END-TO-END ENCRYPTION MESSAGING USING CRYPTOGRAPHY*

BY

JULANTA LEELA RACHEL J[1♣], YATISH SINGH RAJPUT[2]

[1,2]*School of Engineering, Ajeenkya DY Patil University, Pune, India*

julantaleelarachel@gmail.com[1], yatish.rajput@adypu.edu.in[2]

ABSTRACT

The current situation is that security guarantees on large open networks have become an hour's need. With the increase in crime, one needs to take precautionary measures to protect the information effectively from any possible attack. The proposed application plays an important role in providing security for military communications, financial transactions, corporations and political related issues. Mainly due to the drawback in existing security system, a new method has been proposed that provides a secure package with secure environment for data transfer to the user. Cryptography is one of the most influential areas for computer security and data and the most promising guide to cryptography research is known as DNA Cryptography. The computer concept of DNA can be used to encrypt, decrypt, and transmit data.

KEYWORDS

Security, Cryptography, Encryption, Decryption, Advanced Encryption Standard (AES).

I INTRODUCTION

In network security, cryptography has a long history of providing a way to store sensitive information. Due to hackers the information/message has been hacked by the hackers. So, the message can be read by anyone other than the intended recipient. Cryptosystem is a collection of algorithms integrated with conversion keys (Plain-text) helps to encrypted text (Cipher-text) and then turn it back to the recipient side of the target message in the original message (Plain-text). As in this proposed application the text can be encrypted and decrypted.

Encryption is the process of converting information or data into a code, especially to prevent unauthorized access. The proposed system uses encryption to protect sensitive information which is transmitted through online, whereas decryption is the process of converting an encrypted code into some useful information. To convert the text into

* Received 22 September 2021, Accepted 09 October 2021, Published 24 October 2021

♣ Corresponding Author

encryption or decryption there are some algorithms. Some of them are listed below:-

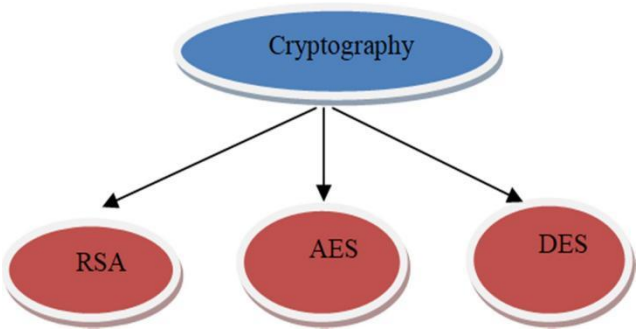

Figure 1.1 Types of cryptographic algorithms

RSA (Rivest–Shamir–Adleman) is a calculation utilized by present day PCs to encode and decode messages. It is a hilter kilter cryptographic calculation. There are two distinct keys. Since one of the keys can be given to anybody, the plain content includes 64-cycle squares and can convert them into text utilizing 48-bit keys. Whereas AES is used in this project as the algorithm is more efficient, secure and has 128 and 256 bit of key.

II LITERATURE SURVEY

A literature survey has been taken and the drawbacks which each paper consists of have been overcomed in the proposed method. The survey description of each paper has been listed below. Kuppuswamy and Al-Khalidi in [1] proposed the technology which is hybrid cryptography which combines two algorithm keys which is compatible key and public key. Here proposed system has a two-way secured encryption and decryption, which addresses user security. Proposed system uses two algorithms which makes the system powerful. But as there are two keys used it will lead to slower down the process of both encryption and decryption. The user will be confused weather the key is public key or compatible key. Whereas it is way more secure and cannot be easily hacked or steel data. Kansal and Mittal in [2] proposed that increasing use of the Internet in various fields such as banking, military and government, the security and privacy of information has been a major issue. As all the things are getting online where data are also managed online only where e-transactions are also there. So, when the user sends the data or information from his side to the recipient side there is an risk of data confidentiality so for this problem they uses method called encryption. Encryption will change the data into the format which cannot be read by

the hackers. There are some algorithms which are good to use for data encryption here they have searched about some algorithms which are Symantec key algorithms which means encryption and decryption can be done by a single key only.

