International Journal of Research
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

Mobile Text Data Encryption System

[1]Mr. Vadipina Amarnadh, [2]Ch. Roja Reddy, [3]J. Naveen Kumar, [4]U. Swathi
[1]Assistant Professor, [2, 3, 4] B.Tech Student
[1,2,3,4] Department of CSE
[1,2,3,4] Anurag Group of Institutions, Venkatapur, Ghatkesar, Hyderabad, Telangana, 500038
Email: [1] amarnadhcse@cvsr.ac.in, [2] 16h61a072@cvsr.ac.in, [3] 16h61a0584@cvsr.ac.in, [4] 16h61a05b7@cvsr.ac.in

Abstract **- For modern organizations, speed and agility is the key to success built on enhanced IT efficiency and performance driven by the cloud. As always security must be a priority when migrating to cloud, but network teams are being let down by existing tools. Taking all this on board, we set about designing a network-based solution to handle the scale and performance demands of the cloud, without introducing extra fraction of operations. Mobile Text Data Encryption is a mobile app which allows users to store text files of their mobile by storing it in encrypted form in the server using AES algorithm without having to worry about confidentiality even if the mobile is lost. User need to login with his credentials and enter secret key to access his data. Other malicious user can't retrieve the data without the user credentials. If user mobile device is lost, he can access his text data by logging in to the system using another mobile and user will be free from worrying about the leakage of his confidential data.**

Index Terms **– Encryption, Decryption, Firestore, Firebase, Android, AES.**

I. INTRODUCTION

Lack of effective protection of sensitive data in mobile devices is a major concern that prevents the mobile devices from being used widely as part of enterprise networks or personal area networks. The proposed system will remove the barrier and enable users to enjoy the high efficiency and convenience brought by mobile devices. It will lead to another wave of prosperity of wireless networks and pervasive computing. Physical attacks have been proved effective in breaking some well-designed ciphers in practice. Unfortunately, it is challenging to designers to theoretically investigate the robustness of a cipher scheme against various physical attacks.

For anyone who needs a mobile device with higher-than-usual security to secure their information such as text files, there are a number of options. One such option is to encrypt your entire text data to secure. This means that every time you power your phone on, you'll need either a numeric pin or password to decrypt the device. An encrypted device is far more secure than an unencrypted one. When encrypted, the only way to get into the phone is with the encryption key. That means your data is going to be safe.

Encryption is a means of encoding data such as words, numbers, and images, using mathematical algorithms in order to make that data undecipherable to unauthorized viewers. Over the past several decades encryption has evolved and changed to meet the demands of evolving technology. Today the encryption algorithm accepted as the highest standard is the Advanced Encryption Standard (AES). AES is a formal encryption method adopted by the National Institute of Standards and Technology (NIST) of the US Government, and is accepted worldwide. In the process of encrypting data, an encryption key is created that allows users to encrypt and decrypt the data when it needs to be accessed. The encryption key must be protected in order to prevent access to the data from malicious or unauthorized users. Encryption key management is essential to a successful encryption solution, and it is often required or strongly recommended by most industry regulations.

In an encryption scheme, the data or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original data. An authorized party, however, is able to decode the cipher text using a decryption algorithm, which usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys. There are two basic types of encryption schemes: symmetric-key and Asymmetric-key encryption. In symmetric-key schemes, the encryption and decryption keys are the same. Thus, communicating parties must agree on a secret key before they wish to communicate. In asymmetric-key schemes, the encryption key and decryption key are different. One is a public key by which a sender can encrypt data and the other is a private key by which a recipient can decrypt the data. However, only the receiving party has access to the decryption key and is capable of reading the encrypted data or information. Asymmetric-key encryption is a relatively recent invention: historically, all encryption schemes have been private-key schemes.

Mobile text data encryption project allows users to store text files data of their mobile phones in encrypted form without having to worry about is confidentiality even if the mobile is lost. Here in this system, encryption is the process of converting text data into a code, especially to prevent unauthorized access. This code can't be understood unless it is decrypted. To decrypt the data, we need the same key that was used during encryption process. In case of symmetric key encryption, same key is used for both encryption and decryption. In case of asymmetric key encryption, different keys are used for encryption and decryption. The need for encryption is to prevent malicious users or unauthenticated users to access sensitive information text files stored in phone media.

II. LITERATURE SURVEY

1. **Role of Encryption in Mobile Database Security**
   Author: D. Roselin Selvarani and Dr. T. N. Ravi
   In this paper the authors presented security issues of Mobile database system as well as Mobile network and discussed the solutions for it. They classified the security issues in four different areas such as Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. They also identified a set of vulnerabilities on mobile database and provided some techniques to decrease the side effect of vulnerability of mobile database.

