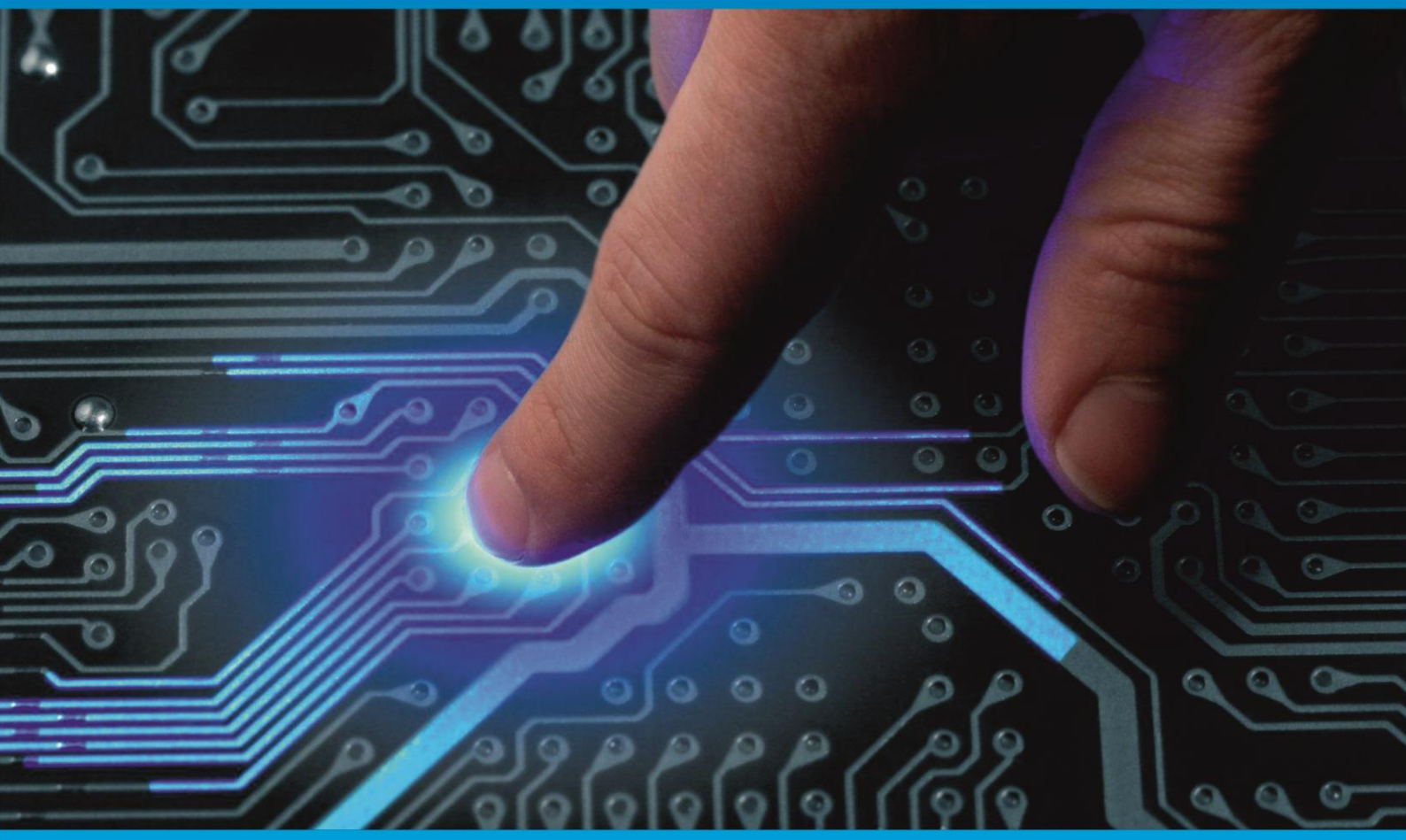
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905017 |

An Overview of Encrypto the Encryption Keyboard Android Application

Nishant Gautam[1], Prof. Nirupma Singh[2]

