International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Enhancing the Mobile Cloud Server security by MAC Address

Kamalpreet Kaur[1], Navpreet Kaur Walia[2]

[1]Department of Computer Science and Engineering, SGGSW University, Fatehgarh Sahib, Punjab, India 140406

[2]Assistant Professor, Department of Computer Science and Engineering,
SGGSW University, Fatehgarh Sahib, Punjab, India 140406

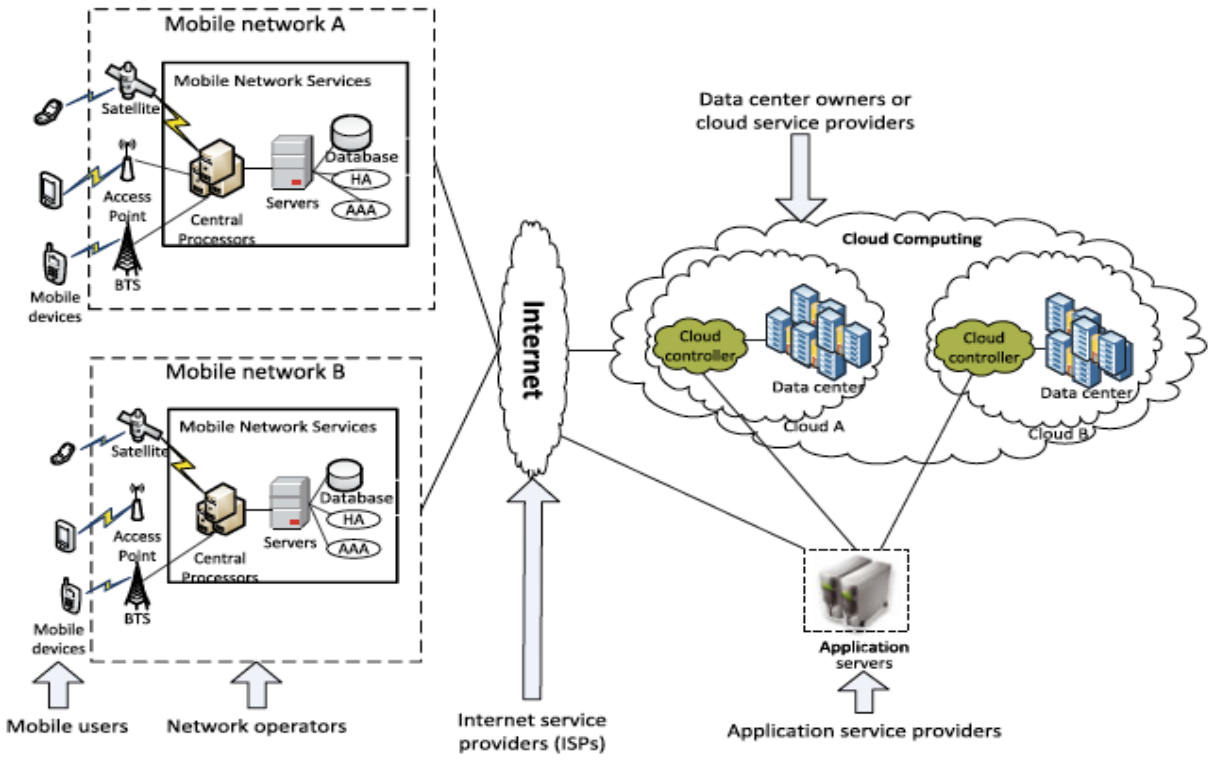
Abstract: ***Mobile Cloud computing is an emerging and vast area for the field of research. In the era of advanced technology the client and server architecture is been shifting from distributed or cluster to cloud architecture. Smart phone devices are booming in market and it covers most of the works of people which was earlier used to done by the help of computer. We can read mails with push notifications facility; we can communicate and store large number of data in mobile devices. As the Internet-enabled mobile devices including smartphones and tablets continue to grow, web-based malicious threats will continue to increase in number to make more complex. Securing data is more critical in the Mobile Cloud Environment. So, one of the key challenges is to design the cloud computing security architecture for mobile device on the internet. In this paper we proposed security architecture for mobile cloud computing***.

