is a two-edged sword since a new release can decrease its overall performance and the user's productivity. From a security perspective, updates can trigger the revetting process to confirm security clearance. In order to ensure that a mobile application conforms to an organization's security requirements and is free from vulnerabilities, a series of rigorous and comprehensive analyses take place. One has to keep in mind that app vetting might also include updated external components (e.g., third-party libraries) and new mandatory versions of the operating systems. Mark (2020), wrote that Mobile device users often create vulnerabilities due to the blurred line dividing personal and business use. Some of the blameworthy behaviors include turning off all types of security apps, downloading apps from third-party application stores, and sharing confidential information with unauthorized recipients. With smartphones, it becomes even easier to obtain sought-after information. Controlling user behavior is considered to be one of the greatest challenges in mobile device security.

According to Hein (2020), Mobile phones are considered to be personal devices on which users store lots of different types of data, either personal or business. In is research, mobile device users, most frequently, simply lose their devices. Mobile device owners are themselves the greatest threat when it comes to losing sensitive data, yet, at the same time, their proper behavior can help protect such data. Implementing 2FA (two-factor authentication), avoiding automatic logins, and using password-lock applications can minimize the probability of losing sensitive data *Chris et al.,(2015)* described a technique for enhancing text message security when using open text communication technologies like SMS and email. Before delivering the communication by email or text message (SMS), content encryption is used to ensure that even if the message is received and seen by an unauthorized person, it cannot be deciphered. Therefore, that application was run in LabVIEW and can be used to send emails with encoded content using open email services between at least two clients. Their suggested application uses content encryption techniques including balanced and deviated encryption and uses either a private encryption key or an open encryption key for encryption. The instant message must first be recently scrambled in order to transmit encoded SMS using that program, following which the encoded message will be copied to the content window of the SMS sending application operating on the mobile device. A similar program can also be made for mobile devices running operating systems like Android, iOS, Windows Mobile, and so forth. These applications can be used in conjunction with any instant messaging service, including Facebook Messenger and others.

According to Tankovska (2021), the AES is a cryptographic method that is used to both encrypt and decrypt data. A Key Schedule is produced by Key Expansion and utilized in the cipher and inverse cipher procedures. The system's goal is to minimize the hardware structure. It is more cost-effective and uses less hardware than the pipeline structure. Additionally, this technology is highly reliable and secure. A Rijndael compact data channel architecture was outlined that effectively divides hardware resources between encryption and decryption. In the earlier methods, the crucial arithmetic component S-Box has been implemented utilizing ROMs or look-up table logic, which necessitates extensive hardware support. The terminal equipment can make extensive use of this Advanced Encryption Standard (AES) system. Cryptography, the science of secret codes that ensures the confidentiality of communication over insecure channels, is used to build the Field Programmable Gate Arrays based Advance Encryption Standard (FPGA-based AES) algorithm.

Ankit et al., (2017) explains how to encrypt data in a way that keeps it safe from prying eyes. With the growing need to protect one's privacy in communications and transactions, it defines encryption, explains how it works, and provides examples of both. They covered a variety of topics, including the idea of creating a key detail, cryptography, the most widely used encryption methods, how encryption operates, digital signatures, digital certificates, and—most importantly—digital signatures.

In this paper, we propose end-to-end security, which ensures that only the sender and recipient can access messages without a third party, with a focus on security, privacy, and speed. Protection of storage and quick communication transfer between the parties are also taken care of.

1.1 Research Motivation

Due to the everyday security risks offered by our smart phones and tablets, new security difficulties and problems, such as online fraud, money theft, spam messages, and spoofing, may arise.

The current system was found to be flawed since it was unable to achieve its intended goal. The following are a few of the issues with the current system:

i. Inadequate security and privacy for personal messages
ii. Is susceptible to Man-in-the-Middle (MIM) assaults.
iii. Absence of key control
iv. Keeps messages in the database as plain text.

To overcome these issues, this paper uses a secure development pipeline and resources like the Java programming language and Google's Firebase, to name a few.

1.2 Design Approach

The program designed used a modular approach; therefore the intricate design was broken down into a number of components. Each module has a black box defined in the module interface specification, which was written for it. The programmer of another module can access the facilities of a module by using the information provided in the interface definition for that module, among other things. The implementor needs the same details. Specifically, this means:

a) Creating a secure chat program for online text, SMS messages, and discussion forums.
b) Use Apple iOS and Android as case studies for the secured application implementation.

2.0 Research Methodology

2.1 Data Collection

The following method of data collection was used in writing this paper:

i. Interview
ii. Observation
iii. Review of procedure or existing system or procedural manual
iv. Evaluation of forms

2.2 System Architecture

The process of defining a system's architecture, components, modules, interfaces, and data in order to meet specific criteria is known as system design. It is a step in the design process where the goals of the design are grasped. According to its definition, a system is a group of interconnected components and processes that work together to complete a task or resolve a problem. One quality of this system is that it can be used effectively and efficiently for a long time by competent individuals of average intelligence. The system design should guarantee the accuracy, timeliness, and comprehensiveness of the system output.

