Secure Crypto System Framework for Data Sharing Through Mobile Cloud

K. Suresh
M.Tech,Dept of CSE
KMM Institute of Technology and Science
Tirupati, Andhra Pradesh, India

Dr. K. Venkataramana
Associate Professor,Dept of CSE
KMM Institute of Technology and Science
Tirupati,Andhra Pradesh

Abstract: **Now a days the Mobile cloud allows sharing the data between the organizations and suppliers and customers is very easily. According to a survey by InformationWeek [3], nearly all organizations shared their data somehow with 74 % sharing their data with customers and 64 % sharing with suppliers. But the data sharing at cloud having many security and privacy issues, according to survey the 45% mobile cloud users facing the security is top challenging issue, such as direct access of stored data and steal the data to sell to third parties in order to gain profit. In today's world, there is a strong need to share information to groups of people around the world. Since the Cloud is riddled with so many privacy issues, many users are still apprehensive about sharing their most critical data with other users, for example sharing the patient details to remotely located doctors. This paper describes the types of security and privacy issues in the cloud and explains the one method or framework to achieving security and privacy for data sharing through the cloud and handling the group and group members for sharing the data.**

Keywords: Mobile cloud computing, encryption, decryption, hashing, OTP etc.

I. INTRODUCTION

Mobile cloud computing is a new platform combining the mobile devices and cloud computing to create a new infrastructure, whereby cloud performs the heavy lifting of computing-intensive tasks and storing massive amounts of data. In this new architecture, data processing and data storage happen outside of mobile devices. The "computing" component of the cloud consists of a number of pre-configured, pre-built and scalable services for consumption with mobile applications. Cloud runtimes are also offered as a mechanism to offload business logic from mobile devices. All these fit within the cloud platform as a service (PaaS) model and are collectively known as mobile backend as a service (MBaaS).

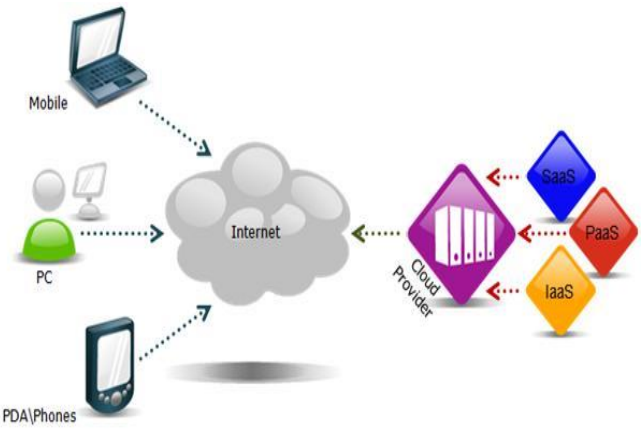

Fig1 Mobile Cloud Computing Architecture

Cloud computing involves the multiple cloud components that communicate with each other with the help of application interfaces mostly web services, however now it has started to server as applications as well mostly in recent Smartphones. UNIX operating system follows the same theoretical techniques for its tasks. The task complexity is divided into all the components making balanced and manageable results. The two most important components of the back end and front end, the front end is the interfaces or the main screen that is visible to the customers and users through which they interact with the system. This interface can be browsed with the help of web browsers and all the applications can be used with this interface. Usually this interface is GUI based.

The back end involves all the components, the complete architecture and programming technique of cloud computing that is totally remains hidden from the users. Only system knows what is going on at the back of very user request. The back end device involves, cloud server, Assistant computers, Data storage media and many connectors.

A fourth of the surveyed organizations consider data sharing a top priority. The benefits organizations can gain from data sharing are higher productivity. With numerous users from different organizations contributing to data in the Cloud, the time and cost will be much less compared to having to physically exchange data and hence creating a confusion of redundant and possibly out-of-date documents. In modern healthcare environments, healthcare providers are willing to store and share electronic medical records via the Cloud and hence remove the geographical dependence between healthcare provider and patient [6]. The sharing of medical data allows the remote monitoring and diagnosis of patients without the patient having to leave their house. In one particular scenario, a patient can connect sensors to monitor their ECG to detect any heart problems [7]. They can then run an app on a Smartphone device which receives ECG data from the sensors via Bluetooth. The app can then periodically send ECG data to the Cloud. Any authorized doctor or nurse can then get the ECG data via the Cloud without having to visit the patient hence saving costs and time. Therefore, data distribution becomes such a useful feature to implement in Cloud-based environments.

Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group. The data owner should also be able to revoke access rights against any member of the group over his or her shared data. No member of the group should be allowed to revoke rights or join new users to the group.

One best solution to achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users. When the data owner wants to share his data to a group, he sends the OTP to a specific member of the group for while accessing the data/file from the cloud in encryption format. Any member of the group can then get the encrypted data from the Cloud and decrypting is done based on his/her IMEI, that is completely taken care by the application of the member(group application). If the IMEI is not matched the file, then file is not open in his/her device. However, the problem with this technique is that it is computationally inefficient and storing the data at mobiles or cloud (the file size increasing vastly)when we are using like RSA algorithms. (why we are mentioning RSA here, The RSA is the best asymmetric secure algorithm in the world, but for the file sharing it is inefficient, because this algorithm having the security 1024 bits minimum and today's real world using the 2048 bits security .Consider an example if we send the text like "Sharing the data securely through Mobile cloud computing" in the encrypted format using RSA with 1024 bit modulo. The length of the plain text is 56, and each encrypted character size is 308(approximately), so the total encrypted text size is 308x56=17248. So the file size will be increasing immensely and at mobile side computations also very difficult.) We changed the RSA related to file transfer in the network and storing the data at mobiles or cloud without increasing the original file size is called as HP-RSA (High performance RSA).HP-RSA reduces the number of computations than the general asymmetric key cryptography RSA and storing the data at mobiles is same as symmetric algorithms like DES, AES etc.

II. RELATED WORK

Anand Surendra Shimpi [8] proposed a secure framework (MobiCloud) for processing data in mobile cloud computing. This framework stores data in a secured fashion which helps in protecting the user's privacy. In addition, he has implemented a project named "Focus Drive" which improves the driving safety of teenagers. In MobiCloud mobile users must trust the cloud service provider to protect the data received from mobile devices. The mobile cloud is composed by three main domains: (i) the cloud mobile and sensing domain, (ii) the cloud trusted domain, and (iii) the cloud public service and storage domain. In this framework, each mobile device is virtualized as an ESSI in the cloud trusted domain and each ESSI can be represented as an SN in a particular application (a.k.a., a service domain). The introduced ESSIs can be used to address communication and computation deficiencies of a mobile device, and provide enhanced security and privacy protections. A mobile device and its corresponding ESSI can also act like a service provider or a service broker according to its capability, e.g., available computation and communication capabilities to support a particular communication or sensing service. This approach takes maximum advantage of each mobile node in the system by utilizing cloud computing technologies. In this way, the cloud's boundary is extended to the customer device domain. Note that an ESSI can be an exact clone, a partial clone, or an image containing extended functions of the physical device. The networking between a user and its ESSI is through a secure connection, e.g., SSL, IPSec, etc. Jibitesh Mishra [9] proposed a secure architecture for MCC to integrate mobile applications with the various cloud services. This architecture improves the storage and processing of data on mobile devices in a secured manner. It helps in maintaining the integrity and security of data. Itani et al [10] proposed a framework which was energy efficient for mobile devices to assure mobile user's integrity i.e. using *incremental cryptography and trusted computing*, the data/files of users are stored in the cloud. This framework results in saving 90% of processing energy on the mobile devices when compared to other conventional techniques with more security. Eugene E. Marinelli [11] developed *Hyrax*, a platform from Hadoop which supports cloud computing on Smartphones. It allows user's applications to utilize data and computing process on

networks on Smartphones. It offers a sane performance in data sharing and tolerates node departure. Eugene also implemented a distributed media search and data sharing approach. Jia et al. [12] provide a secure data service mechanism through Identity based proxy re-encryption. This mechanism provides confidentiality and fine grained access control for data stored in cloud by outsourcing data security management to mobile cloud in trusted way. The goal of this protocol is that only authorized persons/sharer can access the data while unauthorized sharer will learn nothing. Identity based encryption is that user encrypt the data through his identity (Id). This encryption scheme is based on bilinear pairing. A bilinear map is e: G1 × G2 →GT where G1 and GT be cyclic multiplicative group with prime order q and g be generator of G1, having the properties of bilinearity, non degeneracy and computability. Proxy based re-encryption is used by mobile user to provide access control capability to cloud, which could grant access to an authorized users by transferring cipher text encrypted by data owner's identity to one with sharer's identity. In this mechanism 3 entities are involved: Data owner (DO), Data Sharer (DS) and Cloud Servers (CSs). Both DO and DS utilize data storage service to store and retrieve file. CSs provide services to mobile clients.