2. **Mobile Database Review and Security Aspects**
   Author: Bhagat.A.R Prof. Bhagat.V.B
   In a mobile database application a part or a replica of the database is locally installed on the mobile device. This is a significant difference compared to a conventional client-server application where all data is centrally stored in a database server. The approach with a mobile database provides the necessary autonomy to the mobile device to work independently from the central database. The client application can work with the mobile database asynchronously, and needs to connect to the central database only when it is necessary to synchronize. This approach has several advantages compared to a conventional approach where the clients do not use local storage.

3. **Distributed Certified Information Access for Mobile Devices**
   Author: C. Galdi, A. Del Sorbo, and G. Persiano
   In this paper we describe a primitive, which we call, Certified Information Access, in which a database answers to a query by providing the information matching the query along with a proof that such information are consistent with the actual content of the database.

4. **Securing Distributed Storage: Challenges, Techniques, and Systems**
   Author: V. Kher and Y. Kim Storage
   The rapid increase of sensitive data and the growing number of government regulations that require long-term data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems The main advantage of SIDS (running directly on the storage server or on the disk firmware) as compared to host-based IDS is that an intruder having full access to the host can disable a host-based IDS, whereas a SIDS can still continue to function properly and are independent of host (or OS) compromise.

III. EXISTING SYSTEM

In the existing system, the data that the user want to secure by encrypting, will be stored in the mobile phone locally. When such important data is being stored in the mobile phone, if the phone is lost then the data will also be lost. If the mobile is lost, the user will not have any chance to retrieve the lost data back.

Disadvantages of Existing System:

- Cannot access from any mobile phone
- When the phone is lost then the data will be completely lost

IV. PROPOSED SYSTEM

For modern organizations, speed and agility is the key to success built on enhanced IT efficiency and performance driven by the cloud. As always security must be a priority when migrating to cloud, but network teams are being let down by existing tools. Taking all this on board, we set about designing a network-based solution to handle the scale and performance demands of the cloud, without introducing extra fraction of operations. Mobile Text Data Encryption allows users to store text data of their mobile phones by storing it in encrypted form in the server without having to worry about confidentiality even if the mobile is

lost. The user need to register and set his pin during registration process which will be used in encryption and decryption processes. During encryption, if the pin is matched, the data will be encrypted and uploaded into cloud storage which is firebase. During decryption, if the pin is matched then list of files that are uploaded will be displayed. If we want to download a file, then the file will be decrypted and will be downloaded into our local storage.

