engineering proceedings

MDPI

Proceeding Paper

Mobile Cloud Computing: A Survey on Current Security Trends and Future Directions †

Bisma Sheikh, Ayesha Butt * and Javeria Hanif

Computer Science Department, Shaheed Zulfikar Ali Bhutto Institute of Science & Technology, Hyderabad 71000, Pakistan; shaikhbisma099@gmail.com (B.S.)

* Correspondence: ayesha.butt@hyd.szabist.edu.pk

† Presented at the 2nd International Conference on Emerging Trends in Electronic and Telecommunication Engineering, Karachi, Pakistan, 15–16 March 2023.

Abstract: Mobile cloud computing (MCC) is an emerging concept that is gaining popularity in the IT sector. It is a significant topic of debate because it is being discussed as one of the most important trends for the future. After the COVID-19 pandemic, we saw the rapid emergence of mobile computing, which also created massive hype over mobile application usage. This survey paper's introduction is a literature review of the latest advanced prominent publications, highlighting its definition, infrastructure, advantages/limitations, and challenges, and is followed up with a discussion and results section, concluding with discussions on the future of MCC work that will be undertaken in the coming years.

Keywords: cloud computing; mobile cloud computing; artificial intelligence; machine learning; augmented reality; quality of services

Citation: Sheikh, B.; Butt, A.; Hanif, J. Mobile Cloud Computing: A Survey on Current Security Trends and Future Directions. *Eng. Proc.* **2023**, *32*, 22. https://doi.org/10.3390/engproc2023032022

Academic Editors: Muhammad Faizan Shirazi, Saba Javed, Sundus Ali and Muhammad Imran Aslam

Published: 11 May 2023

1. Introduction

Mobile technology combines with the cloud to offer tremendous services and extensive changes. Mobile cloud computing (MCC) aims to use cloud computing methods for processing and storing data on mobile devices. According to ABI Research, the global mobile market will reach USD 613 billion by 2025 at a CAGR of 37.8%. However, MCC raises concerns about data and resource privacy, particularly in virtual business, education, and healthcare technologies. Cloud computing provides users with storage capacity, computing and services, and applications over the internet, increasing demand for their services.

2. Literature Review

As we discussed earlier, MCC is becoming increasingly important in the field of cloud computing; a lot of research and surveys have been conducted since 2010, and a lot of improvement has been seen following all of the research conducted on MCC. Here, we are going to discuss some prominent work that has been previously carried out on MCC, also All of these past recent evaluations on MCC shown in 1. Jegadeesan et al. [1] have proposed a private and safe authentication technique for MCC in smart city applications. They have analyzed the strength of this mutual authentication technique's security in previous work and suggested different algorithm methods to handle privacy concerns. Almusaylim et al. [2] give a comprehensive review on how to keep secure the data of any user who used different location based service applications like snapchat etc. they give the previous related work review on it with the help of their techniques that previously used for it. Shabbir et al. [3] have described how health-related information is at risk as the technology progresses and how it needs to be secured. They also discussed how to secure health-related information using a Modular Encryption Standard (MES) algorithm in MCC. Baharon et al. [4] proposed an approach to preserve data privacy with MCC to ensure users' personal information is kept safe using the homomorphic cryptosystem technique.

Shamshirband et al. [5] presented a survey on work that has been previously carried out on the technique of a computational intelligence (CI)-based ID model, its classification with the implementation methods, and issues, and compared this technique with other techniques. Akbar et al. [6] give a scalable solution for efficient mobile cloud hybrid (MCH) applications and also present previous related work on mobile cloud frameworks. They present multi-objective optimization (MOO) algorithms for the betterment of MCC usage, and give two scenarios to determine the best result for MOO as well as future MCH work on MCC. AlAhmad et al. [7] discuss the current models of MCC as well as give an overview of the client-to-client model technique, including existing models and common security issues and weaknesses of MCC. Maray et al. [8] present the concept of offloading techniques on mobile edge technology (MEC), along with previous work on taxonomy architecture and previous algorithms that provide different computing services on MCC, with a comparison between MCC and MEC, and its future directions. Abidin et al [9] present modern quantum cryptography direction (QKD) and service provider architectures with the comparison of other previous work techniques for the betterment of the security of MCC. Ali et al. [10] proposed dynamic decision task scheduling and a micro-service-based computational offloading (TSMCO) technique for mobile cloud servers and presented architecture or algorithms for the enhancement of TSMCO framework on different applications, such as health care, games, and augmented reality. They also presented a literature review on previous offloading frameworks with their presented work performance evaluation as shown in Table 1.