U.G. Student, School of Engineering, Ajeenkya DY Patil University, Pune, Maharashtra, India[1]

Assistant Professor, School of Engineering, Ajeenkya DY Patil University, Pune, Maharashtra, India[2]

ABSTRACT- A mobile keyboard will flip a frustrating work session into a productive one by eliminating the sound on the small keys onscreen. All of those keyboards work 3 criteria: they need a decent keyboard that handles typewriting, they're terribly moveable in style, and that they work with any Windows, Android, or IOS device. we tend to square measure getting to create a keyboard that will quite the traditional keyboard. This keyboard can create US safer and create our spoken language a lot of non-public. As we tend to all recognize privacy could be a story as a result of each messages and pictures you send to somebody is keep within the server and might be viewed by the administration or will be seen by the government officers. We'll create such keyboard that do encoding and shield our privacy.

KEYWORDS: Encryption, keyboard, Security.

I. INTRODUCTION

As we all know that the chatting we do on any social media account is not fully secure. The accounts can be hacked the chats can be leaked and many more. But the main problem is about the companies who provide these platforms to us can read and store all of our personal data and chats and then this companies target us by using our personal data for selling products and many more. As we all know is near past the news regarding WhatsApp and Facebook they compromise our security to resolve this issue we will make such keyboard app who will convert our normal chatting into hypertext or do Encryption. The reality is that every social media website or app have our private data and they can use it in many ways. Even WhatsApp end to end encryption is not 100% secure government or company employs can read your or get your personal messages as seen in so many drug cases in Mumbai. Our goal is to give power of Encryption to the hands of the user so that even if someone is ready our messages he/she can't get it.

II . LITERATURE REVIEW

1. Treat metric weight unit projected that network security may well be associate endless battle between the system vogue engineers and laptop hackers. In an effort to remain the hackers out, engineers have developed a formidable array of cryptography algorithms, authentication protocols, and intrusion detection systems. to not be outdone, the hackers have developed equally spectacular ways in which around the arsenal of security protecting our most sensitive laptop networks (as the attacks on many industrial websites have clearly shown). However, every groups have continued to overlook one in {every of} of the foremost vulnerable links in every laptop network: the client's keyboard.

2. Deshpande et. al silent Advanced cryptography customary (AES), a Federal information science customary (FIPS), is associate associate approved scientific discipline formula which is able to be familiar with protect electronic data. The AES is programmed in package or designed with pure hardware. however Field Programmable Gate Arrays (FPGAs) offer a quicker and extra customizable resolution. This paper presents the AES formula with connectedness FPGA and conjointly the really High-Speed circuit Hardware Description Language (VHDL).

3. Jasmin M et. al projected that business economic the commercial communication systems of this time area unit to associate large extent supported commercial operational systems, open protocol implementation & communication application that are not secure. By connecting to the net or various public networks these risks area unit exposed to potential assailant and cause damage to the industries. tackle this case we've an inclination to stand live introducing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905017 |

associate encrypting/decrypting module (ENIGMA) which could be connected at one end of the plant and one end of the area.

4. Verma et. al counselled that stealing or loss of a mobile device may well be associate info security risk because it may result in loss of confidential personal information. ancient cryptanalytic algorithms aren't appropriate for resource-constrained and hand-held devices. during this paper, we've developed associate economical and easy tool referred to as "NCRYPT" on the golem platform. "NCRYPT" application is employed to secure the information at rest on golem so creating it inaccessible to unauthorized users. it's supported light-weight cryptography theme i.e. Hummingbird-2. the applying provides secure storage by creating use of password-based authentication in order that associate opponent cannot access the confidential information keep on the mobile device. The cryptanalytic secret's derived through the password-based key generation methodology PBKDF2 from the quality SUN JCE cryptanalytic supplier. numerous tools for cryptography area unit obtainable within the market that area unit supported AES or DES cryptography schemes. The reported tool is predicated on Hummingbird-2 and is quicker than most of the opposite existing schemes. it's conjointly immune to most of the attacks applicable to dam and Stream Ciphers. Hummingbird-2 has been coded in C language and embedded within the golem platform with the assistance of JNI (Java Native Interface) for quicker execution. This application provides a selection for encrypting the complete information on associate Coyote State card or selective files on the smartphone and defends personal or steer obtainable in such devices.

