Research on mobile cloud services and future data security and privacy

ChaitanyaKrishna Hanumantarao Chundiwar

Northwest Missouri State University, Maryville MO 64468, USA
chaitanyachundiwar.k@gmail.com

1 Introduction

Because of the gigantic no of times of Mobile-cloud-based versatile Applications utilized in numerous spaces of our life like schooling, banking, and medical care, the security of information and correspondences has turned into a high-need issue. Among the innovation models that empower cell phones to utilize cloud administrations is versatile distributed computing. Mobile cloud Services is moving in the innovation space for both industry and exploration, as both endeavor to present and execute better models that further develop effectiveness while keeping an elevated degree of safety Mobile cloud is a moving innovation utilized in a few spaces to defeat the restrictions of cell phones by utilizing cloud capacities. Correspondence between cell phones and mists is kept up with by means of remote media to utilize cloud administrations. Consequently, MCC models bring along indispensable security issues connected with many disciplines, particularly validation, protection, and trust. Current Mobile cloud models miss the mark on capacity to get and safeguard information, assets, correspondence channels, and confirmation. Mobile cloud applications acquire the issues and attributes of both cloud and versatile figuring.This rsearch paper fills the hole of current Mobile cloud services studies through a deliberate examination of the Mobile cloud security issues in the writing by satisfying specific targets: (I) surveying normal Mobile cloud security issues, (ii) exploring Mobile cloud models, (iii) dissecting the Mobile services models against the security issues found, and (iv) talking about future ramifications for the security privacy protection issues of Mobile cloud service models

1.1 Mobile cloud computing and analyze

In addition to outlining a technique for building cloud applications, the paper raises security issues linked to cloud computing, such as those relating to user privacy and cloud access security. As part of the process, a national survey standard for developing cloud service apps is being developed. As the use of mobile service applications rises, mobile cloud computing will unavoidably play a part in the future of mobile devices. An online cloud computing environment is provided in a mobile cloud service by a mobile phone app that a user uses to access data and services.

Cloud computing technology introduces a brand-new danger. Mobile devices and services are changing how users connect to the Internet and how they communicate with service providers. Users can use them to access their accounts, devices, and data even when they are not online. The service providers must concurrently present a novel strategy to ensure the data's security and privacy. cloud Security, privacy problems are being emphasized as priority priorities because cloud computing for smartphones is still in its infancy. This presentation will investigate the current state of mobile cloud computing and look into its future.

2 Survey of Information security and privacy threats on mobile cloud service

Mobile based cloud computing poses several new security and privacy threats due to the inherent insecurity of untrusted devices and users. Mobile devices come with numerous sensitive and personal data, including location, phone number, photos, and video. However, as a general trend in the industry, many manufacturers of mobile devices do not keep security and privacy issues a top priority As a result, end users are required to safeguard the device using strong passwords and biometrics.

If the user's mobile devices are breached with sensitive personal information, it is tough to restore data because the device is lost. Therefore, enterprises need to ensure the security and privacy of mobile devices by implementing mobile device cloud management and policies. There are several mobile cloud computing security and privacy issues with the surveys, and the problems are more than one or two problems.

There are mainly three big problems: the survey methodology, the definition of mobile cloud computing security, and the measurement method So, the three issues could not be resolved, and either the measuring method could not consider security nor mobile cloud computing security. There is no perfect solution yet, but the three problems are the most critical. Here are the three problems. Please go through them and find what the best method is.

2.1 Problem

The survey methodology cannot find the mobile cloud security in computing and privacy problems, so we need to know how serious the mobile cloud service computing security and privacy problems are (Gupta et al., 2018). The survey result cannot distinguish the mobile cloud computing security and privacy problems from other security and privacy issues, so we cannot identify how serious the mobile cloud computing security and privacy problems are. That is in the first problem of the measurement method One of the most pressing concerns of mobile end users is building trust in their rapidly expanding cloud providers.

Although some research has been conducted to improve the reliability of cloud resources, there are many concerns about unsecured wireless networks

(locations that are not closely monitored) and the Internet for data storage in the cloud (user We cannot avoid sending user data via The heterogeneity of cloud infrastructure and the unique nature of resource availability and mobile devices exacerbate trust issues. Encryption and decryption techniques are used to protect user data. They need to measure the three aspects of mobile cloud computing security and privacy problems: the security and privacy protection mechanism, the security and protection of mobile devices, and the privacy and security issues of mobile cloud services computing. This is the first problem of the Measurement Method As mobile data storage and access to and from the cloud become commonplace, data security challenges such as data theft, deletion, corruption, and misuse arise.

