End-To-End Encryption For Android Chatting App

Rushikesh Dighe[1], Rohit Katare[2], Akshay Bodhare[3], Prathmesh Pote[4]
[1, 2, 3, 4] Dept of Information Technology
[1, 2, 3, 4] Sir visvesvaraya Institute Of Technology, Nashik

Abstract- *Here, we'll make a "encryption-decryption" programme. By constructing these programmes, we will be able to understand how to convert plaintext to ciphertext and encrypt our communication. Before converting our communication back to readable form, we'll employ a key to decode it. This tutorial will help you understand the basics of cryptography for Android development.*

I. INTRODUCTION

These days, Android phones are becoming increasingly popular. For a few bucks, everyone may receive an Android phone, as well as an Akash Tablet for students who use the Android operating system. Instant messaging programmes like WhatsApp, Apple iMessage, and BlackBerry Messenger have eclipsed traditional SMS services as the primary form of communication for millions of smartphone users.Instant messaging will become increasingly important in commercial areas such as e-commerce, mobile banking, administrative usage, and ordinary correspondence in the future. Furthermore, instant messaging has become a popular wireless service all over the world since it allows a customer to communicate with any mobile phone subscriber anywhere on the earth.

In recent years, security services such as data confidentiality, authentication, integrity, non-repudiation, access control, and availability have grown more critical. qualities that should be considered while creating safe application frameworks Security elements like these are accessible in mobile chat systems, but there is no plan in place for them. Both the customer and the server of the mobile chat system are subject to passive and hostile strikes.The arrival of communication content is accompanied with passive hazards. While active risks converge, traffic is being examined. adjusting the message's content, masquerading, replaying, andrefusal to provide service (DoS). To be honest, all of the aforementioned dangers exist. are suitable for mobile talking communication.

II. EXISTING SYSTEM

Several chat systems claim to provide safe administrations, but their entire architecture is not available to the public. DES (Data Encryption Standard) is a symmetric cryptographic algorithm that was recognised as a standard for safeguarding non-classified information in the United States by the former National Bureau of Standards (now known as National Institute of Standards and Technology) in January 1977. It's often used to safeguard sensitive data and verify financial transactions..

H.C. Chen et presented a new suggestion for Mobile Text Chat using a revolution session key based transposition cryptosystem plan in May of 2014. Their suggested scheme just handles secure content translation for the mobile chat framework. It adapted the classical block cypher, substitution, and transposition technologies. The network pivot innovation can also generate a new session key. Using the rapid encryption technique, it may be simply implemented to transmit over mobile devices.

R.N. Akram et al. examined the security and privacy-preserving features offered by existing mobile chat services in July of 2014. They also advance a basic system for an end-to-end security and protection mobile chat service, as well as associated requirements. They also advance a basic system for an end-to-end security and protection mobile chat service, as well as associated requirements.Their plan was put into action in order to create a proof-of-concept and assess the technical complexity of meeting the stipulated security and privacy standards.Hsing-Chung Chen et al. planned the basic system for secure end-to-end mobile chat plan and its related requirements in November of 2014. Their idea has been adopted to allow alternative authentication and avoid password estimating attacks as well as undetected on-line password estimating.

III. CONCLUSION FROM EXISTING SYSTEM

There is no specific encryption technique for the Android OS. Currently, certain encryption methods are available that are secure but resource heavy, whereas others are not resource intensive but unsecure. If we employ a high-cost encryption method, the software may halt on Android phones with poor setup, resulting in a bad user experience. However, because we are unable to employ alternative encryption algorithms due to security concerns, we must find an ideal approach that gives maximum security while utilising the fewest resources possible.

IV. BACKGROUND

Smartphone penetration is quite high on a worldwide basis. According to an Ericsson mobility analysis, smartphone subscriptions will reach 6.1 billion by 2020, with 90 percent of the world's population over the age of 6 having access to a mobile phone. There are several causes for this rapid rise, the most prominent of which being more powerful hardware and lower production costs. These considerations make smartphones more inexpensive in growing markets like China and India, which each have a population of over one billion people. Smartphone users have access to millions of apps in various app stores, and while there are several smartphone operating systems, two are the most popular: Android and iOS. Each of these operating systems has its own set of features.