III PROPOSED FRAMEWORK

The new Framework is called " ". It is having the two different applications Group Admin Application and Group members Application. These two applications handle the data sharing securely to all group members through cloud in encrypted format. Here we are using the HP-RSA algorithm, it reduces the number of operations on encryption and decryption and also we send and receive only original file size only.
This framework contains the mainly three modules they are.
1. Group Admin Application
2. Group members Application
3. Encryption and Decryption Module

Group Admin Application: who maintains the group (Group Admin, *Group name should be registered in the cloud*) should be install this application and creates the group and store the data into cloud in encrypted format. This application itself having the interface to encrypt and decrypts the data or file. The Group admin adding the all group member details (IMEIs of their devices) to this application. The Group admin only (who creates the group) having the right to add or delete the group members.

Group members Application: who are group members should be install this application and accessing the data or file from the cloud with Group Admin Application authentication.

Encryption and Decryption Module: **This** allows the all members of the group to encrypt and decrypts the data by using HP-RSA algorithm.

The HP-RSA algorithm works in three phases, Initialization phase, encryption and decryption phase is as follows.

A. Initialization phase

1. Install the Secure Cloud application at both ends (Group Admin and Group members). The Group member should share he/her IMEI number to Group admin, and then group admin provides the unique key for them.
2. The Group admin only knows the public and private keys of HP-RSA algorithm.
3. The Group Admin app itself acts as Server; it has the all group member's details.
4. Both Apps are having the interface for encrypt and decrypt the file, the only difference is Group admin app maintains the all group member's details.

B. Encryption Process

The Group Admin App does the Following:
1. Using (2048 bits modulo) public key (e, n)
2. Each character (c) of Message (M) will be represented as positive integer c < n.
3. Before going to encrypt, search the asci value of character (m) is already encrypted or not? If m is found in the asci[] array then m is substituted by index of hash table. If m is not found in the array asci[], then m is encrypted and applying hashing on it, then searching the hash table, then m is substituted with index.
4. Encrypt the message M with the public key (e, n) like encrypt[i] = c^e mod (n).
5. SIM serial number will be added to first ten characters of cipher text (cipher text + SIM card number).
6. The user Sends the message as cipher text is encrypt[].

C. Decryption Process

The Group member App does the Following:

1. The algorithm at receiver side gets the IMEI number of the device and separates the IMEI numbers list from the cipher text and comparing it. If it is true then the following
2. steps will be done otherwise the message will not possible to decrypt.

2. Uses the private key (d, n) to decrypt the message like
3. Decrypt the all characters in the encrypt[] array as
   3.1. index[i]=encrypt[i]
   3.2. It checks each character before going to decrypt in the index table if it is not there, then
   3.3. temp=index[i]
   3.4. Ptxt[j]=harray[temp]^d mod n
4. Else index[i] substituted by the Ptxt[j].

IV. ARCHITECTURE OF PROPOSED MODEL

The architecture of proposed model can be divided into three modules

1. Installation Process module

2. Encryption process module

3. Decryption process module

Installation Process module allows the users (Group Admin and Group members) to install the (appropriate) software (That is Group admin App or Group members App), who are interested to share the data through cloud securely. The Group Admin should register the App itself (It contains the Group name and IMEI number of that device, user name and password) Based on the Group Admin registration details the App itself maintains the IMEI number and Group name. So it is not possible to open the in any other devices. The Group members should communicates with the Group admin before installing the software (Share the IMEI Number).

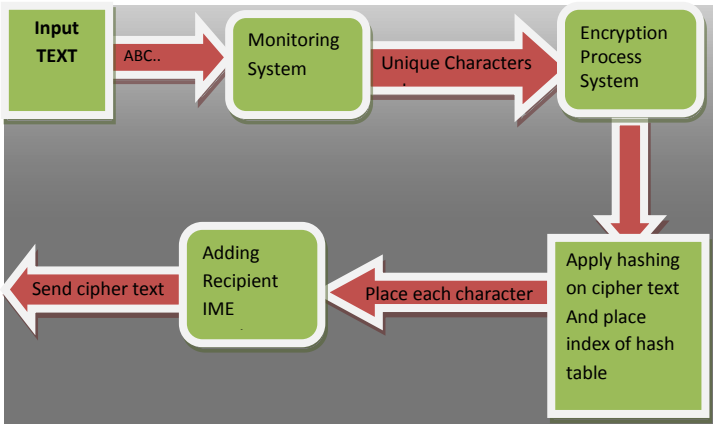

Fig 2: Encryption process.

