Secure Data Transfer & File Sharing Use of Cloud Service for Mobile Application

[1]Swati Sharma, [2]Ravindra Sharma

[1,2] Department of Information Technology,SVITS College Indore (MP), India

***Abstract*—Smart phones are basic needs of our daily life. It's like a small computer which gives you many facilities such as web browsing, downloading and many more but small data storage space and backup are major problem. On the other hand cloud computing provides efficient computational resources and secure data hosting services. But the data transmission among two secure networks is performed over unsecured network. So need a design to secure data transfer.**

Keywords—smartphone, Cloud computing, Security;

I. INTRODUCTION

Cloud computing is the distributed model for provide convenient, on demand network access to a distributed environment of computing resources like services, applications, storages and servers and so on. We can securely store and retrieve the data as we like using cloud computing. But when we transmit the data over a public area network is not much secure, there are various attacks like Byzantine server failures, malicious data modification attack. So we propose an effective and flexible distributed scheme with two algorithms AES and MD5. Use of this algorithm we transmit a data securely in public area network.

A. Mobile cloud computing

Mobile cloud computing is the combine of cloud computing features and mobile web, which is the most popular tool for mobile users to access services and applications on the Internet. It provides users storage services and data processing in clouds. Mobile cloud applications move the data storage and computing power away from mobile phones and into the cloud. . The cloud computing features provided in the mobile phone, which allows users an online access to unlimited computing power and storage space.

Many applications based on Mobile Cloud Computing, such as Google's gmail, Voice Search, Maps and Navigation systems for mobile, , and some applications on an Android platform, LiveMesh from Microsoft, MobileMe from Apple and Motoblur from Motorola, have been developed and served to users[2].

The combination of cloud computing, mobile Web, portable computing devices, wireless communication infrastructure, location-based services etc., has base the foundation for a computing model, called mobile cloud computing.

B. Android Based Application

Android platform is a smart mobile phone platform released by Google. Android is open and free, providing an easy-to-use development kit and runs on the Linux Kernel. Android provides the support of location service and mobile map, which is probably a concern of large numbers of developers. Android depend on Linux for core system services such as security, process management, network stack, memory management, and driver model.

Android consists of the user interface, operating system, and middleware, application software [130]. The Android SDK provides tools and APIs to develop applications using Java language codes on the Android platform. Android supports GPS, compass, Video Camera, and 3d-accelerometer. It enables replacement and reuse of components and an efficient database.

Users can easily access, control and process the free Google map.

II. RELATED WORK

Now a day's mobile devices have replaced by computers and laptop. Mobile phone were used not only for communication but also used for email, chatting, music, playing the games. In mobile phone limited storages space are available so when new file added firstly remove odd files. If we need extra space use of memory card but it is not secure way to store data on memory card. So one of the solution is to store data on cloud. Cloud computing providing anywhere and anytime access to the unlimited access to store data [3].

According to Muhammad Shiraz et al, this paper discusses the cloud computing, mobile cloud computing and explains the different techniques to mobile phone based on resources available within the cloud. The objective is to highlight issues in developing, and implementing mobile applications within MCC domain.

One more solution provided by P.Srinivas et al. [5] is to maintain the data securely on clouds through token generation algorithm for secure cloud storage service. In this scheme data stores in cloud encrypted block data from and perform token checking algorithm on this encrypted blocks and verify the data in case of modifications of files before storing to cloud. This approach provided two way verification of file blocks which result ensure that data will not be modified.

Mainly security is used term surround the characteristics of integrity, authentication, privacy, and Availability. Now a days we depend on the send information over the network; risk of secure transmission over the networks has also increased. For the secure transmission that term are important for data transmission [4].

III. SECURITY REQUIRMENTS

Security requirements are very important in mobile devices and cloud services to protect the information from attacks. Normally, several security services such as availability, authorization, confidentiality, Integrity and Non-repudiation must be applied. The following requirements:

Availability, which ensuring that network services are available even in the presence of attacks. Denial of service is the most danger to network availability. Attackers are able to activate attacks which reduce the performance.