Table 1. Evaluation of previous related work on MCC.

Ref.	Technique	Security	Application	Architecture	Algorithms	Data Storage	Methodology Type
[1]	✓	✓	✓	n/a	✓	n/a	Trusted third party (TTP)
[2]	✓	✓	✓	✓	✓	n/a	Homomorphic encryption technique
[3]	✓	✓	✓	✓	✓	✓	Enciphering scheme, Modular Encryption Standard
[4]	✓	✓	n/a	✓	✓	✓	Homomorphic cryptosystem technique.
[5]	✓	✓	✓	✓	n/a	✓	CI-based IDs
[6]	✓	n/a	✓	n/a	✓	n/a	Multi-objective optimization (MOO) algorithm
[7]	✓	✓	✓	n/a	n/a	n/a	Client-to-client authentication, RQ models
[8]	✓	✓	✓	✓	✓	n/a	Computation offloading, Mobile edge computing (MEC)
[9]	✓	✓	✓	✓	✓	n/a	Quantum cryptography application
[10]	✓	n/a	✓	✓	✓	✓	Task scheduling and microservice-based computational offloading (TSMCO)

3. Methodology

So, the scope of the research on MCC does not demonstrate that it will change the future of the usage of mobile devices. This section presents a detailed view of MCC, its advantages, limitations, architecture, and applications.

3.1. Mobile Cloud Computing (MCC)

MCC enables its consumers to access applications that might not be available to them due to device limitations, such as storage capacity. By combining cloud computing with MCC, wireless systems can implement expensive mobile applications across different mobile devices. Some of the features that has given by MCC to their users given below in Figure 1.

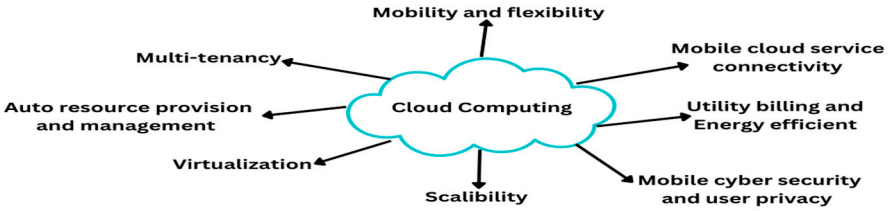

Figure 1. Features of MCC.

3.2. The Architecture of MCC

To understand the current architecture of MCC, the overall architecture of MCC is shown in Figure 2. In this architecture, mobile devices are connected to a network through base stations (satellites and base transfers receiver stations). Users of mobile devices request data through dominant processing that belongs to those servers that are used to connect to MCC services. With the current overview of the architecture of MCC, we can access the MCC services in two ways:

- Access point: with the help of WI-FI devices
- Mobile network service: with the help of mobile communication networks like 3G, 4G, and 5G.

