Journal of Advanced Research in Embedded System
Volume 10, Issue 1 - 2023, Pg. No. 17-20
Peer Reviewed Journal

Review Article

Security Challenges and Solutions in Mobile Cloud Computing Environments: A Review

Ravneet Kaur[1], Gagandeep Kaur[1]

[1]PG Student, Chandigarh Group of Colleges Jhanjeri, Mohali, Punjab, India.

I N F O

Corresponding Author:
Ravneet Kaur, Chandigarh Group of Colleges Jhanjeri, Mohali, Punjab, India.
E-mail Id:
ravneetkaur9017@gmail.com
Orcid Id:
https://orcid.org/0009-0001-5212-3788
How to cite this article:
Kaur R, Kaur G. Security Challenges and Solutions in Mobile Cloud Computing Environments: A Review. *J Adv Res Embed Sys* 2023; 10(1): 17-20.

Date of Submission: 2023-04-10
Date of Acceptance: 2023-04-20

A B S T R A C T

Mobile cloud computing (MCC) is a rapidly emerging technology that integrates cloud computing into mobile devices. MCC provides a promising approach to satisfy the increasing demands of mobile users for high computing power, storage, data processing. However, the security challenges in MCC are becoming more complex due to the heterogeneity of mobile devices and the distributed nature of cloud services. This review paper discusses the various security challenges that arise in MCC environments, such as data privacy, access control, data integrity, confidentiality. Moreover, this paper provides a comprehensive overview of the recent advances in security solutions to mitigate these challenges.

Keywords: Mobile Cloud Computing, Security Challenges, Data Privacy, Access Control, Security Solutions

Introduction

Mobile Cloud Computing (MCC) is a technology that allows mobile devices such as smartphones and tablets to access computing resources over the internet. This computing power is provided by remote servers located in data centers, also known as the cloud.[1-4] With MCC, mobile devices can use the cloud to perform tasks that would typically require powerful hardware and processing capabilities, such as video editing, gaming, data analysis.[5-8] This technology has become increasingly popular due to the growth in mobile device usage and the need for more computing power and storage capacity.[9-10] MCC combines the benefits of cloud computing, such as high computational power and storage capacity, with the mobility and convenience of mobile devices. MCC can be used in various applications, such as mobile gaming, augmented reality, remote data storage.[11-13]

However, security is a critical concern in MCC. Due to the inherent characteristics of mobile devices and cloud computing, MCC is susceptible to various security threats, such as data breaches, unauthorized access, malware attacks. Furthermore, the distributed nature of MCC environments makes it challenging to manage and secure the system. Thus, ensuring the security of MCC systems is essential to protect users' sensitive data and maintain the integrity and availability of the system.[14-17 2.]

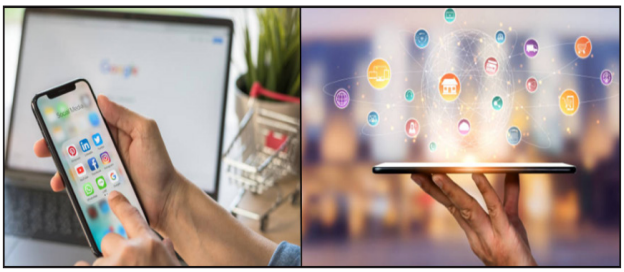

Figure 1.Concept of cloud computing

Security challenges in MCC

Mobile Cloud Computing (MCC) provides a flexible and scalable platform for delivering a wide range of mobile applications and services to users. However, with the growing popularity of MCC, there are several security

Copyright (c) 2023: Author(s). Published by Advanced Research Publications

challenges that must be addressed to ensure the safety and privacy of user data. Some of the major security challenges in MCC environments include:

