PRIVACY PROTECTION IN SMARTPHONE'S BY USING MOBILE CLOUD FRAMEWORK

Ankit Mandal[1], Zohra Khan[2], Ruchi Gupta[3], Swapnil Waghmare[4]
Student[1, 2, 3], Faculty4
Department of Computer Engineering,
Pillai HOC College of Engineering and Technology, Rasayani, India

***Abstract*— we are living in the modern era where we enjoy the benefit brought by various kinds of IoT devices, our private data are leaked. Smartphone, as the typical hub of IoT devices, use various kinds of applications, which collect our private data. In fact, private data leakage, as a possible danger, is caused by the current design trend in industry, which is increasing day-by-day. However, few people notice the side-effect, but they never stop using "smart" devices. In this paper, we have introduced the behaviors of data collection, clarified the motivations and motive behind them. Cloud computing is the perfect way out with sufficient resources and admirable services. This paper introduces a mobile–cloud framework to provide fine-grained permission authorization service for IoT devices. To protect confidentiality of the sensitive data while supporting data is encrypted by the proposed convergent encryption technique before out sourcing, with using AES algorithm.**

Keywords: - IoT, Cloud Computing, Android, AES Algorithm

I. INTRODUCTION

At this moment the demand of internet for wireless communication is increasing day by day and hence the security is necessary to guard such communication by users on unconfident wireless medium. Data which is transfer over the communication channels is vulnerable to attacks because of confidential data it contain. To explain the data from outside threat the belief of Cryptography is emerged, in this methodology of writing such code is cipher and text is converted into cipher text which is commonly called Encryption whereas the reverse practice of converting a cipher text into normal text is known as Decryption. Modern cryptography techniques are more secure than the simple ones and are extensively used such as DES, 3DES, AES, ECC, ECDH, RSA [5]. In the past decade, the Internet of Things (IoT) has subtly influenced our daily life. All kinds of physical objects, including groceries, vehicles, buildings, and others, are connected and combine into a network with the help of all kinds of electronics, such as sensors, mobile devices, another wearable equipment. Everything is becoming smart and convenient for users. Meanwhile, due to the limited resources of IoT devices, cloud servers with sufficient resources can be used to take charge of data processing and storage.

This research is based on how the data is leaked from a Smartphone because of so many other apps collect users' data more than needed for the original function while within the permission scope, including tracking location, accessing photos, accessing address book, accessing calendar, tracking International Mobile Station Equipment Identity (IMEI) and Unique Device Identifier (UDID), and more. By the proposed approach, described in this paper, the low-cost, simple and friendly solution for the private data security will be presented that is user friendly, in this framework the idea is to demonstrate a small reliable cloud framework that is in contact with Android application connecting to the remote main server to provide fine-grained permission authorization service for IoT devices, and show its performance by experimental results, In this framework to get rid of data leakage, the data from the user side is sent to the cloud server in encrypted from, once the data is uploaded it can't be access in phone that leads to data security. For the data to be encrypted key is needed, that'll be given by user, so while decrypting the data key will be the same i.e. "symmetric key for encryption & decryption", and after decrypting the data, the data will be accessible in the Smartphone. The categorization of data is been done on the priority bases the priority of the Image file is been given 1st place and the priority of Video file is on 2nd place and following that the priority level of documents is on 3rd place and so on.

II. PROBLEM STATEMENT

In the present system all data is been directly uploaded to cloud. After the user gets authorized to the system he can upload the data which he wants to but the problem here is that if he is not the valid user he will be able to change the login credential and can see or modify the data which is over the server. And on other hand the problem related to algorithm was also there because for encryption & decryption different keys was using, as the algorithm was not efficient the security related problem was present.

III. RELATED WORK

The detailed working mechanism of the existing system is shown in Figure 1. IoT System sends the request to access data to the cloud. The access control service receives the requests and validates the authorization. The en/decryption service encrypts and decrypts data before data is stored in storage and sent back to IoT devices. If we allow the access control service to authorize apps to access one specific type of data with the same privacy level, our approach can reduce over 2.5 times the privacy grade than original coarse-grained permission authorization. If we set the access control service to only allow apps to access the specific pieces of data they need, our approach can reduce over 35 times the privacy grade than the original. To provide fine-grained permission authorization, the first thing is to classify users' data based on their privacy [1].