3 Techniques to Privacy-Preserving, Securely store and Approaches

The security and privacy issue of mobile cloud computing, a new approach to the problem, has yet to be studied. Most of the current mobile cloud computing security and privacy issues have been resolved through two approaches: i) To improve the security and privacy of mobile clients, where mobile clients are not a focus, and ii) To improve the security and privacy of the service provider, where the focus is mobile service providers.

The current mobile security and privacy issues, including mobile clients, mobile service providers, and mobile devices, were resolved through one of the two approaches or a combination of the two. In the new approach to the problem, however, the focus is changed to the mobile cloud computing issue, mobile phone cloud user, mobiles phone service providers, and mobile devices have become the focus

Mobile Cloud application services Computing is a advance computing paradigm where the computer itself (device) is the main target and is an integral part of the Internet and how we interact. Mobile cloud services may involve multiple mobile devices that are interconnected with each other. The data that passes over these devices may be sensitive and need protection to ensure security and privacy.

It is the core of the next generation of wireless and mobile applications and has become increasingly popular. The future of Mobile cloud services theory will be a complex interaction between these devices and the Internet, with many possible security and privacy issues

Several innovative encryption methods have been developed to address these data security concerns and provide privacy in the cloud. Attribute-based encryption is one of these encryption methods (ABE). There are two types of attribute-based cryptography. The first is Key Policy Attribute Based Encryption theory and the another one is Cipher Text Based Abe.

Instead of encryption, Key Vendor decides which access control model to use in the middle of her Kp abe framework. This limits the use and incentives

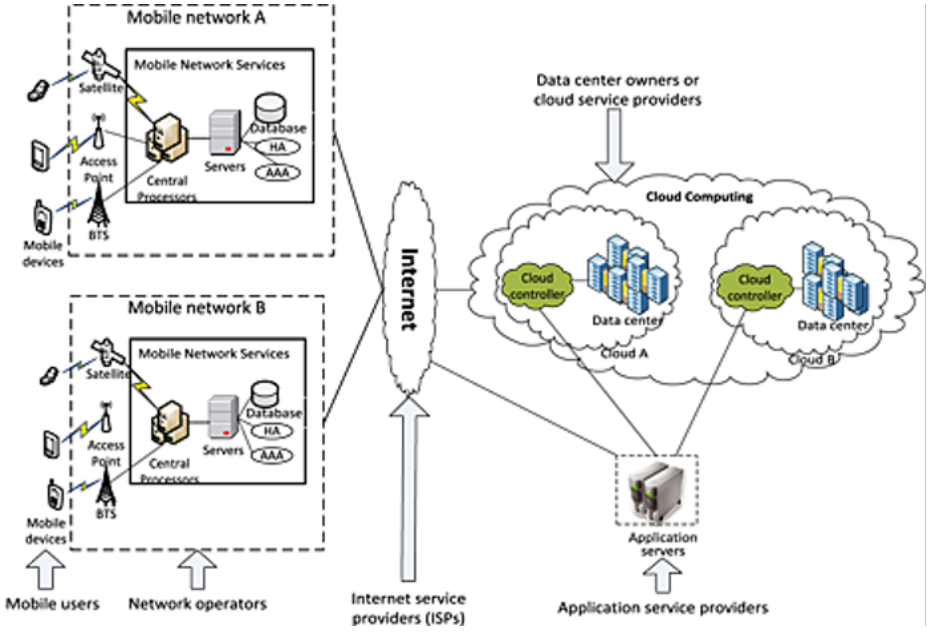

Fig. 1. A Survey of Mobile Services Cloud computing

of frameworks in meaningful applications [2]. The cipher text of this (Cp Abe) scheme that was actually identified is related to maintaining access structures

4 Conclusions

Because of more smart phones are used to keep and processes personal user data and corporate data [2,] there are widespread concern about the confidentiality and privacy of sensitive personal data because the smartphone can be stolen, affected, or hacked. Besides this, applications running on mobile devices should use as little energy as possible. We provide a comprehensive survey of information privacy, security, and mobile cloud service security mechanisms.

To begin, we will provide an overview of mobile cloud security. Then we discuss the potential security and privacy issues with mobile cloud models. Following that, we present very recent related works as well as security solutions, and quantitatively analyze the solutions so that readers in this field can make comparisons, analyze, and direct ongoing research activities. Despite the fact that this research field is still in its infancy and has yet to be thoroughly investigated, many security and privacy related problems are still being researched and remain unsolved. As a result, we will conclude by discussing some existing problems in this regard.

