2021 International Conference on Signal Processing and Machine Learning (CONF-SPML) | 978-1-6654-1734-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/CONF-SPML54095.2021.00032

A Survey of Security Issues in Mobile Cloud Computing

Zimutian Yang
Department of Information
Beijing City University
Beijing, China
zimutianyang@163.com

***Abstract*—Mobile cloud computing (MCC) has been born out of cloud and mobile computing due to the growing demand for mobile platforms. Over the past few years, MCC related work focused on building the architecture, and in recent years it had conducted major research on MCC's actual productivity and security issues. For example, intrusion detection system, location-based service, data security, etc., but there is no paper to summarize and study the security issues of the entire MCC. This paper elaborates the security issues of MCC from three levels of MCC and five security aspects, including privacy security, offloading security, authentication security, device security and other security issues. Describe the various levels of security problems and the solutions to those problems. Finally, this paper looks forward to the future development direction of MCC.**

Keywords—mobile cloud computing security, privacy security, offloading security, authentication security, device security

I. Introduction

Cloud computing and mobile computing and the integration of the Internet has given rise to mobile cloud computing (MCC), 5G development accelerated the development of MCC. It provides users with many advantages, such as storage capacity, scalability, reliability and real-time data availability, which means that users can use cloud services on mobile devices without requiring hardware specifications on the devices. In the past five years, cloud computing has been devoted to the development of frameworks. Such as the above advantages, MCC has a great space for development. For example, service providers can make use of the advantages of big data in the cloud to predict the operation of users in the mobile terminal so as to reduce the misoperation that is difficult to undo.

Back in 2013, there was an article [1] summarizing the definition, architecture, and application of early mobile cloud computing. In recent years, people began to pay attention to the security problems caused by it. Mollah et al. [2] introduced the major security and privacy challenges in this field and introduces some solutions.

In the existing studies, most of the papers have discussed the specified technology. Shamshirband et al. [3] introduced the Intrusion Detection System (IDS) and the introduction of the Intrusion Detection System (IDS) using Computational Intelligence (CI) in the mobile cloud environment. Most of the articles explain the security problems of a single aspect of MCC. Almusaylim et al. [4] introduced the location-based services (LBS) application in which MCC applications provide users with one of various services, and expounds the necessity of location privacy, the harm of disclosure and the challenges it faces. There are also articles [5] that offer helpful review results on the MCC penetration model and technology in order to overcome inherent complexity and reduce costs. Several articles have proposed MCC models for specific purpose environments to create a mature Mobile Commerce-based Safe Mobile Cloud Computing (MCSMCC) framework for mobile commerce [6]. Of course, there are also articles that point out the gap between the existing theory and the actual implementation. Annane et al. [7] explained that in terms of virtualization, malicious users can destroy cloud security methods by spreading their VMs. By analyzing these methods, it can be found that when distributed VMs deployed on different cloud servers exchange data, there is no method that can prevent data theft. However, most of the current studies are still difficult to describe the specific security issues in a comprehensive way.

The Contributions of this study have the following two points: 1) In order to describe the problem more clearly and more simplified, the three layers of MCC are summarized; 2) Starting from the three levels of MCC, this paper systematically summarizes the security issues of MCC, which can be divided into five aspects, including privacy security, offloading security, authentication security, device security and other security problems.

The structure of this article is as follows: Chapter 2 summarizes the three levels of MCC; Chapter 3 describes the security risks existing in each layer from five security aspects, and elaborates on the problems encountered and their corresponding solutions; Chapter 4 summarizes and prospects the development of MCC.

II. Overview of Security in MCC

Mobile cloud computing is divided into the following three layers (Fig. 1).

- Mobile User Layer.

This Layer is composed of Mobile devices (such as Mobile phones or tablets), which are connected to the Mobile Network Layer through WiFi, LTE, 5G and other channels.

- Mobile Network Layer.

This Layer is composed of the operator base station, accepts and processes the request of the Mobile User Layer, and finally connects and sends the request to the Cloud Services Layer and processes the required data back to the Mobile User Layer.

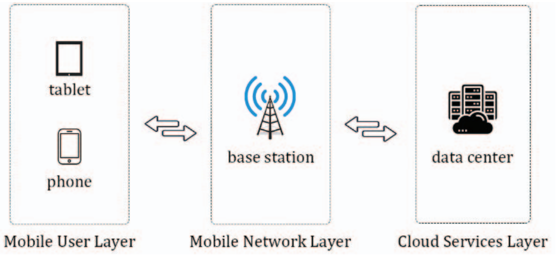

Fig. 1. The three layers of MCC

- Cloud Services Layer.

