International Journal for Science and Emerging Technologies with Latest Trends
ISSN No. (Online):2250-3641, ISSN No. (Print):2277-8136

DATA SECURITY SCHEMES FOR MOBILE CLOUD COMPUTING

Dr. Abhinav Verma

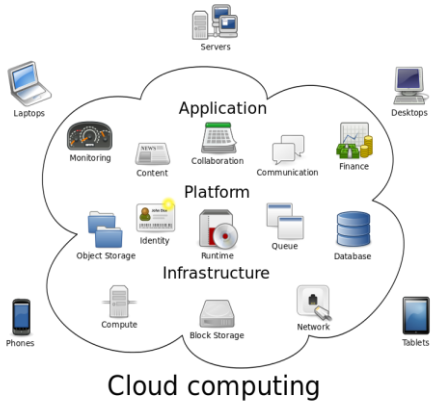
Ext. Lecturer , PT CLS Govt. College, Karnal

Abstract

Mobile Cloud computing is an emerging technology which provides IT services and resources to the customers through public network specifically internet. Mobile the cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. When using the secure mobile 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. Data protection is a critical issue in mobile cloud computing environments. 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.

1.1INTRODUCTION:

In recent year cloud computing has emerged as a new computing example in which various users share the resources in pay per site/ per service basis. The resources in such a computing paradigm are located at distributed sites with control from the service providers. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1] as shown in figure 1



ISSN No. (Online):2250-3641, ISSN No. (Print):2277-8136

Cloud computing is an emerging technology which provides IT services and resources to the customers through public network specifically internet. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing offers an innovative model for the organizations to use software applications, storage and processing capabilities of cloud without investing on the infrastructure. As compared to existing IT models, the cloud computing offers many advantages like scalability, flexibility, efficiency and non-core activities [1]. Despite these extraordinary benefits of cloud computing, the security is a major concern. According to the International Data Corporation (IDC) survey 74% IT managers and Chief Information Officers (CIOs) thinks that security and privacy issues are the main obstacle preventing organizations to adopt cloud computing services and the survey conducted by Garter that more than 70% Chief Technology Officers (CTOs) showed their concern about data security and privacy issues in cloud computing [2, 3].

1.2 Cloud Service Delivery Models

The cloud computing model is based on three service delivery models and three cloud architectural models [2, 3].

- **Cloud Software as a Service (SaaS)**: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email)
- **Cloud Platform as a Service (PaaS)**: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider (e.g., configurations)

Cloud Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.(e.g., host fire walls) According to customers' different demand, cloud computing technology includes three kinds of architectural models, which are public cloud, private cloud and mixed cloud.

- **Public cloud:** Run by a third party, public cloud can put many different customers' operation on the cloud of servers, storage systems and other infrastructure mix. End users do not know to the other users who run their operations on the same server, network or disk.
- **Private cloud**: Private Cloud is built for clients to use it privately, and thus it can make the most effective control of data, security and service quality. The company has the infrastructure, on the basis of the infrastructure, it can control the way to deploy applications, control how and where the applications run. They have server, network and disk, and can determine which users are allowed to use these infrastructures. Private clouds can be deployed in enterprise's data centers; it can also be deployed in a hosting site. Private cloud can be built by the companies themselves or by the cloud providers.
- **Mixed cloud**: The mixed cloud is to mix the public cloud model and private cloud model together.

International Journal for Science and Emerging Technologies with Latest Trends
ISSN No. (Online):2250-3641, ISSN No. (Print):2277-8136

1.3 REVIEW OF EXISTING DATA SECURITY SCHEMES FOR MOBILE CLOUD COMPUTING

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 is not any Trusted Third Party concerned in schemes the cloud servers are assumed fully distrusted for these selected data security schemes. In these secure storage of user data. The existing data security schemes are encryption based scheme, coding based scheme, sharing based scheme, and Block Based sharing scheme [1, 7]. In each scheme, encryption, decryption, and integrity verification operations are perform on Mobile Devices. The Cloud Service Providers and Data Centre owners are responsible for secure data storage management and handling of requests - response of user's file or data.

TABLE-I
COMPARISIONS OF CRYPTOGRAPHIC DATA SECURITY SCHEMES

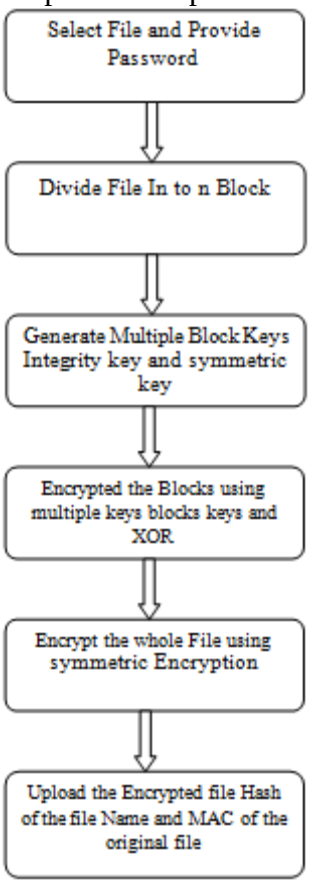
Security Schemes	Supporting Operations	Assumptions	Limitations	Conclusion
Encryption based scheme	Standard Symmetric Cryptographic Algorithm	N/A	Processing Overhead	**1.**Consume more energy on Mobile devices. **2.** Provide additional security.
Coding based scheme	Matrix Multiplications of blocks with coding vector	Construction of Coding Vector	Extra file management overhead on mobile Devices.	**1.**Use less resources as Compared to Encryption based scheme. **2.**Computationally Intensive.
Sharing based scheme	X-OR operations	Generation and uploading of random Shares.	Supporting operations are computationally intensive	**1.** Time consuming **2.** Considerable amount of data Processing and data storage.
Block Based sharing scheme	Block Based Chaining modes of operations	File is logically divided in to Chunks	Depended Block Executions. Simple XOR operations are used as cryptographic Functions.	**1.**Energy-Effiecient **2.** Consume less resources **3.**Provide high speed execution

This symmetric cryptographic algorithm 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.