Keywords: MCC, AES, SAAS, PAAS, IAAS

1. Introduction

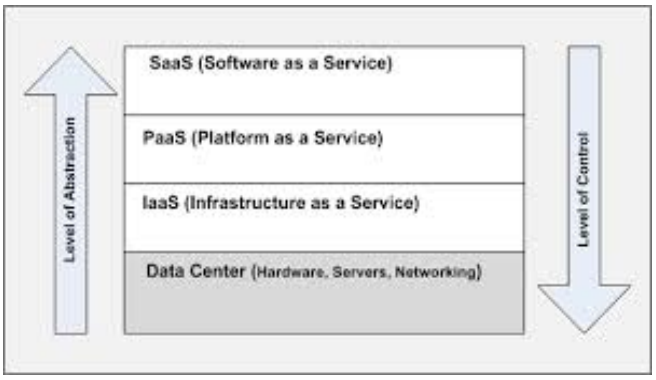
The term mobile cloud computing was introduced not long after the concept of cloud computing launched in mid-2007.Mobile cloud computing is a combination of two technologies i.e. mobile and cloud computing. Mobile cloud computing is defined as the combining the cloud computing services into the mobile ecosystem that brings the wireless network and cloud computing, which provides outstanding services to the users. The Mobile Cloud Computing Forum defines MCC as follows [6]:"Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just Smartphone users but a much broader range of mobile subscribers". In mobile cloud computing main challenge is a security.

1.1 Architecture of Mobile Cloud Computing



Mobile devices are connected to the mobile networks via base stations (base transceiver station (BTS), access point, or satellite) that establish and control the connections and functional interfaces between the networks and mobile devices. Mobile users requests and information (ID and location) are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as AAA (for authentication, authorization, and accounting) based on the home agent (HA) and subscribers data stored in databases. Then subscribers requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services. Generally, a cloud computing is a large scale distributed network system implemented based on a number of data centers. The cloud services are based on a layer concept.

1.2 Layerd Architecture



Data Center Layer: This layer provides the hardware facility and infrastructure for clouds. In data center layer, a number of servers are linked with high-speed networks to provide services for customers. Data centres are built in less populated places, with a high power supply stability and a low risk of disaster.

Infrastructure as a Service (IaaS): It is the delivery of computer infrastructure as a service. IaaS enables provision of storage, hardware, servers and networking components. Infrastructure can b expanded or shrunk dynamically as needed. The client pays on a per-use basis. Thus, clients can save cost as the payment is based on how much resource they really use.

Plateform as a Service (PaaS): PaaS deliver a computing plateform typically including operating system, programming language execution environment, database and web server. Users can develop and run their software solutions on a cloud plateform without the cost and complexity of buying and managing the underlying hardware and software layers. PaaS offers an advanced integrated environment for building, testing and deploying custom applications. The examples of PaaS are Google App Engine, Microsoft Azure, and Amazon Map Reduce/Simple Storage Service.

Software as a Service (SaaS): SaaS supports a software distribution with specific requirements. Users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. Microsoft's Live Mesh also allows sharing files and folders across multiple devices simultaneously.

Rest of the paper is organised as follows. Section 2 presents the related work. Section 3 covers the proposed work. Section 4 gives results of the work and Section 5 concludes the paper.

2. Related Work

Young-Gi Min, Hyo-Jin Shin Young-Hwan Bang [1] defines types of attacks which are current issues of MCC. They have laid stress on system requirement of MCC which openly defines a issue on infrastructure of cloud computing There is always a possibility that the cloud infrastructure is secured with respect to some requirements and the customers are looking for a different set of security. One if the reason why users are very anxious of the safety of their data being saved in the cloud is that they don't know who is managing it while in the server of the cloud computing service provider. Typical users who use the cloud computing service like storing their files on the server to access it anywhere they want through internet, don't bother much about the security of their files, those documents are common files that don't need to be secured. But in the case of big companies which have very important information to take care of, they need to have secured cloud computing.

Swarnpreet Singh, Ritu Bagga [2] discussed the architecture which shifts from cloud to mobile cloud computing. They outlines the architecture of MCC (Mobile cloud computing) with the different services needed by the client and the server in MCC. In this paper, they introduced the concept of Mobile Cloud Computing (MCC), it's inner workings and the various implementable architectures related to the MCC. The concept of cloud computing provides a brand new opportunity for the development of mobile applications since it allows the mobile devices to maintain a very thin layer for user applications and shift the computation and processing overhead to the virtual environment. A cloud application needs a constant connection that might prove to be an Achilles heel for the cloud computing movement. However as mobile internet capabilities continue to get better, it is likely that solutions to this particular problem will become apparent. New programming languages such as HTML 5 already provide a solution by enabling data caching through a mobile device, and this allows cloud application to continue working if connection has been momentarily lost.