This layer is composed of cloud computing providers, providing elastic cloud computing services similar to traditional clouds, and sending demand back to the mobile network layer.

Devices in the Mobile User Layer are mainly managed by users and run applications connected to the cloud, which may have malicious software installed to leak the User's CAPTCHA and lead to the disclosure of User rights. Of course, users on this layer may suffer phishing attacks or social engineering attacks, leading to the opening of insecure websites or files and the device being hacked.

The Mobile Network Layer is mainly responsible for data transmission, and all data are input and output from this Layer. Due to the insecure factor of authentication measures, it is likely to be attacked by man-in-the-middle. The data are exchanged from a single node, which makes the devices in this Layer have too much data, and there are insecure factors. At the same time, the privacy data exchange transfer of legitimate users is also in this layer, which is likely to become the target of attackers, resulting in the violation of the confidentiality and privacy of the VM.

Cloud Services Layer is mainly responsible for by the service Provider, which may be subject to DDoS attack, causing the Mobile Network Layer to be unable to connect to this Layer, thus causing the user's request to be unable to respond. The insecure factors of its internal authority management may also make the attacker launch an overreach attack, thus endangering the privacy data. In addition, applications developed by service providers that can connect to the cloud may also have security risks.

In summary, there are many security issues in MMC, we classify them as shown in the figure below:

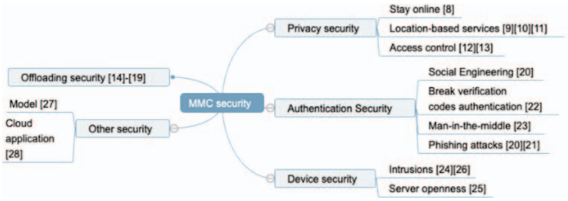

Fig. 2. MCC security classification

The structure of this article is as follows: Chapter 2 summarizes the three levels of MCC; Chapter 3 describes the security risks existing in each layer from five security aspects, and elaborates on the problems encountered and their corresponding solutions; Chapter 4 summarizes and prospects the development of MCC.

III. Security Problem

A. *Privacy security*

With the development of mobile crowd sensing systems, mobile devices (such as smartphones, smart tablets, etc.) are equipped with various sensors (such as positioning modules, accelerometers, compasses, and barometric sensors, etc.) that can collect sensory data and deliver them to the cloud. Processing to complete application functions, such as real-time navigation. Protecting the confidentiality and reliability of users' original sensory data has become a major security issue, and these methods always incur huge costs and require all participants to stay online for interaction and often use on cloud servers. Xu et al. [8] designed an effective and privacy protecting truth discovery (EPTD) method and double shielding protocol in the mobile crowd perception system. This method can tolerate the user offline at any stage, while ensuring the actual efficiency and accuracy in the process of work. Strong security for user privacy can be ensured even if the cloud server colludes with multiple users.

With the increasing demand for location by software, location-based services (LBS) have become an important application. Cloud-based location privacy protection has also become a hot topic, such as how to protect user privacy and data confidentiality. The most direct danger of location leakage is that criminals may use location information to track the parties, thereby posing a threat to personal safety. Liu et al. [9] proposed a responsible outsourcing LBS privacy protection program. In outsourcing scenarios, this solution can ensure the privacy of regional queries and improve query efficiency. It also effectively restrains the abuse of the proxy re-encryption key. Wang [10] designed LoPEC, which is a novel and effective solution to protect the location privacy of MEC equipment. They proposed a noise addition method for fingerprint data through the correct model of the Radio Access Network (RAN) access point, and successfully induced the attacker to identify the real location. LoPEC effectively prevents attackers from obtaining accurate user positions in single point and trajectory scenarios. Shen et al. [11] designed a lightweight privacy protection solution. This scheme uses homomorphic encryption and random replacement methods to protect the location privacy of mobile users. Security analysis shows that the scheme can protect privacy under a certain defined threat model.

Since data users can access shared data through mobile devices anytime and anywhere, it increases the convenience and flexibility of data access through cloud computing. However, it is impractical to use mobile devices to access shared data in the cloud that encrypts sensitive data, because the computing resources of mobile devices are limited when processing heavy encryption operations. Fugkeaw et al. [12] proposed an encryption scheme based on lightweight collaborative ciphertext policy attributes to support fine-grained and lightweight access control for mobile cloud environments. A security access policy sharing and re-encryption protocol has been developed to enable users with write privileges to update data and request the agent to perform data re-encryption.

