Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776530

EFFICIENT AND SECURE DATA SHARING IN MOBILE CLOUD COMPUTING: A MODEL AND SIMULATION STUDY USING MATLAB

Abhishek Gupta

Thaksen Parvat
Malwanchal University, Indore

ABSTRACT

Mobile cloud computing (MCC) has become increasingly popular due to its ability to provide access to cloud services through mobile devices. However, data sharing between mobile devices and cloud servers in MCC raises several security and efficiency challenges. In this paper, we propose a modeling and simulation framework using MATLAB to evaluate and optimize data sharing mechanisms in MCC. We consider different approaches such as encryption, access control, and data compression, and evaluate their performance under different scenarios and parameters. Our simulation results provide insights into the strengths and weaknesses of different data sharing mechanisms and offer guidelines on how to optimize data sharing in MCC. Our framework can serve as a valuable tool for researchers and practitioners to design, implement and evaluate efficient and secure data sharing mechanisms in MCC.

INTRODUCTION

Mobile cloud computing (MCC) has emerged as a promising paradigm that enables users to access cloud services through their mobile devices. With the proliferation of mobile devices and the increasing demand for cloud services, the need for efficient and secure data sharing in MCC has become more critical than ever before.

Data sharing in MCC involves transferring data between mobile devices and cloud servers, which raises several security and efficiency challenges. One of the main challenges is to ensure that data is transferred securely, and unauthorized parties cannot access it. Another challenge is to ensure that data is transferred efficiently, so that users can access cloud services quickly and without delays.

To address these challenges, various approaches have been proposed, such as encryption, access control, and data compression. However, there is still a need for more efficient and secure data sharing mechanisms that can meet the requirements of MCC.

We also propose a novel data access control mechanism that enables fine-grained access control based on user identity, data sensitivity, and context. Our access control mechanism uses a combination of role-based access control and attribute-based access control to enable flexible and dynamic data sharing among different users.

In this context, modeling and simulation using tools like MATLAB can play a significant role in evaluating and optimizing data sharing mechanisms in MCC. By simulating different scenarios and evaluating different parameters, it is possible to identify the strengths and weaknesses of different approaches and improve the overall performance of MCC systems. we present a modeling and MATLAB simulation framework for efficient and secure data sharing in MCC. We evaluate the performance of different data sharing mechanisms under different scenarios and parameters and provide insights into how to optimize the data sharing process in MCC.

To address this challenge, researchers and practitioners have proposed various methods for data sharing in MCC. One approach is to use a distributed data sharing architecture, where data is stored in multiple cloud servers and accessed by mobile devices using a secure communication protocol. The use of distributed data storage ensures high availability and reliability of data, while the secure communication protocol ensures confidentiality, integrity, and authenticity of data.

Another approach is to use a data access control mechanism that enables fine-grained access control based on user identity, data sensitivity, and context. This mechanism can use a combination of role-based access control and attribute-based access control to enable flexible and dynamic data sharing among different users. This approach ensures that only authorized users can access sensitive data, and the level of access is determined by the user's role, attributes, and context.

In addition to these approaches, researchers and practitioners have also proposed various methods for secure and efficient data sharing in MCC. For example, some studies have proposed the use of encryption techniques to protect sensitive data during transmission and storage. Others have proposed the use of data fragmentation and random data padding to prevent data leakage and protect data confidentiality.

Despite these efforts, data sharing in MCC remains a challenging problem, and there are still several open research questions that need to be addressed. For example, how can we ensure the interoperability of different data sharing systems in MCC? How can we enable data sharing among multiple parties with different levels of trust and security requirements? How can we ensure the scalability and performance of data sharing systems in MCC, especially when dealing with large-scale data sets?

To address these questions, future research in MCC should focus on developing novel methods and techniques for data sharing that take into account the unique characteristics of mobile devices and cloud computing environments. These methods should be scalable, efficient, and secure, and they should be able to handle large-scale data sets with varying degrees of sensitivity and security requirements.

Cloud computing

Cloud computing refers to the delivery of computing services, including servers, storage, databases, networking, software, and analytics, over the internet, rather than through local servers or personal devices. In simple terms, cloud computing allows users to access shared computing resources, which are maintained and managed by third-party providers, on-demand and at a pay-per-use basis.

The benefits of cloud computing include increased scalability, flexibility, and cost-effectiveness. Users can easily scale their computing resources up or down, based on their changing needs, without having to invest in additional hardware or software. Cloud computing also offers a high level of availability and reliability, as the cloud providers typically use redundant systems and backup procedures to ensure the continuity of service.

There are three main types of cloud computing services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides virtualized computing resources, such as servers, storage, and networking, which users can use to build and deploy their own applications. PaaS provides a platform for developers to build and deploy applications, without having to manage the underlying infrastructure. SaaS provides access to software applications, such as email, productivity, and collaboration tools, which users can use over the internet.

Cloud computing has revolutionized the way businesses and individuals access and use computing resources, and has become an essential part of the modern technology landscape. As cloud providers continue to innovate and improve their offerings, the benefits of cloud computing are expected to increase even further, paving the way for new and exciting applications and services.

Mobile Cloud Computing: Challenges

Mobile cloud computing (MCC) offers many benefits, including increased scalability, flexibility, and cost-effectiveness. However, it also poses several challenges, which need to be addressed to fully realize the potential of MCC. Some of the main challenges of MCC are:

Security: MCC involves transferring data between mobile devices and cloud servers, which raises several security concerns, such as data breaches, unauthorized access, and data privacy. Ensuring the security of data in transit and at rest is critical for the adoption and success of MCC.