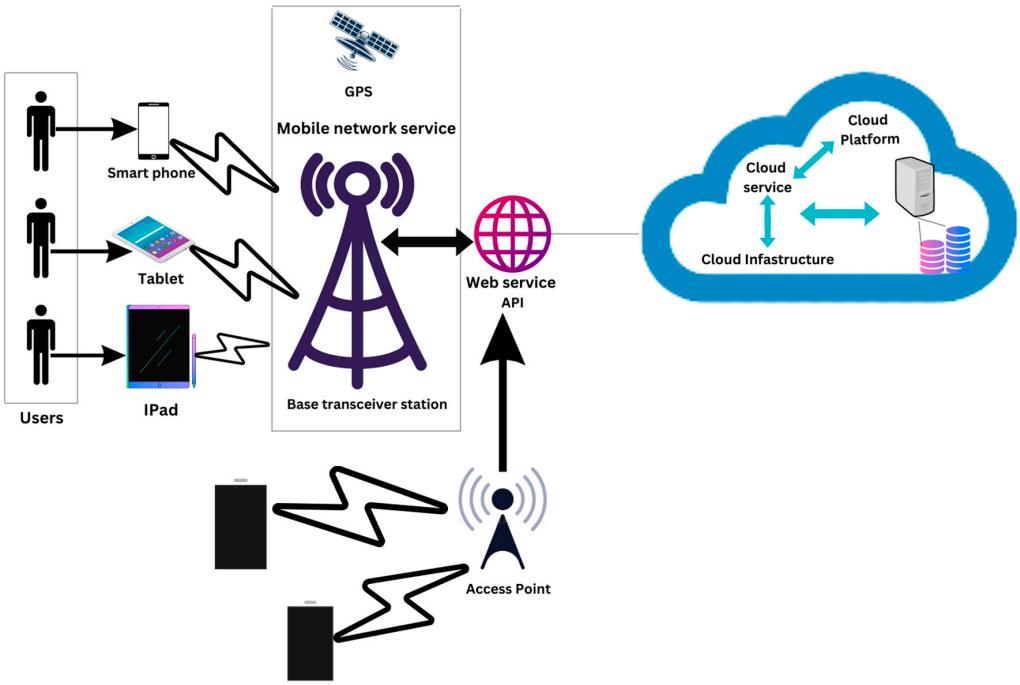

Figure 2. Architecture of MCC.

3.3. Advantages of MCC

MCC has many advantages: it saves battery life for its users, has fewer limitations regarding data storage, has increased processing power, and also provides dynamic provisions.

3.4. Limitations of MCC

A major limitation of MCC is having poor connectivity, which may cause a remote system to face many problems. Additionally, many users face network availability issues just because of the low bandwidth rate of a network, and over time users face security issues that are a bit complicated if their data is not secured. This may lead to a severe loss.

3.5. Challenges of MCC

MCC users face two major challenges: security and mobile application maintenance. Security measures, such as SSL and digital certificates, are used to secure data from mobile phones, while mobile applications need to be maintained through positive MCC infrastructure. Network bandwidth and latency routes should be used to properly manage the computational concentration, network latency, or network bandwidth.

4. Discussion

4.1. Work on MCC after COVID-19

In the twenty-first century, there are many advantages available in the field of IoT, AR, AI, ML, and Machine Learning. After the pandemic, many researchers and authors proposed models for the reliability and security of the data of users. These models include free-pairing incremental re-encryption [11], a secure format for the multi-server authentication (MSA) protocol, and a second level of authentication based on cloud-to-client verification. In the MCC classification, the user requests the data; then, once the request has been sent for the safety segment, the consumer request will safely get the data from a cloud.

4.2. 5G Impact on MCC

5G networks provide ultra-fast communication of information that is 100 times faster than 4G, and Ericsson Mobility expects that by 2023, there will be 1.77 billion 5G subscriptions, representing grow up to 16% of mobile data traffic. 5G uses the infrastructure that supports many network interfaces that use numerous radio technologies and has an additional 1 GB/s of bandwidth, making it very efficient when it comes to large bandwidth access.

5. Result

This survey analyzed previous works on the security of users' data on MCC. Jegadeesan et al. [1] proposed a mutual authentication scheme; Irshad Azeem et al. [12] proposed an improved incremental encryption scheme; Shamshirband et al. [5] analyzed the computational intelligence (CI) identification technique; Shabbir et al. [3] presented a modular encryption standard; and Abidin et al. [9] analyzed different service providers for quantum cryptography applications, and they claimed that quantum cryptography is new compared to classical cryptography techniques and will be beneficial for future cyberspace.

6. Future Work and Conclusions

One of the main future works for MCC AR (augmented reality) applications that have been analyzed in our research is that 6G is to be expected to come out in 2030, with its faster data transfer and a real-time representation of high-quality 3D objects. With the help of the 6G environment, there will be many scalability and resource services for users; with the help of 6G, MCC will be able to provide more enhanced services for AR applications. The enhanced services that will be included with augmented reality are mixed reality (MR) and virtual reality (VR) [13]. This AR application will also help us save mobile battery life, as well, and this will allow for engaging any user in a more interactive way.