In all the security specifications of cloud computing, access control is only one of the basic requirements to prevent unauthorized system access and protect organizational assets. Cloud computing has a set that varies with various security condition units. Moreover, it has unique security, such as the heterogeneity of security domains, rules and policies, and multi-tenant hosting. This resulted in the existing model not being able to meet the demand. Three models are proposed to enhance access control of sensitive data. Information gain is used to calculate data sensitivity[13]. The second data similarity calculation, the Siamese neural network, is used to consider semantic similarity. Considering the classification process of classifying information (or allowable data sets) based on data sensitivity and similarity, this model is proposed as an SNN with an MLP classifier.

Due to the limited computing resources and capabilities of mobile devices, cloud computing cannot perform synchronous data access. Therefore, for mobile cloud applications, low-computing security solutions are very much needed. Bhargavi et al. [13] proposed a lightweight data sharing solution (LDSS) for mobile cloud computing, in order to adapt to the mobile cloud environment, the structure of the access control tree in the ordinary cloud environment was changed.

B. *Offloading security*

When data is migrated from the mobile terminal to the cloud, the data may be stolen and security will be affected. Many studies have shown that sensitive data in a legitimate user's virtual machine is likely to be the target of an attack, leading to violations of the confidentiality and privacy of the virtual machine. Annane et al. [14] proposed a new security agent-based method for mobile cloud, including three strategies of user access control based on secure hash Diffie-Hellman keys, VM deployment, and communication control management. This method performs three well-known attacks (coexistence attacks, hypervisor attacks, and distributed attacks) in a defense environment. The article introduces a new NetworkCloudSim extension called SecNetworkCloudSim [15], which is a secure mobile simulation tool designed to ensure that confidential access to data hosted on mobile devices and distributed cloud servers is preserved. Abd Elminaam et al. [16] proposed a new elastic framework, called the Security Framework for Using Cloud Computing to Enhance Mobility Capability (SMCACC), which can transparently use cloud resources to enhance the functions of resource-constrained mobile devices. Considering that the hybrid encryption method is used to protect data and consider energy consumption, the newly proposed security protocol uses a combination of symmetric and asymmetric cryptographic techniques to avoid the shortcomings of the existing hybrid protocol. These methods help protect users by protecting data that is offloaded to the cloud. Combining Advanced Encryption Standard (AES), Secure Hashing Algorithm (SHA-256) and Diffie-Hellman key exchange technology, Karthikeyan et al. [17] proposed a novel offloading algorithm to improve the security of mobile cloud computing (MCC). Compared with other security algorithms, it has higher energy efficiency and better security. In the paper [18] of Munivel et al., a new security protocol [19] is used to verify mobile and cloud servers using zero-knowledge authentication to verify communication entities and recommend offload the service.

C. *Authentication Security*

The insecurity of the wireless channel makes it vulnerable to various attacks, which poses a great threat when transmitting sensitive data. Therefore, how to create a security mechanism session between the Mobile User Layer and the Cloud Services Layer has aroused interest. Phishing attacks are one of the serious threats to smartphone users. This kind of social engineering attack attempts to obtain private information such as the user's password by pretending to be a trusted service provider. Mo et al. [20] proposed an effective anonymous two-factor user authentication protocol for the mobile cloud computing environment. This scheme not only provides safer and more effective mutual authentication between mobile devices and cloud computing, but also meets known security evaluation standards, and the formal security proof shows that the scheme is safe under the random oracle model. In order to protect data transmission in MCC, Ahmed et al. [21] proposed a dynamic reciprocal authentication protocol. The protocol is not restricted by Diffie-Hellman and uses a secure point-to-point authentication method, and is not affected by basic or complex known attacks.

In order to prevent this kind of password attack in the mobile cloud environment. Munivel et al. [19] proposed a new identity verification scheme that can provide mutual authentication between communicating entities to provide novel security for mobile cloud services. The program would use a zero-knowledge proof-based authentication protocol to authenticate users and service providers without the need to transmit passwords.

Nowadays, we often use SMS verification codes for verification operations, but some security analysts have indicated that the mobile two-factor authentication program may be broken. Derhab et al. [22] proposed a smart virtual card, which is a new two-factor mutual authentication scheme, and also proposed a new offloading architecture for two-factor mutual authentication of applications. Based on the three conditions of security, remaining energy of the mobile device and energy cost, a decision-making process for uninstalling the identity verification application and its virtual smart card is proposed. The article also analyzed the security of the architecture and provided the evaluation results.

Mobile cloud computing has mobile resource management (MRM), and the storage and computing resources of nearby mobile devices are stored in the resource pool. Since mobile devices can access MRM at any time, identity verification is required to determine resources and visitor information. Due to the vulnerability of man-in-the-middle (MITM) attacks and tampering, Kim et al. [23] proposed a human-centered security authentication management scheme (SAMS), which uses blockchain technology for identity verification and makes it trusted to participate in the resource pool. This solution forms a blockchain based on the resource information of the client nodes around the master node in the MRM, and these unauthorized devices cannot forge or access data.

