Mobile Cloud Computing Security Models: An Overview

Manzamasso Kpelou[1] Mr. Keshav Kishore[2]
[1,2]Alakh Prakash Goyal University, India

Abstract— Cloud computing is the on demand of database storage, IT services and application over the internet. When paired with mobile computing, it vastly augments the limited resources of mobile devices in terms of processing power, battery life and storage. Hence raise up the Mobile Cloud Computing technology in which mobile users can access data anywhere and anytime, execute application regardless of the platform and benefit from various cloud services. However the MCC comes along with major challenges in data security and privacy that prevent it to be widely adopted. The purpose of this survey is to present data security and privacy requirement in Mobile Cloud Computing environment and the challenges it introduces. We also present the corresponding solutions that have been identified by various researchers to settle the challenges. Furthermore, we analyze and compare the works done by others researchers. We find out the best practices from each researcher work and combine them to build a framework.

Keywords: Mobile Cloud Computing, Data Encryption, Mobile Cloud Security, Cloud Computing

I. INTRODUCTION

Mobile devices are becoming an essential part of human life as they most effective and convenient communication tools [1]. Such devices like smartphones and tablets are used for data, video and voice transmission over a network. However, the mobile devices are facing many challenges in their resources like battery life, storage, and bandwidth [1]. In order face these challenges, mobile computing leveraged the technology of cloud computing which is the on demand of database storage, IT services and application over the internet. As a result, we assist to the emergence of Mobile Cloud Computing technology in which mobile users can access data anywhere and anytime, execute application regardless of the platform and benefit from various cloud services.

Regarding the evolution of MCC, security is a major issue. Storing data in cloud is a serious concern that worries every mobile cloud user. Data being transferred or stored in MCC environment need to be secured. In mobile clouds, there are multiple third parties who may have chances to reach sensitive information [6]. Encryption can be the solution to secure data and it is better to encrypt the data before storing it in cloud [5]. Data owner should be the one who can give the permission to anyone who wants to access the particular data [5].

Although many security schemas have been proposed, every schema come along with some weaknesses that we intend to mitigate by leveraging their advantages to build a new security framework. Our Framework includes 3 processes: Data fragmentation process, compression of data fragments and the encryption of the compressed data. After the three processes applied on the data on the user side, then it can be securely uploaded to the cloud.

The rest of this paper is organized as follows: Section II briefly review the challenge of data security and privacy in MCC. Section III describes the requirements of data security in MCC. Section IV exposes the various security models in MCC. In Section V, we provide survey of existing security frameworks for MCC. We depicted the conclusion and future work in Section VI.

II. DATA SECURITY CHALLENGE IN MCC

The most serious concern of mobile cloud users is about the security and the privacy of their data outsourced and stored in the cloud environment. Data security is then one of the major challenges in mobile cloud environment. Here are some issues related to security in mobile cloud computing: data privacy, data ownership and other security issues.

A. Data Privacy

Data privacy also called information privacy is state as one of the biggest challenge in mobile cloud computing environment. It tells about how data is collected, shared and used. It states if or how the data can be shared with third parties, if data can be legally collected or stored. Many questions are raised by users:

- How files are created and the back-up is done
- What happen when user delete his files
- Who can access the data
- Where the data are located

B. Confidentiality of Data

Data confidentiality is related to data privacy and ensures data is visible to only authorized user. It refers to the protection of information from being accessed by unauthorized persons. Access to data must be restricted to only those authorized to view the data. Many questions are raised by user:

- Where the encryption and decryption processes are taking place?
- What are the menaces when transferring data client to cloud?
- Ho to perform operations like search on an encrypted form

C. Data Integrity

Data integrity involves maintaining the accuracy, consistency, and trustworthiness of data its life cycle. Integrity of data means data must not change while being transferred and must not be altered by unauthorized persons. From the time the data is uploaded to time the data is download through the time the data spent on cloud storage, there must not be any change or alteration of the data .Data integrity can be guaranteed with access controls and permission on data.

