TOWARDS SECURE MOBILE CLOUD COMPUTING - A SURVEY

Aswathy Divakaran[1], Maya Mohan[2], and Sruthy Manmadhan[3]
[1]M.Tech First Year Student, [2,3]Assistant Professor
Department of Computer Science and Engineering,
NSS College of Engineering, Palakkad
Email: [1]aswathydiv36@gmail.com, [2]mayajeevan@gmail.com, [3]sruthym.88@gmail.com

***Abstract*—Cloud Computing model provides a way to increase the capacity or to add capabilities dynamically. The success of cloud database depends on the gurantees in terms of service availability, scalability, security and data confidentiality. The main advantage of this paradigm is that users only utilize what they require and only pay for what they really use. With an exponential growth of the mobile applications and evolution of cloud computing concept, Mobile Cloud Computing (MCC) has been presented as a potential technology for mobile services. The obstacles related to performance, environment and security are overcome by integrating cloud computing into the mobile environment using MCC. MCC refers to an infrastructure where data processing and storage are performed by mobile device. With this service model, a mobile device can use the cloud for information storage, searching, data mining, multimedia processing etc.**

Despite the advantages, MCC is vulnerable to various security attacks. Also the use of mobile devices causes several issues. Since data is transferred between mobile devices and the cloud servers, confidentiality and privacy is at risk. Outsourcing user's personal data for friend matching process also raises serious privacy concern. Hand over process may degrade the performance of mobile device. This paper considers various issues related to MCC and several methods proposed to ensure secure and energy-efficient architectures for this model.

***Keywords*-Cloud Computing, Mobile Cloud Computing, Confidentiality, Security, Handover**

I. INTRODUCTION

Cloud Computing [1] has become a trend in which local clients access resources from a remote server on an on-demand basis. The main advantage of Cloud Computing is that users only utilize what they require and only pay for what they really use. With the increased growth of the mobile applications and the emergence of cloud computing technology, Mobile Cloud Computing (MCC) [2] has been presented as a potential technology for mobile services. The ultimate goal of MCC is to enable execution of mobile applications on a cluster of mobile devices [3]. With this technology, a set of distributed computing systems or service provider servers participate, connect, and synchronise through mobile communication protocols. Despite its advantages, MCC raises several issues [4].

A mobile device has to be registered with the cloud service provider inorder to access the available services from the cloud. Upon completing this process, both the mobile device and the cloud server authenticates each other. During these phases, user's personal informations are sent to the cloud server. since all messages are transmitted via an insecure WLAN or telecommunication networks, an adversary can easily obtain, interrupt, or modify transmitting messages before they reach the desired recipient. Hence confidentiality and privacy of data in MCC is at risk. Mobile users generally access different types of mobile cloud computing services from a variety of service providers. It is extremely tedious for users to register different user accounts on each service provider and maintain corresponding private keys or passwords for authentication usage. Hence, mobile users will likely be interested in how to access various services from distinct mobile cloud service providers by using only one single private key or password. Thus, key management issue for users has emerged in distributed MCC environment.

Nowadays, many social networks like Facebook recommend friends for us. This is performed by analyzing user's private data. Outsourcing user's personal information for friend matching process seriously affects the confidentiality and privacy of data. Another critical challenge for MCC is the mobility of the mobile phones [5]. When a mobile device enters from one base station area to another base station area, a phenomenon called handover takes place. Handover process degrades the data transfer performance of mobile devices [6]. Hence, an efficient architecture that can improve the handover process in the mobile cloud computing environment is required [7]. The current mobile cloud computing models encompass a cluster of expensive and dedicated machines to provide cloud computing services, incurring significant investment in capital outlay and ongoing costs. A more cost effective solution would be to exploit the capabilities of an ad hoc cloud which consists of a cloud of distributed and dynamically untapped local resources. However, the dynamic and distributed characteristics of ad hoc cloud [8] introduce challenges in system management. Hence, Offloading of mobile applications to remote clouds and the provisioning of services from resource rich cloud to mobile devices is at risk. While designing secure MCC systems these factors becomes the basic building blocks.

II. RELATED WORKS

This section describes various countermeasures that has been proposed to ensure secure and energy-efficient architectures for MCC.