Pragya Gupta and, Sudha Gupta [3] presented research which outlines the facts of MCC which deals with maintenance of resources. During mobile cloud client and server security architecture development various other facts are also important which is needed to be considered to make it reliable. In this paper they gave an overview of Mobile

Cloud Computing that includes architecture, benefits, key challenges, present research and open issues.

A. Cecil Donald, S. Arul Oli, L. Arockiam [4] outlines the issues and challenges which adds another phase towards the area of research towards MCC. They represented the gross figure of their research which shows 69% of mobile devices need to be secured while they use MCC services. They also represent the various services offered by mobile cloud computing companies.

Satveer Kaur [5] in 2012 outlines major security issues towards cloud computing architecture.

1) Identification and Authentication: The multi tenancy in cloud computing allows a single instance of the software to be accessed by more than one users. This will cause identification and authentication problem. Because different users use different tokens and protocols, that may cause interpretability problems.
2) Access control: Confidential data can be illegally accessed due to lenient access control. If adequate security mechanisms are not applied then unauthorized access may exist. As data exists for a long time in a cloud, the higher the risk of illegal access.
3) Data Seizure: The Company providing service may violate the law. There is a risk of data seizure by the some foreign government.
4) Encryption/ Decryption: There is an issue of the Encryption/ Decryption key that are provided. The keys should be provided by the customer itself.
5) Policy Integration: Different cloud servers can use different tools to ensure the security of client data. So integration policy is one of the major concerns of security.
6) Audit: In cloud computing the Cloud Service Provider (CSP) controls the data being processed. CSP may use data while being processed. So the process must be audited. The all user activities must be traceable. The amount of data in Cloud Computing may be very large. So it is not possible to audit everything.
7) Availability: Availability is the major concern in the cloud computing. When the client data is virtualized clients have no control on the physical data. If in the cloud, the data or service is not available, it is rigid to fetch the data.
8) Government restrictions: In some countries there are some rules about the data storage, that what kind of data can be stored by its citizens and there is a time limit for which the data can be stored. Sometimes customer stresses their financial information on the cloud.

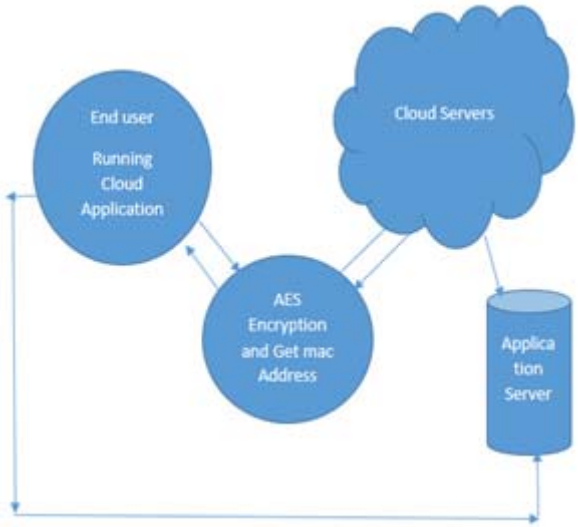
Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang [6] gave a survey of MCC, which helped general readers have an overview of the MCC including the definition, architecture, and applications. The issues, existing solutions and approaches were presented. In addition, the future research directions of MCC were discussed.

3. Proposed Approach

The proposed system exhibits the solid frameworks which consist of two steps:

Step-1 Cloud Based Server-Client Architecture- This cloud based server-client architecture is needed to be developed before moving onto the next levels of Mobile Cloud Computing. The client section is a simple application for user which is made on an android smart phone using Android programming. Application connection is made with Server which is a LAN based server on which data is to be uploaded and downloaded.

Step-2 Security Features- Since backbone network (client and server) is developed, then it needs to be secured with a particular algorithm or technique. We use AES symmetric key oriented algorithm which offers dynamic security on client and server level during communication. The technique for advancing the level of security we used is MAC-ADDRESS cross verification. Since MAC address of every device is unique which helps in identifying the exact device using a cloud application. These features increased the security of an application.