D. Data Ownership

Despite the advantages of cloud services, a person must answer the most important question when going to upload his data on cloud, which is "who owns the data". Sometime when a user decide to download his data or delete them, is that mean the cloud hosted service doesn't make a copy of those data? The situation in which the hosted service keep some

information without the permission of the owner, the user are not any more the data owner.

E. Other Security Issues

Here is other security issues like that affect data security in MCC: Denial of Service, Side Channel attack, Authentication attacks, Man-in-the-middle attacks.

It is also intimidating to transfer important data to the cloud because of the following data concerns that are very common in the cloud [16]:

- Handling of encryption and decryption keys
- Violation of privacy rights
- Risk of data theft
- Lack of standard to ensure data integrity
- Services incompatibility due to the involvement of different vendors

To incent and attract more users to adopt Mobile Cloud Computing, it is important to protect the data from the various security concerns.

III. Data Security Requirement in MCC

Data encryption in the cloud consist of transforming or encoding data before being uploaded to cloud storage. With cloud services, there are two forms of encryption: "Transit" when files uploaded are being transferred between the user and the cloud service using Secure Sockets Layer (SSL) and "resting" when files are stored in encrypted format on cloud storage .Most of the time cloud service providers offer encryption services - ranging from an encrypted connection to limited encryption of sensitive data – and provide encryption keys to decrypt the data as needed [17].

But researcher in their work in order to provide data security and privacy have proposed various framework in which the encryption of data no longer needed to be provided by a third party.

Encryption of the data is the top priority for Mobile Cloud Computing in term of data security and privacy. And there is some minimum requirement that involved in the process on encryption.

A. Data must be encrypted before being upload to the cloud

Encryption of data before being uploaded to the cloud is one the best practice to execute which ensure the data security. Data needs to be protected from unauthorized access and transmitted to the intended receiver with confidentiality and integrity [3]. Data sent in clear through the transmission media can be intercept by adversaries. Sensitive data intercept by a malicious person with attacks such as Man-In-The-Middle are avoid using encryption techniques on data before sending it to the cloud storage.

B. The choice of encryption algorithm for MCC

Many algorithms such like DES, AES, Blowfish, RC2, 3DES, and RC6 can be used to ensure data encryption in mobile cloud computing. Those algorithms can be from Traditional symmetric or asymmetric encryption algorithms. There are many disadvantages for symmetric encryption algorithms like key maintenance and there are also many drawbacks of asymmetric encryption algorithms regarding the consumption of computing resources such as CPU time, memory, and battery. The choice of the encryption algorithm must be suitable for the type of data and also based on how faster and secure it can be.

C. A Secure Communication Channel

After the data being encrypted using an encryption algorithm and ready to be sent on the cloud provider storage space, a secure channel will ensure data security during the transmission. A secure communication channel appear then as a reliable requirement to ensure data security in Mobile Cloud Environment. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers [21].

IV. MCC Security Models

This are the three categories for mobile cloud computing security on which the existing models are based on:

A. Authentication Based Models

Also called Identity Base Encryption (IBE) it is a public-key cryptosystem where any string can be chosen as a valid public key. In particular, email addresses and dates can be public keys [22].

B. Data Access Models

This model secure data access cryptographic schemes, secure resource and allocation methods, data privacy preserving approach, secure network channels.

C. Location based security models

Data security is mapped to a specific location so that data can't be accessed from another area.

V. Literature Survey

To ensure the security and privacy of the data in MCC, various security schemas have been created.

Mohd Rizuan Baharon et al. [1] proposed A New Lightweight Homomorphic Encryption Schema for Mobile Cloud Computing. The New Lightweight Homomorphic Encryption (LHE) minimizes the use of computation power at encryption and key generation. In the paper, the authors deeply look at homomorphic encryption efficiency and proposed the LHE since the primitive encryption schemas are unsuitable for use in cloud environments. According to the authors, Homomorphic Encryption is believed to be one of the potential solutions to allowing arbitrary computation on encrypted data, however its efficiency is still an obstacle for its implementation.

