Annals of R.S.C.B., ISSN:1583-6258, Vol. 24, Issue 2, 2020, Pages. 222 - 226
Received 24 October 2020; Accepted 15 December 2020.

V Chat: Multi-layered Data Encryption/Decryption Chatting Application

Ms. SwaraPampatwar [1] ,VinishaKalyani[2],PrachiShamdasani[3],UrjaRamwani[4]
[1](Assistant Professor,Department of ComputerScience, Jhulelal Institute of Technology, Maharashtra, India)
[2], [3],[4] (Department of Computer Science, Jhulelal Institute of Technology, Maharashtra, India)

Abstract: This paper is focused to implementation of multiple layers of Data encryption and decryption used to transmit data in social networking application as to provide asecure end to end data transmission to users. We seek to go with a different approach ofdynamic key generation which is different for every user to user communication at one layer and a global static key for the second layer of encryption making data hard to decrypt.

Keywords: Encryption/Decryption, Dynamic Key Generation, Multi- layered Encoding/Decoding, Social Communication.

I. INTRODUCTION

In the recent times, there are many social networkingapplicationsavailableinthemarket that promises to provide a secure datatransmission and storage but we all know that they do fail to keep their promises, because evenwith their security protocols our data gets leak into the places where it was notsupposedto. Even though many applications use multi- layered encoding and decoding of data but still they use static pair of private and public keys whichgetsdisclosedbyhackeraftersometime. In the late years, Data Confidentiality, Authentication, Integrity, Non-repudiation, Access control, and Availability are the most imperative security services in the security criteria that ought to be considered in secure applications and frameworks. Not with standing, there is no arrangement for such security services in the mobile chat systems. Both mobile chat system customer and mobile chat system server are defenseless against both passiveandactiveattacks.Passivedangersjoin arrival of message substance, and Traffic examination while active dangers consolidate adjustment of message substance, masquerade, replay, and denial of service(DoS).

II. LITERATURESURVEY

As data security has always been a key issue ofworkbydevelopersmanypapershavebeen issued, demonstrating the implementation of multi-layered data encoding anddecodingapproach for increasing the data security and creating a secure peer to peer communication channelforserverlesscomputations.Someof them are listedbelow:

1. A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers: This paper published in year 2020 at IEEE Access, describes a unique approach of combining the technique of Cryptography and Steganography .in order to transmitdatasecureaswellashidden,theapproach can be used to hide the original meta data in the image after removing it from the actual image.[1]
2. Design of Secure Chatting Application with End to End Encryption for Android Platform: This paper demonstrates the uses of various encoding techniques for different type of data encryption and decryption, like AES and RC4, it also utilises Elliptic Curve Diffie Hellman Key Exchange (ECDH) algorithm to generate a pair of keys used by the asymmetric encoding algorithms and a shared key for symmetric encoding algorithms. [2]
3. A new Cryptographic Algorithm AEDS (Advanced Encryption and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 24, Issue 2, 2020, Pages. 222 - 226
Received 24 October 2020; Accepted 15 December 2020.

Decryption Standard) for data security: The paper introduces a new encryption algorithm Advanced Encryption and Decryption Standard (AEDS) which combines the approaches of Data Encryption Algorithm(DES) and Advanced Encryption Standard(AES), in order to generate a more robust result.[3]Multi-Layer Data Encryption using Residue Number System in DNA Sequence: This paper focuses on performing data encryption using RNS encryption approach and rearranging the generated values with a similar structure of a DNA string sequence, this merge results in a multilayer encryption with different keys which can befurther used as a hash function making it versatile, secure, flexible and less complex.[4]

4. Multi-layered Information Encryption Scheme with Fine-grained Authentication: This paper focuses on encrypting image data with ahelphidden authentication code with the image or part of the image which can be later extracted from itto determine whether the image is original or not. It allowsusertoprovideacustomauthenticationcode too.[5]

III. IMPLEMENTATION

With the proper implementation of the system, our system will help to deliver a truly endto-end encryption based secured internet messaging application. Initial step is to start a background messagereceivingservice,whichwillkeepacheck of received messages.[6] This service will only get registered in system if user is registered inapp.

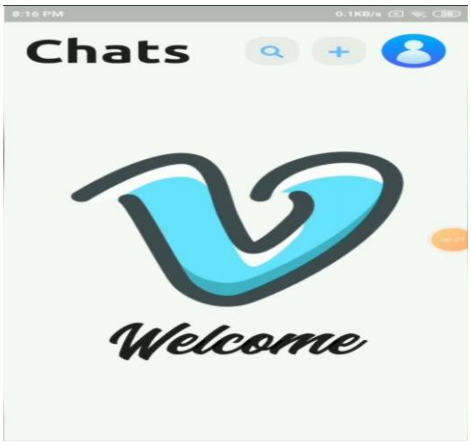
As user start the app it will display a one-time welcome and sign-up screen, if user is a registered user then the system will check backup chats available in offline or not.[7] If not then it will restore them from online backup. Once user is done with the sign-up/sign-in, the next screen in the Home Chat screen where the app will show recent chatordered by timestamp in descending order.