D. *Device Security*

Some existing intrusion detection methods still have some limitations, such as high false positive rate, low classification accuracy rate, and low true positive rate. In view of these limitations, Mugabo et al. [24] proposed an intrusion detection method based on support vector machine (SVM) and information gain (IG). This method uses a support vector machine classifier to classify network data into normal behavior and aggressive behavior, and uses IG to select relevant features and remove unnecessary features. The effectiveness of the method is also evaluated, and the results show that the method can solve the problems and the training speed is fast.

Cloud computing is different from traditional computing in that jobs run on cloud programs instead of locally. This means that the cloud program is open to the Internet, so the attacker can also access him, which will affect the security. Distributed denial of service (DDoS) attacks are common attacks that will have a great impact on the security of mobile cloud computing. The main purpose is to infect the device resource pool, overload the service or make it impossible for authorized users to use it normally. To solve this problem, El-Sofany et al. [25] introduced a new model that can protect the system from DDoS attacks. Analyzing the performance and efficiency of the model and finding that the results are very promising, mobile-based cloud computing systems can be protected from DDoS attacks.

No matter whether it is on mobile devices or cloud infrastructure, intrusions may occur, and most existing solutions require real-time connection to the cloud. Ogwara et al. [26] proposed a method called MINDPRES (Mobile Cloud Intrusion Detection and Prevention System) that uses machine learning (ML) technology to combine host-based IDS and network-based IDS. It dynamically analyzes equipment resources and network traffic to detect UL's malicious activities in the MCC environment. In this model, the detection engine resides at the local device level. This eliminates the limitations of real-time connections.

E. Others

With the similar challenges that mobile cloud computing (MCC) can overcome the limitations of battery life, processing power and security in mobile communications, security is still the main challenge that MCC needs to solve. Kandavel et al. [27] proposed a novel Royal Seal Cloudlet (NRSC) that works based on a specific random private token of a trusted user. The cloudlet uses an end-to-end mobile cloud connection to provide improved security services and environments. A simulation study on cloudlet's security function shows that this method enhances the network service quality and provides complete end-to-end security and reliability.

In order to use mobile cloud computing technology, users need to install applications, which allows attackers to develop programs with malicious code to achieve the purpose of the attack. This requires consideration of security threats before installation. In characterizing application behavior characteristics, resource access is an important feature used to detect malicious programs. The model proposed by Nisha et al. uses the social spider algorithm (SSA) to select the optimal permission feature set and uses classification techniques to detect malicious applications [28]. Experimental results show that the algorithm has excellent performance.

IV. Discussion

Through the research of this article, prior to 2015, the MCC framework was taken seriously. Nowadays, the security issues of MCC are taken seriously. Among the many issues raised, the security issues involving privacy are the most. The ultimate focus of most security issues is how to protect privacy. The security issues of concern are how to ensure that users can use the service stably and how to ensure that users are not deceived by illegal programs. Although the current solutions cover most of the security aspects, there is still little research. Some papers simulate the proposed ideas, and a few papers are deployed and verified in a virtual environment, but they have greater limitations. In the future, MCC still has a lot of room for development, and security issues need to be improved before it can be used, so as to fully demonstrate the functions of Mobile Cloud Computing.

V. Conclusion

As far as we know, this paper is the first time to systematically provide the survey of the research of the security MCC base on the MCC architecture. In this paper, Mobile Cloud computing is divided into Mobile User Layer, Mobile Network Layer and Cloud Services Layer, and the function of each Layer and the possible security problems are described. The security problems are divided into privacy security, offloading security, authentication security, device security and others, and the specific security problems that may occur among them are elaborated in detail and the existing solutions are provided.

References

[1] Dinh, T. Hoang et al. "A survey of mobile cloud computing: architecture, applications, and approaches." Wireless communications and mobile computing 13.18 (2013): 1587-1611.

[2] Mollah, Muhammad Baqer, Md Abul Kalam Azad, and Athanasios Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead." Journal of Network and Computer Applications 84 (2017): 38-54.

[3] S. Shamshirband, M. Fathi, and A. T. Chronopoulos et al., Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues, Journal of Information Security and Applications, 2020, 55: 102582.

[4] Z. A. Almusaylim, N. Z. Jhanjhi, Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing, Wireless Personal Communications, 2020, 111(1): 541-564.

