ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

A Data Security Framework for Mobile Cloud Computing

Chandni Patel[1], SameerSingh Chauhan[2], Bhavesh Patel[3]

Student, Information Technology, SVIT, Vasad, India [1]

Assistant Professor, Institute of Engineering and Technology, India [2]

Assistant Professor, Information Technology, SVIT, Vasad, India [3]

Abstract: When using the secure cloud storage services on resources limited Mobile Devices, the confidentiality of sensitive data must be ensured before uploading the data on cloud storage servers. The complex security operations to ensure security are restricted to execute due to the resource constrained mobile devices. The huge volume of complex security operations are offloaded remotely on cloud storage. By literature review of existing security frameworks focus on reducing the complexity of cryptographic algorithms or methods to offer confidentiality and security. By keep in view the requirements of security and privacy of confidential data of users with resource restricted mobile devices, in this paper, We present a proposed security framework for mobile cloud computing. In this framework the cryptographic methods as well as algorithms are used for encryption and decryption of mobile user data. This Framework ensures the additional security and confidentiality of user's sensitive or significant data. This paper introduces the scheming flow of proposed security framework. This proposed Security framework is for the purpose to secure and provide privacy and integrity to user's confidential data in Mobile Cloud Environment.

Keywords: Mobile Cloud Computing; Cloud Computing; security; confidentiality; cryptography.

I. INTRODUCTION

Mobile Cloud Computing (MCC) is the combination of Two Computing Technologies: 1) Mobile Computing and 2) Cloud computing. MCC is defined as Cloud Computing Extended by Mobility and a new Ad-Hoc Infrastructure based on Mobile Devices. Mobile cloud computing inherits the Advantages and services of Cloud Computing ''Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services"[2]. Mobile Cloud Computing is defines as it provide Infrastructure where both computationally intensive and secure data storage of mobile devices are offloaded or migrate to cloud servers. "A service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access"[4].

The goal of cloud computing are to enhance the computational capacity of the cloud system and to increase the access levels to the services and resources of the cloud at relatively low cost. The mobile users may utilize the computational power and storage capability of cloud for executing the computationally exhaustive and storage demanding processes of an application. The main objectives of the mobile cloud computing are to reduce the energy consumption when perform the computationally intensive tasks and to increase the mobile devices processing power and storage capabilities. The wireless technologies like Wi-Fi, Wi-Max, 3G, 4G, or Satellite Internet connectivity, can be used for interactions between mobile users and cloud services provider.

The security threats or issues of cloud computing are also inherited in mobile cloud computing with the additional limitations of resource constrained mobile devices.

The MCC is facing various challenges that have restricted the expected growth of MCC's subscribers. These challenges are (a) data replication, (b) consistency, (c) limited scalability, (d) unreliability, (e) unreliable Availability of cloud resources, (f) portability (due to lack in cloud provider standard), and (g) trust, security, and privacy[9].

The rest of the paper is prepared as follows. Section 2 presents the review of existing data security schemes for MCC. In Section 3 the proposed data security framework for MCC Environment. Conclusion of my work and research directions for future work is in Section 4.

II. REVIEW OF EXISTING DATA SECURITY SCHEMES FOR MCC

This paper introduced in literature review, the data security schemes that focus on the reduction of the computational complexity of cryptographic algorithms and methods. There are not any Trusted Third Party(TTP) concerned in these selected data security schemes. In these schemes the cloud servers are assumed fully distrusted for secure storage of user data. The existing data security schemes are (a) encryption based scheme (EnS), (b) coding based scheme (CoS), (c) sharing based scheme (ShS), and (d) Block Based sharing scheme (BSS) [1,7]. In each scheme, encryption, decryption, and integrity verification operations are perform on Mobile Devices. The Cloud Service Providers (CSP) and Data Centre owners are responsible for secure data storage management and handling of requests - response of user's file or data.