The entire system is divided into different sets of Moduleseachhasitsownspecifictask/operationto perform:

- UIModule
- Auth/LoginModule
- Global Encryption/DecryptionModule
- Dynamic Key Approach Encryption/Decryption Module.
- Chat RecordModule

1. UIModule:

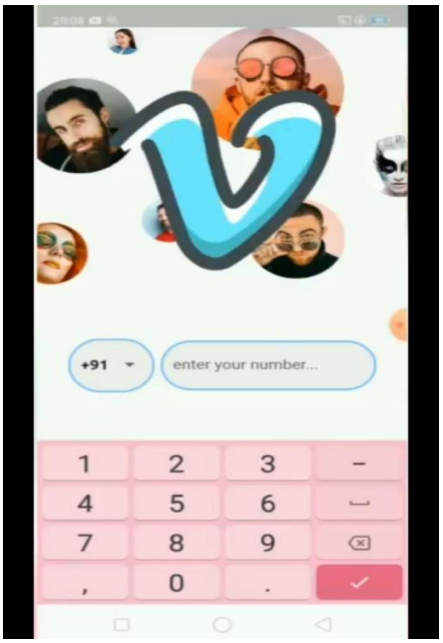
ThisModulecontainsall theUICodeoftheapp. Most of the static UI pages or custom UI components are part of thismodule.



Annals of R.S.C.B., ISSN:1583-6258, Vol. 24, Issue 2, 2020, Pages. 222 - 226
Received 24 October 2020; Accepted 15 December 2020.

2. **Auth/Login Module:**

The task of this particular module is to perform the authentication of user who is joining orlogging in the app. The authentication includesauthenticate via OTP and a optional 2-stepVerification.

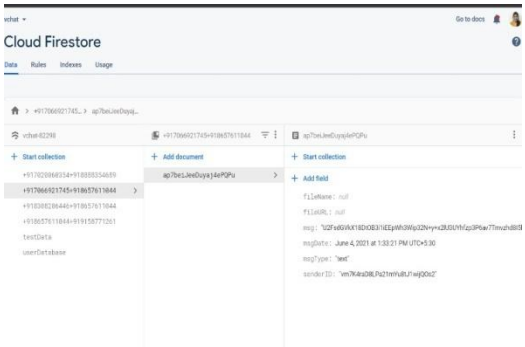


3. **Global Encryption/DecryptionModule:**

The Encryption in our application is applied in two layers, this one is which uses a Global static pair of private and public keys used to encrypt and decryptthedatacomingorgoingtotheonlinecloud database.

4. **Dynamic Key Approach Encryption/Decryption Module:**

The task of this second layer is to performprimary encryption/decryption on data which then goes to a local offline database and also gets globally encrypted by second layer then to cloud database. This module uses a static public key and dynamically generated private key which

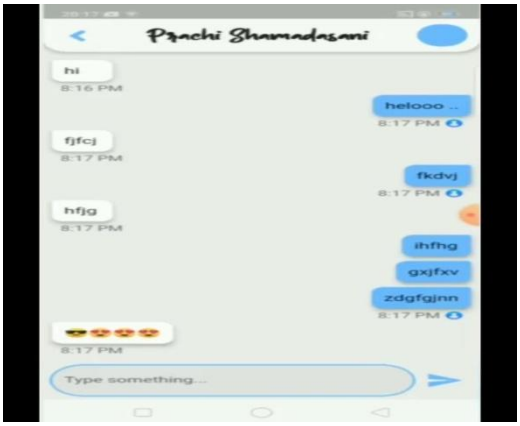


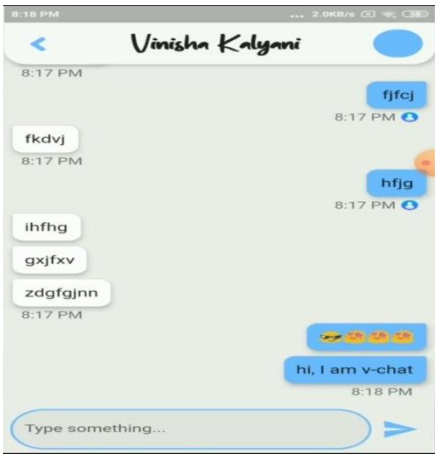
varies for every chat.