Authorization, which ensures that only authorized user can be access in providing information to network services. If authentication is not there, then without any difficulty attackers are easily manipulated data into the network.

Confidentiality is a fundamental security service. Confidentiality which ensures that to keep privacy of data transmitted among network

Integrity ,which ensures that a message cannot be changed or modified by attackers

Non-repudiation, which denotes that a node cannot refuse to admit sending a message it has previously sent [7].

IV. PROBLEM IDENTIFICATION

In cloud storage system and mobile devices only backup the data and that data retrieve it from cloud but simultaneously cannot access the data in mobile and computer. In Android, there is no proper facility to save data and retrieve data in cloud. Memory card have no proper security like user lose the mobile or physical damage.

2. The security of the cloud is essentially strong and the private internet access area is also secured. But the data transmission among two secure networks is performed over untrusted network.

3. Cloud are use to store data but in cloud data is stored at random in the cloud space so our private and sensitive data can be mismanaged and produces the redundancy during their management.

V. PERPOSED CONCEPT

Cloud storage solve the issue of small storage of mobile device i.e. user can store data on cloud. Our main goal is provide security during data transmission in public area network. Security on cloud during data transmission through the public area network is not secure, so we used two securities Advanced Encryption Standard (AES) algorithm and message digest 5 algorithms when data are transmit.

Thus the following computational and properties are require to fulfill in proposed solution using figure 1.

1. User firstly initiated connectivity request from cloud server, then authentication server initiated by cloud storage. Server asks a password which is one of the information which is submitted during the registration process in random manner. If users enter valid user id and password then authentication server give permission to access the cloud storage.

2. Therefore when a user making a service request to the cloud storage the user, mobile pre-estimate the file size and file type. In response of that authentication server are encrypted data uses of Advanced Encryption Standard (AES) algorithm and message digest 5 algorithms.

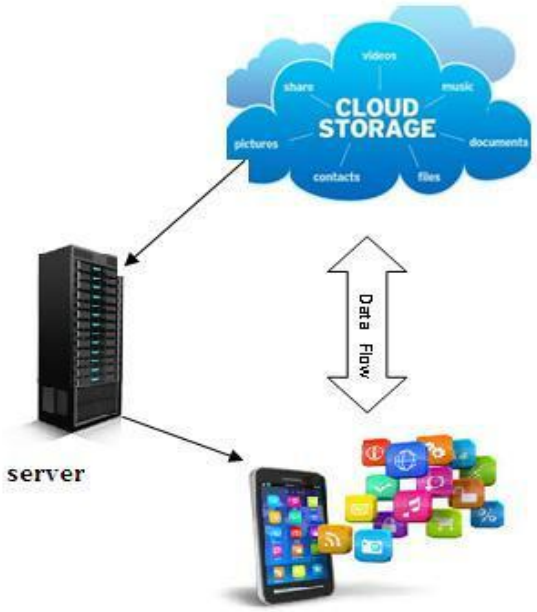


Figure 1 proposed system

Our main aim is provided security during data transmission when data transmit two secure devices so proposed concept is use of two cartographic algorithms AES and MD5 when data

are transmit. In order to achieve the desired goal the above given solution is proposed and simulated using figure 1.

