Secure Data Storage in Mobile Cloud Computing Using RSA

Patil Rahul V. [1], Shinde Pratik M. [2], Sonawane Shriraj M. [3], Somwanshi Akash B.[4]

Prof. C. D. Bawankar.
Department of Information Technology,
SRES COE, Maharashtra, India

ABSTRACT

Generally cloud computing is area where users only use what they required and only pay for what they really use and save the space, money and time too . Mobile Cloud Computing (MCC) refers to an infrastructure where storage & data processing can happen far away from mobile device. A research says that mobile users across the worldwide will reach 7.3 billion by the end of 2014 and more than 8 billion at the end of 2016. Survey by Ericsson also says that mobile users will reach More than 9 billion in 2017. Because of increasing use of mobile phones and various mobile devices the requirement of cloud computing in mobile devices increasing, that give birth to the Mobile Cloud Computing. Mobile devices don't need to have more storage capacity and powerful Computing and processing speed. But because of storing data on cloud there is a problem of data security. The risk concerned with data storage most Information Technology professionals aren't showing their interest in Mobile Cloud Computing (MCC).For ensuring the correctness of user's data on the cloud, we have propose an effective mechanism with some feature of data integrity and data confidentiality. Our mechanism which uses the concept of RSA algorithm and Hash function along with some cryptography tools to provide better security to the data stored on the mobile cloud.

Keyword:- *Cloud; confidentiality; data security; data storage; integrity; mobile cloud computing; mobile user.*

1. INTRODUCTION

Cloud computing promises reliable services delivered through next-generation data centers that are built on compute and storage virtualization technologies. Users will be able to access applications and data from a Cloud anywhere in the world on demand. In other words, the Cloud appears to be a single point of access for all the computing, networking, and storage needs of users. The users are assured that the Cloud infrastructure is robust and will always be available at any time. With the rapid emergence of software systems and their applicability, the volume of users are growing exponentially.

Now a days, the use of mobile phones is increasing day to day. Every person has a mobile phone which provides all facility to move anywhere and access the data at any time. The increasing use of mobile devices has given birth to area called as Mobile Cloud Computing (MCC).MCC provides all type of the services like to users of mobile for fully utilize the advantages of Cloud Computing. The sensitive and secure data is stored as well as processed outside the mobile devices by clouds. The main problem in using mobile cloud computing is of security of data of mobile user stored on mobile cloud (MC). The data or file of a user is very important and may be sensitive too, any unauthorized or illegal person can do changes in it, for harm the data. According to survey 77% of Information Technology Executives and Chief Information Officers are not interested to adopt cloud services due to the risks with security and privacy. So, new architectures are necessary to solve the security problems of the mobile users for using mobile cloud techniques. A number of solutions have been provided but there is lack of any framework presented till now which is up to the remarkable position.

So the aim of cloud service provider is to provide the security of Data or files generated and used on a mobile device or cloud server. The data or files security is very essential for owner for the data or file as it can contain any confidential information of user. For user the integrity of the data is very important. If any unauthorized or illegal person performs changes in data of user's person then it can harm the integrity of the data. Generally any person after finding confidential information of any other person can be harm that person data or file. So, the data confidentiality is also a concern of data owner. To protect data or file of user, encryption is used to secure data in the cloud.

2. LITERATURE SURVEY

Preeti Garg, Dr. Vineet Sharma [1] This research paper has proposed a mechanism to provide confidentiality and integrity to the data stored in mobile cloud. The proposed scheme uses RSA algorithm with other encryption decryption processes to secure the data in such a way that no leakage of data on cloud could be performed. In this scheme encryption is used to provide security to the data while in transmit. Because the encrypted file is stored on the cloud, so user can believe that his data is secure. In the scheme file, only in encrypted form is transferred over the channel, which reduces the problem of information disclosure. No, third person or intruder can get the file because that person do not knows the key of data owner.

Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, Athanasios V. Vasilakos [2] This paper focus on the features that user's aspect from cloud computing such as reliability, customization, quality of service and availability. Instead of taking care of computation security alongside storage security previous analysis was focusing on data storage security. By using techniques such as designated verifier signature, batch verification and probabilistic sampling; a privacy cheating discouragement is designed, which is the bridging protocol that combines together secure storage and secure computation in cloud. A test bed to implement SecCloud, a practical secure aware cloud computing testing environment is built.

Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos [3] This paper focus on challenges and opportunities regarding the security in cloud computing. Cloud has potential to carry valuable resources over the internet, hardware enhancement system, reducing the hardware cost. This paper also focuses on security threats that arise due to vary nature of cloud computing. Also it presents the current solutions presented to find out the security threats and it gives brief view of security vulnerabilities in the mobile cloud computing.

Sujithra M, Padmavathi G, Sathya Narayanan [4] This paper proposed of different cryptographic techniques to store mobile data securely in the remote cloud with minimal performance degradation.