Saraf and Jagtap in [3] proposed that rapid analysis of digital data exchange has taken place in recent years. As a result information security is critical to data retention and transfer process. The security of online bank account passwords, passwords for email accounts etc. requires text protection on digital media. In the same way image transfer and retention during industrial process and research requires image protection. The National Institute of Standards and Technology (NIST) has embarked on a process to develop a Federal Information Processing Standard (FIPS) that should be more flexible, secure, fast and can replace the Data Encryption standard. This new standard is identified by the common name of the Advanced Encryption Standard (AES). The characteristics of the data depend on its types. Therefore the same encryption process cannot be applied to all types of data. Images have large data sizes and also have real-time problems which are why the same method can be used to protect images and text from unauthorized access. However with a few variations of the way AES can be used to protect image and text. In this project I used encryption and deletion to writetext and image using AES.

Yang and Bourbakis in [4] describe algorithms and standards that represent the most encrypted data, digital images and MPEG video. A typical model of a standard encryption / decryption system for the security process is discussed. The goal is to protect data content from attackers. Going back to data encryption is data detection, which gets the original data. There are two types of encryption / decryption key: public key system and private key system. Highly promising features of compound loss, integrated encryption and encryption are based on SCAN language that analyzes different digital image and video formats and searches for advanced security techniques to reduce total computational costs. Hussain and Negi in [5] proposed a method for secure communication to take place. it is very important to use encryption decryption on both sides e.g. It is difficult to provide security for hackers, as they can easily access by getting the encryption key. There are many algorithms which providedata security and most of these uses random key generations, and perform functions by these keys. This paper priorities encryption / decryption algorithm based on ASCII, Binary-Bit sequences and continues to use XOR functionality. It includes encryption in merged sections and the key is providedby the user. In the proposed algorithm, the original data will be encrypted in multiple phases and the key will be used to encrypt the text in the cipher text; The following key will be used for cipher encryption in plain text. The proposed algorithm falls

under the category of Symmetric key algorithms.

Hendi and Dwairi in [6] proposed that multicultural data is now streaming to the internet and demand for cloud systems is now increasing Produced, installed, and duplicate data is increasing in size and expansion applications. Thus the need for encryption methods became an important problem.The process used here should be very simple, efficient, and accurate A very simple and secure encryption algorithm (SHSED) algorithm that can be used for computer-based applications, where it is introduced. It uses simple and effective logical functions. The presented method is also enabled by the flexibility of selecting the secret key length and the number of rounds to produce a cypher text. The test results of the presented method were compared with other method results (LED, AES, DES), and due to the comparison of the method presented gives a good improvement in the encryption. Kumar and Chaudhary in [7] proposed that main objective of this paper is to improve data security and speed processing using a cryptographic compatible process based on ASCII values while data transfer. The purpose of this paper is to generate encrypted content by providing explicit text access to symmetric cryptographic based on ASCII value and to obtain transcribed text as original text as original text by providing a balanced cryptographic encrypted text based on ASCII value. Method: In this paper, we have proposed an algorithm based on the ASCII value to enter written code. This algorithm occasionally creates a human key with a length equal to the length of a clear writing. A random key is converted to another key by replacing the key using a random number and is used to decrypt the original decryption message.