Steps of AES algorithm

- **Encryption:** The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of the data to be encrypted. This array we call the state array.
- **Input:** A set of data(plaintext)
- **Output:** Encrypted data(Ciphertext)
- **Method:** following steps to encrypt a 128-bit block:
  1. Derive the set of round keys from the cipher key.
  2. Initialize the state array with the block data (plaintext).
  3. Add the initial round key to the starting state array.
  4. Perform nine rounds of state manipulation.
  5. Perform the tenth and final round of state manipulation.
  6. Copy the final state array out as the encrypted data (ciphertext).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. Operations in AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data, numbered D_0 to D_{15} are loaded into the array.

Each round of the encryption process requires a series of steps to alter the state array. These steps involve following operations called:

- SubBytes: non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- Add round key: each byte of the state is combined with a block of the round key using bitwise xor.

Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions:

- InvSubBytes
- InvShiftRows
- InvMixColumns

XorRoundKey doesn't need an inverse function because XORing twice takes you back to the original value. InvSubBytes works the same way as SubBytes but uses a different table that returns the original value. InvShiftRows involves rotating left instead of right and InvMixColumns uses a different constant matrix to multiply the columns.

Input: Encrypted data(cipher text)
Output: Original data(Plaintext)

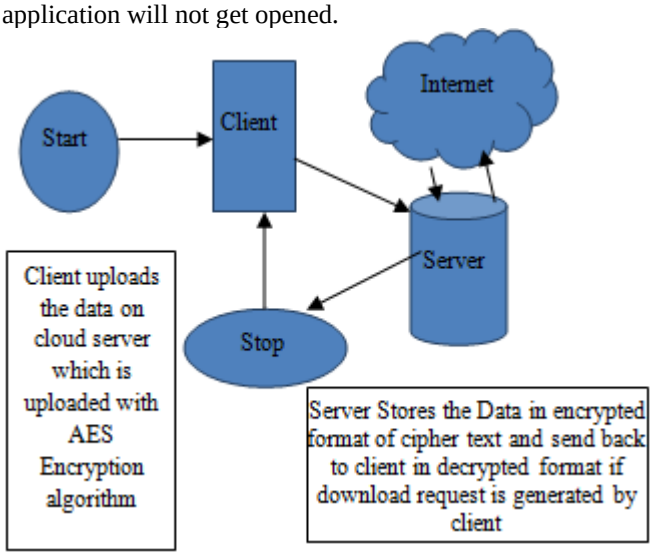
The order of operation in decryption is:

1. Perform initial decryption round:
   XorRoundKey
   InvShiftRows
   InvSubBytes
2. Perform nine full decryption rounds:
   XorRoundKey
   InvMixColumns
   InvShiftRows
   InvSubBytes
3. Perform final XorRoundKey

The same round keys are used in the same order.

