Journal of Applied Computer Science & Artificial Intelligence

Research Paper Vol.-2, Issue- 1, December 2021 ISSN: 2582-8673

A Novel Platform for Secure Communication - VirtuAll

Bikramjit Sarkar[1*], Aritra Dey[2], Somnath Maity[2], Tanmoy Nath[2], Tanmoy Kumar Paul[2], Ankit Bharati[2]

[1] Associate Professor & PG Coordinator, Dept. of Computer Science and Engineering, JIS College of Engineering.
sarkar.bikramjit.@gmail.com

2 Final year student on the Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India

Available online at: http://jacsai.org/

***Abstract*—** Short Message Service (SMS) is a totally famous manner for mobile cell smartphone and portable tool clients to supply and get hold of simple textual content messages. Unfortunately, SMS does no longer offer a comfortable environment for one-of-a-type information finally of transmission. This paper gives with an SMS encryption for cellular communication on Android message software program. The transmission of an SMS in cellular communication is not at ease.[1] Therefore, we've got were given completed 3 of block cipher symmetric cryptography algorithms (i.E., RSA, AES set of rules) and in comparison among three of them in terms of encryption and decryption get rid of time. The confidentiality and integrity mechanisms are incredible targeted as non-compulsory protection skills that may be made available, but they may be no longer obligatory requirements for SMS tool implementation. Users should be conscious that SMS messages is probably assignment to interception. Solutions which include encrypted SMS need to be considered if there may be a want to deliver touchy information through SMS. The messages are encrypted via strong cryptographic algorithms. The encrypted message received with the resource of the customer decrypt the message with the beneficial useful resource of manner of authentication. This is only identified to man or woman. It makes use of RSA set of tips for cozy keys and AES set of recommendations to relaxed message.

***Keywords*—** SMS, encryption, RSA, AES, authentication, cryptography

I. INTRODUCTION

Today, SMS is becoming increasingly popular among mobile phone customers. SMS is a problem for text messaging, internet, or mobile communication systems, using standard communication systems that allow text messaging of text content exchanges between fixed lines or mobile smartphones. [2] Users can use SMS to deliver or collect from one person, or girlfriends and ladies, non-public messages, email notifications, recording services, college hobbies, teacher notification, hobby posts, and stock references. However, the difficulty of SMS security remains a difficult open task. SMS is now the most common form of communication. The protection of SMS messages is not but important and difficult to enforce. Privacy and integrity measures are very clear as mandatory security features that can be made available, but will not be mandatory for the use of an SMS device.

01. Users want to note that SMS messages are likely to be blocked.

02. Shared SMS written solutions should be considered if there is a need to send emotional records via SMS. [4]

03. Messages are encrypted in the form of solid cryptographic algorithms.

04. Encrypted message received by a client by deleting the message with an active verification tool. This is personally visible to the consumer.

05. Uses RSA algorithm with secure keys and AES algorithm to protect message.

213 words (Less than 1 page)

II. RELATED WORK

Key technology: The character have to set a lock pattern to provide a totally particular key.
Sender: A man or woman can ship messages with the idea that they are encrypted as soon as they send it, wherein case the patron should upload a mobile cellphone kind and elegant public key.
Encryption: Encryption is the interpretation of statistics that must be a mystery code. Encryption is an clean way to achieve the safety of records. To view encrypted messages, you want get admission to to a mystery key or password that lets in you to delete it. Unwritten information are known as

clean textual content; encrypted figures are referred to as cipher text. [5]

Coding: It is the alternative of encryption that in the end offers the character a easy and accurate text. In encryption, the encryption set of rules uses a non-public key (public key encryption infrastructure) or a mystery key (human key encryption infrastructure) that translates facts from cipher textual content content material fabric to human readable text content material**.**

III.METHODOLOGY

Design and Implementation

The SMS messaging app works via SMS on the Android platform, where SMS is written in the first step on the sender's side, digitally signed in the second step and sent in the last step (i.e., the Recipient side) which includes