A. Message Digest based Authentication (MDA)

A strong and secure authentication scheme will help in preventing a third party from posing as a legitimate mobile device or as a legitimate cloud service provider is presented in [9]. It is a hashing based authentication scheme which ensures privacy and data confidentiality for MCC environment. MDA consists of three phases: Registration, Authentication and Update phases. Registration phase of a mobile device is a one time process in which *userID* and *password* are created and some encrypted files are exchanged.

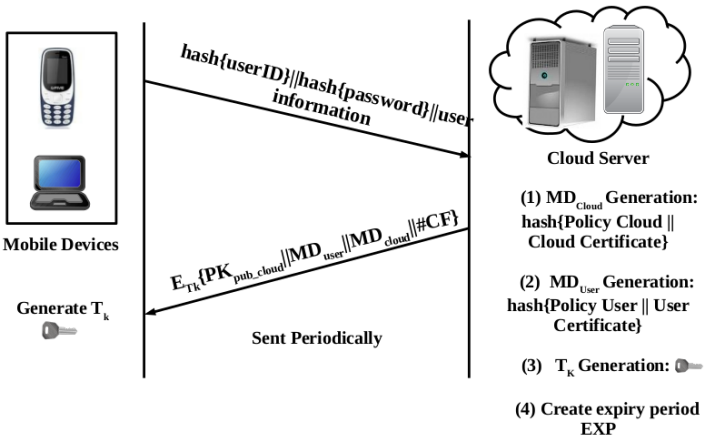

Figure 1. Registration phase [9]

Cloud server generates two message digests MD_{user} and MD_{cloud}. Upon generating these message digests, cloud server creates an encrypted message $E_{T_k}\{Pk_{pub\_cloud} \parallel MD_{User} \parallel MD_{Cloud} \parallel \#CF\}$ to transmit the informations to the mobile device. Pk_{pub_cloud} is the public key of the cloud, and $\#CF$ is the column reference which refers to the cloud authentication database for that particular cloud user information. T_k is generated in both the mobile device and cloud server by XOR-ing hashed *userID* and hashed *password*. The hash algorithm used in this method is SHA 1.

Once the registration process is complete, mobile device and cloud server authenticates with each other. In this phase both mobile device and the server sends some encrypted messages with each other to confirm their identity. Finally in update phase, an expiry timer EXP is assigned to each mobile client who is registered in the server. EXP is a real value which decrements over time. For each authentication request made by the mobile device, the server checks whether EXP is timed out. The mobile device is considered as an unregistered client if the value of EXP is reset or reaches zero. Whenever the registration is expired, the cloud server sends a re-registration request to the mobile device. MDA is completely based on the technique employing simple *userID* and *password* and hashing, it doesnot include any system specific IMSI of the mobile or MAC address of the laptop as in [10].

B. Privacy Aware Authentication Scheme (PAAS)

An anonymous user authentication scheme based on bilinear pairing for distributed mobile cloud computing services is proposed in [11]. Here, distributed mobile cloud service is performed by a trusted Smart Card Generator (SCG). SCG issues one smart card for every registered user. SCG also generates the public parameters and private keys for cloud servers and users. The sheme proposed in [11] consists of three phases: system setup, registration and authentication. During system setup phase, SCG selects a random number as its master private key. It then generates corresponding public key and public parameters. Upon publishing the public key and public parameters, registration phase is executed between the SCG and each one of the mobile users who wish to join the mobile cloud and utilize the authentication services. In this phase, the mobile user and the service provider registers with the SCG with their identities. Upon receiving these identities, SCG generates corresponding private keys for users and the clous servers. Upon completing the registration phase, authentication phase is executed between user and the cloud server whenever a user requests for a mobile cloud service. In this phase, the mobile user and the cloud server authenticates with each other without the involvement of the SCG. A session key is generated inorder to encrypt and decrypt the data sent between the user and the cloud server after the authentication phase. Since identity-based crypto system is used in this system, the identities of users and the cloud servers are also served as their public keys.