The limitation of this framework is that it was related to website only, and the security was not perfectly given to the data of the user, and the project was only related to web application only.

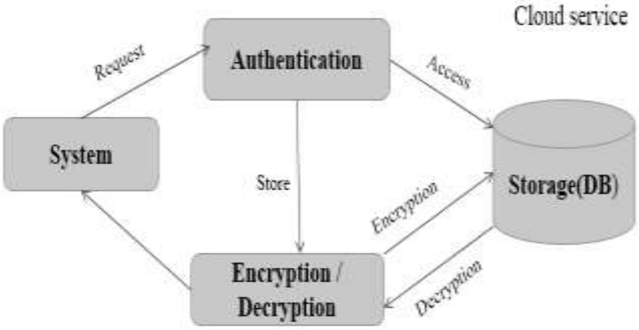


figure.1 authentication and encryption/decryption process in cloud framework

IV. Implemented system

The Smartphone is the pivot, and can be used to control various IoT devices. However, Data over-collection behaviors are ubiquitous, due to the deficiencies of current mobile operating Systems. They only provide coarse-grained permission authorizations and general privacy management. Cloud computing with sufficient resources and fine-grained access control service can be used to solve the data privacy issue [1]. We propose a workflow that allow user to store, modify and to see data at one place only without actually storing at their device. In this project the user will be able to get logged in to the mobile application with the correct login credential and once they get to the actual framework there they can select the data which they want to select and before uploading it to the cloud server they have to give encryption key [4]. This key make the data more secure because by any chances if any unauthorized user get the access to the app he/she won't be able to decrypt is as the key need to be the same for decrypting also. The user will get the list of what data has been uploaded to the server and from that list the data can be retrieve back. The other security provided by this application is that once data is been uploaded to the server it won't be displayed in the Smartphone, as the data is not accessible it won't be tracked by other applications.

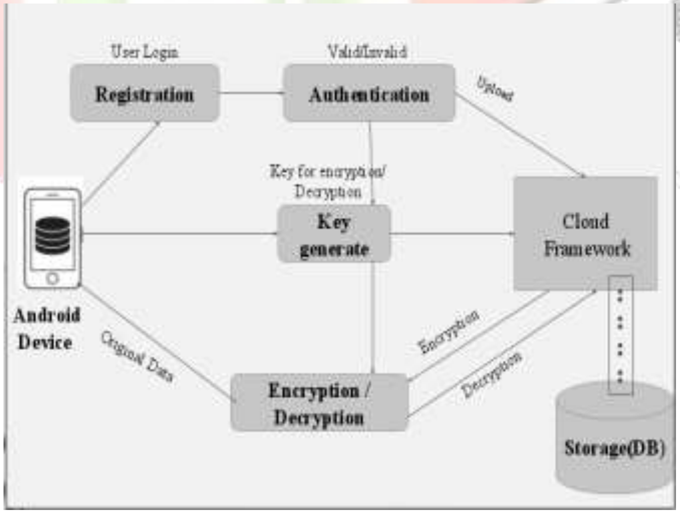


figure.2 working mechanism of the mobile–cloud framework.

And for the encryption & decryption the algorithm which were using is AES, AES is announced as a federal information Processing standard by NIST (National institutes of standards and technology) in 2001. AES is recurrently used encryption technique due to its high security, efficiency and simplicity. It uses the same key for both encryption and decryption process and known as symmetric block cipher. It uses three block ciphers AES-192, AES-128, AES-256. There are different rounds of processing according to the block size such as 10 rounds for 128- bit key, 12 rounds for 192-bit key and 14 rounds for 256-bit key. Different steps for encrypting data with AES are given below: Key Expansion- Rinjndael's Key Schedule is used to calculate the round key using the cipher key. Initial Round- Add round key: Bitwise XOR operation is used to combine each byte of the state with the derived round key.

