South Asian Journal of Engineering and Technology Research Article

Open Access Full Text Article 121(2022) 55-59 DOI: 10.26524/sajet.2022.12.09

Android SMS and File Manager Encrypted Application Using AES-Vigenere and AES/ECB/PKCS5/Padding a Hybrid Encryption Algorithm

CELINE DIANNE MONTANO[a], JERIC NUEZ[a]

[a]College of Information and Communication Technology, Taguig City University, Philippines

Corresponding author.
Correspondence: Celine Dianne Montano
E-Email: mcelinedianne@gmail.com

Article info
Received 10 th December 2021
Received in revised form 7 February 2022 Accepted 19 March 2022

Keywords
AES, Android, Algorithm, Encryption, Hybrid, Hacking, SMS

Abstract
The study, entitled Android SMS and File Manager Encrypted Application Using AES-Vigenere and AES/ECB/PKCS5/Padding a Hybrid Encryption Algorithm, was a proposed solution about Social Engineering and hacking. With the Data Privacy Act of 2012, the study encourages and inspires. The study's goal is to offer users security and safety for their personal information. The purpose of this research is to prevent cyber theft. The theft of financial and/or personal information through the use of a computer/device for fraudulent or other criminal purposes is referred to as cyber theft. For this situation, the study suggested solutions.The research covers the first chapter's Project Context, Purpose and Description, Conceptual Framework, Objectives, Scope, and Limitations. The first chapter offers a general overview of the application. The project background covered the area, challenge, and how the developers came up with the plan, as well as the main point of the research. The objectives were directed at the system's functioning, and the scope and constraints were addressed to determine the study's capability and boundaries. The research also offered the associated literature and study materials synthesized, such as the Changed AES Algorithm Using Multiple S-Boxes, which assists the group in altering and producing a unique and freshly modified algorithm that would improve the security of the application.The research, on the other hand, went into the technical background as well as the hardware and software requirements that the developers employed to improve the program. The research gives information on the system requirements that comprise the versions of software and hardware that the application's proponents utilized to develop it. The design and methodology of our study were also discussed. This includes many schematics depicting the system's flow as well as a constructed prototype. The research demonstrates the concepts and frameworks that the application's proponents utilized to design the application. This chapter contains factual information regarding the actions and techniques taken by the responders in constructing the application. This also includes ways for how the proponents undertake data collection operations.

I. INTRODUCTION

People increasingly rely heavily on mobile phones as their major means of communication. SMS and file transfers on smart phones were not as secure as they could have been if users did not lock or password protect our apps. It's difficult to go a week without hearing about a new leak, breach, or privacy blunder, according to www.digg.com. Consumers have learned that in order for their data to be secure, they must take personal responsibility for it. Because clients spend so much time on their phones, mobile applications are a good place to start. Navigating the murky seas of app store frauds, on the other hand, is time-consuming and

complicated. Navigating the murky seas of app store frauds, on the other hand, is time-consuming and complicated.

There are thousands of privacy-conscious applications to choose from, each with its unique set of features and efficacy levels. So, which should you go with? Which is the most efficient? Another question is why telephones should be secured in the first place. Although most people are aware of the need of utilizing computer security software, hackers can employ hazardous software, or malware, to get access to information on our computers. Malware may even penetrate smartphones, which are basically miniature computers running "mobile operating systems" that are less apparent. As a result, they may be exposed to the same threats and vulnerabilities as computer operating systems. Malware may steal or even keep your data hostage if a cybercriminal has obtained access to your device. In reality, there are several techniques for revealing or disclosing your private conversations, such as social engineering, which entails utilizing deceptive strategies or methods to persuade someone to divulge private or personal and critical information. According to the Data Privacy Act, encryption is one technique to increase smartphone security. In what ways does encryption safeguard mobile devices? Encryption serves several purposes. Much more than simply stopping someone from accessing your phone's dataphone, as the lock screen does. A lock screen is analogous to the lock on a person's front door. A door lock prevents an unauthorized visitor from entering the house and taking personal things, but the homeowner must consider what the criminal would do if the locks were broken and the burglar got entry to the property. To fully protect data, we need multiple layers of defense. In the security profession, this is known as "defense-in-depth," and encryption offers it. Data encryption takes security to a whole new level. It makes the phone's information unreadable. Even if a hacker is able to bypass the locked phone screen, they may be unable to access sensitive information.