4.1. Smartphone Ecosystem :- Anyone, including freelance developers and corporations, may distribute their programmes to the general public through the application store ecosystem. Anyone with an Internet connection who wishes to explore and search through the app store can find the app after it has been approved by the store.An environment like this may help any industry. Smartphone penetration and Internet access are helping several businesses, including insurance, finance, healthcare, and even government organisations, better serve their clients and stakeholders. IM apps are among the most popular mobile applications, with hundreds of millions of users worldwide and a slew of firms offering such a service. Each of these operating systems has a large application ecosystem, allowing billions of people to pick and choose the services they want to access from a device in their pocket. As of July 2014, there were 1,300,000 Android applications in the Google Play Store and 1,200,000 iOS apps in the Apple Store.

4.2. Security Services for Mobile Instant Messaging :- Relevant dangers to any chat application should be identified and defined in order to evaluate it from a security standpoint. A brief explanation of several security elements is provided in the following sections.

security has 3 key components: confidentiality, integrity and availability . Confidentiality ensures that certain sort of records may be accesses by means of legal parties. Integrity approach records can be modified simplest via supposed and licensed events. Availability method that information is available to legal parties at appropriate instances.

4.2.1.Confidentiality :- Messages transferred between two parties over a communication channel should be accessible only by the intended parties, according to confidentiality. Encryption is the method that ensures confidentiality between two parties in order to achieve this purpose. A cryptographic technique is used to encrypt a communication, which can only be read by the intended recipient.

4.2.2. Cryptography :-Cryptography is the study and practise of strategies for securing communication between two entities while a third entity (adversary) is present. Cryptography aids in the creation of an environment or media channel that supports secrecy, integrity, user authentication, and non-repudiation. In cryptography, there are two types of algorithms. Strictly speaking, there are two types of cryptography: symmetric key and public key. Both parties utilise a common key to encrypt and decode communications in symmetric key encryption . Because the opponent does not have access to the shared key, even if he intercepts the communication channel, he will only get encrypted communications that he cannot decipher. Public key cryptography, is also known as asymmetric cryptography, uses anThe programme creates two keys when using public key cryptography. The public key can be published or broadcast to the entire world, while the private key is kept private. In this procedure, one party encrypts the message and sends it to the other using the second party's public key. The encrypted communication is received by the second party, who decrypts it using its own private key. If a malevolent hacker intercepts the communication channel, he will only get encrypted communications that he will be unable to decipher because he lacks the recipient's private key.

4.2.3. Authentication :- One of the most fundamental parts of security is authentication, which requires an entity to identify itself before or during contact. This prevents any attack or harmful conduct in which a malicious user impersonates the user and presents himself to the server as the genuine user. Weak authentication and strong authentication are the two types of authentication techniques. Weak authentication (one-factor authentication) refers to when an entity only employs one sort of identifying credential, such as a PIN* or password-based authentication. It is seen as a flaw in the system since it is vulnerable to a variety of assaults, including brute force attacks.A brute force attack is one in which a malicious person attempts a large number of passwords until they find one that matches the user's selected password. Strong authentication is often achieved through the use of challenge-response cryptography. The client must authenticate his identity and verify himself to the server using numerous factors in this system. One-time passwords (OTP) and certificate-based authentication are two methods for performing such authentication (CBA). A shared secret key is stored on a device owned by the entity, and the system generates one-time passwords using this shared secret key.

4.2.4. Integrity :- The term "integrity" refers to the assurance that a communication has not been modified or changed throughout its passage between organisations. Eavesdropping on the communication channel allows an attacker to change or even replace the message with a new one. In the area of information security, hashing is a technique for achieving such a goal. A cryptographic hash function is a function that converts an encrypted message into an integer of a defined length. A hash function is a one-way function, which means that once someone obtains a hash output, it cannot be reversed.

V. THE PROPOSED APPLICATION MODEL

The system is an Android app that allows users to communicate with one another in a secure manner, and End-to-end secure communication is provided to them. This Data encryption is used in the communication process. sent in an encrypted manner to the internet server and The data is then decrypted and shown as a result of specific searches to the user who will receive the message The application is made up of a number of different components. Design of user interfaces that allow the user to execute the conversation With the rest of the users, you'll be able to complete the procedure. Whether both users are online or the intended receiver is online, the message server facilitates message exchange between them. The message will be stored in the oine message storage if the receiver is oine. These communications are momentarily saved and then destroyed once they have been delivered to their intended recipients. The dotted line depicts virtual communication between users of mobile phones 'A' and 'B' via a messaging server.