Agrawal and Mishra in [8] stated the detailed study of all the algorithms such as AES, des, triple- des and comparing which is best algorithm in case of encryption and decryption, where he fund that AES which is a Symmetric algorithm which is very efficient effective and cannot been decrypted easily by the hackers. Whereas des and triple des are also good but hackers can easily decrypt the data or information. AES also saves the confidentiality of the users as end-to-end encryption is possible through AES only. There are many algorithms which are better than AES but cannot been implemented in java easily which is also an issue. Yasser and Mohamed in [9] stated stated that encryption and decryption are two different things as encryption will help to change the readable text into an un readable format which help in securing the data in the cloud as the attackers cannot easily get the data. But to change the data into readable format we uses the term decryption as this will help to decrypt the data which we have encrypted and saved in cloud. To decrypt the data we need

an special key. Every algorithm has different kinds of keys to which is public key or private key. But themain condition is that the attackers are too smart they can regenerate the key of the encryption. So to overcome from this there are many secure algorithms which should be used to protect the data in cloud.

Khalil in [10] proposed that encryption is a way to protect and validate data sold through social media in front of an incoming group called opponents. As a result, the message conveyed or savedcan be converted into unreadable form without the intended recipients. Encryption techniques allow the intended recipient to display the content of the pre-encrypted message with the secret keys that are only exchanged between the sender and the recipient. Writing and encryption techniques can be applied equally to a message in any way such as text, image, sound or video. The current paper worksand tests both the encryption / decryption capabilities in real-time audio signal. The first is the well- known encryption and removal process for RSA encryption and the second is a newly developed algorithm based on the concept of symmetric cryptography. The Mat lab Simulink simulator tool is used to get real-time audio signal and mimic the proposed algorithms. Considering the statistical nature of the audio signal, test results have shown that the RSA method produces a low quality audio signal while the proposed algorithm produces a high quality audio signal as precise as the original.

Tayde and Siledar in [11] proposed that AES algorithm is designed not only for securing data or information but also to increase the processing speed. It can be implemented on a various platforms such as smartphones application, windows application and web based application. This system uses the des algorithm which is good for small encryption or decryption of data but not secure. This is an web based system which converts the data in SQLite database where java language is preferred for implementing the AES. Murillo-Escobar in [12] proposed the system where it encrypts the map location which is sent by one user to another. This system uses the algorithm which can be easily hacked or the location can be traced by the hacker. So here our proposed application which will get future update of location encryption done through AES is more efficient and user can only access the location. He uses python language which is more efficient then java but algorithm is weak. Singh & Singh in [13] proposed that Elliptic Curve Cryptography has become the latest research center in the field of Cryptography. It offers higher security with a smaller key size compared to other Cryptographic strategies. A new procedure has been suggested in this paper in which the old process of mapping the characters to combine points in the elliptic corner has been removed. The corresponding ASCII values of the explicit text are paired.

Coupled values serve as the inclusion of Elliptic curve cryptography. This new approach avoids the costly operation of the map and the need to share a test table. The algorithm is made so simple that it can do any type of encryption and decryption.

Zeebaree in [14] proposed that algorithms which he uses is DES which is mostly used all over the world as it is simple to implement and cannot easily been encrypted without getting the key. The key of this algorithm is small which is of 128 bit but the key is secure also. The technique is used to encrypt and decrypt the text is complicated. Hackers cannot easily hack the system. It uses the pipeline concept. Zhang and Tang in [15] proposed that corresponding key image cryptosystem based on the exact line map is shown on this page. In this era of cryptosystems, the encryption process and the transcription process are the same. Both include the same rubbing performance associated with a single drop, double scattering and a rotating matrix of 180 degrees four times. The secret key length in the system is 64d when d is the absolute number. The proposed system can combat selected / known attacks of assault cases due to the use of sensitive offensive-related offenses. The results of the simulation and comparison analysis show that the proposed system has many advantages such as high encryption / encryption, high key space, strong key sensitivity, strong sensitivity of writing, strong sensitivity of writing, good hidden arithmetic properties, and large cipher Text entropy details. The proposed system can therefore be used for real communication.

III PROPOSED METHODOLOGIES

The proposed system is divided into two sessions, the user application and firebase. The major component used in design of user sessions includes register new user. Then login using same credentials. Then the menu session includes encryption of plain text and decryption of cipher text. Figure 3.1 shows the work flow of the proposed system.