Different Rounds of Processing

1. Sub Bytes: every Byte is replaced with another using the lookup table, a nonlinear kind of substitution.
2. Shift rows: This is called transposition step where each row will by cyclically shifted to number of times required.
3. Mix columns: four Bytes of each column are combined in a state matrix.
4. Final Round
5. Sub Bytes
6. Shift Rows
7. Add Round Key

So, the final round will not have mixing of columns. During Decryption the processing rounds will be same but the only difference is Inverse of every processing round will be executed. If in encryption we have sub bytes then in decryption it will be Inverse sub bytes. Similarly for shift rows and mix columns in encryption there will be Inverse shift rows and inverse mix columns for decryption.

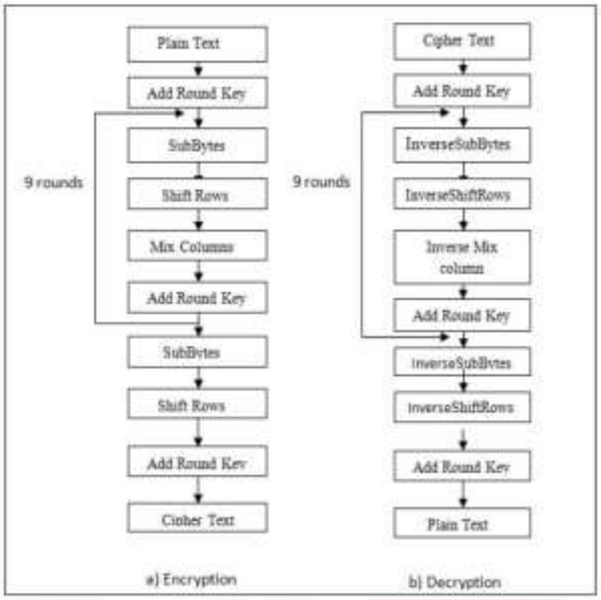


figure.3 work flow of AES algorithm

V. RESULTS

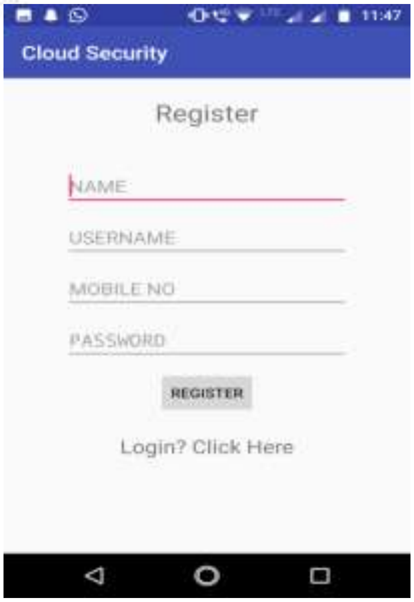
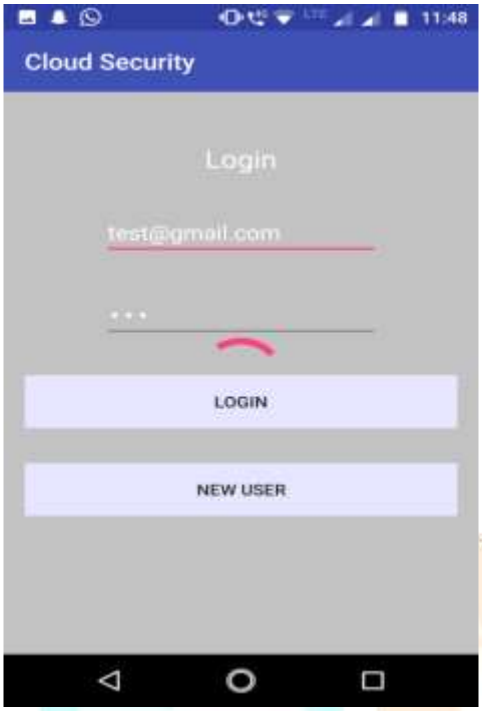


