IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11212

An Enhanced Application for Securing File Transfer Over Android Devices

Abdulrahman Mohammed Saba[1], Musa Sule Argungu[2], Salamatu Musa[3]

Department of Computer Science, Federal Polytechnic Bida, Nigeria[1]

Department of Computer Science, Kebbi State University of Science and Technology, Aliero, Nigeria[2]

Department of Computer Science, Kebbi State University of Science and Technology, Aliero, Nigeria[3]

Abstract: Smartphone have become the major part of human's life. Nowadays mobile applications are playing major role in many areas such as banking, social networking, financial applications, and entertainment and so on. Android applications and its security threats are increasing with interest due to the mass spread of smart devices, and vulnerabilities in developed applications are being exposed while mobile malicious codes are spreading. To avoid malicious codes and attacks we are designing and developing an application which provides security for transferring the file with the help of Advanced Encryption Standard (AES), where it encrypts and decrypts the data with the secret key, here transmission is done in two ways, If the file is public then file is selected and sent to particular receiver, if the file is private it ask for security key and sent towards receiver, this way we achieve the secure transmission of information (file) between end-users. The proposed mechanism was evaluated using ASP.NET based on four performance metrics: (1) Jobs Completion Times, (2) Effective Network Usage, (3) Storage Element Usage, and (4) Computing Element Usage.

Keywords: Smartphone, Mobile application, Security, Threat, Attacks, Encryption, Decryption.

I. INTRODUCTION

A mobile phone is a portable telephone that can make and receive calls over a radio frequency carrier while the user is moving within a telephone service area. The radio frequency link establishes a connection to the switching systems of a mobile phone operator, which provides access to the Public Switched Telephone Network (PSTN) [1]. In this case, a mobile application can be described as a type of software prepared to be used on smartphones and other mobile devices, including independent (without the need to access the internet) and specialized mobile services, client streaming services (access to the internet resources is available on demand), and computer games [2]. Now a day's everyone is need of smartphones for day to day communication and majorly people uses android devices which are are developed for unlimited fun for people's lives and ask made the android system to become popular in the market of smart phones. However, most of our people found it difficult in harnessing the power of these universal devices for themselves and their communities. Most of the problem with smartphones users is that we consume technology but don't know how to produce them, even though local problems can often be solved with mobile devices [3].

In this contemporary day of digital world, importance of networks, its effect and presence can't be neglected. The constant use of digital data in real life applications and its significance craved the need for a new way to ensure safety and usage of electronic gadget possessed by human [4]. Android Operating System (OS) has been, by far, the dominant mobile device OS for several years making up 86.2% of the world mobile market in quarter 2 of 2016 [5]. Hence, this makes attackers to shift target from computers to mobile devices, to overcome from such undesirable situations, this research developed a mobile application that provides security mechanism and features when sending and receiving file between two or more mobile devices.

II. LITERATURE REVIEW

We begin by surveying related work on mobile device development in general, and media leaks in particular. We also discuss existing approaches and tools for investigating the security and development offered by mobile applications.

Researchers in [6], studied the behaviour of these applications using a combination of static and dynamic analysis techniques. Our study reveals several alarming privacy risks in the Android app ecosystem, including apps that over-provision their media permissions and apps that share image and video data with other parties in unexpected ways, without user knowledge or consent. Efforts are being made by researchers to deploy blockchain on a broader domain due to its striking features. A blockchain provides secure, reliable and trust worthy data sharing environment. It records any unauthorized access to data, hence provides traceability.

However, its distributed nature weakens the controlling capability of networks. Moreover, immutable nature of blockchain can induce the threat of a majority attack on network [7]. The security of the cloud is essentially strong and

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11212

the private internet access area is also secured. But the data transmission among two secure networks is performed over untrusted network. Cloud are used to store data but in cloud data is stored at random in the cloud space so our private and sensitive data can be mismanaged and produces the redundancy during their management [8]. An implementation of an intrusion detection system (IDS) that monitors a Kerberos network, and reports and responds to malicious activities or policy violations. The designed IDS system detects anomaly activities using a Markov chain to build a stochastic model to represent Kerberos session states [9].