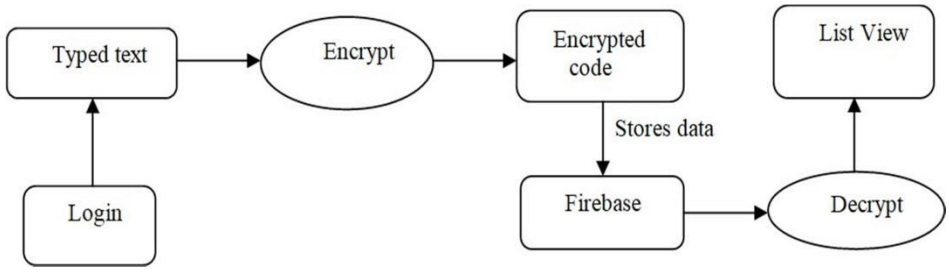

Figure 3.1 Work flow of the Proposed Application.

In the proposed methodology, Encryption process includes a message or a file to be read only by certain group of people. Encryption uses an algorithm to mock or encrypt data and then uses the receiving group key to resolve or delete data. The message contained in the encrypted message is called the text. By the way it is encrypted; the unreadable is called cipher text. It determines encrypted data so that the authorized user can encrypt data only because encryption requires a privatekey or password.

Advanced Encryption Standard (AES)

There are many encryption algorithms used to keep data secure. Their toughness and ability to withstand attacks vary from one algorithm to another. A key part of the encryption process is the algorithm that works for the basic purpose in various ways. The most widely used algorithms include DES, Triple DES, RC2, RC4, Blowfish, Two Fish and Rijndael (AES) as mentioned in the abstract. The National Institute of Standards and Technology (NIST) in 1997 officially announced that the Rijndael algorithm would be an Advanced Encryption Standard (AES) that would replace the outdated Data Encryption Standard (DES). The AES algorithm is a block cipher text block which has size 128, 192 or 256 bits. Among them, 128 are for (AES -128), 192 are for (AES -192) and 256 are for (AES -256) and the pieces of key length are in-between the range [5-7]. The Rijndael algorithm is based on circular operations, and a different combination of algorithms is created by repeating this circular function at different times. Each circular function consists of four identical and equal steps, switching by location, line rotation, column 147 mixing and key insertion

IV IMPLEMENTATION WORK

The application when it will come to usage, it will firstly show the splash screen which is of 2000ms and then the registering link will open where the new user can easily register. The credentialsuser typed is saved in firebase which is also used in login page also. Then after successfully completion of login the user can see the main screen of the application where the user will type the message and the message will get encrypted and saved in firebase in encrypted form and it will retrieve the data in decrypted form in the list view. Here are some screenshots of the proposed application as in the fig 4.1 the user have to type the text as per his choice and click on the send button the above list view will show the typed

text, whereas firebase stores the encrypted text.