A system's strengths and shortcomings can be identified, and the necessity to eradicate all of these weaknesses while maintaining the strengths motivates the creation of a new system.

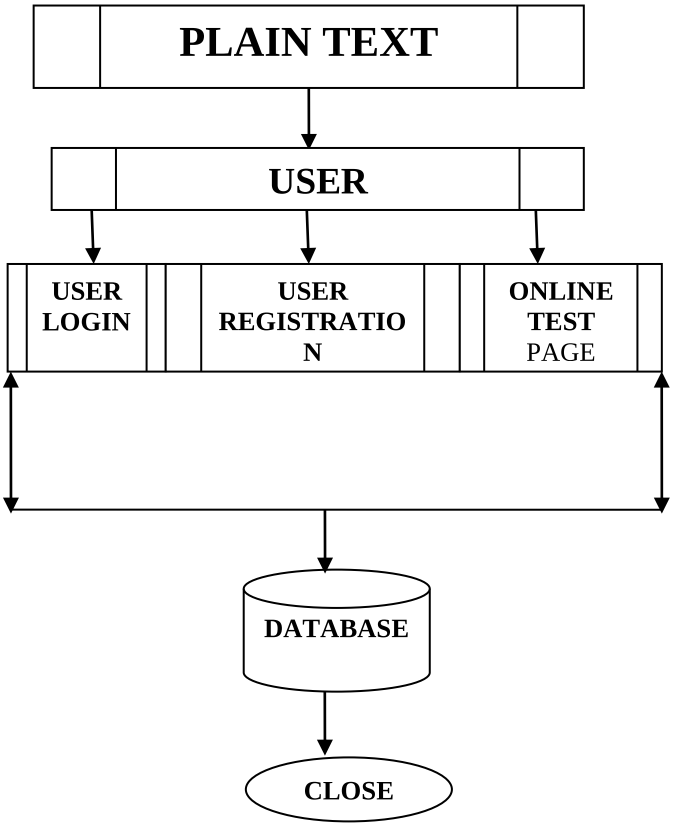


Fig 1: System Architecture

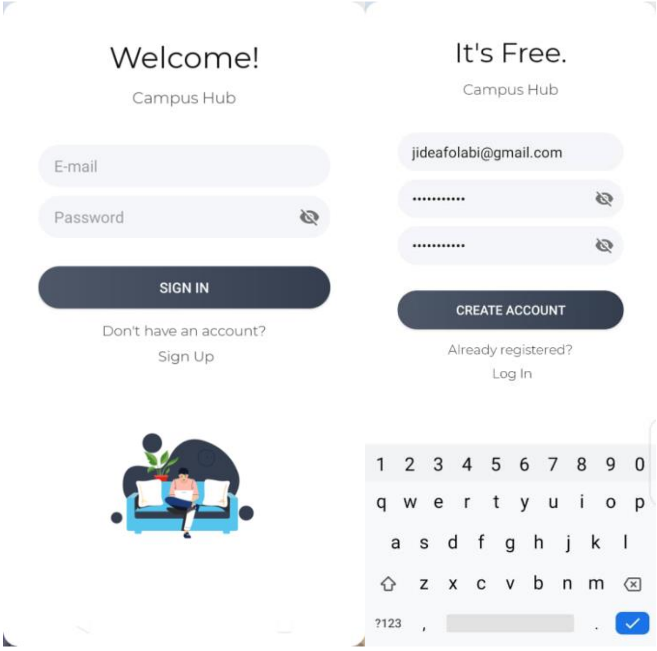
3.0 Results and Discussion

The design of computers, appliances, software programs, and websites with a user's experience and interaction in mind is known as user interface design. The aim of user interface design is to create a fantastic user-system interaction that is effective, user-friendly, and compatible with the system's intended users. The system flow should be properly organized, making the interfaces easy to learn and use.

3.1 Main Menu Specification

3.2 User Login

This displays the system's login page. The user must input their login and password on this page. Based on the user name and password, the system will determine whether the user is an administrator, a lecturer, or a student. The common data that will be entered into the system is contained in the Log in Specification. It is significant in that it contributes to the solution of a specific issue.



Welcome!

Campus Hub

It's Free.

Campus Hub

jideafolabi@gmail.com

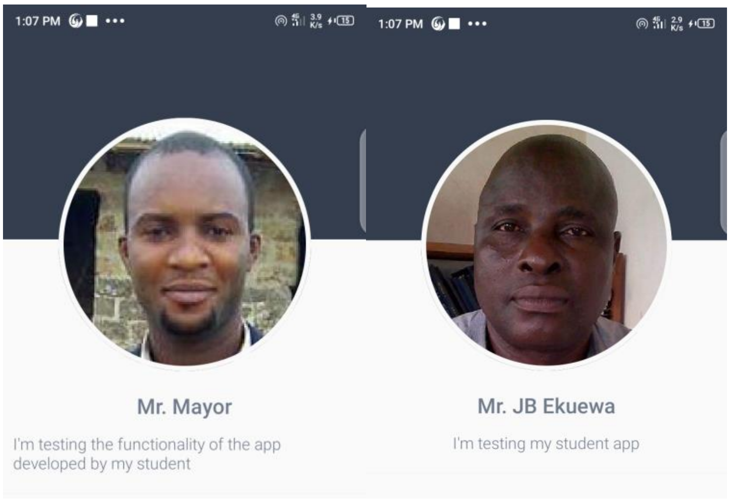
•••••••••••

•••••••••••

Figure 2: User Login

3.3 User Registration

This page shows registered users.