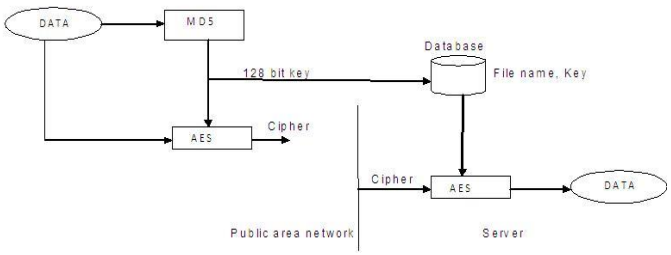


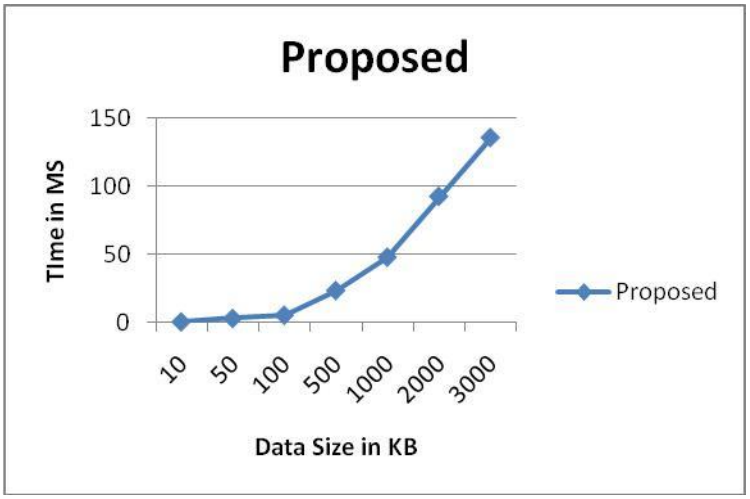
Figure 2 Upload File

1. Firstly data are goes to MD5 and AES algorithms; MD5 algorithm generates 128 bit keys.
2. That keys are going to AES algorithm and database
3. AES generate a cipher text use of MD5 key.
4. Now data are upload in cloud database, in this database contains file name and key
5. In server side AES use of cipher text and MD5 key, that key contain in database and decrypt the data.
6. Same processes are repeated in reverse order when we download the data.

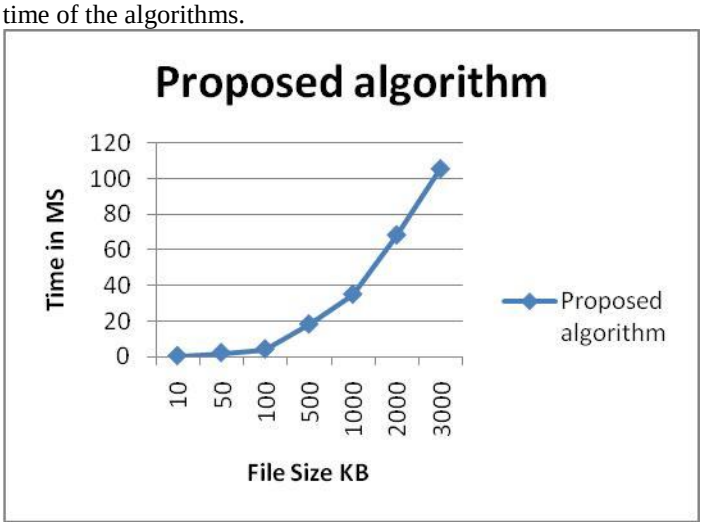
VI. RESULT

The experimental evaluation and the system performance are computed and parameters are obtained and listed with their obtained observations.

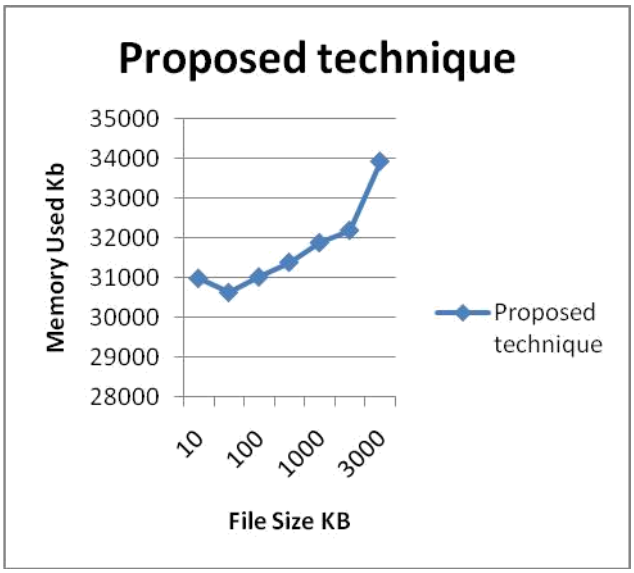
Encryption time- The amount of time required to perform encryption using the selected algorithm is termed as the encryption of the cryptosystem.