5. Ariffi et. al recommended that short Message Service (SMS) could be a extremely popular manner for transportable and transportable device users to send and receive straightforward text messages. sadly, SMS is doesn't supply a secure setting for confidential information throughout transmission. This paper deals with AN SMS cryptography for mobile communication on mechanical man message application. The transmission of AN SMS in mobile communication isn't secure, so it's fascinating to secure SMS by extra cryptography. during this paper, there's planned the utilization of 3D-AES block cipher trigonal cryptography algorithmic rule for SMS transfer securing. From the experiment, the 3D-AES has low cryptography time once message size is additional then 256 bits. It are often indicate that SMS cryptography application victimisation the 3D-AES block cipher are going to be planned running when 256 bits.

6. Rayarikar et. al understood that encryption is of prime importance once confidential information is transmitted over the network. Varied cryptography algorithms like AES, DES, RC4 et al. square measure out there for constant. the foremost wide accepted algorithmic rule is AES algorithmic rule. we've developed AN application on mechanical man platform that permits the user to write the messages before it's transmitted over the network. we've used the Advanced cryptography Standards algorithmic rule for cryptography and coding of the information. This application will run on any device that works on mechanical man platform. This application provides a secure, fast, and robust cryptography of the information. there's an enormous quantity of confusion And diffusion of throughout cryptography that makes it terribly troublesome for an assailant to interpret the cryptography pattern and therefore the plain text variety of the encrypted data. The messages encrypted by the developed application are immune to Brute-Force and pattern attacks. the varied uses of this application in reality and its practicality square measure explained during this paper.

7. Tayde et. al planned that these days sensible gadgets as well as sensible phones and tablets square measure gaining large quality. examination with standard pc, sensible phone is definitely dispensed and provides abundant pc practicality, like process, communication, information storage similarly as several computers services like application, video or audio player, video call, GPS, wireless network. However, sensible phone got to return good distance in terms of security. cryptography is employed for security in data storage and transmission method. numerous cryptography algorithms like DES, 3DES, Blowfish, RSA et al. square measure out there to secure the information. In DES, key size is just too tiny. In 3DES, key size is increase however the method is slower than different strategies. we've used the Advanced cryptography customary algorithmic rule to beat the on top of issues. AES algorithmic rule isn't just for security however conjointly for nice speed. It are often enforced on numerous platforms particularly in tiny devices sort of a transportable. Everyday information is shared, transmitted, hold on for several functions like banking, production, research, and development. Hence, we'd like security for info. cryptography will give security. This application permits users to run this application on the mechanical man platform to write the file before it's transmitted over the network. it's used for all kinds of file cryptography like text, Docx, pdf, and image cryptography. AES algorithmic rule is employed for cryptography and coding.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905017 |

II. FLOW CHART

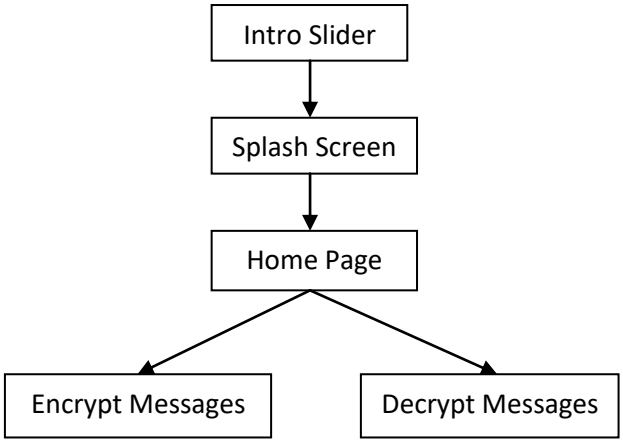


Fig.3 Block Diagram of Proposed Flowchart

System Flow Diagram:

1. In our proposed system after the intro sliders then splash screen will be there.
2. After that user can see two options on the main screen.
3. Option one will lead you to new page for encryption of the message.
4. Option two will lead you to new page for decryption of the message.