Its having the following components is

A. Monitoring System.

B. Encryption process

C. Hashing process.

Where the function of **monitoring system** is every character is checked before send to encryption process, if it is unique character then allowed, otherwise looking into the hash table and place the appropriate index of character. The asci[],encrypt[] arrays are maintains the asci values and indexes of the hash table respectively.

The function of the **Encryption process system** is encrypting the given character with given modulo (1024 bits minimum). It is same as Basic RSA.
The function of the **Hashing process** is generates the hash value for each unique encrypted character. We know hashing creates a collision problem that will be overcome using linear probing method.

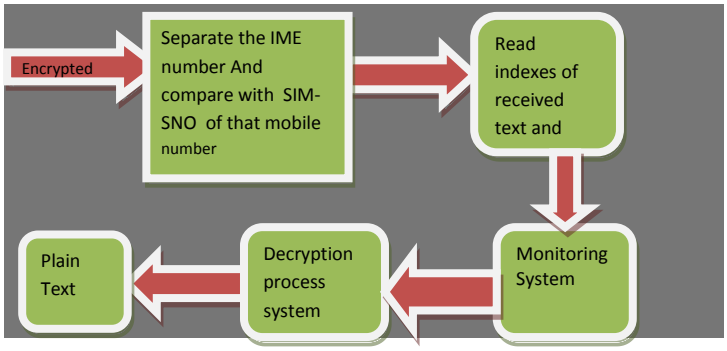

Fig 3 showing Dencryption Process

The above diagram represents the Decryption process. Its having the following modules is
1. Authentication process

2. Hash table process

3. Monitoring System.

4. Decryption process

The function of **Authentication process** is to verify the recipient mobile is valid or not. If it is valid it allows further process otherwise, the message not possible to decrypt. When the file is reach to recipient the Application will active and get the IMEI number using "getIMEINumber()" method and verify it.

The function of Hash table process is to read the each character of cipher text and matching with the Hash table values. If the matching is done then it will be send to Monitoring system. The below diagram represents the Hash table, it maintains encrypted text of the all possible characters of the keyboard. Those indexes are not actual asci values of characters, so it avoids the mobile side attacks. To store the important messages always in encrypted format, when we need to view the messages then decrypt it.

V. RESULTS

We use the Android os for developing secure data/file sharing crypto system for mobiles through cloud, in that we consider the hash table with encrypted values and encryption process and decryption process modules. Fig-1 represents the Group Admin crypto system interface; it allows the Admin to send the file to cloud in encrypted format. User browse the file from local sd card and then click the Encrypt button then it will encrypted using HP-RSA algorithm where the monitoring system plays an important role, it allows only unique characters to encryption process.

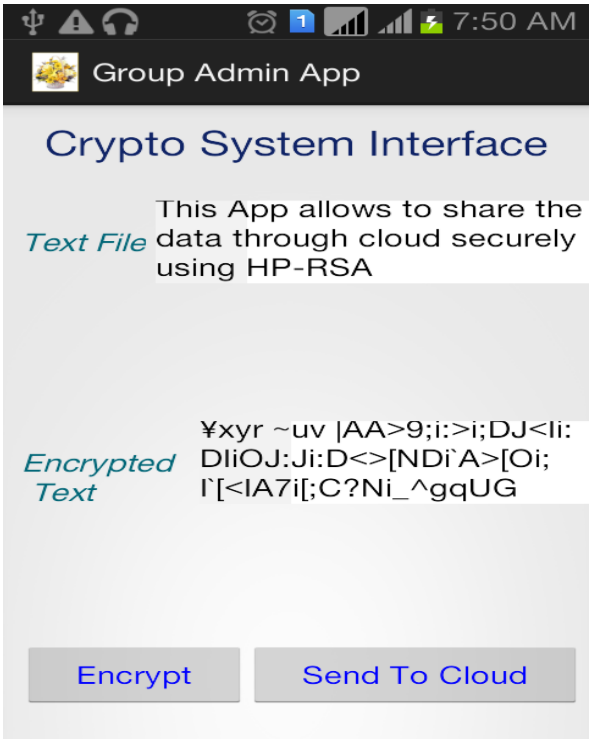

Fig: 4 Android App showing Encrypted data

Fig-4 represents the Group members Application side application, after authentication from group admin application, he/her allows to accessing the data from the cloud. He/her getting the file in encrypted format, when it receives automatically the app invokes and show the file in crypto system interface and then click on the decrypt button the original text will be shown.