- **Data Privacy Challenges:** MCC environments often involve the transfer and storage of sensitive user data, such as personal information, financial details, health records. Ensuring the privacy of such data is crucial to prevent identity theft, financial fraud, other cybercrimes
- **Access Control Challenges:** MCC environments require effective access control mechanisms to prevent unauthorized access to sensitive data and resources. However, due to the diverse range of devices and users accessing the system, implementing robust access control policies can be challenging
- **Data Integrity Challenges:** Maintaining data integrity in MCC environments is critical to ensure the accuracy and consistency of data. However, due to the distributed nature of cloud computing and the high mobility of devices, ensuring data integrity can be challenging
- **Confidentiality Challenges:** MCC environments require confidentiality mechanisms to protect sensitive data from unauthorized access or disclosure. However, implementing effective confidentiality measures can be challenging due to the diverse range of devices and communication channels involved
- **Network Security Challenges:** MCC environments are vulnerable to a wide range of network-based attacks, such as man-in-the-middle attacks, phishing, denial-of-service (DoS) attacks. Implementing effective network security measures is essential to prevent these types of attacks
- **Application Security Challenges:** MCC environments involve the use of a wide range of mobile applications and services, many of which may be developed by third-party developers. Ensuring the security of these applications is critical to prevent data breaches and other security incidents
- **Device Security Challenges:** MCC environments involve the use of a wide range of mobile devices, each with its own security features and vulnerabilities. Ensuring the security of these devices is critical to prevent unauthorized access to sensitive data and resources

Overall, addressing these security challenges is essential to ensure the safety and privacy of user data in MCC environments. This can be achieved through the use of a range of security technologies and best practices, such as encryption, authentication, access control, network security monitoring.[18-24]

Security Solutions in MCC

There are several security solutions that can be implemented to address the challenges in MCC. Some of these solutions include:

- **Encryption:** Data encryption is a widely used solution to protect data privacy and confidentiality in MCC. Encryption algorithms can be used to protect data both in transit and at rest, can be implemented at various levels, such as application, network, or storage
- **Access Control:** Access control solutions can be used to ensure that only authorized users can access data in MCC environments. This can be achieved through techniques such as multi-factor authentication, identity and access management, role-based access control
- **Secure Data Storage:** Data stored in the cloud can be protected using various solutions such as encryption, secure key management, secure storage systems
- **Secure Data Transmission:** Data transmitted between mobile devices and cloud servers can be protected using secure communication protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL)
- **Data Backup and Recovery:** Data backup and recovery solutions can be implemented to ensure that data can be restored in the event of data loss or system failure
- **Continuous Monitoring and Threat Detection:** Continuous monitoring and threat detection solutions can be implemented to detect and respond to security threats in real-time, reducing the impact of security breaches

By implementing these solutions, organizations can address the security challenges in MCC and ensure the confidentiality, integrity, availability of their data in the cloud.[25-30]

Recent Advances in Security Solutions for MCC

In recent years, several security solutions have been proposed to address the challenges faced in MCC. In this direction following developments have been made:[31-35]

- One of the significant developments in this area is the integration of blockchain technology with MCC to enhance security and privacy. Blockchain provides a decentralized and immutable ledger that can prevent data tampering and unauthorized access
- Another advance is the use of machine learning algorithms for detecting and preventing security threats in real-time
- Also, the use of biometric authentication and encryption techniques has gained popularity in securing the communication between mobile devices and cloud servers

Importance of Addressing MCCSecurity Challenges

Mobile cloud computing (MCC) has become an essential component of modern-day computing, with its ability to provide ubiquitous access to services and resources. However, with the benefits of MCC, there come security

challenges that can put the privacy and security of users' data at risk. Addressing these challenges has become an urgent necessity, given the increasing reliance on MCC in our daily lives.

The importance of addressing MCC security challenges lies in the need to ensure the confidentiality, integrity, availability of data and services. With MCC, data is stored and processed remotely, this introduces a new set of risks that need to be addressed. These risks include data breaches, unauthorized access, data loss, other security threats.

The impact of a security breach in MCC can be significant, affecting both individuals and organizations. For individuals, data breaches can result in the loss of personal information, financial loss, reputational damage. For organizations, a security breach can result in financial loss, loss of intellectual property, damage to their reputation.