C. Scalable and Privacy-preserving Friend Matching in Cloud (SPFM)

Many social networks like Facebook, Line, etc are recommending friends for people nowadays. "People you may know" in Facebook is an example. This task is performed by analyzing user's personal information. Outsourcing user's personal information for friend matching process raises serious concern. A solution for this issue is presented in [12]. A novel SPFM protocol is presented which performs the friend matching and recommendation without revealing user's personal information to the cloud. Figure 2 shows the protocol framework. Here, user's personal data is obfuscated before sending to the cloud. Eventhough cloud server has no idea about the original data it can perform friend matching and recommendation services. This process involves three steps.

In the first step, server setsup a masking generation probability P_k. Value of P_k is greater than 0.5 and determines the masking degree. This value is a common knowledge for both the cloud as well as the users. In the second step, data masking is performed on each user's device. Each original data is obfuscated using a masking sequence of same length. Upon obfuscating the entire sequence of data, user will upload both the obfuscated data and the data tag to the cloud server. Data tag is nothing but an identifier of certain original private data, which has only limited information about the original data. In the third step, profile matching is performed. This step considers two terms: threshold (n_{th}) and matching ambiguity (K_{th}). Threshold is used to describe matching criteria. It is defined as the minimum number of same bits in two scrambled sequences. Matching ambiguity is the ratio between threshold and original data's length.

The key idea behind friend matching process is to find out the number of mutual friends between them. Inorder to perform a

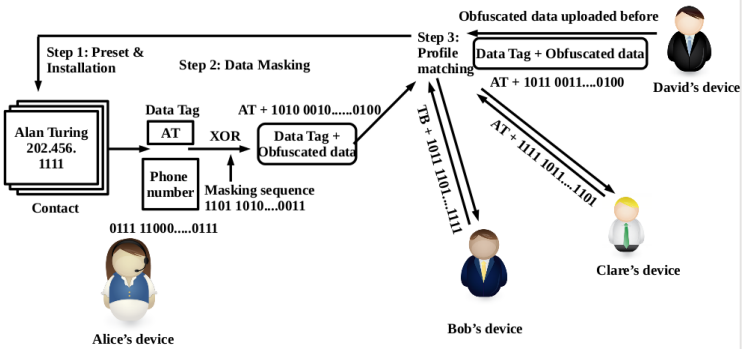

Figure 2. SPFM Protocol [12]

friend matching, cloud server uses both the obfuscated sequence of data and the data tag for matching. The server goes through both the user's data tags and finds out all the same data tags. For one of the same data tags, it performs XOR operation between the data tag and the corresponding obfuscated data are performed. If the number of zeroes in the XOR result is greater than the threshold value, server considers that the original data of both users are the same. After a thorough traversal through all the data tags, server will get an idea about the number of mutual frirends between them. The server thus judges whether both the users are friends in reality.

D. Energy-Efficient Quality-of-Service Architecture (EEQoSA)

One of the critical challenge for MCC is the flexible nature of the mobile devices. The mobile device may rapidly change its location from one base station area to another resulting in frequent handover sessions. While initiating a handover process, the mobile device significantly degrades its performance. In [13], a multi-service handoff mechanism using Session Iniation Protocol (SIP) is used inorder to make all the services active during handoff and ensures an energy-efficient QoS [14] architecture for MCC. Also a rapid and seamless handover mobile IPv6 (FHIPv6) is introduced to support mobility management. This architecture consists of four layers:

- Application layer
- Internet Protocol Multi-media Subsystem (IPMS) layer
- Communication layer
- Media with Connectivity Layer (MCL)

Application layer consists of Home Subscriber Station (HSS) which interconnects the cloud servers as an enterprise server and links to the IPMS layer inorder to maintain data communication successfully. HSS consists of Subscriber Related Information (SRI), Location Update (LU) severs and role managers, which stores mobile cloud user profiles and user's current location respectively. IPMS layer provides services such as video conferencing, VoIP services, e-mail, internet and web browsing. A Call Session Control Function (CSCF) is used to bind a public user identity to IP address of the mobile device. A Strong and Secure Authentication (SSA) is performed in this layer to protect its services. Authentication key is fragmented and distributed to different cloud servers. Hence it is difficult for an adversary to