Syam Kumar Pasupuleti et al. [12] Use probabilistic public key encryption algorithm for encryption of data and invoked ranked keyword search over the encrypted data to retrieve the files from the cloud. That approach aim to achieve an efficient system for data encryption without scarifying the privacy of data unlike several keyword searchable encryption schema. Data is protected against privacy violations, the schema also verifies the integrity of data. ESPPA satisfies the security and efficient requirements through the security and performance analysis.

In the future work, ESPPA will be enhanced to support efficient dynamic data operations and ranked keyword search over the encrypted big data in cloud.

Yinghui Zhang et al. [13] introduce a novel technique called match-then-decrypt, that enhance the anonymous attribute-based Encryption (ABE) in which matching phase is introduced before the decryption phase. This technique has the advantage of Fast decryption and it is more suitable for mobile cloud computing where users may be resource- constrained. A matching phase introduced before the decryption phase greatly improve decryption efficiency in anonymous ABE.

Jiang Zhang et al. [14] Leverage several cryptographic primitives such as new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC, which provide data privacy, data integrity, data authentication, and flexible data distribution with access control. The system is a lightweight and easily deployable solution for mobile users in Mobile Cloud Computing since no trusted third parties are involved.

Mehdi Bahrami et al. [7] proposed a new light-weight method for mobile clients to store data on one or multiple clouds by using pseudo-random permutation based on chaos system. Client mobile devices can store data in the cloud(s) without using cloud computing resources for encryption to maintain user's privacy.

Ibtihal Mouhib et al. [5] are concern with data security in mobile cloud computing environment. The authors proposed a hybrid architecture based on Encryption as a service. It empowers the cloud clients to be in control of their cryptographic operations and keys independently of the cloud provider.

Yibin Li et al. [9] proposed a scheme entitled as Security-Aware Efficient Distributed Storage (SA-EDS) model to prevent Cloud Service operator to directly access partial data. The proposed approach divides the file and separately stores the data in distributed cloud servers.

Future work would address securing data duplication in order to increase the level of data availability since any of datacenter's down will cause the failure of data retrievals.

Jun Shao et al. [11] proposed a new sharing protocol for cloud computing by using a new cryptographic primitive named online/offline attribute based on proxy re-encryption and the transform key technique that give a fine-grained access control, flexible sharing, data confidentiality, and minimum online computational cost on the user side at the same time.

Hongwei Li et al. [8] developed a fine-grained data search scheme and discuss it's implementation on Encrypted mobile cloud data in way to balance the QoP (Quality of Protection) and QoE (Quality of Experience) because encryption only increase the QoP of data outsourcing and significantly reduces data usability and thus harms the mobile user's Quality of Experience (QoE).

Deepanshu Goyal et al. [8] present a security framework for data access using Location Based Service (LBS) that act as an additional layer in authentication process. User having valid credentials in location within the organization are enabled as authenticated user.

For further work, (LBS) can be extended to include sensor attributes and extend the functionality of MCC applications.

PARAMETERS / PAPER TITLE	symetric	Asymetric	Key lenght	Block size	Number of round	Complexity	performance	Type of attacks	Encryption on the user side	Computation on encrypted data	Data compression	Data fragmentation	Algorithm used
a new lightweight homomorphic encription scheme for mobile cloud compution	no	yes	-	-	-	-	-	-	yes	yes	no	no	RSA
An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing	no	yes	-	-	-	-	-	-	yes	no	no	no	RSA, SHA-1
Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing	no	yes	-	-	-	-	-	-	Yes	yes	no	no	ABE,AES