figure.4 Starting Page

figure.5 Registrati on Page



test@gmail.com

• • •

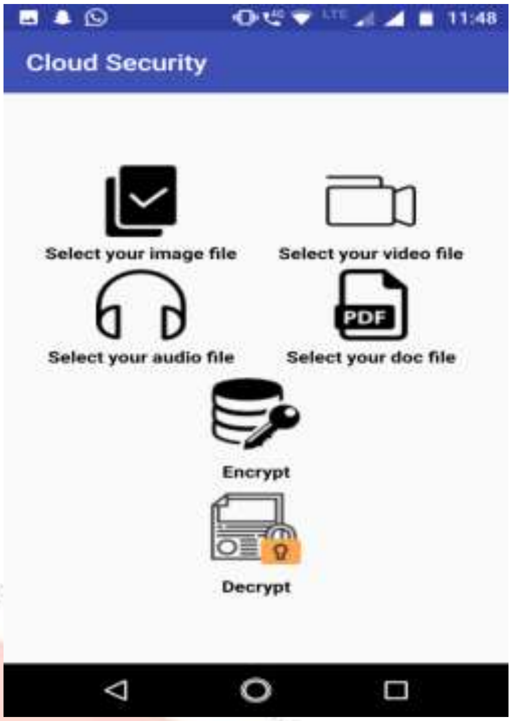
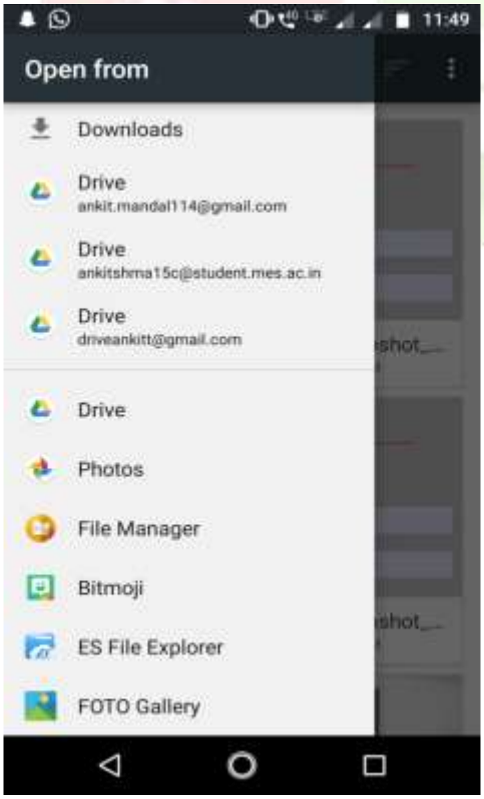
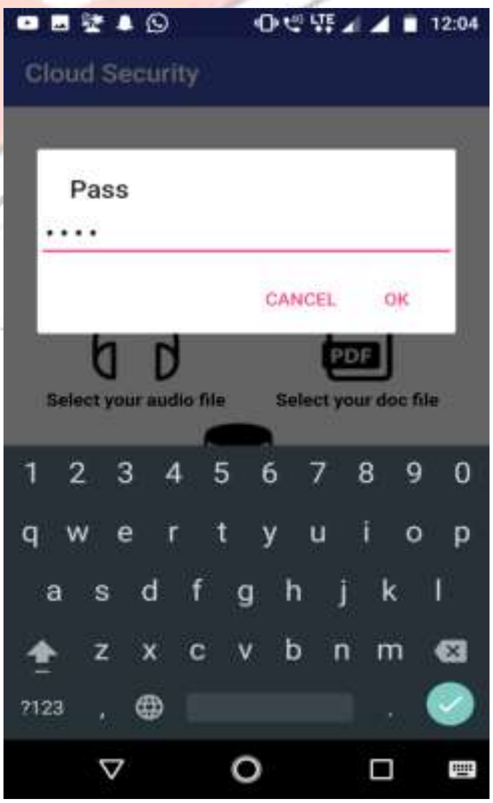