Therefore, it is essential to address MCC security challenges to ensure the privacy and security of data, which is critical in building trust among users and enhancing the adoption of MCC services.

Future Directions

The field of MCC security is continuously evolving due to the increasing use of mobile devices and cloud computing services. One promising area of future research is the development of secure and privacy-preserving data sharing mechanisms in MCC environments. Additionally, research can focus on designing efficient access control mechanisms that can ensure authorized access to data and services in the MCC ecosystem. Another research direction can be to investigate the impact of emerging technologies such as the Internet of Things (IoT) and edge computing on MCC security.

Conclusion

Mobile cloud computing offers numerous benefits, such as ubiquitous access to computing resources and services, but it also poses significant security challenges. In this paper, we have discussed various security challenges faced in MCC environments, including data privacy, access control, data integrity, confidentiality. We have also presented some of the recent advances in security solutions, such as blockchain, machine learning, biometric authentication, encryption techniques. Finally, we have outlined some future research directions for MCC security, emphasizing the need for privacy-preserving data sharing mechanisms and efficient access control mechanisms. Overall, addressing the security challenges in MCC is crucial to ensure the safe and secure use of mobile cloud computing services.

References

1. Kitanov S, Janevski T. State of the art: Mobile cloud computing. In 2014 Sixth International Conference on Computational Intelligence, Communication Systems and Networks 2014; 153-158. IEEE.
2. Gupta P, Gupta S. Mobile cloud computing: the future of cloud. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,* 2012; 1(3): 134-145.
3. Rahimi MR, Ren J, Liu CH. Mobile cloud computing: A survey, state of art and future directions. *Mobile Networks and Applications* 2014; 19: 133-143.
4. Padma M, Neelima ML. Mobile Cloud Computing: Issues from a Security Perspective. *International Journal of Computer Science and Mobile Computing* 2014; 3(5): 972-977.
5. Dinh HT, Lee C, Niyato D. A survey of mobile cloud computing: architecture, applications, approaches. Wireless communications and mobile computing, 13(18), 1587-1611.
6. Mishra S, Mohapatra SK, Mishra BK. Analysis of mobile cloud computing: Architecture, applications, challenges, future perspectives. In Applications of security, mobile, analytic, cloud (SMAC) technologies for effective information processing and management 2018; 81-104. IGI Global.
7. Somula RS, Sasikala R. A survey on mobile cloud computing: mobile computing+ cloud computing (MCC= MC+ CC). Scalable Computing: *Practice and Experience*, 2018; 19(4): 309-337.
8. Chuah SP, Yuen C, Cheung NM. Cloud gaming: a green solution to massive multiplayer online games. *IEEE Wireless Communications* 2014; 21(4): 78-87.
9. Qureshi SS, Ahmad T, Rafique K. Mobile cloud computing as future for mobile applications-Implementation methods and challenging issues. *In 2011 IEEE International Conference on Cloud Computing and Intelligence Systems* 2011; 467-471. IEEE.
10. Bhat MP, Alavandar SR, Ananthanarayana VS. Distributed public computing and storage using mobile devices. In 2018 IEEE Distributed Computing, VLSI, *Electrical Circuits and Robotics* (Discover) 2018; 82-87. IEEE
11. Biswas M, Whaiduzzaman MD. Efficient mobile cloud computing through computation offloading. *Int J Adv Technol* 2018; 10(2): 32.
12. Dinh HT, Lee C, Niyato D. A survey of mobile cloud computing: architecture, applications, approaches. Wireless communications and mobile computing, 2013; 13(18): 1587-1611.
13. Costa MC, Manso A, Patrício J. Design of a mobile