5. **Chat RecordModule:**

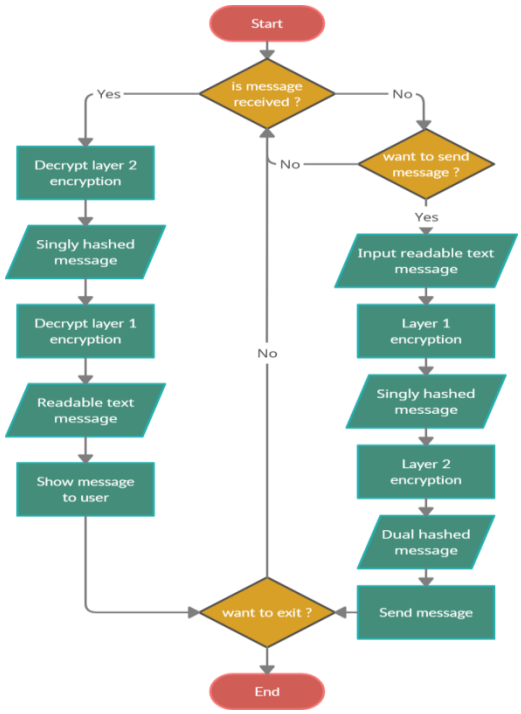
Since a lot of encoding and decoding of data is happening over here therefore, there was a need of this module. The task of this module is to store the datacomingfromfirstlayerofencryptiontoalocal database like SQLite, which is then used foroffline availability of chats, faster retrieval of data, easy searching in a largedataset.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 24, Issue 2, 2020, Pages. 222 - 226
Received 24 October 2020; Accepted 15 December 2020.





IV. FLOWCHAT



Annals of R.S.C.B., ISSN:1583-6258, Vol. 24, Issue 2, 2020, Pages. 222 - 226
Received 24 October 2020; Accepted 15 December 2020.

V. CONCLUSION

Data Security will always be a key issue of interest to work on and no matter how much security dowe provide; it will remain secure only for a limited time as it is following a static algorithm with no variance in it. Usage of Dynamic key pair generation is the best approach to improve the effectively of data encoding and decoding algorithms in case of both Asymmetric and Symmetric EncryptionAlgorithms.

VI. FUTURESCOPE

With the increasing development in technology, wecannot deny the fact that there will be a time when there will exist a system capable of decrypting any kind of security layer within seconds. In that scenario, the approach which can be involved in a multi-layered encoding/decoding datatransmission is the use block chain technology to store data, as I willmakethedatainaccessiblefortheunauthorized users.

VII. REFERENCES

[1] Edward YellakuorBaagyere, Peter AwonNatemiAgbedemnab,ZhenQin,Mohammed Ibrahim Daabo, Zhiguang Qin, A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers, Vol. 8, IEEE Access, 2020.

[2] AmmarHammad Ali, Ali M Sagheer, Design of Secure Chatting Application with End to EndEncryption for Android Platform, Vol. 43, Iraqi Journal for Computers and Informatics (IJCI), 2017.

[3] Ali Mohammed Ali Argabi, Md Imran Alam,A new Cryptographic Algorithm AEDS (Advanced Encryption and Decryption Standard) for data security, Vol. 6, IARJSET,2019.

[4] M. I. Youssef, A. E. Emam, M. AbdElghany, Multi-Layer Data Encryption using Residue Number System in DNA Sequence, Vol. 45, International Journal of Computer Applications, 2012.

[5] Yi-HuiChen,Ching-HuLu,Po-YuHsu, Multi layered Information Encryption Scheme with Fine- grained Authentication, APSIPA Annual Summit and Conference, 2015

[6] D. Veeraiah and J. N. Rao, "An Efficient Data Duplication System based on Hadoop Distributed File System," *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 197-200, doi: 10.1109/ICICT48043.2020.9112567.

[7] Rao, J. Nageswara, and M. Ramesh. "A Review on Data Mining & Big Data." *Machine Learning Techniques. Int. J. Recent Technol. Eng* 7 (2019): 914-916.

[8] D.R.V.A.Sharath Kumar, Y.Nagalakshmi and G.Sahithi, presented the paper in the International Conference on “Asynchronous techniques in Nano technology” at Sreenidhi Institute of Technology and Science, Hyderabad on January 2012.

[9] S. N. Ajani and S. Y. Amdani, "Probabilistic path planning using current obstacle position in static environment," 2nd International Conference on Data, Engineering and Applications (IDEA), 2020, pp. 1-6, doi: 10.1109/IDEA49133.2020.9170727.

[10] S. Ajani and M. Wanjari, "An Efficient Approach for Clustering Uncertain Data Mining Based on Hash Indexing and Voronoi Clustering," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 486-490, doi: 10.1109/CICN.2013.106.