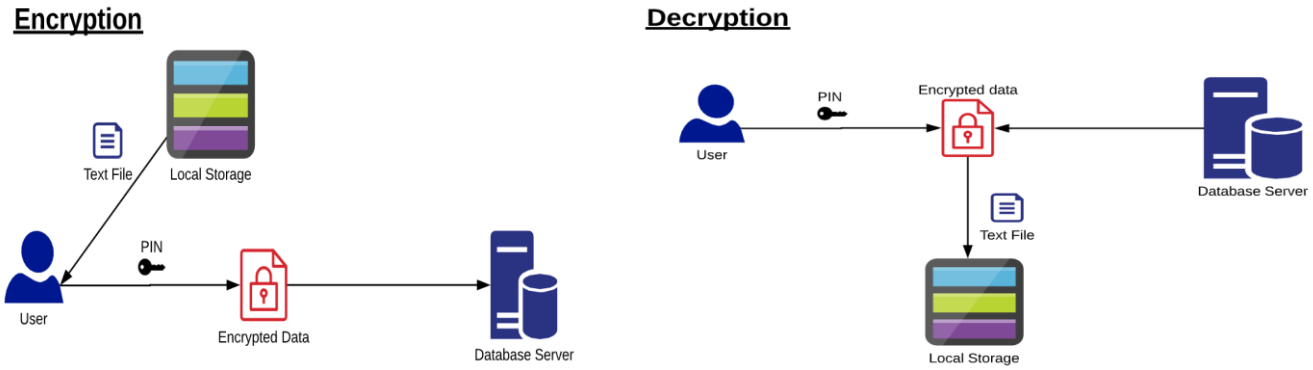

Fig.1: Architecture of proposed system

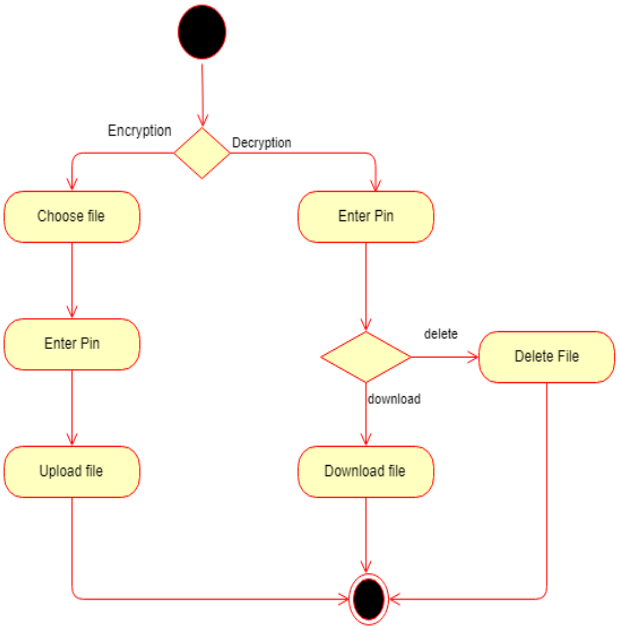

Fig.2: Activity diagram

Advantages of Proposed System:

- Fast processing
- Can access encrypted data from any mobile phone
- Use of Firebase firestore to store encrypted data makes the data well organized as the data is stored in the form of key-value pairs
- Use of 256 bit key in AES algorithm and SHA-512 for key generation increases the security
- Easy to use

SOFTWARE REQUIREMENT SPECIFICATION:

Software Requirements:

Programming Language: JAVA
Database: Firebase
Operating system: android 4 and above versions

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

Presentation Logic: XML

Hardware Requirements:

Storage: 16 GB
RAM: 1.00 GB

V. IMPLEMENTATION

1. **Encryption Module:**
In this module, file to be encrypted is chosen from the storage and pin should be entered. The entered pin is then converted into secret key using SHA-512. If the generated secret key matches with the key set by the user then using this secret key, the data to be encrypted will be encrypted using AES algorithm with 256 bit key. The encrypted data will be uploaded into the firebase firestore in the form of key-value pair.

