Advances and Applications in Mathematical Sciences
Volume 18, Issue 8, June 2019, Pages 767-774

COMPARISON OF DATA SECURITY SCHEMES FRAMEWORK FOR MOBILE CLOUD COMPUTING

SUMANT RAJ CHAUHAN,[1] PANKAJ KUMAR[1] and VIKRAM BALI[2]

[1]NIILM University
NH-65, Kaithal, Ambala Road
Kaithal, Haryana 136027, India

[2]JSS Academy of Technical Education
Noida, India

Abstract

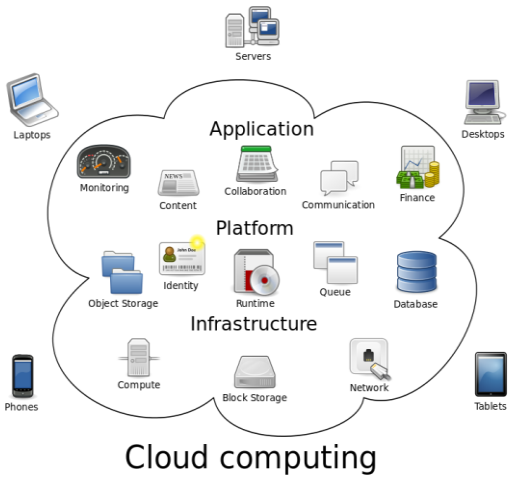
Mobile Cloud compute is an up-and-coming technology which provide IT services and resources to the customers from side to side public network exclusively internet. Mobile cloud computing services and infrastructure are generally own by a moderator called cloud service providers. When using the secure mobile cloud storage space services on resources limited Mobile Devices, the confidentiality of sensitive data must be ensure before uploading the data on cloud storage servers. The composite security operations to ensure security are limited to implement due to the resource embarrassed mobile devices. Data protection is serious issues in mobile cloud compute environment. In this paper, we present a projected security framework for mobile cloud compute. In this structure the cryptographic methods as well as algorithms are used for encryption and decryption of mobile user data. This structure ensures the supplementary security and discretion of user's aware or considerable data. This paper introduces the scheme stream of projected security structure. This projected Security structure is for the principle to secure and offer privacy and reliability to user's not to be disclosed data in Mobile Cloud Environment.

1.1. Introduction

In contemporary year cloud computing has emerge as a new computing paradigm in which various users divide the capital in recompense per site/ per service basis. The resources in such a computing example are situated at circulated sites with manage the service providers. Cloud computing is a model for enable suitable, on-demand network access to a mutual band of configurable computing resources as well as networks, servers, storage,

2010 Mathematics Subject Classification: 68-xx.
Keywords: cryptographic, Mobile Cloud, SaaS, PaaS, IaaS
Received February 1, 2019; Accepted March 17, 2019

applications, and services that can be quickly provisioned and unconstrained with minimal supervision effort or service provider communication [1] as shown in figure 1



Cloud computing is a budding technology which provide IT services and possessions to the customers through public network particularly internet. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing offer an inventive model for the organization to use software applications, storage and dealing out capability of cloud without invest on the infrastructure. As compare to existing IT models, the cloud computing offers many recompense like scalability, flexibility, effectiveness and non-core actions [1]. Even though these unexpected reimbursement of cloud computing, the security is a most important concern. According to the Global Information Firm (GIF) survey 74% IT manager and Head Information Officer (HIOs) think that security and privacy issues are the main obstruction prevent organization to accept cloud computing services and the survey conduct by Garter that more than 70% Head Information Officer (HIOs) show 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 release 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 easy to get to from various user devices during a thin client interface such as a web browser example web-based email.
- **Cloud Platform as a Service (PaaS)**: The competence provide to the user is to organize against the cloud infrastructure consumer-created or acquire application created using encoding languages and apparatus support by the source example configurations

Cloud Infrastructure as a Service (IaaS): The facility provide to the user is to stipulation dispensation, storage, networks, and other elementary computing assets where the consumer is able to organize and run random software, which can include operating systems and application. (e.g., host fire walls) According to customers different command, cloud computing technology include three kind of architectural model, which are public cloud, private cloud and miscellaneous 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 combine. End user do not recognize to the other users who run their operation on the same server, network or disk.
- **Private cloud**: Private Cloud is built for clients to use it confidentially, and thus it can make the most efficient manage 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 resolve which users are allowed to use these infrastructures. Private clouds can be deployed in enterprise data centers; it can also be deployed in a hosting site. Private cloud can be built by the company themselves or by the cloud providers.
- **Mixed cloud**: The mix cloud is to mix the public cloud model and private cloud model mutually.