As we have done so much research related to our project, we found that research in [10] showed that they are using a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. This gives us agility, global scale, and durability, with "anytime, anywhere" data access. One of the cloud Storage which we are going to Use is Mongo DB Atlas which is a fully managed cloud database for modern applications. We develop techniques to (1) share capabilities for anonymity and distribute them anonymously, (2) create and checkpoint a verifiable anonymous history, and (3) support concurrent operations on a single object with a hash-chain-based history [11].

Below is the view of some researchers on mobile applications and its security:

TABLE 1: RELATED WORKS ON MOBILE APPLICATIONS AND ITS SECURITIES

S/N	Authors/Year	Title	Problem	Area/Domain	Methodology	Res. Gap
1	E. Pan, J. Ren, M. Lindorfer, C. Wilson & D. Chofffnes, 2018	Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications	Applications share image and video data with other parties in unexpected ways, without user knowledge or consent	Information Security	Empirically gathered data and measured media leaks by Android applications.	Media sent over the network should be potentially transformed before transmission
2	M. Naz, et al., 2019	A Secure Data Sharing Platform Using Blockchain and Interplanetary File System	Misuse and misinterpretation of data	Information Security	Experimental method was used to test the mechanism	Limited to the following tools: 1.Visual Studio Code 2.Ganache 3.Metamask
3	S. Sharma, and R. Sharma, 2016	Secure Data Transfer & File Sharing Use of Cloud Service for Mobile Application	1.Small data storage space and backup. 2. Data transmission among two secure networks is performed over unsecured network.	Information Security	Experiment	Limited to two algorithms: 1. Advanced Encryption Standard (AES) algorithm and 2.Message digest 5 algorithms
4	F. Al-ayed, C. Hu, and H. Liu, 2018	An Efficient Practice of Privacy	Malicious behaviours	Information Security	Experiment	Limited to Kerberos and Markov Chain

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11212

		Implementation: Kerberos and Markov Chain to Secure File Transfer Sessions				
5	R. B. Madhumala, S. Chhetri, K. C. Akshatha and H. Jain, 2021	Secure File Storage & Sharing on Cloud Using Cryptography	Security Threat	Information Security	Experiment	Add push notifications and shareable links that will expire after the stipulated time
6	Y. Hu, S. Kumar, and R. A. Popa, 2020	Ghostor: Toward a Secure Data-Sharing System from Decentralized Trust	Weak threats models	Information Security	Experiment	Limited to decentralized trust
7	D. Hadapad and S. N. Raj, 2013 [12].	Android Application For Secure File Transferring Using Data Encryption Standard	Malicious application	Information Security	Empirical	Supporting tool used is android SDK and it will run on windows XP/Vista/07/08 only

III. CURRENT LIMITATIONS

From the review of related works on mobile applications and its securities, it is observed that most of the researchers focuses on the development and security of the application. Android studio is the wide used software with Software Development Kit (SDK) as its supporting tool and some research works are limited to some operating system. However, this research is to develop an application using the successor to Microsoft's Active Server Pages (ASP) technology, ASP.NET which is built on Common Language Runtime (CLR) environment that will run across android devices and development environment is supported for MacOS, Linux and Windows operating systems.

IV. AIM AND OBECTIVES

The main aim of this research is to develop a mobile application for securing file transfer over android devices. In pursuance of this central goal, the following sub-objectives are formulated:

i. To develop a mechanism that will encrypt and secure files.
ii. To design an interface that allows users to download files.
iii. To evaluate the proposed mechanism using jobs completion times, network bandwidth consumption, storage element usage and computational element usage metrics using ASP.NET.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11212

V. PROPOSED SYSTEM

This application is focused on authenticating the user for both encryption and decryption of files. We are trying to create an application that lets users encrypt and decrypt any type of file without changes in their sizes during encryption and decryption process. The application allows users to download files in encrypted form and most importantly, the application works smoothly in an effective network environments.