II. LITERATURE REVIEW

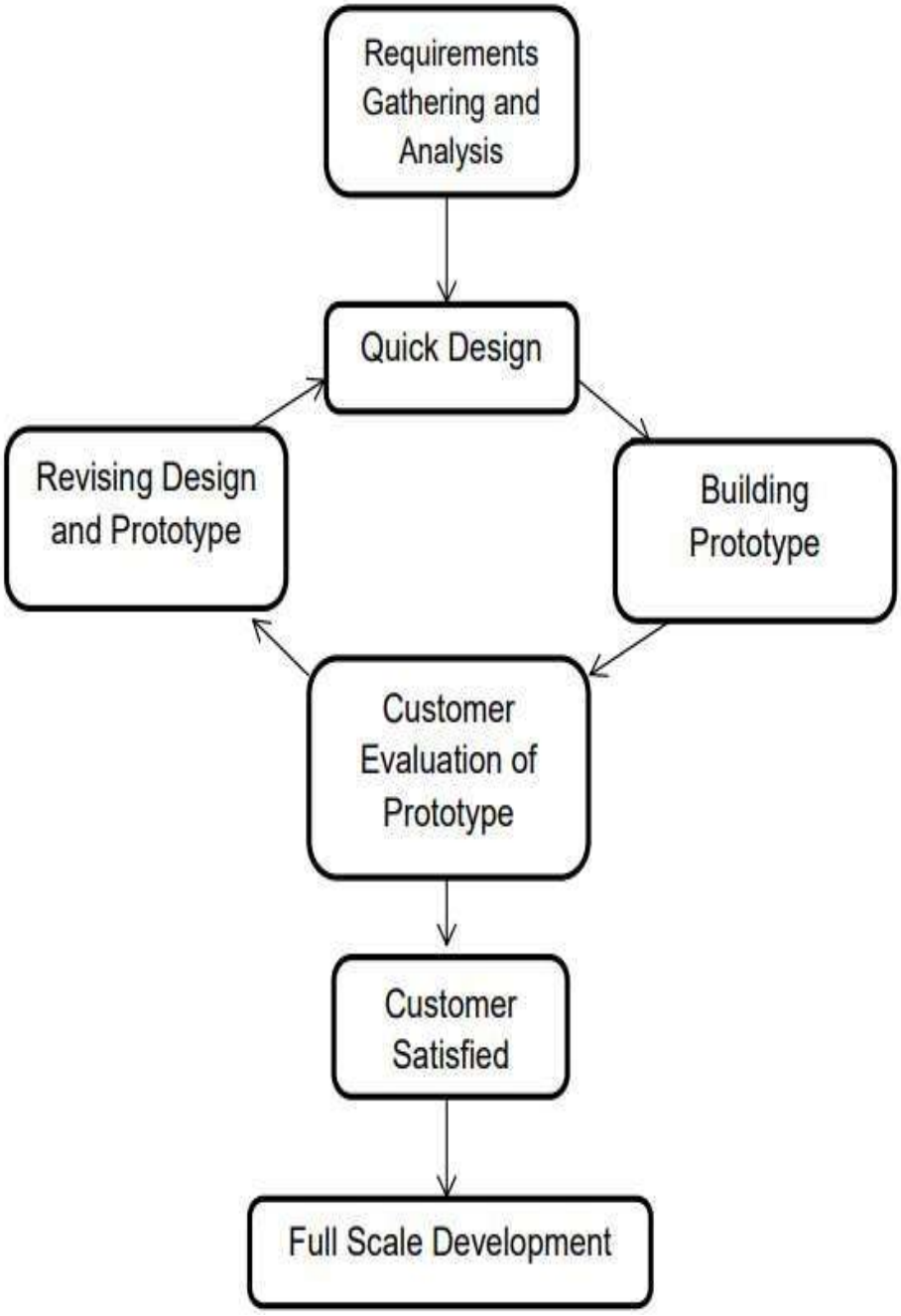
SMS communication is well-designed to allow end-to-end secure communication through SMS utilizing AES and MD5 encryption between mobile clients. SMS is the most well-known information advantage. SMS technology is employed in high-security businesses such as e-account management and e-government. SMS is sent unencrypted between the versatile client (MS) and the SMS focus. SMS communications are preserved in the frameworks of system administrators and can be viewed by their personnel. SMS does not provide a secure environment for the transfer of confidential data.