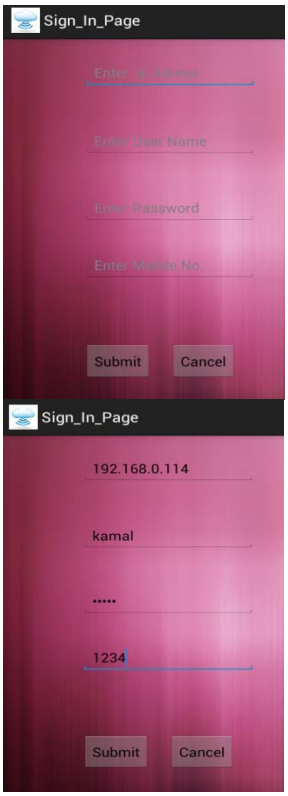
4. Methodology

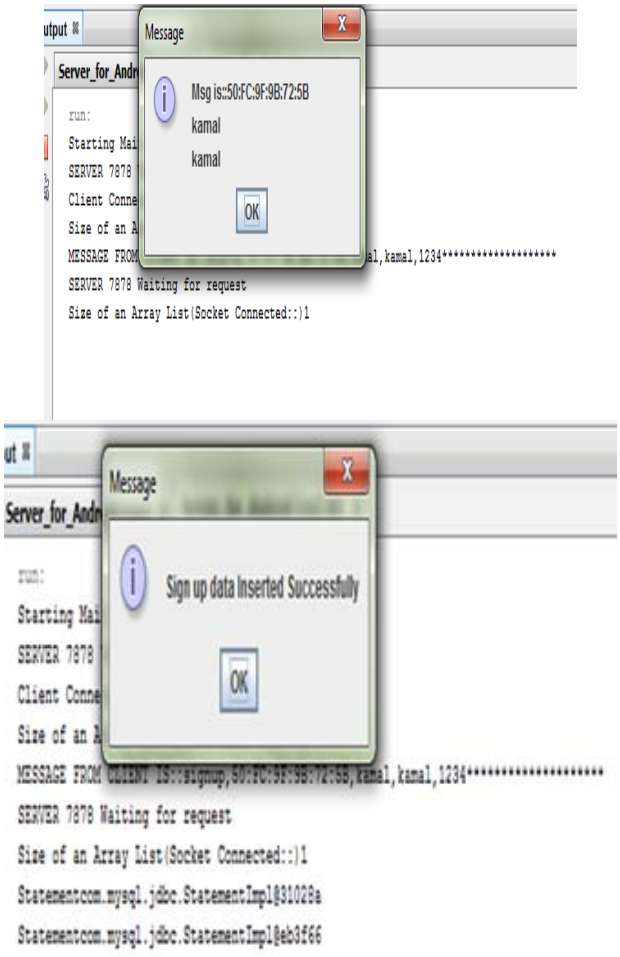
This section explains the flow chart of proposed system which is been developed for Mobile Cloud Computing on Android Operating system as a client. On client end the application is been made from where a user can upload and download the content. The user uploads the confidential documents to cloud based server to retain its data. The data is being uploaded into server and secured through AES. For maximal protection we have added a technique of MAC address verification which benefits the user in terms of authenticity. During sign up the MAC address is fetched and saved into database. Whenever the user Logins the MAC address get verified. If MAC address is matched the user of application is a genuine owner. If it doesn't matches the application will not get opened.



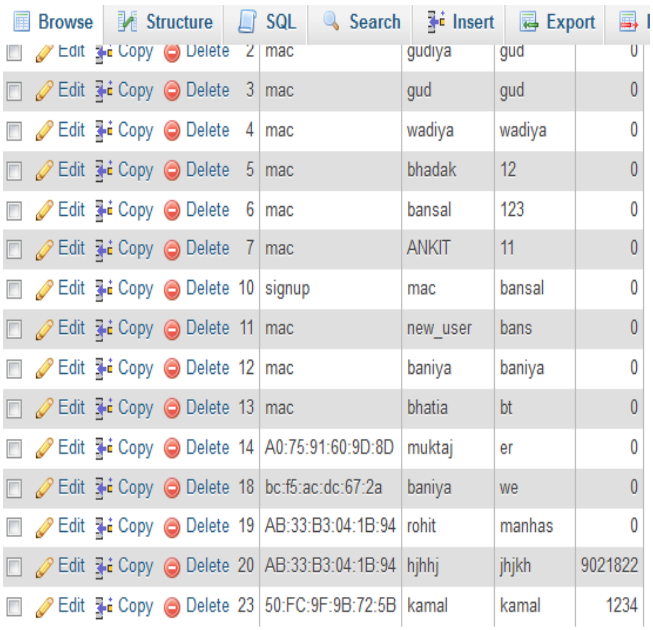
5. Results

When a user signup MAC address of user device are stored on a server. Every time user try to login MAC address will be cross verified and only authorization user will enable to access data. Sign in page