M Sulochana, Ojaswani Dubey [5] The main problem of cloud computing is that outsourcing of sensitive and business related data and processes, so this paper gives information regarding how to provide integrity and confidentiality to the user data using multi-cloud architecture so that no cloud provider will gain the complete knowledge of the user data.

M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya [6] A public-key cryptosystem i.e. RSA algorithm is used for both confidentiality and authentication. In this paper, an enhanced technique based on RSA public-key cryptosystem is developed. The proposed algorithm makes use of four prime numbers which increases the time and space complexity of the system as compared to traditional RSA algorithm which is based on only two large prime numbers. A comparison is done between the traditional RSA schemes, a recent RSA modified scheme and our scheme to show that the proposed technique is efficient.

3. PROPOSED SYSTEM

A. Problem Statement:

Development of a system that helps the user and he/she is able to Encrypt the data of the end user before storing that data on cloud as well as decrypt data after accessing those data form loud With help of this application user will enable to store their data with full security on the mobile cloud. Because of this application the one of the major issue of security on MCC will get sort out, which helps to increase use of mobile cloud computing for storing very confidential and important data.

B. Proposed System Architecture:

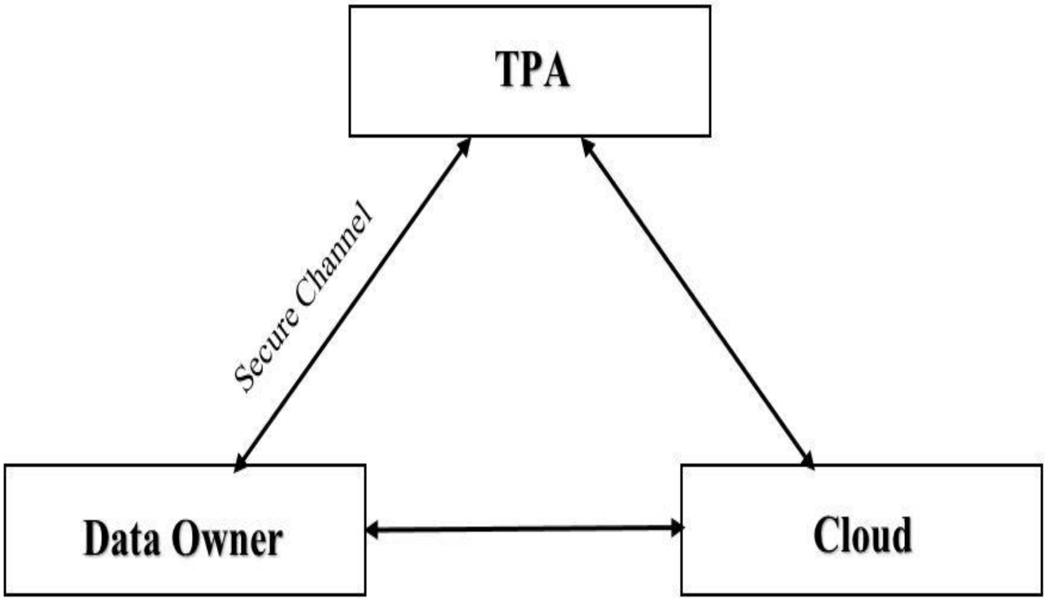

Figure 1: System Architecture

C. Participants:

In the proposed scheme to provide secure data storage three participants are involved. These participants are Data Owner (DO), Third Party Auditor (TPA) and Cloud Service Provider (CSP).

1. Data Owner (DO):

Data owner is a person who utilizes the storage services provided by the cloud service provider.

2. Third Party Auditor (TPA):

TPA checks the integrity of the data stored on mobile cloud.

3. Cloud Service Provider (CSP):

CSP provides the storage services to the mobile users.

4. PROPOSED MECHANISM:

Here a mechanism is proposed to provide secure data storage in Mobile Cloud Computing. This proposal uses the concept of Hash function along with several cryptographic tools to provide better security to the data stored on the mobile cloud. Here we also have a Trusted Third Party Auditor (TPA) who is very well trusted. TPA checks the integrity of the data stored on mobile cloud on behalf of the data owner. TPA checks the hash and message to verify the integrity of the data. In this scheme data owner has two keys, one of which is only known to him called private key and another is public key. Here message/_le is encrypted twice firstly, by owner's private key and secondly by public key of TPA. So this provides the confidentiality to the data of mobile user. In proposed method RSA algorithm is used for performing encryption and decryption which provides message authentication. Here the hash function of the message is also calculated to provide security to the data.

1. Key Generation:

Data Owner uses RSA algorithm for generation of public key and private key for himself. TPA also uses RSA algorithm for key generation. The private key of TPA is pk1 and of Data Owner is pk2, while public key of TPA is dl and public key of data owner is d2.