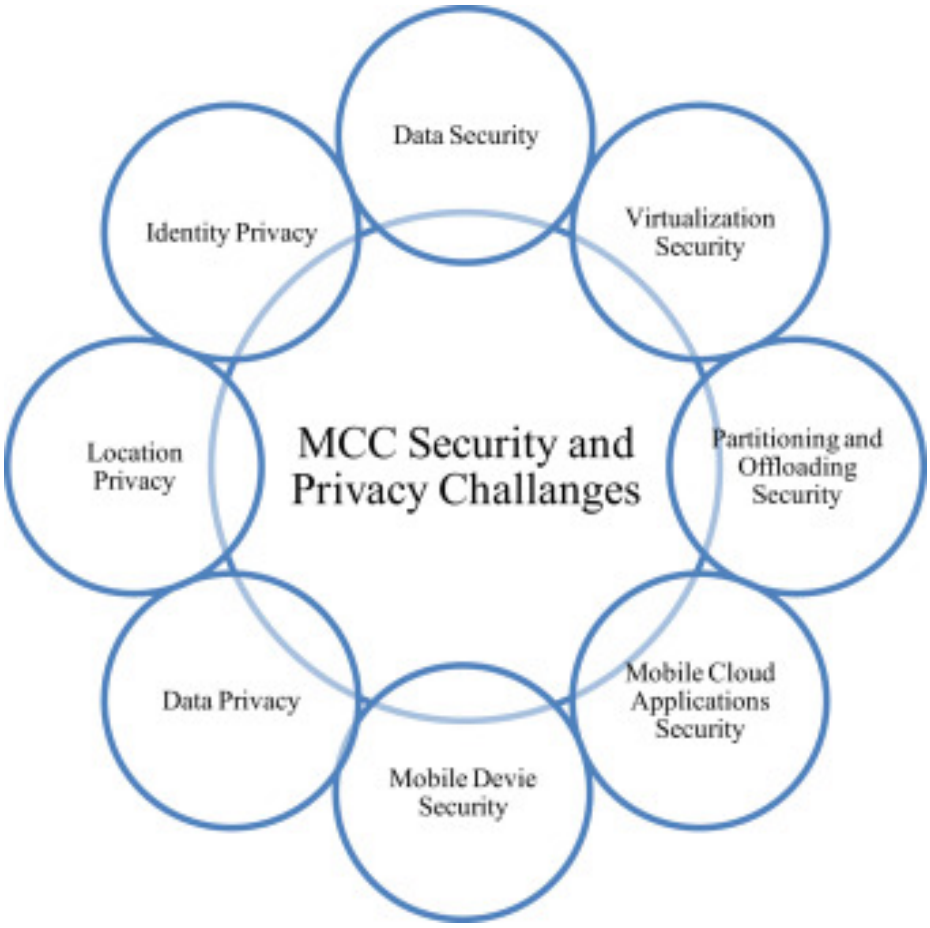

Fig. 2. Main security and privacy challenges in Mobile cloud services

References

1. AlAhmad, A.S., Kahtan, H., Alzoubi, Y.I., Ali, O., Jaradat, A.: Mobile cloud computing models security issues: A systematic review. Journal of Network and Computer Applications **190**, 103152 (2021)
2. Alqahtani, H.S., Kouadri-Mostefaou, G.: Multi-clouds mobile computing for the secure storage of data. In: Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. p. 495–496. UCC '14, IEEE Computer Society, USA (2014). https://doi.org/10.1109/UCC.2014.68, https://doi-org.ezproxy.nwmissouri.edu/10.1109/UCC.2014.68
3. Chaoui, H., Makdoun, I.: A new secure model for the use of cloud computing in big data analytics. In: Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing. ICC '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3018896.3018913, https://doi-org.ezproxy.nwmissouri.edu/10.1145/3018896.3018913
4. Javaid, M., Haleem, A., Singh, R.P., Rab, S., Suman, R., Khan, I.H.: Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers. International Journal of Cognitive Computing in Engineering (2022)
5. 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. Sustainable Cities and Society **49**, 101522 (2019)
6. Lo'ai, A.T., Saldamli, G.: Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences **33**(7), 810–819 (2021)
7. Moorthy, V., Venkataraman, R., Rao, T.R.: Security and privacy attacks during data communication in software defined mobile clouds. Computer Communications **153**, 515–526 (2020)
8. Nawrocki, P., Pajor, J., Sniezynski, B., Kolodziej, J.: Modeling adaptive security-aware task allocation in mobile cloud computing. Simulation Modelling Practice and Theory **116**, 102491 (2022)
9. Parast, F.K., Sindhav, C., Nikam, S., Yekta, H.I., Kent, K.B., Hakak, S.: Cloud computing security: A survey of service-based models. Computers & Security **114**, 102580 (2022)
10. VasanthaAzhagu, A.K., Gnanasekar, J.M.: Cloud computing overview, security threats and solutions-a survey. In: Proceedings of the International Conference on Informatics and Analytics. ICIA-16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2980258.2982046, https://doi-org.ezproxy.nwmissouri.edu/10.1145/2980258.2982046

□