ARCHITECTURAL DIAGRAM

The architecture diagram for proposed system has a client-server architecture, the application server stores your work and help you keep records of your projects. In this web application, users can transfer files in encrypted form. The password based encryption tool lets users enter a unique set of passwords to encrypt the file and same applied to the password based decryption tool that allows user to also enter a unique set of passwords to decrypt file. The below system architecture is adopted for this research:

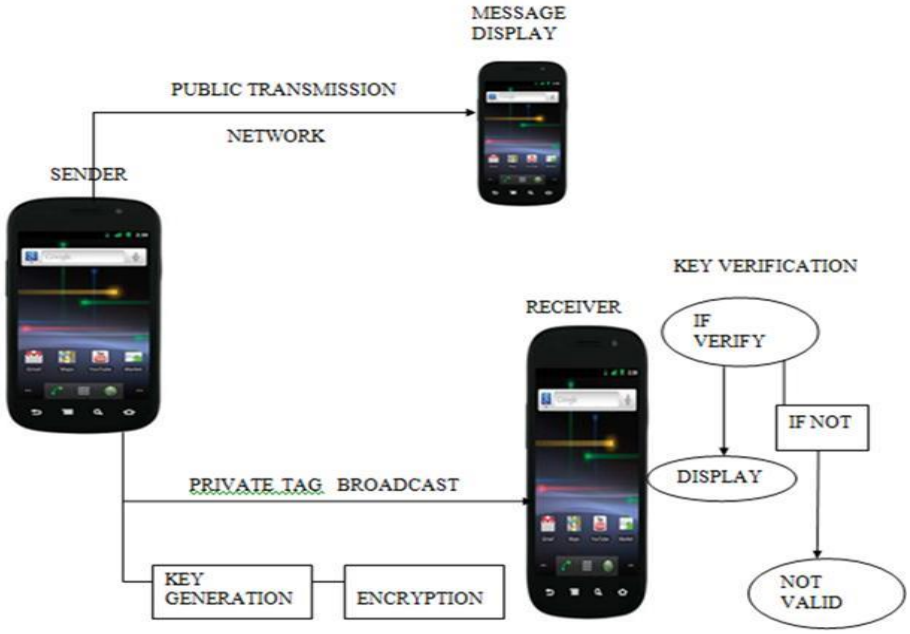

Fig. 1 System design architecture (D. Hadapad and S. N. Raj, 2013)

The above diagram represents the system architecture which gives an overview of the work flow, it includes the android devices, transfer mode, encryption, decryption and random key generation. As a web application based application, there is need for internet access for transferring of files on this application. The transfer mode is in two ways (1) public mode, which has nothing to do with security key when transferring files from one android device to another while (2) private mode, it uses the security features of both encryption and decryption of files from one android device to another. Our research is improved by providing two steps verification for the application, which is the authentication for encryption and decryption and the verification process shows that if the login credentials is valid then it displays and sent to the receiver's device. Otherwise if the login credentials are not valid then it will show not valid message.

VI. METHODOLOGY

This research adopts the Design Research Methodology (DRM) for its exceptional ability to generate a prototype solution close to reality [13]. The following design methods are used for this research:

A. Login for Encryption

The user must be authenticated before the whole process occurs. The application will provide a secure login to the application. By clicking on the Log in button, the user will be redirected to login form where the user must enter a valid username and password to be authenticated and use the application. If the user provides an invalid credential, then the login will fail and the end-user won't be able to log in.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11212

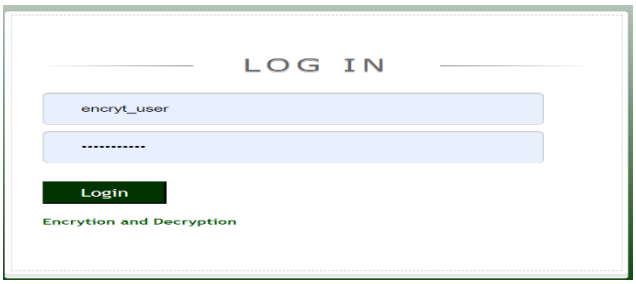

Fig. 2 Login encryption page

B. **Text Encryption**

The encryption tool can be accessed via the encrypt button on the menu. The user gets redirected to the tool once the button is clicked. The Encryption process mainly involves three steps:

Step 1: Input the messages in the box

Step 2: Click on encrypt message

Step 3: The message is encrypted

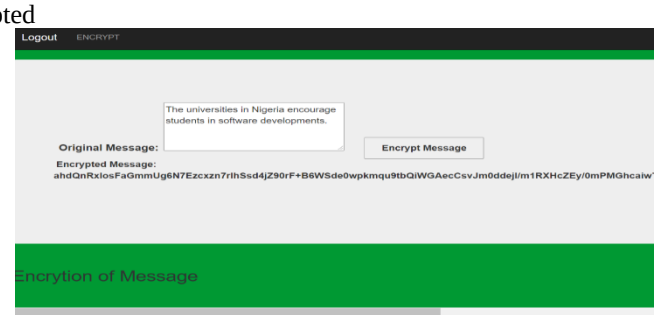

Fig. 3 Text encryption page

C. **File Encryption with Attachment**

The encryption tool can be accessed via the encrypt button on the menu. The user gets redirected to the tool once the button is clicked. The Encryption process mainly involves three steps:

Step 1: Attach a file

Step 2: Click on encrypt file

Step 3: The file is encrypted and automatically saved on the android device

Fig. 4 File encryption page

D. **Login for Decryption**

The user must also be authenticated before the whole process occurs. The application will provide a secure login to the application. By clicking on the Log in button, the user will be redirected to login form where the user must enter a valid username and password to be authenticated and use the application. If the user provides an invalid credential, then the login will fail and the end-user won't be able to log in.

Fig. 5 Login decryption page

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11212

E. **Text Decryption**

The decryption tool can be accessed via the decrypt button on the menu. The user gets redirected to the tool once the button is clicked. The decryption process mainly involves three steps:

Step 1: Input the messages in the box

Step 2: Click on decrypt message

Step 3: The message is decrypted

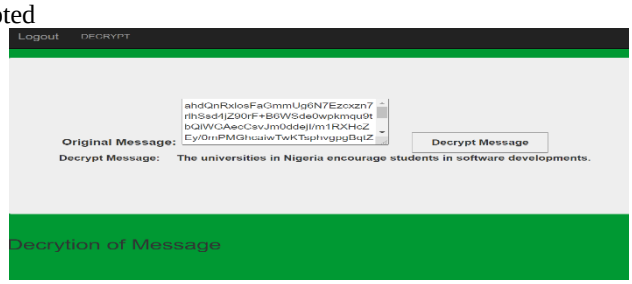

Fig. 6 Text decryption page

F. **File Decryption with Attachment**

The decryption tool can be accessed via the decrypt button on the menu. The user gets redirected to the tool once the button is clicked. The decryption process mainly involves three steps:

Step 1: Attach a file

Step 2: Click on decrypt file

Step 3: The file is decrypted and automatically saved on the android device

Fig. 7 File decryption page

VII. RESULTS AND DISCUSSIONS

In this research, the proposed web application was built to provide an encryption/decryption tool and securely transfer files using ASP.NET modules. From the practical implementation we got the following results:

TABLE 2: ENCRYPTED AND DECRYPTED TIME IN SECONDS

No of Jobs	File Name	Encrypted Time	Decryption Time
1	Paper_format_IJCSMC.doc	1	1
2	NDI B&F S2019_2020.xlsx	1	1
3	My Thesis.pdf	1	1
4	Boss.jpg	1	1
5	Rifan media.mp3	1	1
6	Justice & fairness.mp4	1	1

Table 2, shows the time taken for encryption and decryption of the files in our application. The Encryption and Decryption tool takes almost similar time to encrypt and decrypt the file, although it may vary with size of the file.

TABLE 3: ENCRYPTED AND DECRYPTED FILE SIZE IN KILOBYTES

No of Jobs	File Name	Original size	Encrypted File Size	Decrypted File Size
1	Paper_format_IJCSMC.doc	460	460	460
2	NDI B&F S2019_2020.xlsx	51.76	51.78	51.76
3	My Thesis.pdf	595	595	595
4	Boss.jpg	145	145	145
5	Rifan media.mp3	586	586	586
6	Justice & fairness.mp4	435	435	435

Impact Factor 7.39 ⁜ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11212

Table 3, it shows that there is a little difference in encrypted file size. This happens because the blocking length in the header cipher text file is caused by both the encryption process and the use of the extension .encrypted. But the decrypted file does not change the file contents and maintains the original size. Also the tool can encrypt various file types. It is also observed that this application maintains almost all except a little of the encrypted file size.