2. Key Sharing:

Key set of TPA: {pk1, dl}
Key set of DO: {pk2, d2}

3. Encryption:

Firstly, At first, data owner encrypt the message/ file (F) using his public key (d2) E(F,d2) and then generate the hash of encrypted message H(E(F,d2)). Then, the encrypted file is re-encrypted with public key (dl) of TPA E(E(F,d2),dl). After that the hash is re-encrypted with public key of TPA (dl) E(H(E(F,d2)),dl). Now, these two packages are appended and the result E(E(F,d2),dl) II E(H(E(F,d2)),dl) is sent to TPA. The encrypted Hash function of the message is stored by TPA to ensure the data integrity. TPA decrypts the package E(E(F,d2),dl) received, by its private key. TPA generates a random key for performing encryption on the message E(F,d2) generated after encryption. TPA uses DES (Data Encryption Standard) for performing encryption to provide better security. This generated random key is stored by TPA for performing decryption in future. The result is send to the cloud for storage.

4. Decryption:

When required to verify the data correctness, the encrypted package {Encrypt(E(F ,d2))} after DES operation stored on cloud is send to TPA. TPA firstly decrypts the message by random key stored by him. Then TPA generates the Hash of the encrypted file. Now, TPA decrypts the hash value stored by it, this decrypted hash value is compared with the one generated by it. Then according to the result obtained TPA sends file to owner indicating the correctness or not and the requested file. Here the file transferred to owner is encrypted by his public key so that only owner can decrypt it. Owner after receiving encrypted file, decrypt it by private key of himself.

Computational Overhead:

<table>
<tr><th colspan="4">ENCRYPTION PROCESS</th></tr>
<tr><td></td><td>Exponential Operations</td><td>Hash Function</td><td>Pairing Operation</td></tr>
<tr><td>USER</td><td>3</td><td>1</td><td>1</td></tr>
<tr><td>TPA</td><td>1</td><td>0</td><td>1</td></tr>
</table>

<table>
<tr><th colspan="4">DECRYPTION PROCESS</th></tr>
<tr><td></td><td>Exponential Operations</td><td>Hash Function</td><td>Pairing Operation</td></tr>
<tr><td>USER</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td>TPA</td><td>2</td><td>1</td><td>0</td></tr>
</table>

Figure 2: Computational Overhead

Storage Requirement:

PARTICIPANT	STORAGE REQUIREMENT
Mobile Device	Stores Public key of TPA and Public and Private key of owner
TPA	Stores Public key and private key of itself and Hash of the file received from mobile user
CSP	Stores encrypted file of mobile user

Figure 3: Storage Requirement

5. EXPERIMENTAL RESULT

An application has been designed and developed in android platform where client have an android application from which the client can upload the Text, Image, etc. on the cloud in encrypted format and retrieve the same and decrypt it using his Private Key for original file. Therefore the required result has been achieved.

6. CONCLUSION

In this Paper, it is concluded that with the technological advancement and progress in the field of Android OS and Cloud, we present a system that integrates Smartphones and Cloud Computing for secure data storage of mobile user on mobile cloud. Starting by describing challenges that user applications are facing when using traditional applications for computing. The system addresses the issues related to security and confidentiality and integrity of data. We explained this with the help of proposed Secure Data Storage in Mobile Cloud Computing Using RSA application.

REFERENCES

1. Preeti Garg, Dr. Vineet Sharma "An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function" International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), (IEEE-2014) pp.334-339.

2. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, Athanasios V. Vasilakos "Security and privacy for storage and computation in cloud computing" (ELSEVIER 2014),Information Sciences 258 (2014) pp.371-386.

3. Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos "Security in cloud computing: Opportunities and challenges" (ELSEVIER 2014), Information Sciences 305 (2015) pp.357-383.

4. Sujithra M, Padmavathi G, Sathya Narayanan "Mobile Device Data Security: A Cryptographic Approach by outsourcing Mobile data to cloud" Procedia Computer Science 47 (2015) pp.480-485.

5. M Sulochana, Ojaswani Dubey "Preserving Data Confidentiality using Multi-Cloud Architecture "Procedia Computer Science 50 (2015) pp.357-362.

6. M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)" journal of information security and applications 20 (2015) pp.3-10.

7. Miss. Shakeeba S. Khan, Miss. Sakshi S. Deshmukh "Security in Cloud Computing Using Cryptographic Algorithms" IJCSMC, Vol.3, Issue.9, September 2014, pp.517-525.

BIOGRAPHIES

	Patil Rahul V. is pursuing B.E. Information Technology in SRES COE, Kopargaon. His area of research interest include Cloud computing.
	Shinde Pratik M. is pursuing B.E. Information Technology in SRES COE, Kopargaon. His area of research interest include Cloud computing.
	Sonawane Shriraj M. is pursuing B.E. Information Technology in SRES COE, Kopargaon. His area of research interest include Cloud computing.

	Somwanshi Akash B. is pursuing B.E. Information Technology in SRES COE, Kopargaon. His area of research interest include Cloud computing.