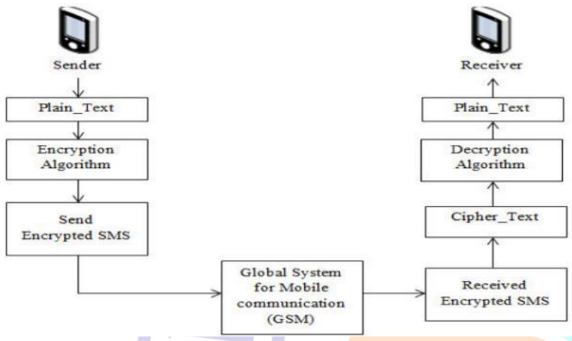


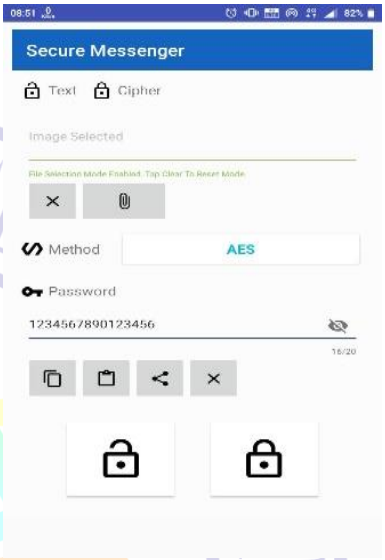
Figure 01: application construction

to reverse everything that happened in the encryption process As mentioned earlier, this app has been tested on Android OS, v4.1.2 (Jelly Bean), 1 GHz Cortex-A5 mobile processor with dual SIM option, and 2 GB Internal Memory and RAM 512 MB . Activity data is collected using a random SMS message set (i.e., Plaintext) with a different mobile size 107 words (Less than 1 page)

Figure 02: application architecture

get the encryption cipher symmetric cryptography algorithms AES algorithm. [9]

Figure 03: application design



IV.RESULTS AND DISCUSSION

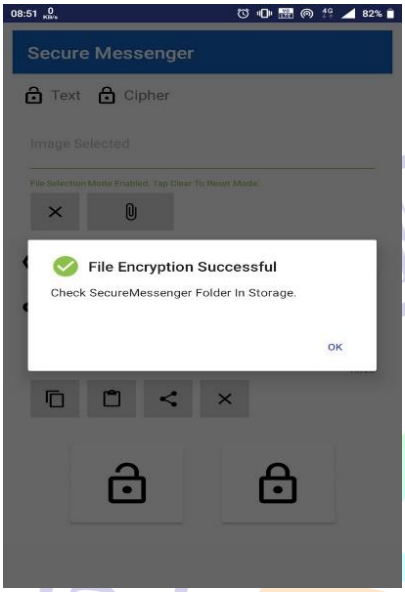
1.According to the picture in bellow, there are a media file section for choosing any kind of image as your wish from mobile storage and the application also have a password generating section.[6]

2.The first thing we have to do is go to the media file section and select the particular image that you want to encrypted. When once your selection process is over and the image file selected successfully and the application send a pop-up message as like “file selected successfully”.

4.After that we have to come the password section. Then create a password whatever you want like picture in bellow.

5.After adding the image file successfully and generating the password, in the application shows two option one is lock and another one is unlocked below the password section.6. Go to the lock option and touch it, your normal image file convert to encrypted image file and save to the secure messenger folder in your mobile.

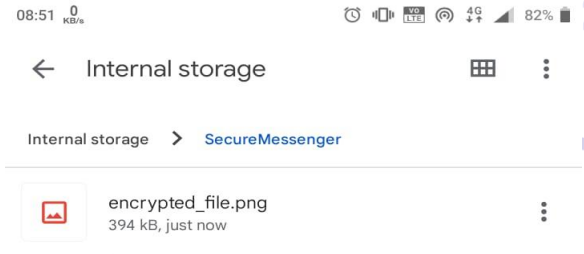
Figure 04: Encryption Procedure for Image encryption through AES Method



Result: -
you can see the encrypted image save to the secure message folder in mobile.

Image Encryption to normal image (AES Method)

Figure 05: encrypted file on phone



Decryption Procedure for Image encryption through AES Method:
1.First thing we have to do go to the secure message folder and select the encrypted image.
2. When once your selection process is over and the image file selected successfully and the application send a pop-up message as like “file selected successfully”.
3.After selecting process is over go to password section and enter the password.
4. Above the image shows lock and unlock option below the password section go to the unlock option and touch it, your encrypted image converts to normal image and save to the secure messenger folder in your mobile [10]

Result: -
you can see the decrypted image save to the secure message folder in mobile.

