Available online at: https://proceeding.researchsynergypress.com/index.php/ihsatec
Proceeding on International Halal Science and Technology Conference (IHSATEC)
ISSN 2828-1500 (Online) | 2828-1985 (Print)
Volume 1 Number 1 (2021): 90-93

Android File And Message Encrypted Application Using Advanced Encryption Standard-Vigenere and Electronic Codebook/ Public Key Cryptography Standards/Padding a Hybrid Encryption Algorithm

Montano, Celine Dianne T., Nuez, Jeric T.
College of Information and Communication Technology, Taguig City University, Philippines

Abstract

The study, entitled Android File And Message Encrypted Application Using Advanced Encryption Standard-Vigenere and Electronic Codebook/ Public Key Cryptography Standards/Padding a Hybrid Encryption Algorithm, was a proposed solution about Social Engineering and hacking. With the Data Privacy Act of 2012, the study promotes and inspires. The study's goal is to provide users with security and protection 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 illegal purposes is referred to as cyber theft. The objectives were aimed at the system's functionality, and the scope and limitations were considered to determine the study's capability and boundaries. For this case, the study proposed solutions. The first chapter provides 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 study's major argument. The Android SMS and File Manager Encrypted Application employs two distinct hybrid encryption algorithms. The prototype is the model that is appropriate in our system development because the proponents are developing a mobile application. This application promotes the Data Privacy Act, which protects and maintains the customer's or user's right to confidentiality. The survey results are positive, and almost everyone would like to have this type of application that can secure their files and messages. As a result, the proponents conclude that this application is feasible and long-term.

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

INTRODUCTION

People nowadays rely heavily on mobile phones as their primary mode of communication. SMS and file transfers on smartphones 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 realized that for their data to be secure, they must take personal responsibility for it. Because customers spend so much time on their phones, mobile apps are a good place to start. Navigating the murky waters of app store scams, on the other hand, is time-consuming and difficult. There are thousands of privacy-conscious apps to choose from, each with its own set of features and efficacy levels. So, which should you go with? Which is the most efficient? Another question is why cell phones should be protected in the first place. Hackers can use dangerous software, or malware, to get access to information on our computers, although most people are aware of the need to use computer security software. Malware can even infiltrate cellphones, which are effectively small computers that run "mobile operating systems," which may be less visible. As a result, they may be

Corresponding author
Montano, Celine Dianne T
mcelinedianne@gmail.com
DOI: https://doi.org/10.31098/ihsatec.v14i1.490

vulnerable to the same threats and vulnerabilities that affect computer operating systems. Once a cybercriminal has gained access to your device, malware can steal or even hold your data hostage. In truth, there are many ways to reveal or divulge your private chats, such as social engineering, which involves using misleading strategies or methods to persuade someone into divulging private or personal and crucial information. Encryption is one way to improve security on smartphones, according to the Data Privacy Act. Encryption protects mobile devices in what ways? Encryption performs several functions. A lot more than merely preventing someone from accessing your phone's dataphone, just like the lock screen. Consider a lock screen to be similar to the lock on a person's front door. A lock on a door stops an uninvited guest from entering the house and stealing personal belongings, but the homeowner must consider what the thief would do if the locks were broken and the thief gained access to the house. To protect data fully, we need to have numerous layers of defense. This is known as "defense in depth" in the security field, and encryption provides it. Encrypting data raises security to a whole new level. It renders the phone's information illegible. Even if a hacker managed to get past the locked phone screen, they might still be unable to access personal information.

LITERATURE REVIEW

SMS communication is well-designed to provide end-to-end secure communication over SMS between mobile clients using AES and MD5 encryption. The most well-known information benefit is SMS. SMS technology is used in security-sensitive industries, including e-account management and e-government. Between the versatile client (MS) and the SMS focus, SMS is sent as unencrypted. SMS messages are saved in system administrators' frameworks and can be seen by their employees. SMS does not provide a secure environment for private data transmission. Many Android developers have created a system that encrypts SMS messages using the AES algorithm. Short Message Service (SMS) has evolved into a useful tool and has played an important role in the lives of its users. SMS provides food for installation, portable money-saving, vital updates such as stock and news alarms, activity refreshes, climatic data, and business-related data. Security and impersonation concerns are at the forefront of the examination. The investigation used a fall encryption procedure designed for transmitting SMS through any type of communication channel. The quality of the computation based on the structure was focused on developing an anchored encryption procedure and adapting AES (Advanced Encryption Standard) encryption with two additional encryption layers. It looked into the system's impact on the encryption process. Security Assurance Framework for SMS Using Cascaded Encryption Algorithm is being developed by other developers. Security validation is required in all media transmission lines. Everyone desires to keep any data conveyed across unbound and anchored media transmission lines mysterious. Short Message Service (SMS) has evolved into a useful tool and has played an important role in the lives of its users. SMS provides food for installation, portable money-saving, vital updates such as stock and news alarms, activity refreshes, climatic data, and business-related data. Security and impersonation concerns are at the forefront of the examination.