DOI 10.17148/IJARCCE.2015.4256

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

TABLE-I
COMPARISIONS OF CRYPTOGRAPHIC DATA SECURITY SCHEMES[1,5,7]

Security Schemes	Supporting Operations	Assumptions	Limitations	Conclusion
EnS	Standard Symetric Cryptographis Algorithm	N/A	Processing Overhead	• Consume more energy on mobile devices. • Provide additional security
CoS	Matrix Mulptiplications of blocks with coding vector	Construction of Coding Vector	Extra file management overhead on mobile devices.	• Use less resources as compared to EnS. • Computationally Intensive
ShS	X-OR operations	Generation and uploading of random Shares.	Supporting operations are computationally intensive	• Time consuming • Considerable amount of data processing and data storage.
BSS	Block Based Chaining modes of operations	File is logically divided in to Chunks	Depended Block executions. Simple XOR oprations are used as cryptographic functions.	• Energy-Effiecient • Consume less resources • Provide high speed execution

We have selected these schemes because of the following reasons:
• Goals of these data security schemes are on the reduction of the computational complexity of the cryptographic methods and algorithms for providing security, confidentiality and integrity services.
• Entire security operations are executed on the mobile device which helps to provide confidentiality of user's private data and improve the security of private data.

The comparisons of the existing security schemes with some limitations are presented in the TABLE-I.

III.PROPOSED DATA SECURITY FRAMEWORK FOR MCC ENVIRONMENT

As of the analyse of literature Survey of various data security frameworks in mobile cloud computing the problem related to security and privacy issues are identified in Mobile Cloud Computing Environment. To conquer these data security and privacy issues, there should be some mechanisms to resolve this problem. There is a need to implement or develop the data security framwork that provide security, confidiantiality and integrity of users data.
We have planned the security framework for providing the confidiantiality and integrity of mobile users data or file. There should be some techniques to improve the security of mobile user's private data to avoid the attacks by adversary. Some mechanisms are essential to provide the confidiantility to user's personal data, which only the owner can access his own data and no any other users permitted to access to data without data Owner's permission. The uploading and downloading steps for user's file are presented in figure 1 and figure 3.

A. Poposed Framework Considerations

In the proposed data security Framework, We will use three different cryptographic implimentation techniques for improving the security and privacy of data.

1) Counter modes of block based Encryption and Decryption.

The CTR mode of operation is used to provide energy efficient cryptographic functions by using simply XOR operations on Blocks and keys. This technique also offer - some advantages and security as compared to other chaining block modes of operations.

2) MAC- Message Authentication Code[8].

This cryptographic mechanism is used for validate the integrity of file or data. Standard hash function is used to genrate the intigrity key from Password provided by mobile user.

3) Blowfish Symmetric Cryptographic Algorithm[6].

This symmetric cryptographic algorithms is used to improve the security of data. This algorithm present high execution speed and throughput. It also consume less energy for execution as compared to other symmetric algorithms.

DOI 10.17148/IJARCCE.2015.4256

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

B. Proposed Flow for Uploading the User File on the Cloud Storage

Step 1: Select the File 'F' and provide the password upto 6 to 20 characters from mobile user.

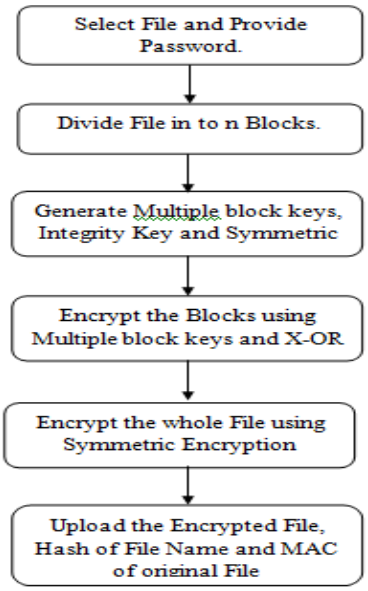

Fig.1: Flow diagram for uploading of User's Data

Step 2: Divide the File 'F' in to 'n' numbers of equal size Blocks. For symmetric defragmentation some extra bits should be padded at the end of file if required for equal size.