The safety of the application relies upon largely on Elliptic Curve Cryptography, and using ECDH set of rules that's a variant of the Diffie-Hellman calculation for elliptic bends. it’s far surely a key-information convention, greater than an encryption set of rules. ECDH characterizes how keys ought to be produced and exchanged between events. After the generation of the important thing pairs those key may be used to generate the comfy shared key, that is 160 bit key length. The statistics might be encrypted in uneven algorithms(AES 128 for textual content, RC4 for voice and picture) through using the generated comfortable shared key. for this reason, the encryption algorithms take key duration which differs from the generated key, the generated secret is submitted in key scheduling algorithm (KSA) with a view to be in appropriate duration shape. The proposed chatting utility employs a symmetric key encryption method where the message is encrypted and decrypted with the generated mystery key. the chosen algorithm to be employed on this system for the text message is AES 128-bits with cipher block changing mode (CBC).before encrypting the message, the generated key (one hundred sixtybit) is minimized to 128 bit length by means of choosing the primary 128bit of the generated key. in the direction of the start of the Cipher,the enter is copied to the state array using the conventions. After an initial round Key growth, the state array is modified by using actualizing a spherical feature 10, 12, or14 times (contingent upon the key duration 128, 192, 256 bit),the proposed utility makes use of 10 rounds characteristic with 128bit key length. All ten rounds are identical with the exception of the final round, which does exclude the Mix Columns()trade. The last country is then replicated to the output. also, on the decryption facet, the generated key (one hundred sixty bit) is minimized to 128 bit length. The decryption manner is theinverse of the encryption system. The method of decryption of an AES ciphertext is like the encryption procedure within the opposite order. every spherical includes the four procedures (InvShiftRows, InvSubBytes,AddRoundKey and InvMixColumns) except the remaining spherical that now not carry out the InvMixColumns. in view that sub-methods in every spherical are backward way, never like for a Feistel Despite their tight relationship, the cypher, encryption, and decryption algorithms should be run individually.

VI. SYSTEM IMPLEMENTATION

6.1. AES Algorithm :- The United States National Institute of Standards and Technology (NIST) announced in January 1997 that it will host a competition to replace DES with another block cypher known as the Advanced Encryption Standard, or AES. The plaintext square size for the encryption is 128 bits, or 16 bytes. The length of the key might be 16, 24, or 32 bytes (128, 192, or 256 bits). The key length determines whether the computation is AES-128, AES-192, or AES-256.A single 128-piece block is used as the input to the encryption and decryption techniques. A 4*4 square matrix of bytes is used to define this block. This block is duplicated in the State array, which is updated throughout each encryption or decryption step. State is duplicated to an output matrix after the last stage. The key is also represented as a square matrix of bytes. After that, this key is entered into a list of key schedule words. Each word is four bytes long, making the entire key timetable for the 128-piece key 44 words long. The cypher is made up of N rounds, the number of which is determined by the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14rounds for a 32-byte key.

6.1.1. :- What Is AES?

The Advanced Encryption Standard (AES) is a symmetric block cypher that the United States government has

chosen to safeguard confidential information. AES is used to encrypt sensitive data in software and hardware all around the world. It's critical for government computer security, cyber security, and data security. When the National Institute of Standards and Technology (NIST) recognised the need for an alternative to the Data Encryption Standard (DES), which was becoming vulnerable to brute-force assaults, AES was born.

The newer, powerful encryption method would be declassified, according to NIST, and would have to be "capable of securing sensitive government information long into the [21st] century." It was designed to be simple to implement in hardware and software, as well as in constrained contexts like a smart card, and to provide enough protection against a variety of attack tactics.