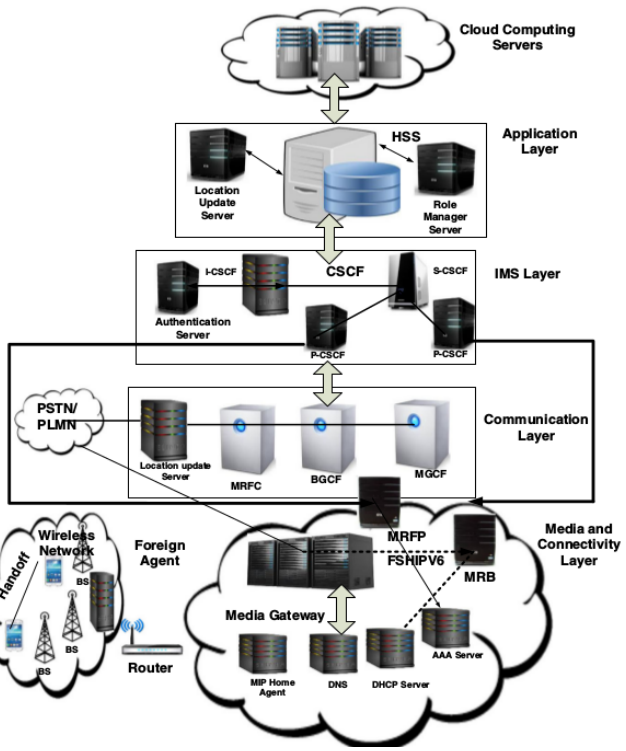

Figure 3. EEQoS Architecture [13]

capture tha authentication key. Eventhough an adversary obtains the fragments of the key, it is not possible for them to identify the key pattern. Communication layer provides data routing functions and also synchronises MCL and IPMS layers. MCL provides media and connectivity related services. This layer is comprised od Media Resource Function Controller (MRFC) and Media Resource Agent (MRA). MRA is coupled to the DHCP servers to support handover process. Media gateway is linked to the DNS servers.

A handover process in [13] includes two states: Peridic Re-Registration (PRR) and Re-registration Change Capabilities (RCC). A timer is kept ON during both the states. In PR, the mobile device is attached to the same Base Station (BS) area until it becomes attached with another BS inorder to keep sending the data. This state aims to identify whether the mobile device is still registered with the home network. Whenever the registration tim er times out, PR initiates re-registration process. In RCC, mobile user uses the utility services and gets attached with another BS. Inorder to efficiently initiate new session, atimer is require for both PR and RCC. Since IPMS refreshes the registration timer during session establishment process and cloud server access, time consumed by PR is also reduced.

E. Autonomic Mobile Cloud (AMCloud)

Most of the popular cloud computing models are very expensive since they uses expensive and dedicated machines to provide the cloud computing services. A cost-effective solution is to use ad hoc which consists of a cloud of distributed and dynamically untapped local resources. Due to the distributed and dynamic nature of ad hoc mobile cloud computing networks,

existence of such a system has become one of the major challenge. Autonomic Mobile Cloud (AMCloud) management framework is implemented in [15], which ensures efficient working of an ad hoc mobile cloud. AMCloud is closely related to the work done in [16]. Figure 4 shows an AMCloud management framework in which the cloud applications are created and controlled by a Mobile Cloud Application Enabling Fabric. It is a composition of manageable autonomic cloud elements. Each element basically virtualizes physical resources according to monitor, analyse, plan and execute control loop.

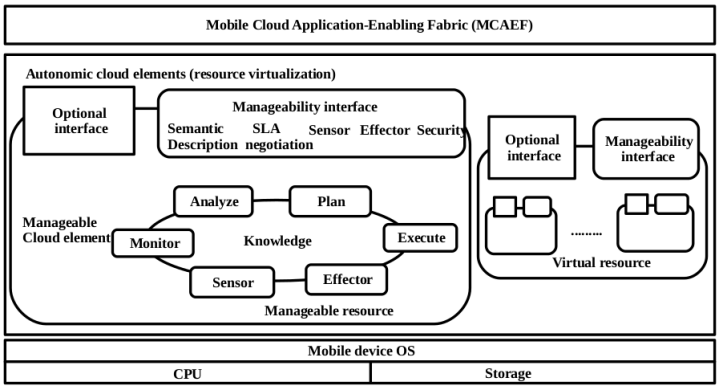

Figure 4. AMCloud Management Framework [15]

Security framework for AMCloud is shown in figure 5. The architecture consists of two layers: Device layer and Communication layer. Each layer is composed of several security components. The components in device layer includes task/application isolation, intrusion detection system and secure key storage. These components helps to prevent the user's private data from leaking to the cloud. They also prevents malicious malware from damaging cloud user's devices. Secure key storage component imposes an extra layer of protection for encryption keys, account passwords, etc.