Many Android developers have devised a system that uses the AES algorithm to encrypt SMS messages. SMS has grown into a helpful technology that has played an essential part in the lives of its users. SMS offers installation supplies, portable money-saving, important updates such as stock and news alerts, activity refreshes, meteorological data, and business-related data. Concerns about security and impersonation are at the heart of the investigation. The research made use of a sophisticated encryption process built for SMS transmission across any form of the communication link. The quality of the computation was focused on constructing an anchored encryption technique and adopting AES (Advanced Encryption Standard) encryption with two extra encryption layers depending on the structure. It investigated the system's effect on the encryption process. Other developers are working on a Security Assurance Framework for SMS Using Cascaded Encryption Algorithm. All media transmission lines must have security certification. It is everyone's aim to keep any data sent via unbound and anchored media transmission cables hidden. SMS has grown into a helpful technology that has played an essential part in the lives of its users. SMS offers installation meals, portable money-saving, important updates such as stock and news alerts, activity refreshes, meteorological data, and business-related data. Concerns about security and impersonation are at the heart of the investigation.

III. RESEARCH METHODOLOGY

Since the proponents are creating a mobile application, the prototype model is appropriate for our system development. Prototyping is a paradigm in which a prototype is built, tested, and then revised until an acceptable prototype is obtained from which the entire system or product may be constructed. It's a cycle that allows for system adjustments and repeats the quick design if something has to be modified or updated. In this case, the supporters will upload our system to the Play Store, and the group will progressively develop the system's scope and capabilities in response to user comments and needs. Our group will keep track of their comments and reviews on our system, and then the supporters will create and update new versions, which will then be released to the Play Store for people to download new versions of our system. The researcher targeted computer science students to be the responders. Computer Science has 695 students enrolled. This information was given by Taguig City University's Registrar's Office. Because Slovin's Formula is applied to the entire population, the total number of respondents to whom the proponents must provide survey questionnaires is 255. The proponents picked Computer Science Students as their responders because they are better conversant with the function that we are aiming to execute. Furthermore, the researchers interviewed a group of Computer Science students and teachers. The group responds to a few questions on how happy they are with their present

mobile phone experience and how safe they feel. They've also included similar items on the survey forms they'll be filling out.



IV. FINDING AND DISCUSSION

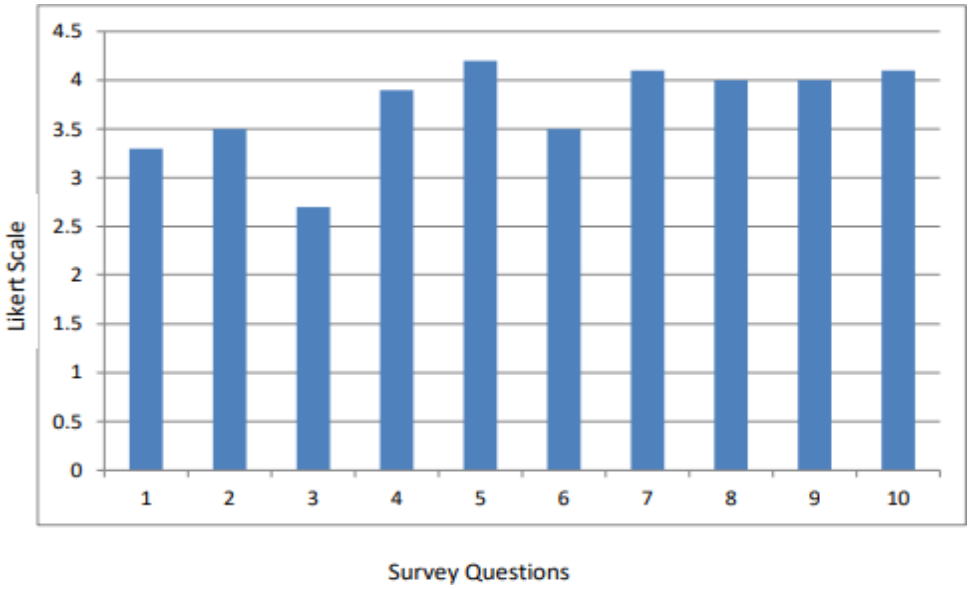
The proponents conducted a survey to learn about the needs and wishes of the users. The survey findings are good, and almost everyone would want to have a program like this to secure their data and messages. As a result, proponents conclude that this usage is both viable and long-term. Anyone with an Android phone may use the Android SMS and File Manager Encrypted Application. This is a program that may protect their SMS and File Manager. The method of safeguarding a user's message content and files in a file manager is known as encryption. This software will be submitted to the Google Play Store and user reviews will be conducted. The system's functionality and capabilities will be preserved if the system's supporters monitor and examine every user proposal and review.