Towards Secure Data Distribution Systems in Mobile Cloud Computing	no	yes	128	128	-	-	-	-	yes	no	no	no	AES, SHA-256
A Light-Weight Permutation Based Method for Data Privacy in Mobile Cloud Computing	-	-	-	-	-	-	-	brute Force	yes	no	no	yes	chaos system
Encryption as a service for securing data in mobile cloud computing	-	-	-	-	-	-	-	-	no	no	no	no	RSA, ElGamal Cryptosystem, homomorphic encryption, Elliptic Curve
Intelligent cryptography approach for secure distributed big data storage in cloud computing	yes	no	-	-	-	-	-	-	yes	no	yes	yes	Alternative Data Distribution, Secure Efficient Data Distributions, Efficient Data Conflation
Fine-grained data sharing in cloud computing for mobile devices	-	-	-	-	-	-	-	-	yes	no	no	no	Attribute-based encryption, ElGamal Cryptosystem
Engineering searchable encryption of mobile cloud networks: when QoE meets QoP	yes	no	-	-	-	-	-	-	yes	yes	no	no	-
Secure framework for data access using Location based service in Mobile Cloud Computing	yes	yes	-	-	-	-	-	-	no	no	no	NO	AES, RSA

VI. Conclusion and Future Work

In this paper we discuss various schemas used for data security and privacy in mobile cloud Environment. The advantages and weaknesses of each security schema have been discussed. And based on our analysis of this related works, we proposed a novel security framework which ensure a better security and privacy of user's data in the mobile cloud environment as the data is fragmented, compressed and encrypted before being uploaded. All this processes are operated on the user side, this require no third party to ensure the data security and give the user a total control on his data.

References

[1] Baharon M. R., Shi Q. & Llewellyn-Jones D. (2015). A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing. 2015 IEEE International

Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.
[2] Shakeeba S. Khan et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.9, September- 2014, pg. 517-525
[3] Zoran Hercigonja et al, Comparative Analysis of Cryptographic Algorithms. International Journal of DIGITAL TECHNOLOGY & ECONOMY Volume 1, Number 2, 2016
[4] David, S., Xavier, B., & Kathrine, J. W. (2017). A panoramic overview on fast encryption techniques for outsourced data in mobile cloud computing environment. 2017 International Conference on Inventive Computing and Informatics (ICICI).
[5] Gai K., Qiu M., Thuraisingham B. & Tao, L. (2015). Proactive Attribute-based Secure Data Schema for Mobile Cloud in Financial Industry. 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems.
[6] Bahrami M. & Singhal M. (2015). A Light-Weight Permutation Based Method for Data Privacy in Mobile Cloud Computing. 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering.
[7] Li H., Liu D., Dai Y. & Luan T. H. (2015). Engineering searchable encryption of mobile cloud networks: when QoE meets QoP. IEEE Wireless Communications, 22(4), 74–80.
[8] Li Y., Gai K., Qiu L., Qiu M. & Zhao H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, 103–115.
[9] Goyal D. & Krishna, M. B. (2015). Secure framework for data access using Location based service in Mobile Cloud Computing. 2015 Annual IEEE India Conference (INDICON).
[10] Shao J., Lu R. & Lin X. (2015). Fine-grained data sharing in cloud computing for mobile devices. 2015 IEEE Conference on Computer Communications (INFOCOM).
[11] Pasupuleti S. K., Ramalingam S. & Buyya R. (2016). An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. Journal of Network and Computer Applications, 64, 12–22.
[12] Zhang Y., Chen X., Li J., Wong D. S., Li H. & You I. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences,
[13] Zhang J., Zhang Z. & Guo H. (2017). Towards Secure Data Distribution Systems in Mobile Cloud Computing. IEEE Transactions on Mobile Computing, 16(11), 3222–3235.
[14] Mouhib I., Driss E. O. & Zine-Dine K. (2015). Encryption as a service for securing data in mobile cloud computing. 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA).
[15] https://blog.appknox.com/security-challenges-in-mobile-cloud-computing/
[16] https://www.agileit.com/news/data-encryption-methods-secure-cloud/
[17] https://www.enlume.com/mobile-data-security/
[18] https://greengarageblog.org/8-pros-and-cons-of-asymmetric-encryption
[19] https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
[20] https://en.wikipedia.org/wiki/Secure_transmission 21
[21] https://crypto.stanford.edu/ibe/