figure.6 Login Page

figure.7 Mobile framework

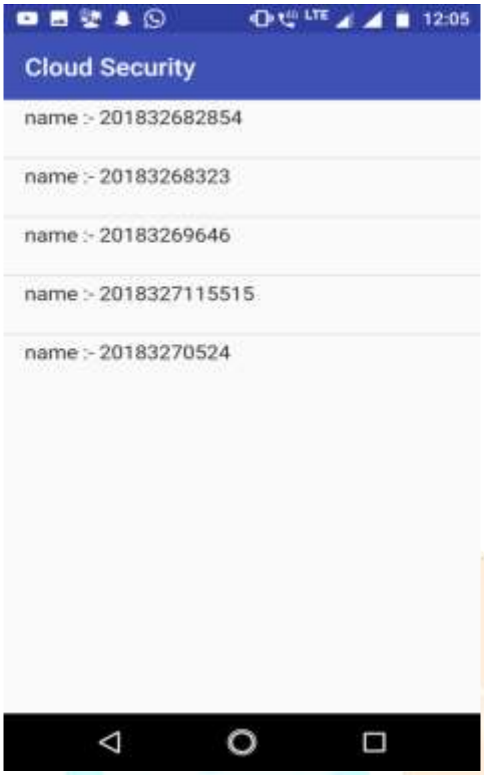




• • • •

figure.8 selection of image files from gallery

figure.9 key to encrypt file



Cloud Security

name :- 201832682854

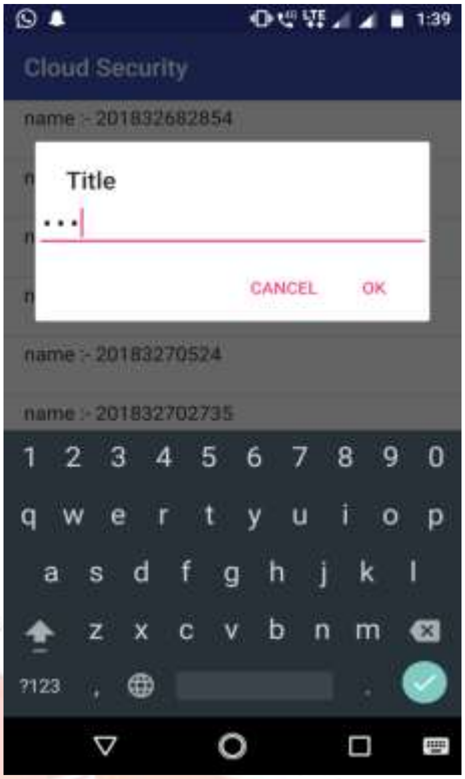
name :- 20183268323

name :- 20183269646

name :- 2018327115515

name :- 20183270524

figure.10 encrypted file



Cloud Security

name :- 201832682854

Title

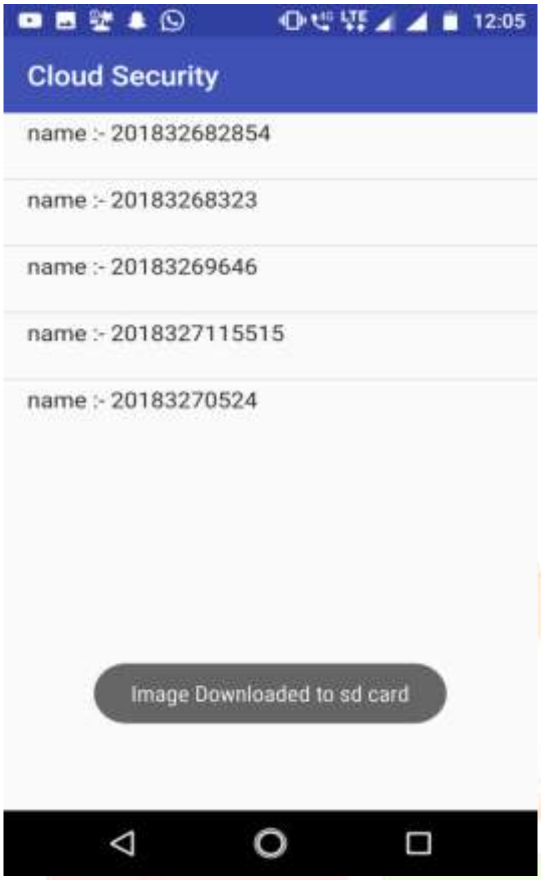
•••

CANCEL OK

name :- 20183270524

name :- 201832702735