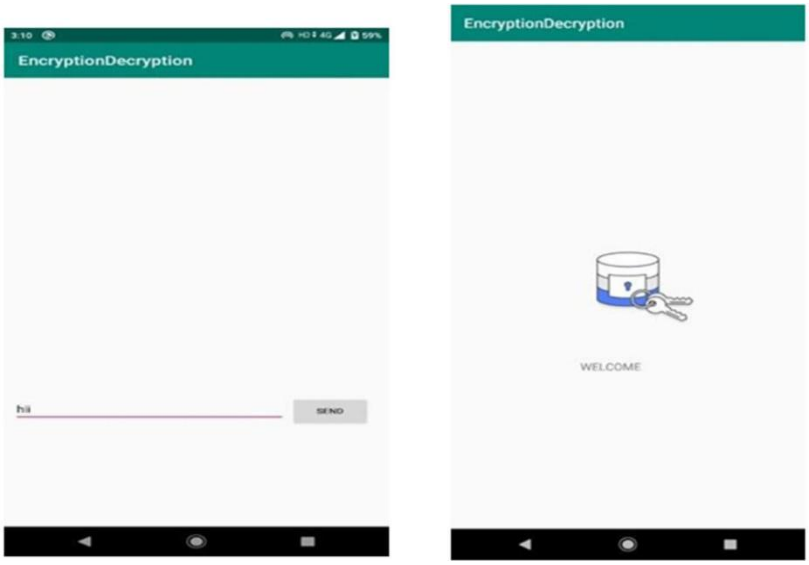

Figure 4.1 Main menu and splash screen of the proposed application

Figure 4.1 also shows the splash screen of the proposed application, where you will find an icon similar to a lock which will be there for 2000 milliseconds.

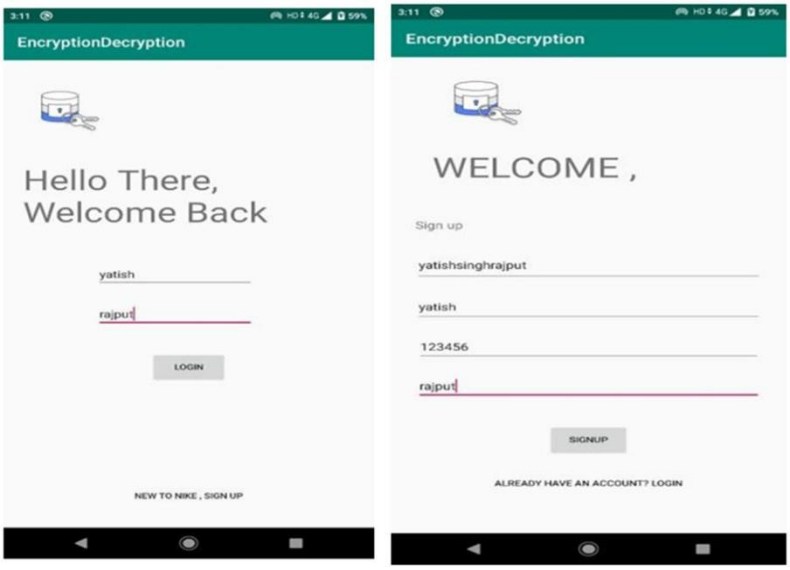

Figure 4.2 Login and signup screen of the proposed method

Figure 4.2 shows signup screens and login screen. In signup screen, the user needs to register their details and details are saved in firebase database. In login screen, it retrieves

the data stored in firebase and authenticates the user and logs in. Figure 4.3 shows how the data is stored in the database in an encrypted format.