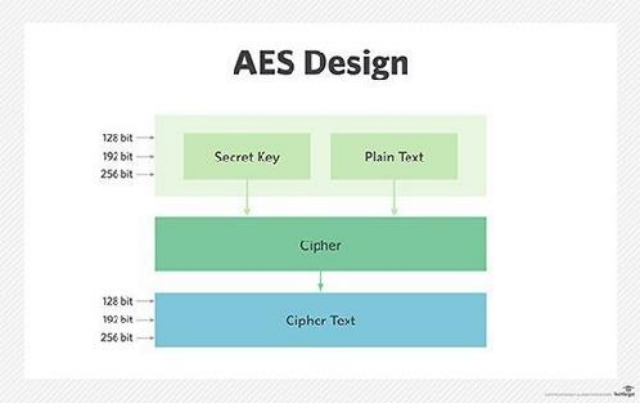
AES was developed for the US government, but it is also freely available for use in public or private, commercial or non-commercial encryption applications. However, nonprofit groups that choose to employ AES are subject to export control restrictions imposed by the United States.

6.1.2. :- How AES Works?

Three block cyphers are included in AES:

- AES-128 encrypts and decrypts a block of messages with a 128-bit key length.
- AES-192 encrypts and decrypts a block of messages with a 192-bit key length.
- AES-256 encrypts and decrypts a block of messages with a 256-bit key length.

Each cypher encrypts and decrypts data in 128-bit blocks using 128, 192, and 256-bit cryptographic keys, respectively. Symmetric cyphers, often known as secret key cyphers, encrypt and decode using the same key. Both the sender and the recipient must have access to the same secret key. Information is classified by the government into three categories: confidential, secret, and top secret. The Confidential and Secret levels can be protected with any Key lengths of 192 or 256 bits are required for top-secret information.For 128-bit keys, there are 10 rounds, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A round includes of numerous processing stages that change the input plaintext into the final output of ciphertext, including substitution, transposition, and mixing.



The AES encryption technique specifies a number of changes to be applied to data in an array. The cipher's initial step is to organise the data into an array, following which the cypher modifications are done over and over again.

The replacement of data using a substitution table is the first transformation in the AES encryption algorithm. The data rows are shifted in the second transformation. The third is a column mix. Each column undergoes the final transformation, which employs a different component of the encryption key. Longer keys need more rounds.

6.1.3. What are the features of AES?

The new AES algorithm must be a block cypher capable of processing 128-bit blocks and employing keys with sizes of 128, 192, and 256 bits, according to NIST.

The following were some of the other criteria for becoming the next AES algorithm:

Security. In comparison to other submitted cyphers, competing algorithms were to be rated on their ability to withstand assault. The competition's most essential factor was supposed to be security strength.

Cost. The potential algorithms were to be evaluated on computational and memory efficiency before being provided on a worldwide, nonexclusive, and royalty-free basis.

Implementation. The algorithm's versatility, appropriateness for hardware or software implementation, and general simplicity were all factors to consider.

VII. RESULTS AND DISCUSSIONS

The suggested system was installed and tested on a variety of Android-based mobile phone devices with varying CPU capabilities and Random Access Memories (RAM) to

confirm that it functions effectively on all of them. Table 1 lists the many types of phone handsets that were utilised to implement and test the system, as well as their specs.

Table 1: Specifications of the test devices

Device Name	Android Version	RAM	CPU
Vivo Y53	7.0	2 GB	1.4 Ghz
Oppo A3S	7.0	3 GB	1.8 Ghz
Mi Note 5 Pro	8	4 GB	1.8 Ghz

Table 2 shows the outcomes of encrypting and decrypting text message fragments. The findings are expressed in milliseconds of execution time. The AES standard is utilised to encrypt text messages in the proposed application, which is slower than alternative block cyphers but offers more security. Table 2 illustrates that the findings are acceptable execution speed for mobile phone processors with limited power and cost resources, real-time computing needs, and other special features such as limited programmability. It's worth noting that, as seen in (Mi Note 5 pro), time encryption and decryption, as well as CPU capabilities and Random Access Memories (RAM), are influenced by available memory and smartphone usage.