Mr. Mayor

I'm testing the functionality of the app developed by my student

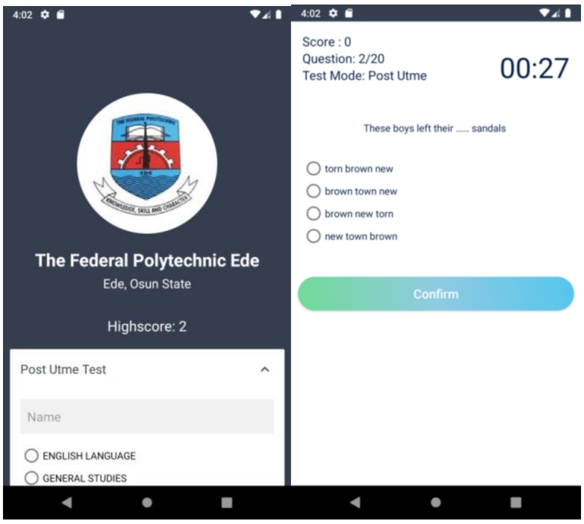
Mr. JB Ekuewa

I'm testing my student app

Figure 3: Friend request page

3.4 Online Test Page

These page allow all registered users to take an online test



The Federal Polytechnic Ede

Ede, Osun State

Highscore: 2

Post Utme Test

Name

○ ENGLISH LANGUAGE

○ GENERAL STUDIES

Score : 0

Question: 2/20

Test Mode: Post Utme

00:27

These boys left their ...... sandals

○ torn brown new

○ brown town new

○ brown new torn

○ new town brown

Figure 4: Online page test

4.0 Recommendation & Conclusion

4.1 Conclusion

In conclusion, the secure mobile application for text messaging, forums, and online tests benefits both the school and the students because it offers a safe means for people to communicate with one another, work remotely, and take exams online.

4.2 Recommendation

The following are suggested for the new system's effective and efficient performance:

1. It should be stated what hardware and software must be installed.
2. The required security measures should be implemented.
3. The importance of having knowledgeable database and network administrators cannot be overstated. This will prevent unauthorized individuals from accessing the software and database.

REFERENCES

1. B. Guo, Y. Ouyang, T. Guo, L. Cao, and Z. Yu, “Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review,” IEEE Access, vol. 7, pp. 68557–68571, 2019.

2. S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, “Survey on threats and attacks on mobile networks,” IEEE Access, vol. 4, pp. 4543–4572, 2016.

3. A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, “Security and privacy analysis of mobile health applications: the alarming state of practice ,” IEEE Access, vol. 6 pp. 9390–9403, 2018.

4. Y. Chen, W. Xu, L. Peng, and H. Zhang, “Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT,” IEEE Access vol. 7, pp. 15210–15221, 2019.

5. Ling E, Noor B, Nadler R. (2016). The social psychology of collective victimhood on secure text messaging applications and various mobile applications.

6. HPatel, “14 best practices for your mobile app security,” 2020,https://www.tristatetechnology.com/blog/best practices-to-improve-mobile-app-security/

7. J. Mark, “8 best practices for mobile device security,” 2020, https://www.jmark.com/8-best-practices-mobile device-security/.

8. D. Hein, “7 essential mobile security best practices for businesses,2020, https://solutionsreview.com/mobiledevice-management/7-essential -mobile-security-best-practicesfor-businesses/.

9. Chris Quirk, Raymond Mooney, and Michel Galley. (2018). Language to code: Learning semantic parsers for if-this-then-that recipes. In Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics, pages 878– 888, Beijing, China, July.

10. Tankovska A. (2021). Learning to generate pseudo-code from source code using statistical machine translation. In 30th IEEE/ACM International Conference on Automated Software Engineering (ASE), Lincoln, Nebraska, USA, November.

11. Akint L, D. Dasgupta, A. Roy, and A. Nag “Multi-factor authentication,” in Advances in User Authentication, pp. 185–233, Springer, Cham, Switzerland, 2017.

12. , Nachiketh R.(2006). "A study of the energy consumption characteristics of cryptographic algorithms and security protocols."*IEEE Transactions on mobile computing*5.2: 128-143.

13. Rayarikar, Rohan, SanketUpadhyay, and Priyanka Pimpale.(2012). "SMS encryption using AES algorithm on android."*International Journal of Computer Applications* 50.19