figure.11 key to decrypt file



Cloud Security

name :- 201832682854

name :- 20183268323

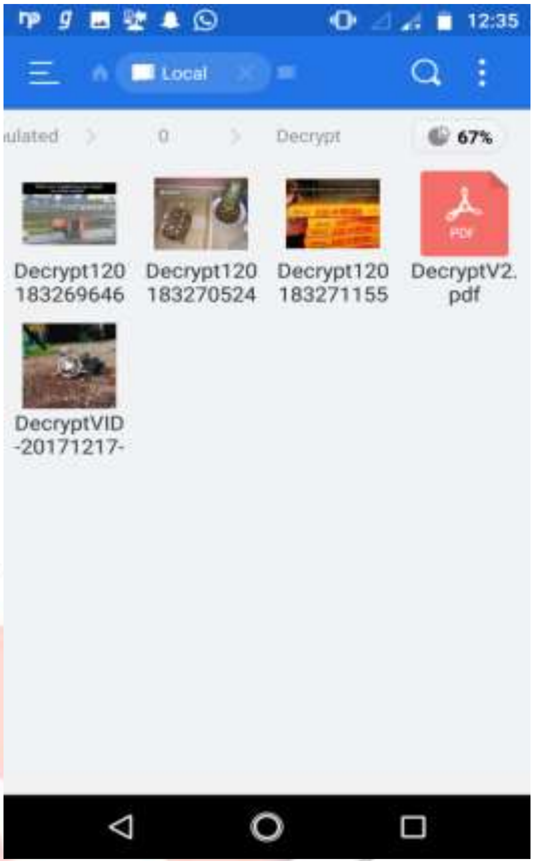
name :- 20183269646

name :- 2018327115515

name :- 20183270524

Image Downloaded to sd card

figure.13 decrypted data in smartphone



Decrypt120183269646

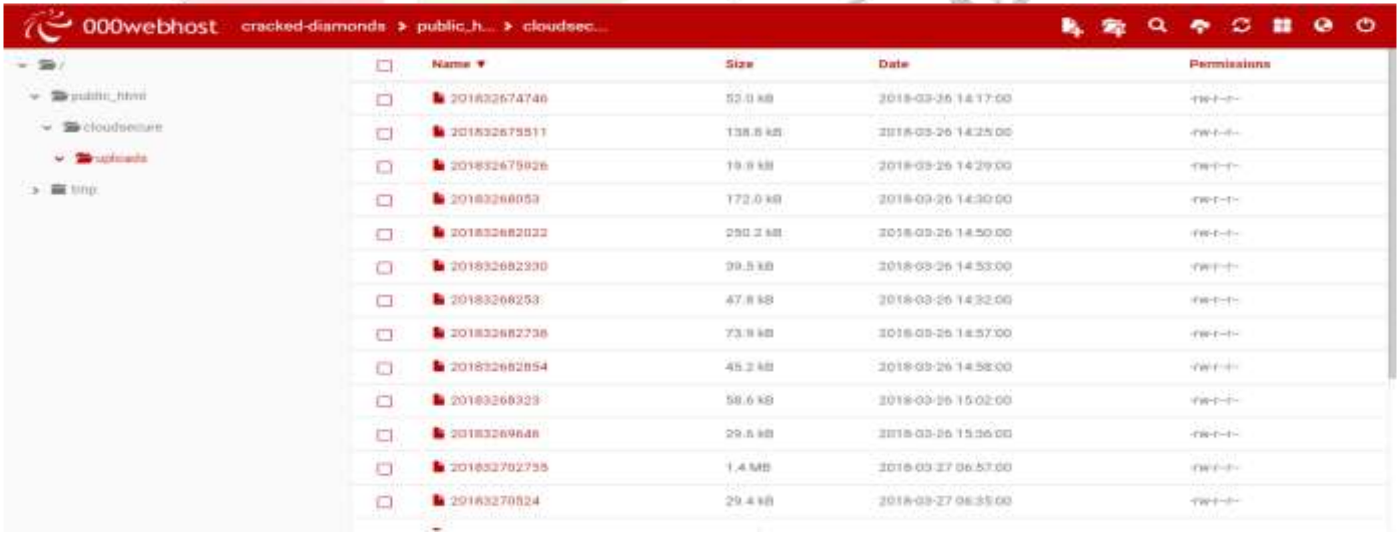
Decrypt120183270524

Decrypt120183271155

DecryptV2.pdf

DecryptVID-20171217-

figure.12 decrypted file downloaded



000webhost cracked-diamonds > public_h... > cloudsec...