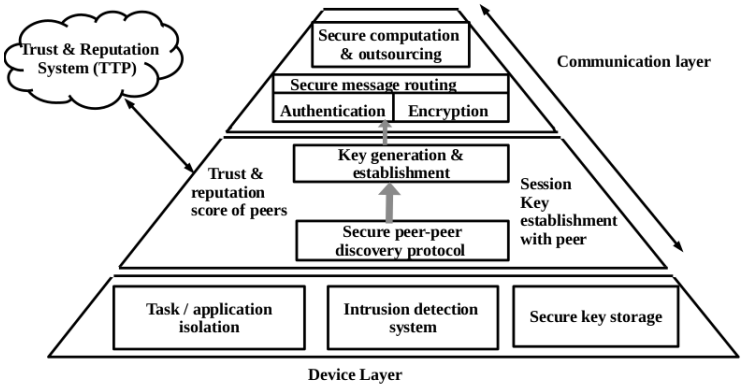

Figure 5. Security Architecture [15]

The moment when a user joins an ad hoc cloud, communication layer protection is started. The first step is a peer discovery phase in which the user wisely choose their cloud task participants by eliminating malicious or misbehaving users based on information from the trust and reputation system. This phase is followed by key generation and establishment phase in which a session key for cloud is established among all the cloud users. This key is used to encrypt private data and hence provide confidentiality and integrity while transferring cloud data.

III. DISCUSSIONS AND FINDINGS

MCC has gained more and more attention in recent years. Hence various issues related to this environment was studied in this survey. There exists several systems which overcomes the challenges faced by MCC. Recently, MDA [9] has been proposed as a technique to ensure confidentiality and privacy for user information. The use of hashing algorithm SHA 1 in this method ensures security and implicitly provides integrity check. This method is vulnerable to any kind of mobile devices since system specific properties like IMSI are not used. Since each time a mobile user has to register with the cloud server, this technique cannot be used in a distributed MCC environment. This system is not able to meet the need of users who generally access different kinds of mobile cloud services from a variety of service providers. It is extremely tedious task for users to register with the server each time they need to access service from the cloud server. A privacy-aware authentication scheme in [11] can be considered as a solution for this challenge. Here, a trusted third party server is assigned for registration process. Since the trusted SCG service is not involved in individual authentication process, authentication processing time is reduced. Nonce generation used in this scheme makes MCC more secure. But since pairing based cryptosystem is significantly losing its advantages, this cannot be considered as an efficient implementation.

A novel solution for the issue raised by friend matching process in mobile cloud was presented in [12]. SFPM protocol aims at exposing only an identifier of user's personal information to the "honest-but-curious" cloud server. Eventhough this technique prevents the issue of personal data outsourcing, in some cases it is possible for an adversary to obtain the private data by performing mathematical computations. The energy-efficient architecture in [13] is a solution for performance degradation of the mobile devices during handover process. But the implementation of such an architecture is expensive since it requires a cluster of expensive and dedicated machines. Nowadays, ad hoc mobile cloud computing models are becoming popular because of their cost-effectiveness. The AMCloud architecture implemented in [15] provides automatic and efficient service management of ad hoc cloud. A comparison of the security frameworks discussed in this paper are shown in the table III.

TABLE I
COMPARISON

System	[9]	[11]	[12]	[13]	[15]
Confidentiality	Yes	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes	Yes
Privacy	Yes	Yes	Yes	Yes	Yes
Energy-efficient	No	No	No	Yes	No
Cost-effective	No	No	No	No	Yes

In todays fast faced technology, WI-FI direct widely used as a way to share data between mobile devices. In this scenario with higher mobility, Key management has become a critical problem. Hence, a proper key management scheme with key updation is of critical importance. This can be built on top of the AMCloud security arcitecture. Eventhough various systems exists which aims at the security of MCC, attckers find ways to intrude in one or the other way. Security techniques need to evolve continuously to meet ever changing technology and service offerings.