[5] A. S. Al-Ahmad, H. Kahtan, F. Hujainah et al., Systematic literature review on penetration testing for mobile cloud computing applications, IEEE Access, 2019, 7: 173524-173540.

[6] Al_Janabi, Samaher, and Nawras Yahya Hussein, "The reality and future of the secure mobile cloud computing (SMCC): survey." International Conference on big data and networks technologies. Springer, Cham, 2019.

[7] B. Annane, A. Alti, O. Ghazali, Research gaps based virtualization in mobile cloud computing, International Journal of Advanced Computer Research, 2020, 10: 51.

[8] G. Xu, H. Li, S. Liu et al., Efficient and privacy-preserving truth discovery in mobile crowd sensing systems, IEEE Transactions on Vehicular Technology, 2019, 68(4): 3854-3865.

[9] Z. Liu, L. Wu, and J. Ke et al., Accountable outsourcing location-based services with privacy preservation, IEEE Access, 2019, 7: 117258-117273.

[10] Y. Wang, Z. Tian, S. Su et al., Preserving location privacy in mobile edge computing//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.

[11] H. Shen, M. Zhang, H. Wang et al., A lightweight privacy-preserving fair meeting location determination scheme, IEEE Internet of Things Journal, 2020, 7(4): 3083-3093.

[12] Fugkeaw, Somchart. "A Fine-Grained and Lightweight Data Access Control Model for Mobile Cloud Computing." IEEE Access (2020).

[13] P. Bhargavi , D. Murali, and M. V. Ramesh, "Providing Key Exposure to Enabling the Cloud Data Service Security."

[14] B. Annan, O. Ghazali, A. Alti, A new secure proxy-based distributed virtual machines management in mobile cloud computing, International Journal of Advanced Computer Research, 2019, 9(43): 222-231.

[15] B. Annane, A. Alti, and O. Ghazali, Secnetworkcloudsim: an extensible simulation tool for secure distributed mobile applications, International Journal of Communication Networks and Information Security, 2020, 12(1): 47-62.

[16] D. S. Abd Elminaam, F. T. Alanezi, K. M. Hosny, SMCACC: Developing an Efficient Dynamic Secure Framework for Mobile Capabilities Augmentation Using Cloud Computing, IEEE Access, 2019, 7: 120214-120237.

[17] B. Karthikeyan, T. Sasikala, S. B. Priya, Key exchange techniques based on secured energy efficiency in mobile cloud computing, Applied Mathematics & Information Sciences, 2019, 13(6): 1039-1045.

[18] E. Munivel, A. Kannammal, "Secure Authentication Protocol for Efficient Computational Offloading Service in the Mobile Cloud Computing," Journal of Internet Technology 21.2 (2020): 457-467.

[19] Munivel, E., and A. Kannammal. "New authentication scheme to secure against the phishing attack in the mobile cloud computing." Security and Communication Networks 2019 (2019).

[20] Mo, Jiaqing, et al. "An efficient and provably secure anonymous user authentication and key agreement for mobile cloud computing." Wireless Communications and Mobile Computing 2019 (2019).

[21] Ahmed, Abdulghani Ali, et al. "Dynamic Reciprocal Authentication Protocol for Mobile Cloud Computing." IEEE Systems Journal (2020).

[22] Derhab A, Belaoued M, Guerroumi M, et al. Two-factor mutual authentication offloading for mobile cloud computing[J]. IEEE Access, 2020, 8: 28956-28969.

[23] Kim, Hyun-Woo, and Young-Sik Jeong. "Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain." Human-centric Computing and Information Sciences 8.1 (2018): 1-13.

[24] Mugabo, Emmanuel, and Qiu-Yu Zhang. "Intrusion Detection Method Based on Support Vector Machine and Information Gain for Mobile Cloud Computing." IJ Network Security 22.2 (2020): 231-241.

[25] El-Sofany H, Abou El-Seoud S. A Novel Model for Securing Mobile-based Systems against DDoS Attacks in Cloud Computing Environment[J]. 2019.

[26] Ogwara, Noah Oghenfego, et al. "Enhancing Data Security in the User Layer of Mobile Cloud Computing Environment: A Novel Approach." arXiv preprint arXiv:2012.08042 (2020).

[27] Kandavel, N., and A. Kumaravel. "A Novel Royal Seal Cloudlet for Security Enhancement in Mobile Cloud Computing." International Journal of Computer Science and Information Security (IJCSIS) 17.1 (2019).

[28] Nisha, OS Jannath, and S. Mary Saira Bhanu. "Detection of malware applications using social spider algorithm in mobile cloud computing environment." International Journal of Ad Hoc and Ubiquitous Computing 34.3 (2020): 154-169.