□	Name ▾	Size	Date	Permissions
□	201832674746	52.0 kB	2018-03-26 14:17:00	-rw-r--r--
□	201832675511	138.8 kB	2018-03-26 14:25:00	-rw-r--r--
□	201832675926	19.9 kB	2018-03-26 14:29:00	-rw-r--r--
□	20183268053	172.0 kB	2018-03-26 14:30:00	-rw-r--r--
□	201832682022	250.2 kB	2018-03-26 14:50:00	-rw-r--r--
□	201832682330	39.5 kB	2018-03-26 14:53:00	-rw-r--r--
□	20183268253	47.8 kB	2018-03-26 14:32:00	-rw-r--r--
□	201832682736	73.9 kB	2018-03-26 14:57:00	-rw-r--r--
□	201832682854	45.2 kB	2018-03-26 14:58:00	-rw-r--r--
□	20183268323	58.6 kB	2018-03-26 15:02:00	-rw-r--r--
□	20183269646	29.6 kB	2018-03-26 15:36:00	-rw-r--r--
□	201832702755	1.4 MB	2018-03-27 06:57:00	-rw-r--r--
□	20183270524	29.4 kB	2018-03-27 06:35:00	-rw-r--r--

figure.14 encrypted data uploaded on cloud server

VI. Conclusion

This project elaborates the design and construction of mobile framework. The smartphone is the pivot, and can be utilized to control different IoT gadgets. However, data over-collection behaviors are present, due to the deficiencies of current mobile operating systems. This application will permit end client to store their private information over the cloud. By symmetric encoding and decoding method, once information is transferred to server it won't be accessible in the portable smartphone. The client needs to decode the file and download it in smartphone to access it again. The future aspect of this project is that we can select multiple data at a time to encrypt.

References

[1] W. Dai, H. Chen, and W. Wang, “RaHeC: A Mechanism of Resource Management for Heterogeneous Clouds,” Proc. IEEE 17th Int’l. Conf. High Performance Computing and Commun., 2015, pp. 40–45.

[2] P. Prajapati, N. Patel, R. Macwan, N. Kachhiya and P. Shah, “Comparative Analysis of DES, AES, RSA Encryption Algorithms”, International Journal of Engineering and Management Research, vol. 4, no. 1, (2014), pp. 132-134.

[3] P. Kumar and S. B. Rana, “Development of modified AES algorithm for data security”, OptikInternational Journal for Light and Electron Optics, vol. 127, no. 04, (2016), pp. 2341-2345.

[4] A. K. Mandal, C. Parakash and A. Tiwari, “Performance evaluation of cryptographic algorithms: DES and AES”, Electrical, Electronics and Computer Science (SCEECS), (2012).

[5] Samiksha Sharma," Cryptography: An Art of Writing a Secret Code" IJCST Vol. 8, Issue 1, Jan - March 2017

[6] G. Wu et al., “A Decentralized Approach for Mining Event Correlations in Distributed System Monitoring,” J. Parallel and Distrib. Computing, vol. 73, no. 3, 2013, pp. 330–40.

[7] M. Qiu et al., “Phase-Change Memory Optimization for Green Cloud with Genetic Algorithm,” IEEE Trans. Computers, vol. 64, no. 12, 2015, pp. 3528–40.

[8] M. Qiu et al., “Informer Homed Routing Fault Tolerance Mechanism for Wireless Sensor Networks,” J. Sys. Architecture, vol. 59, no. 4, 2013, pp. 260–70.

[9] T. Chen et al., “Software Defined Mobile Networks: Concept, Survey, and Research Directions,” IEEE Commun. Mag.,vol. 53, no. 11, Nov. 2015, pp. 126–33.

[10] W. Li et al., “Mechanisms and Challenges on Mobility-Augmented Service Provisioning for Mobile Cloud Computing,”IEEE Common. Mag., vol. 53, no. 3, Mar. 2015, pp. 89–97.