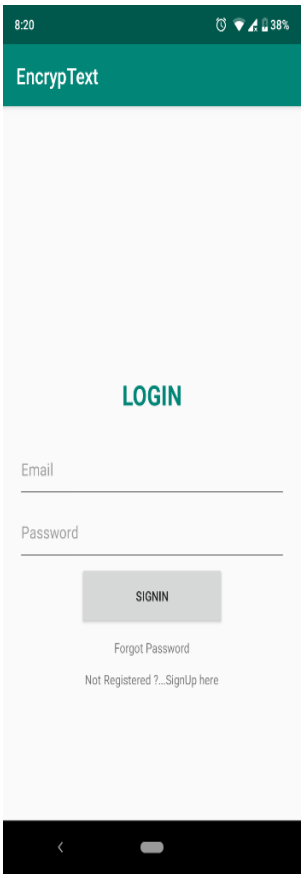

Fig.3: Login Page

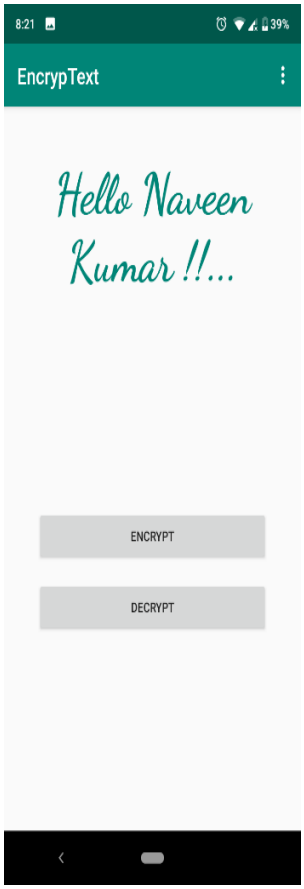

Fig.4: Home page with encrypt and decrypt options

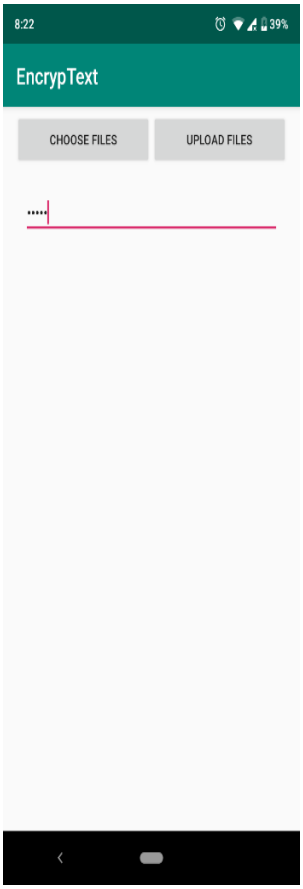

Fig.5: Encryption page

2. **Decryption Module:**
In this module, the pin is to be entered to display all the uploaded files. From the entered pin, the secreted key is generated and if it matches with the default key then the list of uploaded files will be displayed. The user can either download the file from the firebase or delete it from firebase. When the user tries to download the file, the file will be decrypted using the entered pin and will be stored in the local storage of the mobile.

Fig.6: Decryption Page

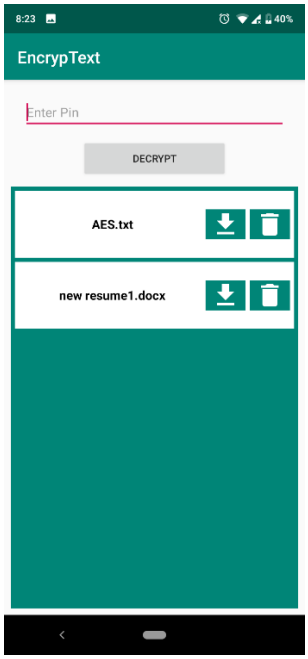

Fig.7: List of encrypted files

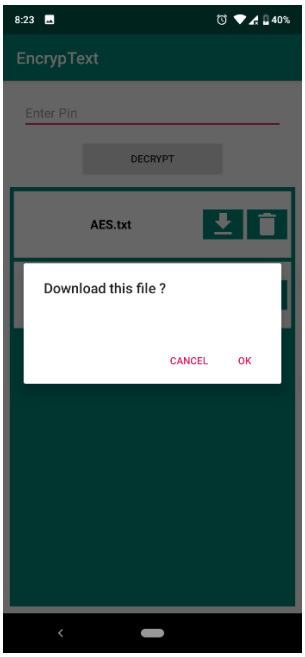

Fig.8: Decrypt and download required file

VI. CONCLUSION

The Mobile Text Data Encryption System is a mobile application. Its basic function is to encrypt the text data in the mobile phone using AES algorithm and store it in Firebase Firestore which is a cloud storage. This application will simplify the process of accessing the encrypted data from the cloud storage as the user is able to access his private data by logging in to his account from any mobile phone. The project is developed in such a way that, the user can easily encrypt and decrypt the required data using his mobile phone without any difficulty. Whenever the user want to encrypt or decrypt data, he has to enter the security pin that was set by the user at the time of registration. The project reduces effort that is to be made by the user to restore his lost data in the absence of the device where the data is stored.

VII. REFERENCES

[1] Heeks, R. (2008). Meet Marty Cooper – the inventor of the mobile phone, Accessed June,2013 from htpp://news.bbc.co.uk/2/hi/programmes, from IRKHS 2040 at International Islamic University Malaysia.
[2] Murphy, L. (2009). A textbook "Beginning Android2", published by Apress L. P. USA.
[3] Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. & Roback, E. (2000). "Report on the Development of the Advanced Encryption Standard (AES)" Computer security division information technology laboratory national institute of standards and technology administration, U.S. Department of Commerce, USA
[4] eSTREAM, ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream.
[5] D. J. Bernstein, "Which eSTREAM ciphers have been broken?" http://www.ecrypt.eu.org/ stream/, submitted 2008- 02-21.
[6] A. Biryukov and A. Shamir, "Cryptanalytic time/memory/data tradeoffs for stream ciphers," in Proceedings of Asiacrypt'00, no. 1976 in Lecture Notes in Computer Science, pp. 1–13, Springer-Verlag, 2000.
[7] C. Galdi, A. Del Sorbo, and G. Persiano, "DistributedCertified Information Access for Mobile Devices," Workshop in Information Security Theory and Practices(WISTP'07), Crete, Greece, May 8-11, 2007.
[8] A. Biryukov, "Block Ciphers and Stream Ciphers: The State of the Art," Lecture Notes in Computer Science, in Proceedings of the COSIC Summer course, 2003.
[9] A. J. Nicholson, M. D. Corner, and B. D. Noble, "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, vol. 5, no. 11, pp. 1489-1502, Nov., 2006.