1.3. Assessment of Presented Data Security Scheme for Mobile Cloud Computing

This paper introduce in journalism analysis, the data security scheme that center of attention on the decrease of the computational difficulty of cryptographic algorithms and method. Present is not any trust Third Party worried in scheme the cloud servers are understood fully distrust for these selected data security scheme. The existing data security scheme is encryption based proposal, code based scheme, sharing based scheme, and block based sharing scheme [1, 7]. In each scheme, encryption, decryption, and integrity confirmation operations are complete on Mobile Devices. The Cloud Service Providers and Data Centre owner are accountable for safe data storage administration and treatment of requirements-reaction of user's file or data.

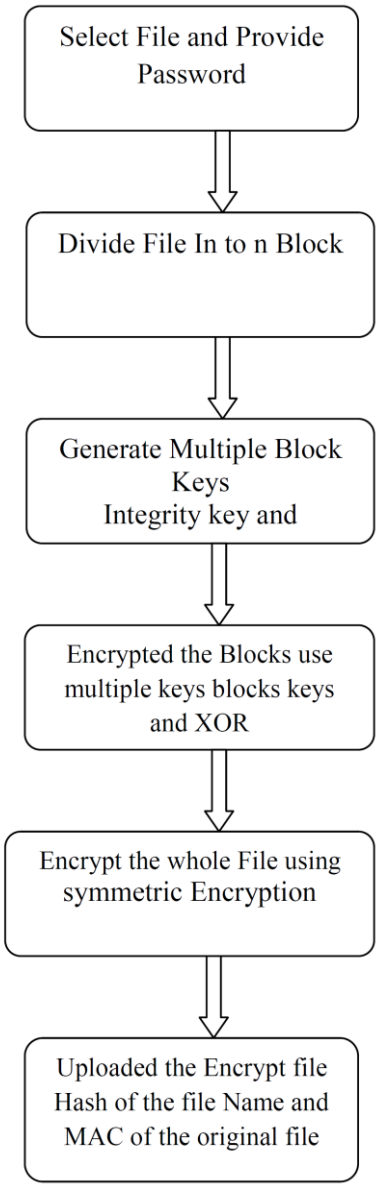
Table 1. Analysis of cryptographic data security scheme.

Security Schemes	Supporting Operations	Assumptions	Limitations	Conclusion
Encryption based scheme	Normal Symmetric Cryptographic Algorithm	Not applicable	Process Overhead	**1.**Consume extra power on Mobile devices. **2.** Supply extra 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 arbitrary Share.	Supporting operations are computationally intensive	**1.** Time consuming **2.** Considerable amount of data Dispensation and data storage.
Block Based sharing scheme	Block base chain mode of operation	File is reasonably separated in to chunk	Depended Block Execution. Simple XOR operation are used as cryptographic Function.	**1.**Power -Efficient **2.** Consume less resources **3.**Present high speed implementation

The symmetric cryptographic algorithm is used to advance the security of data. This algorithm presents high implementation speed and throughput. It also consumes less energy for implementation as compare to additional symmetric algorithms.

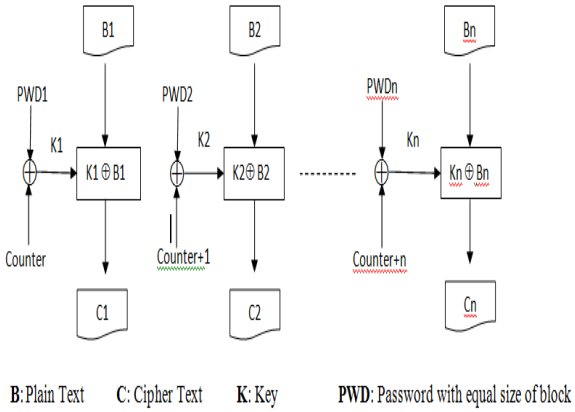
Projected Flow for Uploading the User File on the Cloud Storage

Choose the File *X* and supply the password up to 8 to 20 characters from mobile user



split the File "*X*" in to "*n*" numbers of equivalent size block. For symmetric defragmentation some additional bit should be padded at the end of file if