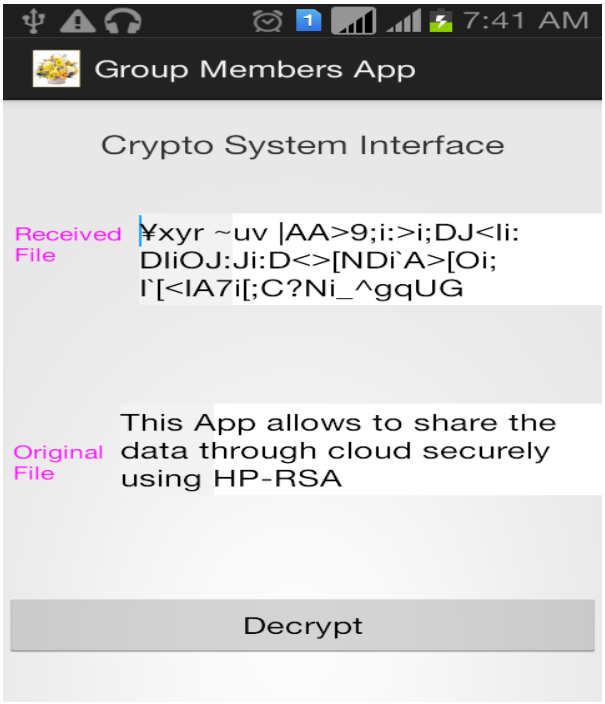

Fig: 5 showing Android App Decrypting the data

VI CONCLUSION

In the current trend mobile applications are used immensely for various purposes especially in area of social networks which generates large amounts of data which can be stored in cloud data centres. As cloud is vulnerable to security and privacy, a secure scheme is proposed to ensure security to data stored at cloud. In this paper we have simulated a mobile application which provides encryption and decryption to mobile data and the results are generated.

VII REFERENCES

[1] Rafat, Ali, The SMS Privacy Problem, Textually.org website,http://www.textually.org/textually/archives/2004/04/003489.htm, last accessed 19 October 2006

[2] Breed, Allen G., Ubiquitous message technology can be powerful tool for good or ill, TMCNet Website, http://www.tmcnet.com/usubmit/2006/10/17/1985881.htm, last accessed 19 October 2006.

3. HealeyM(2010) Why IT needs to push data sharing efforts. InformationWeek. Source: http://www.informationweek.com /services/integration/why-it-needs-to-push-data-sharing-effort/225700544. Accessed on Oct 2012

[4] GSM World, GSM Services, http://www.gsmworld.com/services/index.shtml, last accessed 17 October 2006.

[5] Sri Rangarajan, N. Sai Ram, N. Vamshi Krishna "Securing SMS using Cryptography"

6. Wu R (2012) Secure sharing of electronic medical records in cloud computing. Arizona State University, ProQuest Dissertations and Theses

7. Pandey S,VoorsluysW, Niu S,Khandoker A, BuyyaR(2012) An autonomic cloud environment for hosting ECG data analysis services. Future Gener Comput Syst 28(1):147–154

[8] Anand Surendra Shimpi and R. Chander, "Secure Framework in Data Processing for Mobile Cloud Computing", International Journal of Computer & Communication Technology, ISSN (Print) 0975- 7449, vol. 3, Iss. 3, 2012.

[9] Jibitesh Mishra, Sanjit Kumar Dash and Sweta Dash, "Mobile Cloud Computing: A Secure Framework of Cloud Computing for Mobile Application", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, pp. 347-356.

[10] Itani et al, "Towards secure mobile cloud: A survey", Proceedings of Analyses paper, 2012.

[11] Eugene E. Marinelli, "Hyrax: Cloud Computing on Mobile Devices", Dissertation of Thesis, Carnegie Mellon University, Pittsburgh, 2009.

[12] W. Jia, H. Zhu, Z. Cao, L. Wei, X. Lin, "SDSM: a secure data service mechanism in mobile cloud computing," in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China,Apr. 2011.