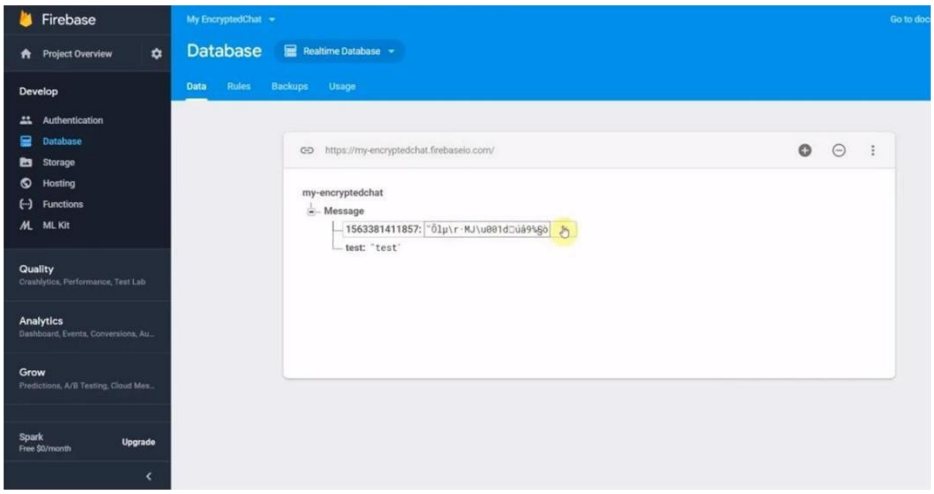

Figure 4.3 Data stored in firebase in an encrypted form

V CONCLUSION

The paper has introduced a new encryption method for encryption and decryption. Although there have been many researchers in cryptography, most of the existing algorithms have several weaknesses caused by low security levels or increased latency due to the algorithm structure itself. The proposed algorithm was tested for various known attacks and proved to be safe from them. Therefore, it can be considered as a good alternative to other applications due to the high level of security and intermediate time required for encrypting and deleting data encryption using the proposed algorithm which is much smaller than the AES algorithm. Encryption and encryption programs are used to improve data security to protect data, thus providing an improved level of authentication such as encrypted data cannot be viewed by unauthorized groups in the event of theft, loss or blocking. This program replaces the data encryption and encryption system by adding additional functionality as a digital signature. Future tasks may be offered to optimize the system so that it can encrypt and decrypt other types of files, including audio, video, image, and three.

REFRENCES

[1] P. Kuppuswamy and S. Q. Y. A. Khalidi, “Hybrid encryption/decryption technique using newpublic key and symmetric key algorithm,” Int. j. inf. comput. secur., vol. 6, no. 4, p. 372, 2014.

[2] S. Kansal and M. Mittal, “Performance evaluation of various symmetric encryption algorithms,”in *2014* International Conference on Parallel, Distributed and Grid Computing, 2014.

[3] Saraf, K. R., Jagtap, V. P., & Mishra, A. K. (2014). Text and image encryption decryption usingadvanced encryption standard, IJETTCS, 118-126.

[4] M. Yang, N. Bourbakis, and S. Li, “Data-image-video encryption,” IEEE Potentials, vol. 23, no.3, pp. 28–34, 2004.

[5] Hussain, I., Negi, M. C., & Pandey, N. (2018, August). Proposing an encryption/decryptionscheme.ICRITO) (pp. 709-713). IEEE.

[6] Hendi, A. Y., Dwairi, M. O., Al-Qadi, Z. A., & Soliman, M. S. (2019). A simple and highly secured method for data encryption-decryption. International Journal of Communication Networks and Information Security, 11(1), 232-238.

[7] N. Kumar and P. Chaudhary, “Performance evaluation of encryption/decryption mechanisms toenhance data security,” Indian J. Sci. Technol., vol. 9, no. 20, 2016.

[8] Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryptiontechniques. International Journal on Computer Science and Engineering, 4(5), 877.

[9] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, “An encryption/decryption frameworkfor secured communications,” Entropy (Basel), vol. 22, no. 11, p. 1253, 2020.

[10] Khalil, M. I. (2016). Real-time encryption/decryption of audio signal. International Journal ofComputer Network and Information Security, 8(2), 25-31.

[11] Tayde, S., & Siledar, S. (2015). File encryption decryption using aes algorithm in androidphone.IJCNIS, 5(5).

[12] Murillo-Escobar, M. A., Abundiz-Pérez, F., Cruz-Hernández, C., & López-Gutiérrez, R. M. (2014, February). A symmetric text encryption algorithm based on map. In Proceedings of the ICCC, signal processing and computers (Vol. 4953).

[13] L. D. Singh and K. M. Singh, “Implementation of text encryption using cryptography,” Procedia Comput. Sci., vol. 54, pp. 82, 2015.

[14] S. R. M. Zeebaree, “DES algorithm implementation based on FPGA,” Indones. j. electr. eng. comput. sci., vol. 18, no. 2, p. 774, 2020.

[15] Y. Zhang and Y. Tang, “A plaintext-related image encryption algorithm based on chaos,” Multimed. Tools Appl., vol. 77, no. 6, pp. 6647–6669, 2018.