Figure 06: Image decryption to normal image (AES Method)

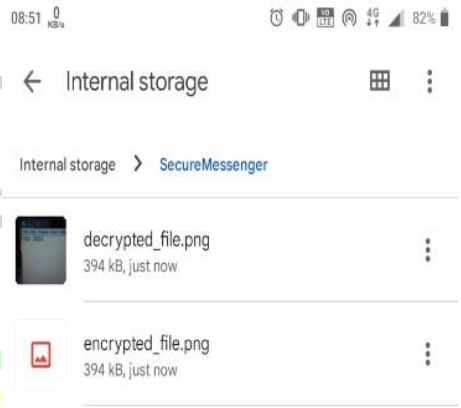
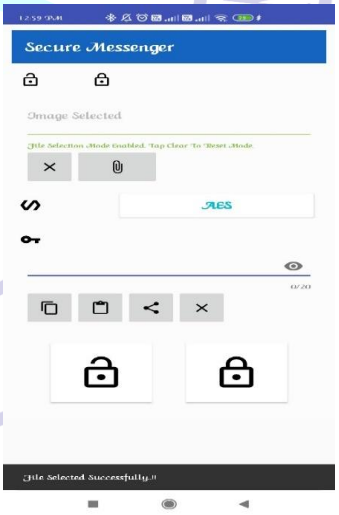


Figure 07: Image and Text file after encryption



V. Conclusion and Future Scope

Using SMS for verbal exchange and facts change, care need to be taken at the identical time as sensitive statistics is transmitted using SMS via unsecure channel. The clients want to be aware that SMS messages might be undertaking to interception from un-prison get admission to.[7] In this paper, the software application program of SMS encryption for a number of block cipher cryptographic encryption set of pointers (i.E., AES) on android software program program software software program application software program software program software program has been designed and finished. The SMS encryption software program application utility software application software program software software software program program software program is strolling in the cellular mobile mobile cellphone which does now not require any more encryption gadgets. The experimental check confirmed that the encryption set of guidelines (i.E., AES) is appropriate and easy to area into effect in cellular tool.

- Now a day security is the most valuable thing in our life that's why we will build this application in such a way that it can be used on all the platforms.
- We will try to develop a history list for the encryption and decryption contents..
- We can delete any file from that list of history encryption and decryption so that everytime we whant to delete or share any previous content and can be easier.
- We can add various types of encryption algorithm to encrypt and decrypt data.
- We can enhance the app to encrypt confidential data or file and also in decryption.[11]
- We want to active an automated message send system so that we just need to select the time and email id of a user and our application can automatically decrypt/encrypt a file and send it to the desired user at the ideal time.
- The application will show the messages to the recipient in decrypted mode. The recipient will not have to decrypt the messages.
- Features like End-to-End encryption can be used in case of audio and video calling.

References

[1] Hybrid Compression Encryption Technique for Securing SMS
[2] Tarek M Mahmoud
[3] Bahgat A. Abdel-latef 2009
[4] SMS Encryption Using 3D-AES Block Cipher on Android Message Application
[5] December 2013
Real Implantation for SMS Encryption–Based on Android Message Application Monther H. M. Al-Bsool Department of Information Technology, AL-Balqa' Applied University/ AL-Huson College, PO box 50, Al-Huson, Irbid – Jordan
[6] [4] Real Implantation for SMS Encryption–Based on Android Message Application,July 2016
[7] Authors:Monther Al-Bsool,Al-Balqa' Applied University
[8] [5] IJCSMC, Vol. 8, Issue. 5, May 2019, pg.132 – 142
[9] [6] SMS SECURITY SYSTEM USING ENCRYPTION TECHNIQUES
[10] IJCSMC, 2019,IJCSMC Journal IJCSMC Journal ,jitha p v,Ambarish A
[14] M. Bishop. Computer Security: Art and Science. Addison-Wesley, 2002.
[15] K. Fu, E. Sit, K. Smith, and N. Feamster. Dos and Don'ts of Client Authentication on the Web. In Proceedings of the 10th conference on USENIX Security Symposium-Volume 10, pages 19{19. USENIX Association, 2001.
[16] B. Lampson, M. Abadi, M. Burrows, and E. Wobber. Authentication in distributed systems: Theory and practice. ACM Transactions on Computer Systems (TOCS), 10(4):265{310, 1992.
[11] W. Stallings. Cryptography and network security: principles and practice. Prentice Hall Press, 2010.

Authors Profile

Dr. Bikramjit Sarkar).
Associate Professor & PG Coordinator
Dept. of Computer Science and Engineering
JIS College of Engineering

Mr. Aritra Dey
Registration No : 001642
4th year student on the Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India
Email: aritra1999.dey@gmail.com
Contact: 85829 70748

Mr. Somnath Maity
Registration No : 003163
4th year student on the Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India
Email: s.maity30996@gmail.com
Contact: 87772 60977

Mr. Tanmoy Nath
Registration No : 181230110110
4th year student on the Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India
Email: nathtanmoy011@gmail.com
Contact: 70638 52644

Mr. Tanmoy Kumar Paul
Registration No : 181230110109
4th year student on the Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India
Email: paultanmoy9163@gmail.com
Contact: 91632 24695

Mr. Ankit Bharati
Registration No : 008479
4th year student on the Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India
Email: ankitbharati2905@gmail.com
Contact: 6291 787 205