RESEARCH METHODOLOGY

The prototype is the model that is appropriate in our system development because the proponents are developing a mobile application. Prototyping is a paradigm in which a prototype is produced, tested, and then reworked as needed until an acceptable prototype is achieved from which the whole system or product can be developed. It's a cycle that allows for system adjustment and repeats the rapid design if it has to be changed or updated. It is intended to communicate the key features or benefits to potential users or other stakeholders in an effective manner. It can be done in something as simple as Balsamiq or even on paper, and the goal is to visualize the main things people will be able to do with the tool as a way of assisting stakeholders in attaching the solution to the problem you are solving. This term is also frequently used by developers when they want to quickly hack together a quick version of the proposed tool to hit and work to understand or even resolve likely technical challenges. In this situation, the proponents will publish our system to the Play Store, and the group will gradually improve the scope and capabilities of the system in response to user feedback and demands. Our group will keep track of their feedback and reviews on our system, and then the proponents will design and update new versions, which will then be uploaded to the Play Store so that users may download new versions of our system.

FINDINGS AND DISCUSSION

The proponents performed a survey to learn about the users' requirements and desires. The Computer Science Students were chosen as the respondents by the researchers. There are 695 students enrolled in Computer Science. The Registrar's Office of Taguig City University provided this information. The Slovin's Formula is applied to the entire population. Hence the total number of respondents to whom the proponents should at least provide survey questionnaires is 255. Because they are more familiar with the function that we are attempting to perform, the proponents chose Computer Science Students as their respondents. In addition, the researchers interviewed a group of Computer Science students and professors. The group answers a few questions on how satisfied they are with their current mobile phone experience and how secure they are. They also added such items to the survey forms they will fill out. The survey results are positive, and nearly everyone would like to have an application like this to protect their files and messages. As a result, the proponents conclude that this use is realistic and long-term. Android SMS and File Manager Encrypted Application is for anyone who owns an Android phone. This is an application that can secure their SMS and File Manager. Encryption is the process of securing a user's message content and files in a file manager. This app will be uploaded to the Google Play Store and reviewed by users. The system's functionalities and capabilities will be maintained if the proponents monitor every user suggestion and review.

CONCLUSION AND FURTHER RESEARCH

The Android SMS and File Manager Encrypted Application employs two-hybrid encryption algorithms: the first is the AES-Vigenere Encryption Algorithm, which encrypts the contents of SMS messages, and the second is the AES/ECB/PKCS5/Padding, which encrypts the bytes of files in the file manager. This program promotes the Data Privacy Act, which protects and maintains the right to privacy of the customer or user. The proponents conducted a poll to learn about the needs and desires of the users. The survey results are positive, and almost everyone would like to have a program like this to protect their files and messages. As a result, the proponents conclude that this application is feasible and long-term. Based on the findings and conclusions reached, the following is presented. Android SMS and File Manager Encrypted Application Using AES-Vigenere and AES/ECB/PKCS5Padding a Hybrid Encryption Algorithm will be available for everyone to use and test on the Google Play Store. The proponents will review the user reviews and comments for the application's upkeep. Due to human error, the application will still require some options for password recovery. The application will send you various password recovery options via email. Enhance the program by maintaining and enhancing the system's features: The application will provide a vault for the user's encrypted files to be stored in. This can improve the security of the user's data. They are updating the application's user interface and experience for better accessibility and use by users.

REFERENCES

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.
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).
Cordero-Batac, E. R., & King Kay, C. O. (2018). Data Protection Laws of the World Philippines. Republic Act No. 10173. Philippines: DLA PIPER.
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
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.
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.
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.
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
Yadav, R. K. (2013). Cryptography on Android Message Applications – A Review. India: PDM College of Engineering Bahadurgarh.