Respondent's Assessment:

Question no.	Weighted Mean
Functionality: 1. Do you think that encryption can help in protecting your data in your file manager?	3.3
2. Are you aware of file encryption?	3.5
Speed: 3. Do you think that encryption will affect in your phone's performance?	2.7
4. In encrypting big files, are you willing to wait for encryption process?	3.9
Security: 5. SMS is part of our personal information; do you want to secure the content by using encryption?	4.2
6. Do you want to have an application that could secure your file manager using encryption?	3.5

Accuracy: 7. Do you think that the application can provide an accurate security to your SMS?	4.1
8. Do you think that the application can provide an accurate security to your File Manager?	4.0
User Friendliness: 9. Do you think that the encryption application is easy to use?	4.0
10. Do you think that the application is considered as a user friendly application?	4.1

Assessment Survey Graph:



V. CONCLUSION AND FURTHER RESEARCH

The Android SMS and File Manager Encrypted Application uses two hybrid encryption algorithms: the AES-Vigenere Encryption Algorithm, which encrypts SMS message contents, and the AES/ECB/PKCS5/Padding, which encrypts file bytes in the file manager. This initiative supports the Data Privacy Act, which protects and maintains the right to privacy of the consumer or user. The proponents conducted a poll to learn about the needs and wishes of the users. The survey findings are good, and almost everyone would want to have a program like this to secure their data and messages. As a result, the proponents conclude that this use is realistic and long-term. Based on the observations and conclusions gained, the following is presented.

Android SMS and File Manager Encrypted Application Using AES-Vigenere and AES/ECB/PKCS5Padding a Hybrid Encryption Algorithm will be accessible for everyone to use and test on the Google Play Store. The proponents will analyze the user evaluations and comments for the application's upkeep. Due to human mistakes, the program will still require certain options for password recovery. The program will provide you with numerous password recovery options through email. Improve the software by keeping and improving the system's features: the application will provide a vault for the user's encrypted data to be kept in. This can help to increase the security of the user's data. Updating the user interface and experience of the program for improved accessibility and use by users.

REFERENCES

1. Albert, J. R. G., Serafica, R. B., & Lumbera, B. T. (2016). Examining Trends in ICT Statistics: How Does the Philippines Fare in ICT?. Discussion Paper Series No. 2016-16. Philippines: Philippine Institute for Development Studies.
2. Basharat, I., Azam, F., & Muzaffar, A. W. (2012). Database Security and Encryption: A Survey Study. Volume 47– No.12. Pakistan: National University of Sciences and Technology (NUST).
3. Cordero-Batac, E. R., & King Kay, C. O. (2018). Data Protection Laws of the World Philippines. Republic Act No. 10173. Philippines: DLA PIPER.
4. Ibrahim, Mr S. Jafar Ali, K. Singaraj, P. Jebaroopan, and S. A. Sheikfareed. "Android Based Robot for Industrial Application." International Journal of Engineering Research & Technology 3, no. 3 (2014).
5. Degabriele, J. P. (2014). Authenticated Encryption in Theory and in Practice. Thesis Paper. London: Information Security Group Department of Mathematics Royal Holloway, University of London
6. Joshi , M. R., & Pathak, V. M. (2011). A survey of SMS based Information Systems. Master's Thesis. Finland: University of Eastern Finland School of Computing.
7. Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks."Advances in Information Communication Technology and Computing, pp. 461-471. Springer, Singapore, 2022.
8. Kaur, E., & Singh, E. N. (2015). SMS Encryption using NTRU Algorithm. Vol. 3, Issue 2. India: International Journal of Advanced Research in Computer Science & Technology.
9. Lalis,J. T., Gerardo, B. D., & Byun, Y. (2014). Securing Bluetooth Communication with Hybrid Pairing Protocol. Vol. 8, No. 4. Philippines: Institute of ICT, West Visayas State University, Iloilo City.
10. Karthikeyan, B., K. Alhaf Malik, D. Bujji Babbu, K. Nithya, S. Jafar Ali Ibrahim, and NS Kalyan Chakravarthy. "Survey of Cooperative Routing Algorithms in Wireless Sensor Networks." Annals of the Romanian Society for Cell Biology (2021): 5316-5320
11. Nimmya Unnikreshanan, D. K. (2015). End to End Secure SMS Communication: A Literature Survey. Volume 4, Issue3. India: Vidya Academy of Science and Technology Thalakkott
12. Yadav, R. K. (2013). Cryptography on Android Message Applications – A Review. India: PDM College of Engineering Bahadurgarh.