Step 3: Generate the Multiple Block Keys from given password and also generate the Integrity Key and Symmetric Key by using the Hash function on password as well as other unique factors reated to user file

Step 4 : Encrypt the individual Blocks by using Counter Mode of Operations. The generated Multiple Block keys is used for each different Block. The X-OR operations are performed for encryption of each block. The Counter is also used to produce the keys as a input for block encryption. In these operations the multiple blocks keys and counter are increment one by one from previous block to next succeed blocks.

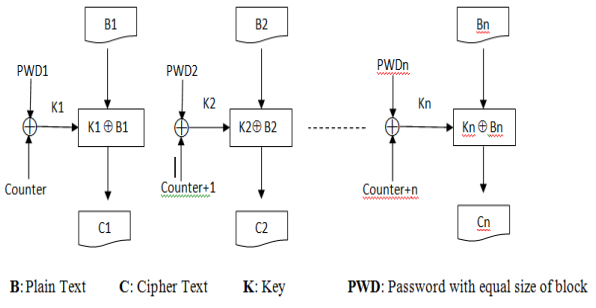

Fig. 2: Encryption Process of Proposed Framework

Step 5: Concatenate all blocks to build one file. Encrypt the complete fil with symmetric encryption algorithm. The generated Symmetric Key is used as a Encryption Key.

Step 6: Mobile User Upload the Encrypted File, Hash of File Name and MAC of Original File. Integrity Key is apply in MAC for File Integrity Verification. These complete Information is Uploaded on cloud storage servers by mobile users and keep saving only the file name.

C. Proposed Flow for Downloading the User File from the Cloud Storage

Step 1: Mobile user send the request for file download to Cloud Service Provider(CSP). CSP send the Encrypted File with MAC of original File. Mobile user download the encrypted File and MAC.

Step 2: The Passwor.d is provided by mobile user for generation of various Keys. The keys for blocks and for decrypt the encrypted file is generated from provided password.

Step 3: The Symmetric Key, Integrity Key and Multiple Block Keys are generate from given password by mobile user.

Step 4: The complete Encrypted File is decrypt with generated Symmetric Key and Symmetric Cryptographic Algorithm.

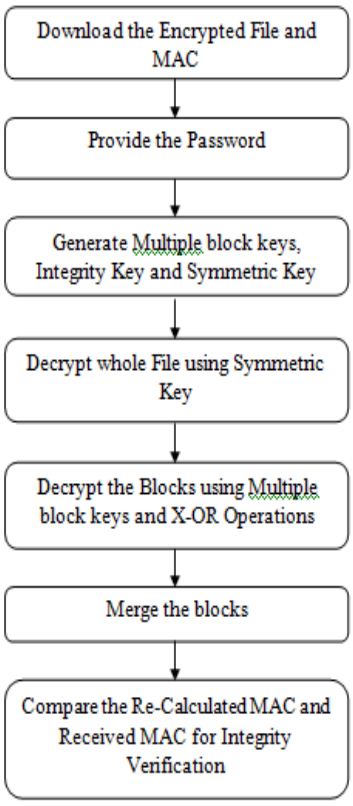

Fig. 3: Flow Diagram for Downloading Encrypted file

Step 5: Every Blocks are decrypted by generated Multiple Block Keys and X-OR operations. the Counter Mode of Operations are used to obtain the original File Blocks or Plaintext of Blocks.