To conclude all of this, we just wanted to say that MCC will tend to do a lot of work in the future of mobile technology, especially in AR applications, and virtual reality. Some of the major challenges that a user faced such as network latency, and privacy issues of users, all of these can be overcome with the help of continuous research and development on these major challenges. Overall MCC is an advanced technology in which we utilize cell phones and access our personal data in coming years.

Author Contributions: Conceptualization, B.S. and J.H.; methodology, A.B.; validation, B.S., A.B. and J.H.; formal analysis, A.B.; investigation, B.S.; data curation, J.H.; writing—original draft preparation, B.S.; writing—review and editing, A.B.; visualization, B.S.; supervision, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Suggested Data Availability Statements are available in sec-tion "MDPI Research Data Policies" at https://www.mdpi.com/ethics.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jegadeesan, S.; Azees, M.; Kumar, P.M.; Manogaran, G.; Chilamkurti, N.; Varatharajan, R.; Hsu, C.H. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. *Sustain. Cities Soc.* **2019**, *49*, 101522. [CrossRef]
2. Almusaylim, Z.A.; Jhanjhi, N.Z. Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. *Wirel. Pers. Commun.* **2020**, *111*, 541–564. [CrossRef]
3. Shabbir, M.; Shabbir, A.; Iwendi, C.; Javed, A.R.; Rizwan, M.; Herencsar, N.; Lin, J.C.W. Enhancing security of health information using modular encryption standard in mobile cloud computing. *IEEE Access* **2021**, *9*, 8820–8834. [CrossRef]
4. Oh, E.N.; Baharon, M.R.; Yassin, S.M.W.M.S.M.M.; Idris, A.; MacDermott, A. Preserving Data Privacy in Mobile Cloud Computing using Enhanced Homomorphic Encryption Scheme. *J. Phys. Conf. Ser.* **2022**, *2319*, 012024. [CrossRef]
5. Shamshirband, S.; Fathi, M.; Chronopoulos, A.T.; Montieri, A.; Palumbo, F.; Pescapè, A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *J. Inf. Secur. Appl.* **2020**, *55*, 102582. [CrossRef]
6. Akbar, A.; Lewis, P.R.; Wanner, E. A self-aware and scalable solution for efficient mobile-cloud hybrid robotics. *Front. Robot. AI* **2020**, *7*, 102. [CrossRef] [PubMed]
7. AlAhmad, A.S.; Kahtan, H.; Alzoubi, Y.I.; Ali, O.; Jaradat, A. Mobile cloud computing models security issues: A systematic review. *J. Netw. Comput. Appl.* **2021**, *190*, 103152. [CrossRef]
8. Maray, M.; Shuja, J. Computation offloading in mobile cloud computing and mobile edge computing: Survey, taxonomy, and open issues. *Mob. Inf. Syst.* **2022**, *2022*, 1121822. [CrossRef]
9. Abidin, S.; Swami, A.; Ramirez-Asís, E.; Alvarado-Tolentino, J.; Maurya, R.K.; Hussain, N. Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC). *Mater. Today Proc.* **2022**, *51*, 508–514. [CrossRef]
10. Ali, A.; Iqbal, M.M. A cost and energy efficient task scheduling technique to offload microservices based applications in mobile cloud computing. *IEEE Access* **2022**, *10*, 46633–46651. [CrossRef]
11. Sheth, H.S.K.; Tyagi, A.K. Mobile cloud computing: Issues, applications and scope in COVID-19. In *Intelligent Systems Design and Applications*; Springer International Publishing: Cham, Switzerland, 2022.
12. Irshad, A.; Chaudhry, S.A.; Shafiq, M.; Usman, M.; Asif, M.; Ghani, A. A provable and secure mobile user authentication scheme for mobile cloud computing services. *Int. J. Commun. Syst.* **2019**, *32*, e3980. [CrossRef]
13. Elmeadawy, S.; Shubair, R.M. 6G wireless communications: Future technologies and research challenges. In Proceedings of the 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 19–21 November 2019.