III. PROPOSED METHODOLOGY

1. List View: A list of scrollable items can be displayed in android studio by using a widget called List View. List View is there in the xml file in the design area under the Containers option in the widgets area. It can be added to the xml by drag and drop or hard coding it. The users can easily select any items that are displayed in the List View in a scrollable manner, which will lead the user to a new activity.

2. Module: Splash screen is used in the project to display the logo of the application to do so we created a XML file in layout folder in the android studio project and define the timing of the splash screen up to 2000 delay millis to properly show our logo to the user. We used intro slider to inform the users what you are getting it within the application and what they can use this application for. To achieve this we created three different XML files in Layout folder and designed it in such way that the user can go from first to last one by one.

3. Encryption: Encryption is that the technique by that info is reborn into code that hides the information's true which means. The science of encrypting and decrypting info is termed cryptography. In computing, unencrypted information is additionally called plaintext, and encrypted information is termed ciphertext to try and do it for our app we have a tendency to use (string.replace) and replaced the conventional string words into symbols and numbers so nobody will get the picture.

4. Decryption: The conversion of encrypted information into its original kind is termed Decryption. It's typically a reverse method of encoding. It decodes the encrypted info so a certified user will solely rewrite the information as a result of coding needs a secret key or parole. To attain this in our application we have a tendency to reverse the codes of encoding and used same technique.

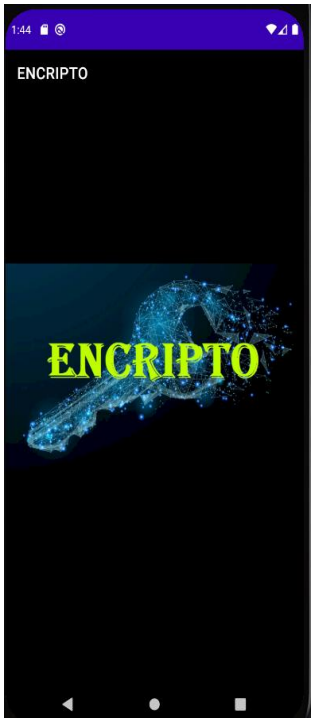
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