DOI 10.17148/IJARCCE.2015.4256

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

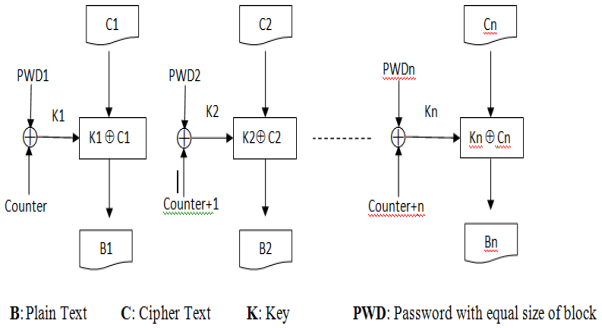

Fig.4: Decryption Process of Proposed Framework

Step 6: Following decryption of every blocks the plaintext of all blocks are produced. Thereafter, merge or concatenate every plaintext blocks for collect the original file.

Step 7: Compare the MAC of received MAC from CSP and re-calculated MAC of original file subsequent to decryption, with generated Integrity Key.

IV. CONCLUSION AND RESEARCH DIRECTIONS FOR FUTURE WORK

There are numerous cryptographic techniques and algorithms are available to provide the data security and privacy to mobile user's data for firmly stored on public cloud storage servers. I will use three cryptographic techniques to improve the security of confidential data. CTR modes of block based cryptographic technique, Blowfish symmetric cryptographic algorithm and MAC will be applying for proposed Data Security Frameworks.
For future work there will be the opportunities for researchers to present the secure sharing schemes for sharing the essential data among authorized users.
The files must be shared among users according to access privileges assigned by data owner to specific authorized users. There will be additional opportunity to decrease the overhead of cryptographic standard algorithms and research the schemes to afford same security with low overhead as provided by standard cryptographic algorithms.

ACKNOWLEDGEMENT

We would like to acknowledge the greatfull support of our institute to providing the resources to carrying out these research experiments.

REFERENCES

[1] Wei Ren, Linchen Yu, Ren Gao, Feng Xiong, "Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing",Volume 16, Number 5, October 2011, 09 pp.520-528
[2] Niroshinie Fernando , Seng W. Loke , Wenny Rahayu, "Mobile cloud computing: A survey" ScienceDirect- 2012.
[3] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", 2012.
[4] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani "Towards secure mobile cloud computing: A survey", ScienceDirect-2013.
[5] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, Atta ur Rehman Khan "A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environments" , IEEE-2013.
[6] A.Ramesh, Dr.A.Suruliandi ME., Ph.D," Performance Analysis of Encryption Algorithms for Information Security",International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013], pp.840-844
[7] Abdul Nasir Khan, M. L. Mat Kiah , Mazhar Ali,Sajjad A. Madani , Atta ur Rehman Khan,Shahaboddin Shamshirband," BSS: block-based sharing scheme for secure data storage services in mobile cloud environment", Springer Science+Business Media, August 2014,pp. 946–976
[8] William Stallings, Cryptography and Network Security,4th ed., 2005.

BIOGRAPHIES

Ms. Chandni Patel is a student of Masters of Engineering in Specialization of IT System and Network Security from Gujarat Technological University. She had completed her B.E and also pursuing M.E from Sardar Vallabhbhai Institute and Technology, Vasad, GTU. att many workshops and seminars. Her Research interest is Cloud Computing and Network Security and cryptography.

Mr. SameerSingh Chauhan is working as Assistant Professor in Institute of Engineering and Technology, JK Lakshmipat University. He completed his M.Tech from IIT.He has 12.5 years experience in teaching. He has attended many International and National Conferences, Seminars and Workshops. He has published many research Articles. His interest in area of research are: Cloud Computing, Grid Computing and IoT.

Mr. Bhavesh Patel is working as Assistant Professor in SVIT, Vasad. He has completed his B.E in IT from SVIT, Vasad in Gujarat University and M.E in CSE from Govt. Engineering Collage, Gandhinagar from GTU. He has 10.5 years experience in teaching. He has published two research articles in international journal and conference. He has attendent one Workshop, two STTP and one Expert Talk. His area of interest in research are: Network Security, Network Forensics, Java and Data Compression.