augmented reality platform with game-based learning purposes. *Information* 2020; 11(3): 127.
14. Shon T, Cho J, Han K, Choi H. Toward advanced mobile cloud computing for the internet of things: Current issues and future direction. *Mobile Networks and Applications* 2014; 19: 404-413.
15. Allam H, Nassiri N, Rajan A. A critical overview of latest challenges and solutions of Mobile Cloud Computing. In 2017 Second international conference on fog and mobile edge computing (FMEC) 2017; 225-229. IEEE.
16. Chaubey NK, Tank DM. Security, privacy and challenges in Mobile Cloud Computing (MCC) a critical study and comparison. *International Journal of Innovative Research in Computer and Communication Engineering* 2016; 4(2): 1259-1266.
17. Chakraborti A, Curtmola R, Katz J. Cloud computing security: foundations and research directions. Foundations and Trends® in Privacy and Security 2022; 3(2): 103-213.
18. AlAhmad AS, Kahtan H, Alzoubi YI. Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications* 2021*;* 190: 103152.
19. Qayyum R. Data security in mobile cloud computing: a state of the art review. Rida Qayyum, Hina Ejaz," Data Security in Mobile Cloud Computing: A State of the Art Review *International Journal of Modern Education and Computer Science (IJMECS)* 2020; 12(2): 30-35.
20. Almusaylim A, Jhanjhi NZ. Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. *Wireless Personal Communications* 2020; 111: 541-564.
21. Aliyu A, Abdullah AH, Kaiwartya O. Mobile cloud computing: taxonomy and challenges. *Journal of Computer Networks and Communications* 2020*;* 1-23.
22. Alnajrani HM, Norman AA, Ahmed BH. Privacy and data protection in mobile cloud computing: A systematic mapping study. Plos one 2020; 15(6): e0234312.
23. Ogwara NO, Petrova K, Yang ML. Data security frameworks for mobile cloud computing: A comprehensive review of the literature. In 2019 *29th International Telecommunication Networks and Applications Conference (ITNAC)* 2020; 1-4. IEEE.
24. Maray M, Shuja J. Computation offloading in mobile cloud computing and mobile edge computing: survey, taxonomy, open issues. Mobile Information Systems, 2022.
25. Fugkeaw S, Sanchol P. A Review on Data Access Control Schemes in Mobile Cloud Computing: State-of-the-Art Solutions and Research Directions. SN Computer Science 2022; 3: 1-11.
26. Ogwara NO, PetrovaK, Yang ML. Data security frameworks for mobile cloud computing: A comprehensive review of the literature. In 2019 *29th International Telecommunication Networks and Applications Conference (ITNAC)* 2019; 1-4. IEEE.
27. JR MN, Lutimath NM. A Review on Offloading and Security Schemes in Mobile Cloud Computing. *In Proceedings of the International Conference on Innovative Computing & Communication (ICICC)* 2021.
28. Agrawal, N. (2021). Autonomic cloud computing based management and security solutions: State-of-the-art, challenges, opportunities. Transactions on Emerging Telecommunications Technologies, 32(12), e4349.
29. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-rimy, B. A. S. (2021). Secure cloud infrastructure: a survey on issues, current solutions, open challenges. Applied Sciences, 11(19), 9005.
30. Al Nafea, R., &Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779-786). IEEE.
31. Zaid, Y. W., Cavus, N., Omonayajo, B., Şekeroğlu, B., & Al-Turjman, F. (2021, December). Deep Learning in Mobile Devices and the Blockchain Era: An Overview. In 2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era (FoNeS-AIoT) (pp. 4-8). IEEE.
32. Akhai, S. (2023). From Black Boxes to Transparent Machines: The Quest for Explainable AI. Available at: Social Science Research Network, (http://dx.doi.org/10.2139/ssrn.4390887).
33. Shokry, M., Awad, A. I., Abd-Ellah, M. K., & Khalaf, A. A. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, future vision. Future Generation Computer Systems.
34. Bronx Community College Library. (2015). Library game day: A successful campus collaboration. Urban Library Journal, 21(2), 1-14. https://academicworks.cuny.edu/bx_pubs/108/
35. Chattu VK. A review of artificial intelligence, big data, blockchain technology applications in medicine and global health. *Big Data and Cognitive Computing,* 2021; 5(3): 41.
36. Yang W, Wang S, Sahri NM et al. Biometrics for internet-of-things security: A review. Sensors 2021; 21(18): 6163.