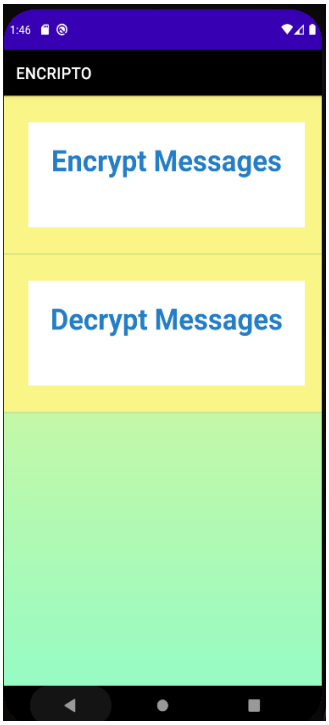
| DOI: 10.15680/IJIRCCE.2021.0905017 |

IV. IMPLEMENTATION

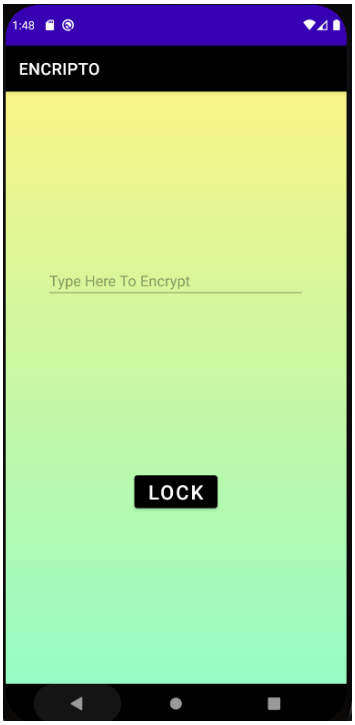
Screenshot 5.1 Introduction Screens



Screenshot 5.2 Slash Screen



Screenshot 5.3 Home Screen

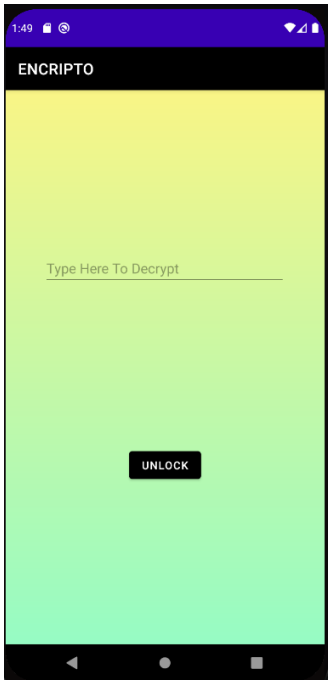


Screenshot 5.4 Encryption Screen

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905017 |



Screenshot 5.5 Decryption Screen

1. Intro Screen: - In this we have three slider screens which tell user what they will get in this application and use of it.
2. Splash Screen: - Splash Screen shows the logo of the app to the user.
3. Home Screen: - Home screen contain List View, It has two options for encrypting the messages and decrypting the messages.
4. Encryption Screen: - In this screen user types his/her messages to encrypt them.
5. Decryption Screen: - In these screen user types encrypted messages to decrypt them.

IV. RESULT

As the result of this app user can encrypt any message or any text which user want to make secure and safe. Users can also decrypt the messages by providing this facility to the users they can encrypt there message and can send it to any social media website or anywhere else. It can also be used to encrypt or decrypt text of any important files or document which we do not want to disclose so we can be more secure.

V. CONCLUSION

In today's digital age, mobile vulnerability is at an all-time high. There are too many unseen threats out to retrieve private information on your mobile device. Luckily, there are amazing and effective ways to protect the information on your mobile device. So the conclusion of this whole project is that it makes you more secure and make your personal chats in encrypted form so that if any one hack or try to read your messages he fails to do so. In future we will work on making the images and videos shared on the social media more secure and encrypt them too so that we can make our chats fully secure form the threats out there and make the app more user friendly and easy to use.

REFERENCES

1. Treat DG. Keyboard encryption. IEEE Potentials. 2002 Nov 7;21(3):40-2.
2. Deshpande AM, Deshpande MS, Kayatanavar DN. FPGA implementation of AES encryption and decryption. In2009 international conference on control, automation, communication and energy conservation 2009 Jun 4 (pp. 1-6). IEEE.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905017 |

3. Jasmin M, Beulah Hemalatha S. Security for industrial communication system using encryption/decryption modules. International Journal of Pure and Applied Mathematics. 2017;116(15):563-8.
4. Verma, S., Pal, S. K., & Muttoo, S. K. (2014, February). A new tool for lightweight encryption on android. In *2014 IEEE International Advance Computing Conference (IACC)* (pp. 306-311). IEEE.
5. Ariffi, S., Mahmod, R., Rahmat, R., & Idris, N. A. (2013, December). SMS encryption using 3D-AES block cipher on android message application. In *2013 International Conference on Advanced Computer Science Applications and Technologies* (pp. 310-314). IEEE.
6. Rayarikar, R., Upadhyay, S., & Pimpale, P. (2012). SMS encryption using AES algorithm on android. *International Journal of Computer Applications*, *50*(19), 12-17.
7. Tayde, S., & Siledar, S. (2015). File encryption decryption using aes algorithm in android phone. *International Journel of Advanced Research in computer science and software engineering*, *5*(5).

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details