Table 2: Text message encryption/decryption time

Size In Bytes	Time (ms)					
	Vivo Y53		Oppo A3S		Mi Note 5 Pro	
	Enc	Dec	Enc	Dec	Enc	Dec
32	17	20	19	22	21	24
128	22	24	20	23	23	29
512	30	25	21	24	37	31
2048	34	27	23	26	39	33
4096	43	37	24	27	42	36

VIII. SYSTEM REQUIREMENT AND SPECIFICATION

8.1 Requirements to Develop/Run Android Application on PC:-

Hardware Requirements

- Minimum 1Gb RAM
- Minimum 20 GB HDD
- Dual Core processor or above

Software requirements

- Eclipse
- JDK compiler 1.5 and above
- SDK manager Revision 21
- ADT 21.0.0
- At least one Android Platform Package (prefer API 10)

8.2 Requirements to Run Android Application on Mobile:-

- 600MHz processor
- 128 MB RAM
- Android-2.3 and above OS on Mobile/Simulator
- Minimum API Level 10
- 525 KB memory on SD card or phone memory.
- At least Medium Screen Density Mobile

8.3 Connectivity Requirements:-

- In order to use encrypted message service over internet your mobile/emulator (PC) must connected to internet.
- To use chat service you must have your own account on that service.

IX. CONCLUSION

Users that wish to transmit text messages to each other without the need for extra hardware or physical tokens can use the suggested architecture for a secure mobile chat application, which ensures confidentiality, integrity, and privacy. Users may be certain that no one, even the service provider, would be able to access their communications. Even if the phone falls into the wrong hands, no readable information can be recovered from the phone's hardware memory. Several issues arose during the execution of the design. Some of these issues have been resolved as a result of numerous experiments and workarounds, while others remain. Some of the issues stemmed from the setting of distinct software.

For example, it was discovered throughout the course of this thesis that configuring a PKI infrastructure, even in its most basic version (tier-one), is a difficult operation that requires hands-on expertise. Appendix A contains more information on these problems as well as helpful hints.

X. FUTURE WORK

Different elements should be considered while designing a highly effective security system.

Although the purpose of this thesis was to secure messages between two clients, there are several additional variables that might be investigated in the future, such as the application's usability, server scalability, or how the design affects implementation costs. The following subjects are proposed for future scholars in order to finish this research:

Performance: The proposed design has not been investigated to see how it affects the mobile phone's performance. How much CPU power it will require and how it will influence battery depletion Different security methods or encryption cyphers may require greater processing resources and operating system support.

Unfortunately, in many circumstances, **privacy and profiling** are entirely dependent on the mobile operating system version and platform. Many useless pieces of data are sent to servers by free and premium versions of instant messengers, and the user is often unaware of it. Further study should be carried out to explore how metadata transmitted to the server by any chat programme may be restricted or removed.

To prevent **reverse engineering** attacks, it's always a good idea to erase all cache data whenever the IM application activity changes. When the application moves to the background, for example. This implies avoiding several errors in the application's implementation and code. For this, OWASP* offers a wonderful standard and checklist paper.

It's also possible that the **"group chat"** option will be implemented. More than two people can participate in group chat and converse with one another. Security in a group chat is more challenging, especially when the chat programme may send offline messages, and it necessitates extra considerations during the architectural design process, which could be the subject of a new study.

REFERENCES

[1] M. Toorani and A. A. Beheshti Shirzai, SSMS - A Secure SMS Messaging Protocol for the M-Payment Systems, IEEE Symposium on Computers and Communications, 2012, 700-705.

[2] "Most popular global mobile messenger apps 2014 | Statistic," Statista. [Online]. Available: http://www.statista.com/statistics/258749/most-popular-global-mobilemessenger-apps/. [Accessed: 02-Dec-2014].

[3] Symmetric key Cryptography, http://en.wikipedia.org/wiki/Cryptography.

[4] An Overview of Cryptography, http://www.garykessler.net/library/cryp to.html.

[5] Decryption, http://www.webopedia.com/TERM/D/decryption.html.

[6] Marko Hassinen, SafeSMS - End-to-End Encryption for SMS Messages, IEEE International Conference on Telecommunications, 2008, 359-365.

[7] S. Kumar, M. Girimondo, A. Weimerskirch, C. Paar, A. Patel, and A. S. Wander, "Embedded End-to-End Wireless Security with ECDH Key Exchange", 2003 46th Midwest Symposium on Circuits and Systems.

[8] Suchita Tayde and Seema Siledar. "File Encryption, Decryption Using AES Algorithm in Android Phone", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5(5), pp. 550-554, 2015.

[9] William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, Boston, 5th Ed, 2011.

[10] Bhimrao Patil, "SMS SECURITY USING RC4 & AES", Indian J.Sci.Res, Vol. 11(1), pp. 34-38, 2015.