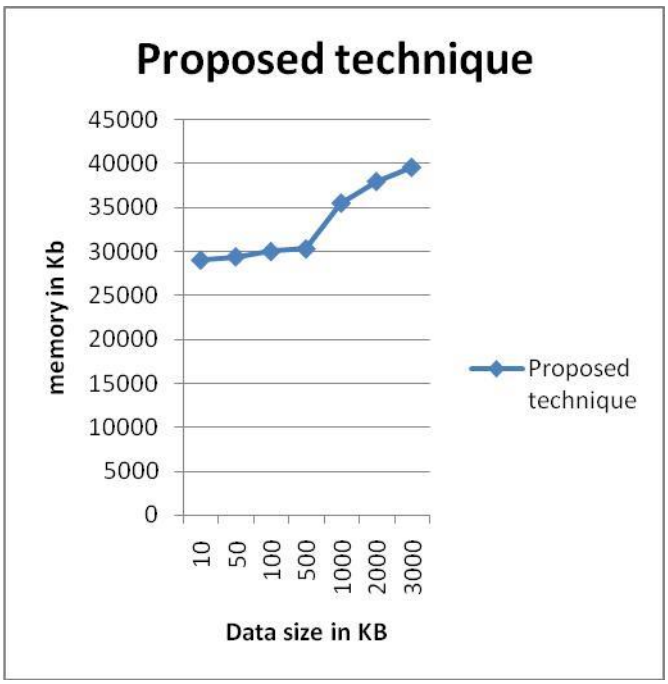
Decryption time-The amount of time required to recover the original data from the cipher text is known as the decryption time of the algorithms.



Encryption memory- The amount of main memory required to execute the algorithm with the input amount of data is known as the encryption memory.



Decryption memory The amount of main memory required to recover the original file from the cipher text is known as the decryption memory consumption



VII. CONCLUSION

In this paper we study about smartphone, mobile cloud computing, Android technology. We proposed a scheme of secure data and file sharing for public area network use of two algorithms Advanced Encryption Standard (AES) algorithm and message digest 5 algorithms when data are transmit. This security system is implementation on android mobile device. Use of this design we securely transfer the data and easily store and retrieve data on both cloud and mobile device.

VIII. REFERENCES

[1]Pragya Gupta et al., "Mobile Cloud Computing: The Future of Cloud"
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 1, Issue 3, September 2012

[2] Suhas Holla et al., "ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY" International Journal of Computer Trends and Technology- volume3Issue3- 2012

[3] V.Malligai et al.," Cloud Based Mobile Data Storage Application System" ternational Journal of Advanced Research in Computer Science & Technology (IJARCST 2014).

[4] Muhammad Shiraz et al.," A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing" IEEE communications survey & tutorials, vol 15 no 3, third quarter 2013.

[5] P.Srinivas et al.,"Secure Data transfer in Cloud Storage Systems using Dynamic Tokens" International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 2, Issue 1, January ,2013.

[6] Al-Sakib Khan Pathan et al., "Security in Wireless Sensor Networks: Issues and Challenges" ISBN 89-5519-129-4, Feb. 20-22, 2006 ICACT2006

[7] Yong Wang et al., "A Survey of Security Issues In Wireless Sensor Networks" IEEE Communications Surveys & Tutorials • 2nd Quarter 2006