International Journal for Science and Emerging Technologies with Latest Trends
ISSN No. (Online):2250-3641, ISSN No. (Print):2277-8136

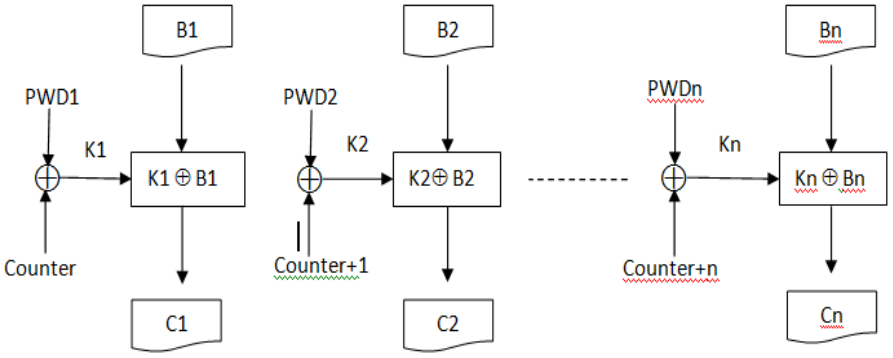
Proposed Flow for Uploading the User File on the Cloud Storage

1. Select the File F and provide the password up to 6 to 20 characters from mobile user



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.
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 related to user file.Encrypt the individual Blocks by using Counter Mode of Operations. The generated Multiple Block keys are 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.
Concatenate all blocks to build one file. Encrypt the complete file with symmetric encryption algorithm. The generated Symmetric Key is used as a Encryption Key.
Mobile User Upload the Encrypted File, Hash of File Name and MAC of Original File. Integrity Key is applying in MAC for File Integrity Verification. This complete Information is uploaded on cloud storage servers by mobile users and keeps saving only the file name.

International Journal for Science and Emerging Technologies with Latest Trends
ISSN No. (Online):2250-3641, ISSN No. (Print):2277-8136



B: Plain Text **C**: Cipher Text **K**: Key **PWD**: Password with equal size of block

Proposed Flow for Downloading the User File from the Cloud Storage

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

The Password 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.

The Symmetric Key, Integrity Key and Multiple Block Keys are generated from given password by mobile user.

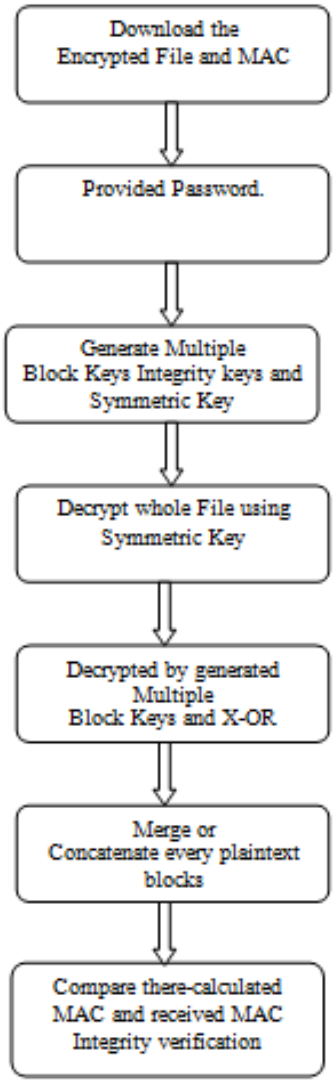
The complete Encrypted File is decrypt with generated Symmetric Key and Symmetric Cryptographic Algorithm.

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.

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

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

International Journal for Science and Emerging Technologies with Latest Trends
ISSN No. (Online):2250-3641, ISSN No. (Print):2277-8136



CONCLUSION

In this paper overview of cloud computing is given which includes types of clouds, characteristics of cloud, architecture of cloud, security and risk issues, Due to the nature of cloud computing, such as resource sharing/pooling and web-based remote connections, security plays an important role in cloud system designs. Cloud service providers need to protect authenticity and confidentiality of customers' data transmitted to and stored in the cloud, and prevent unauthorized access of customers' resources. This paper has comparison cryptographic data security scheme various authentication and encryption algorithms that protect cloud systems, including modes of operation for data encryption and authentication, block ciphers for encryption, password hashing algorithms for password-based authentication and key derivation functions and password-less or two-factor authentication mechanisms.

ISSN No. (Online):2250-3641, ISSN No. (Print):2277-8136

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

[5]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: blockbased sharing scheme for secure data storage services in mobile cloud environment”, Springer Science+Business Media, August2014,pp. 946–976

[8] William Stallings, Cryptography and Network Security,4th ed., 2005.