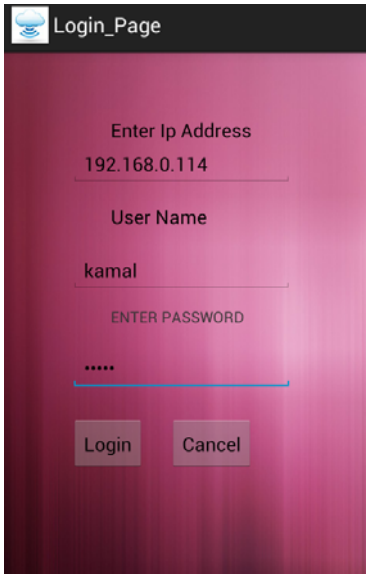


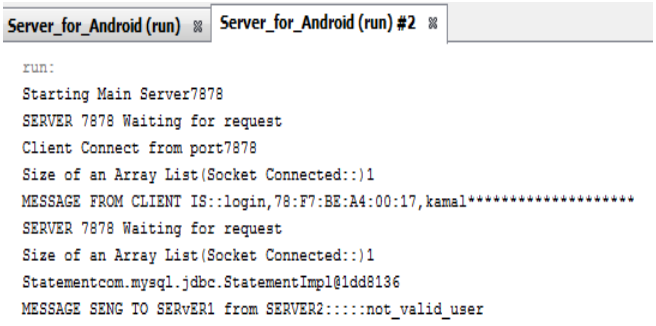
Data store on a server along with mac address



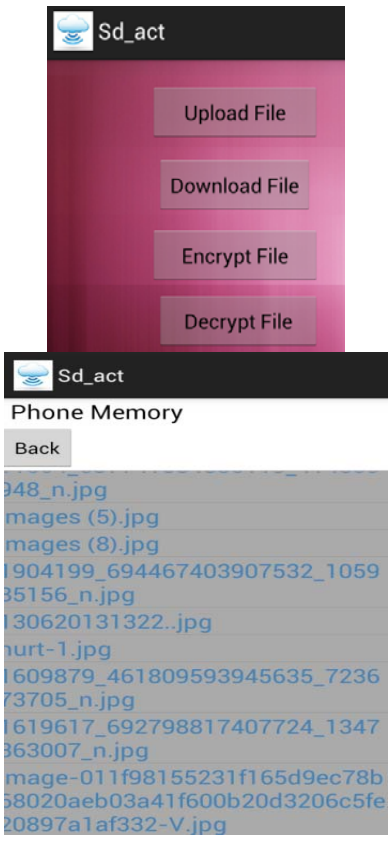
Edit Copy Delete	2	mac	gudiya	gud	0
Edit Copy Delete	3	mac	gud	gud	0
Edit Copy Delete	4	mac	wadiya	wadiya	0
Edit Copy Delete	5	mac	bhadak	12	0
Edit Copy Delete	6	mac	bansal	123	0
Edit Copy Delete	7	mac	ANKIT	11	0
Edit Copy Delete	10	signup	mac	bansal	0
Edit Copy Delete	11	mac	new_user	bans	0
Edit Copy Delete	12	mac	baniya	baniya	0
Edit Copy Delete	13	mac	bhatia	bt	0
Edit Copy Delete	14	A0:75:91:60:9D:8D	muktaj	er	0
Edit Copy Delete	18	bc:f5:ac:dc:67:2a	baniya	we	0
Edit Copy Delete	19	AB:33:B3:04:1B:94	rohit	manhas	0
Edit Copy Delete	20	AB:33:B3:04:1B:94	hjhhj	jhjkh	9021822
Edit Copy Delete	23	50:FC:9F:9B:72:5B	kamal	kamal	1234

If unauthorised user trying to access using authorized username and password on his device, he will not enable to access the data