VIII. CONCLUSION

The coverage of this research work has unlocked a number of avenues for further study. Despite the experiments, comprehensive discussions and analysis of the obtained results, yet, this research is subject to further enhancement in many aspects. This section highlights on the possible areas of improvement in this research. As the future of mobile application is shifting to security based computing infrastructure, which evolves to provide a platform, which will support a variety of operating systems, including programming languages, tools and the cloud computing, this research could be expanded to cover the full mobile application security.
This research addressed the problems of leaked files and malicious codes and applications. In the future, there are plans to compare two or more secure file sharing mechanisms based on selected features such as job completion time, network usage, storage and computational usage.

ACKNOWLEDGMENT

First of all, we will like to express our gratitude to Allah for seeing us through this program successfully, we also like to express our utmost gratitude to our main supervisor **Dr. Musa Sule Argungu** for the immense support, motivation and encouragement he has given us throughout the duration of this work. He has painstakingly read every line of our work and offered useful suggestions that have helped in the conduct and compilation of this work. Parts of this work would not have been possible without the support of my great friend, **Sayuti Musa Shafi'i and Salihu Isah Kantigi,** they have been of the greatest help throughout the time of this research, **Dr. Musa Sule Argungu** Research Group, friends and the host of others, too numerous to mention, have all provided the much needed help support that saw to the completion of this work. Thank you very much for your tremendous efforts.

REFERENCE

[1] B. R. Goud and M. Gopichand, Mobile Application Development, Shamshabad, India: Vardhaman College of Engineering, 2017.
[2] W. Chmielarz, "The Usage of Smartphone and Mobile Applications from the Point of View of Customers in Poland," MDPI, pp. 1–13, Apr. 2020.
[3] E. W. Patton, M. Tissenbaum, F. Harunani, "MIT App Inventor: Obectives, Design and Development," Massachusetts Institute of Technology, pp. 31–49, May. 2019.
[4] E. O. Ibam, O. K. Boyinbode, and I. O. Ayelabowo, "Crypto Model of Real-Time Audio Streaming Across Paired Mobile Devices," EAI Endorsed Transactions on Mobile Communications and Applications, pp. 1–8, Oct. 2019.
[5] T. Nguyen, J. T. MacDonald, and W. B. Glisson, "Exploitation and Detection of a Malicious Mobile Application," Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 6181–6190, 2017.
[6] E. Pan, J. Ren, M. Lindorfer, C. Wilson & D. Chofffnes, "Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications," Proceedings on Privacy Enhancing Technologies, pp. 33–50, Jun. 2018.
[7] M. Naz, C. Zhu, F. A. Al-zahrani, R. Khalid, N. avaid, A. M. Qamar, M. K. Afzal and M. Shafiq, "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," MDPI, vol. 11, pp. 1–24, Dec. 2019.
[8] S. Sharma, and R. Sharma, "Secure Data Transfer & File Sharing Use of Cloud Service for Mobile Application," IJCSIT, pp. 30–33, 2016.
[9] F. Al-ayed, C. Hu, and H. Liu, "An Efficient Practice of Privacy Implementation: Kerberos and Markov Chain to Secure File Transfer Sessions," International Journal of Network Security., vol. 20, pp. 655–663, Jul. 2018.
[10] R. B. Madhumala, S. Chhetri, K. C. Akshatha and H. Jain, "Secure File Storage & Sharing on Cloud Using Cryptography," International Journal of Computer Science and Mobile Computing., vol. 10, pp. 49–59, May. 2021.
[11] Y. Hu, S. Kumar, and R. A. Popa, "Ghostor: Toward a Secure Data-Sharing System from Decentralized Trust," Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI '20), pp. 851–877, Feb. 2020.
[12] D. Hadapad and S. N. Raj, "Android Application for Securing File Transfer using Data Encryption Standard," International Journal of Engineering Research & Technology, vol. 2, pp. 1890–1895, Jul. 2013.
[13] M. S. Argungu, "An Enhanced Dynamic Replica Creation and Eviction Mechanism in Data Grid Federation Environment," PhD. thesis, Universiti Utara Malaysia, Malaysia, May. 2018.