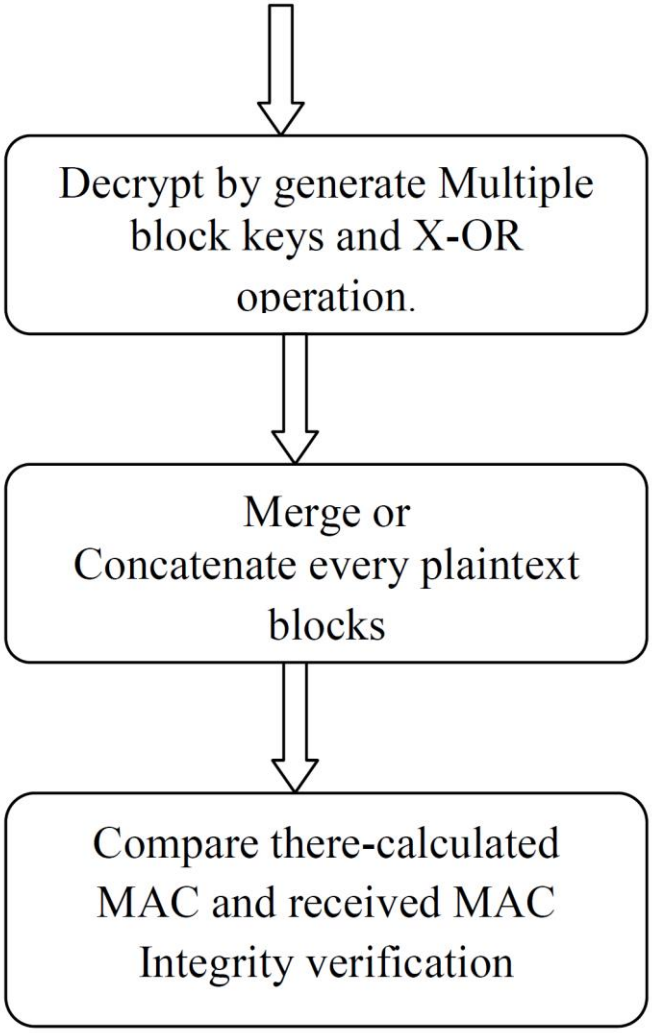
compulsory for equivalent size. produce the several Block Keys from given password and also generate the Integrity Key and Symmetric Key by using the Hash function on password as well as other unique factors related to user file. Encrypt the individual Blocks by using respond to Mode of Operations. The generated several Block keys are used for each dissimilar Block. The *X*-OR operations are perform for encryption of each block. The Counter is also used to produce the keys as input for block encryption. In this operation the various blocks keys and counter are increment one by one from prior block to next be successful blocks. Concatenate all blocks to construct one file. Encrypt the whole file with symmetric encryption algorithm. The generate Symmetric Key is use as a Encryption Key. Mobile client upload the encrypted file, Hash of file name and MAC of original file. Integrity key is applying in MAC for file integrity verification. The total information is uploaded on cloud storage servers by mobile user and keep saving only file name.



Proposed Flow for downloading the client File from the Cloud Storage

Mobile users send the demand for file downloaded 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 providing by mobile user for generation of various Keys. The keys for block and for decrypt the encrypted file is generate 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

generate Symmetric Key and Symmetric Cryptographic Algorithm. Every Blocks are decrypted by generated Multiple Block Keys and *X*-OR operations. The Counter Mode of Operations is used to get the original File Blocks or Plaintext of Blocks. Subsequent decryption of every blocks the plaintext of all blocks are produced. After that, join 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 generate Integrity Key.



Conclusion

In this paper summary of cloud computing is known which include type of clouds, characteristics of cloud, architecture of cloud, security and risk issue, due to the character of cloud computing, such as resource sharing/pool and web-based remote connections, security plays an imperative role in cloud system design. Cloud service provider requires protecting authenticity and confidentiality of customers' data transmit to and stored in the cloud, and check unconstitutional access of customers' resources. The term paper has assessment cryptographic data security method a variety of authentication and encryption algorithms that protect cloud system, including mode 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 mechanism.

References

[1] Wei Ren, Linchen Yu, Ren Gao and Feng Xiong, Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing 16(5) (2011), 520-528

[2] Niroshinie Fernando, Seng W. Loke and Wenny Rahayu, Mobile cloud computing: A survey Science Direct- 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 and 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 and A. Suruliand, 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 and Shahaboddin Shamshirband, BSS: blockbased 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.