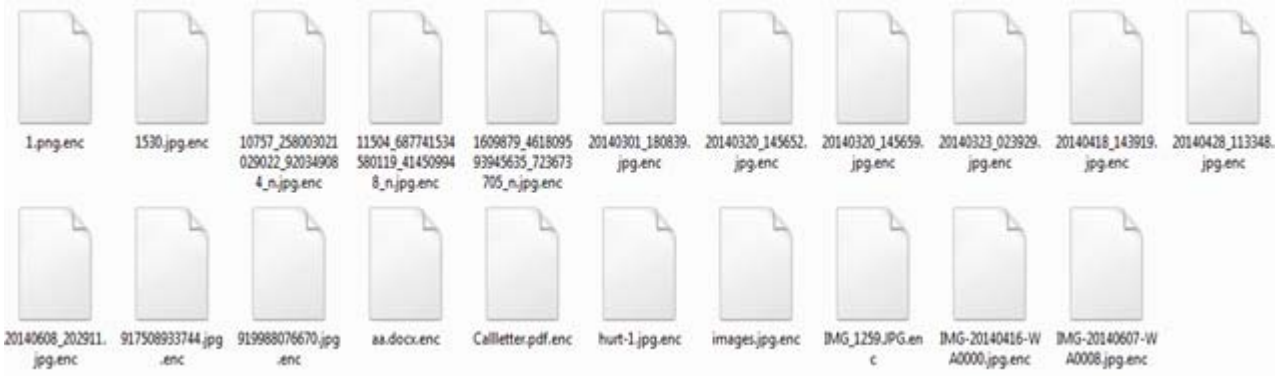




Data will store on cloud in encrypted form



Data store on server



6. Conclusion

In this proposed approach issues on mobile cloud computing and after its successful implementation. It's been concluded that AES was successful and provides a strong point of security to existing mobile cloud architecture. The Purpose of adding Mac-Address verification in client side secured the data from manipulation and preserves authenticity of users. It has build the more trust level on users as if any 3rd user if got credentials of particular user of cloud application, he/she will not be able to open the application in their devices. The man in middle attack is also ruled out since AES provides a strong encryption security along with a public and private key system.

7. Future Scope

Since AES provides a strong security measure to existing system. It will be always a area of research as AES takes lot of power during generation of public and private key. On mobile OS AES performance can be analyzed in terms of battery consumption and throughput. Preserving the power of smart phones can be new area of research in mobile cloud computing since every application back-end phase is shifting from cluster / grid to cloud based system. These applications usually take lot of battery power and can affect the battery life of particular phones. Since smart phones processor and RAM runs 24 hours if it's not on switched off mode the application running in background can eat up RAM and Processor which leads to decrease in battery life of a smart phone.

References

[1] Young-Gi Min,Hyo-Jin Shin, Young-Hwan Bang,"Cloud Computing Security Issues and Access Control Solutions ,"journal of secuirty engineering,PP 135-142,2012
[2] Swarnpreet singh,Rittu Bagga,Devinder Singh,Tarun Jangwal," Architecture of Mobile Application,Security Issues and Service involved in Mobile Cloud Computing Environment" International Journal of Computer and Electronic Research(IJCER) Vol 1,Issue 2,PP 58-67,2012
[3] Pragya Gupta,Sudha Gupta,"Mobile Cloud Computing: The Future of Cloud" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, PP 134-145, 2012
[4] Cecil Donald ,S. Arul Oli, L Arockiam.,"Mobile Cloud Security Issues and Challenges" International Journal of Engineering and Innovative Technology (IJEIT) Vol3, Issue 1,PP 401-406 ,2013
[5] Satveer kaur,Amanpreet singh," The Concept of Cloud Computing and Issues Regarding its Privacy and Security" Interntional Journal of Engineering Research and Technology(IJERT) vol1,Issue 3,PP 1-4,2012
[6] Hoang T. Dinh ,Chonho Lee, Dusit Niyato, Ping Wang," A Survey of Mobile Cloud Computing:Architecture, Applications, and Approaches",Wireless Communications and Mobile Computing-Wlley,Vol 13,Issue 18,PP 1587-1611,2013
[7] Fernando Niroshinie,Loke Seng W., Rahayu Wenny ,"Future Generation Computer System The International Journal of Grid Computing and Escience"Vol 29,Issue 1,PP 84-106,2013
[8] Qi Han, Gani Abdullah,Research on Mobile Cloud Computing:Review,Trends and Prospective
[9] M Sumalatha Patil,M Mala L,"International Journal of Current Engineering and Technology" Design of High Speed 128 bit AES Algorithm for Data Encryption pp 339-343,2013
[10] Sumitra,"International Journal of Scientific and Research problem" Comparitive Analysis of AES and DES security algorithms,vol 3.Issue 1,2013
[11] KumarAman,Dr Jakhar Sudesh,Mr. Makkar Sunil ," International Journal of Advanced Research in Computer Science and Software Engineering" Comparitive Analysis between DES and RSA algorithm,Vol 2,Issue 7,PP 386-391,2012
[12] http://www.mobilecloudcomputingforum.com/
[13] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Author Profile

Kamalpreet Kaur is currently pursuing Master of Technology from Sri Guru Granth Sahib World University Fatehgarh Sahib. She has the received bachelor of technology degree in Information Technology from Baba Banda Singh Bahadur Engineering college Fatehgarh Sahib in the year 2008.She is currently writing thesis on "Mobile Cloud Computing".

Navpreet Kaur Walia is currently working as Assistant Professor at Sri Guru Granth Sahib World University Fatehgarh sahib. She obtained her master of technology and bachelor of technology degrees in CSE.