IV. CONCLUSION

MCC has become popular with the increased use of mobile devices and the emergence of cloud computing. Eventhough this technology provides a platform for accessing remote services. The most challenging aspects in MCC are guaranteeing user privacy and the provision of mobile application security that uses cloud resources. Despite the advantages, MCC raises several issues. The objective of this survey was to study various security threats faced by MCC and the techniques implemented to recover from them. Today's fast faced technology has lead MCC towards a secure, energy-efficient and cost-effective environment. Eventhough different systems exists which aims at the security of mobile cloud computing, there are still significant security challenges in its development. The security threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. Security techniques need to evolve continuously to meet ever changing technology and service offerings.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, and R. Buyya (2013) "Dynamically scaling applications in the cloud", *ACM SIGCOMM Computer Communication Review*, vol. 41, pp. 45-52.

[2] Guan L, Ke X, Song M, Song J (2011) "A Survey of Research on Mobile Cloud Computing", *In: IEEE/ACIS International Conference on Computer and Information Science*, pp. 387-392.

[3] Yuan H, Kuo C-CJ, Ishfaq A (2010), Energy efficiency in data centers and cloud-based multimedia services: An overview and future directions", *In: Green Computing Conference*, 2010 International, pp. 375-382.

[4] Popovic K, Hocenski Z (2010) "Cloud computing security issues and challenges", Vol. 2010.

[5] Sanaei Z, Abolfazli S, Gani A, Buyya R (2014) "Heterogeneity in mobile cloud computing: taxonomy and open challenges", *IEEE Communications Surveys Tutorials*, pp. 369-392.

[6] Abolfazli S, Sanaei Z, Ahmed E, Gani A, Buyya R (2014) "Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges", *IEEE Communications Surveys Tutorials*, pp. 337-368.

[7] Qi H, Abdullah G (2012) "Research on mobile cloud computing: Review, trend and perspectives", *In: Digital Information and Communication Technology and it's Applications (DICTAP)*, 2012 Second International Conference, pp 195-202.

[8] L. Wei et al (2014) "Security and Privacy for Storage and Com- putation in Cloud Computing", *Information Sciences*, Vol. 258, pp. 371-86.

[9] Saurabh Dey, Srinivas Sampalli, Qiang Ye (2016) "MDA: Message Digest based Authentication for mobile cloud computing", *Springer Journal of Cloud Computing: Advances, Systems and Applications*.

[10] Ahmad Z, Mayes KE, Dong S, Markantonakis K (2011) "Considerations for mobile authentication in the Cloud", Inf Secur Tech Rep 16(3-4): 123-130, ISSN 13634127.

[11] Jia-Lun Tsai, Nai-Wei Lo (2015) "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", *IEEE Systems Journal*, Vol. 9, Issue 3.

[12] Mengyuan Li, Ruan Na, QiYang Qian, Haojin Zhu, Xiaohui Liang, Le Yu (2017) "SPFM: Scalable and Privacy-preserving Friend Matching in Mobile Cloud", *IEEE Internet Of Things Journal*, Vol. 4, issue 2.

[13] Qassim Bani Hani, Julius P Dichter (2017) "Energy-efficient Service-oriented Architecture for Mobile Cloud Handover", *Springer Journal of Cloud Computing: Advances, Systems and Applications*.

[14] Marquez-Barja J, Calafate CT, Cano J-C, Manzoni P (2011) "An overview of vertical handover techniques:Algorithms, protocols and tools", *Comput Commun*, pp. 985-997.

[15] Devu Manikantan Shila, Wenlong Shen, Yu Cheng, Xiaohua, Xuemen (Sherman) Shen (2017) "AMCloud: Toward a Secure Autonomic Mobile Ad Hoc Cloud Computing System", *In: IEEE Wireless Communications*, Vol. 24, issue 2.

[16] Y. Cheng, A. Leon-Garcia, and I. Foster (2008) "Towards an Autonomic Service Management Framework: A Holistic Vision of SOA, AON, and Autonomic Computing", *IEEE Commun. Mag*, vol. 46, pp. 138-46.