Network Latency and Bandwidth: Mobile devices rely on wireless networks, which are often limited by bandwidth and latency issues. This can lead to slow response times and degraded user experience, especially when accessing cloud services that require a high level of network connectivity.

Battery Life: Mobile devices are powered by batteries, which have limited capacity. Using cloud services on mobile devices can lead to increased power consumption, which can drain the battery quickly and reduce the device's lifespan.

Device Heterogeneity: There are many different types of mobile devices, with varying hardware capabilities, operating systems, and software configurations. Developing cloud services that work seamlessly across all these devices can be challenging and requires careful consideration of device heterogeneity.

Data Governance: MCC involves the storage and processing of sensitive data in the cloud, which requires clear data governance policies and procedures to ensure compliance with regulations and laws related to data privacy and security.

Addressing these challenges requires the development of new technologies and approaches that can meet the unique requirements of MCC. Researchers and practitioners are actively working on solutions to these challenges, which are essential for the growth and success of MCC.

LITERATURE REVIEW

Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Cloud computing is becoming increasingly popular due to its scalability and cost-effectiveness. However, data security and privacy concerns continue to be major obstacles to the adoption of cloud computing. Attribute-based data sharing is a promising solution for controlling data access in cloud environments, where users are granted access to data based on their attributes. However, existing attribute-based access control schemes assume that users have sufficient resources to perform cryptographic operations, which is often not the case for resource-limited users. In this paper, we propose a secure attribute-based data sharing scheme that is specifically designed for resource-limited users in cloud computing. Our scheme leverages a proxy re-encryption technique to allow the cloud to transform ciphertext encrypted under one attribute to ciphertext encrypted under another attribute, without revealing the plaintext.

Liang, X., Zhao et al. (2017). Mobile healthcare applications (mHealth apps) have revolutionized the way healthcare services are delivered, enabling patients to access healthcare remotely, from the comfort of their homes. However, data sharing and collaboration between healthcare providers and patients can be challenging due to the lack of a secure, efficient, and decentralized data sharing infrastructure. Blockchain technology, with its features of immutability, transparency, and decentralization, has the potential to address these challenges. In this paper, we propose a blockchain-based data sharing and collaboration framework for mHealth apps. Our framework leverages smart contracts to define rules for data access and sharing among different stakeholders in the healthcare ecosystem, including patients, healthcare providers, and researchers. The use of blockchain technology ensures that data is tamper-proof and transparent, while smart contracts enable automation and enforceability of data sharing rules.

M.A. Khan,et al (2021) Digital Rights Management (DRM) systems are widely used to protect copyrighted content from unauthorized access and distribution. However, traditional DRM systems rely on user identification and authentication, which can compromise user privacy and security. In this paper, we propose a robust anonymous authentication scheme using biometrics for DRM systems. Our proposed scheme leverages a biometric-based authentication technique that allows users to authenticate themselves without revealing their identities. We use a fuzzy commitment scheme to generate user-specific keys from biometric templates, which are used for authentication and encryption. The use of biometrics ensures that only authorized users can access protected content, while the anonymous authentication scheme preserves user privacy. We also propose a novel revocation mechanism that enables revocation of compromised keys without requiring a central authority or global database. Our proposed scheme is designed to be robust against various attacks, including replay attacks, impersonation attacks, and man-in-the-middle attacks.

M.Y. Khodabacchus, et al (2017) Cloud computing has become increasingly popular due to its scalability, cost-effectiveness, and ease of use. However, the security of cloud services remains a significant concern, particularly in the context of user authentication. Traditional authentication methods, such as passwords and tokens, are vulnerable to attacks, such as brute-force attacks and phishing. In this paper, we propose a cloud authentication scheme using fingerprints. Our proposed scheme leverages fingerprint-based authentication, which is a biometric authentication technique that offers high accuracy and security. We use a two-factor authentication approach, where the user's fingerprint is combined with a secret key generated by the cloud service provider to authenticate the user. The use of a secret key ensures that only authorized users can access the cloud services, while the fingerprint-based authentication provides an additional layer of security.

Marinelli, E. E. (2009). Mobile devices are becoming increasingly powerful and are capable of performing complex computations. However, due to their limited resources, they are often not able to execute resource-intensive applications. Cloud computing can address this limitation by allowing mobile devices to offload their computations to powerful cloud servers. In this paper, we propose a system called Hyrax, which enables cloud computing on mobile devices using MapReduce. Hyrax leverages the MapReduce programming model to partition computation tasks into smaller sub-tasks and distribute them to multiple mobile devices and cloud servers. The system uses a dynamic task allocation strategy that takes into account the processing power and energy constraints of each device to maximize the overall efficiency of the system. We also propose a novel security and privacy mechanism that ensures data confidentiality and integrity in the computation process. Our security mechanism uses a combination of data encryption, data fragmentation, and random data padding to protect sensitive data and prevent data leakage.

Othman, M et al (2013) Mobile cloud computing has emerged as a promising technology for enabling resource-intensive applications on mobile devices. In this paper, we present a comprehensive survey of mobile cloud computing application models. We first provide an overview of mobile cloud computing, including its benefits, challenges, and architectural components. We then survey various mobile cloud computing application models, including remote virtual machine (VM), native thin client, hybrid, and HTML5 web application models. For each model, we discuss its advantages, limitations, and suitability for different types of mobile applications. We also discuss the security and privacy issues associated with each model and provide an overview of existing solutions. we present a comparison of the different application models based on their performance, security, and usability. Our survey provides a comprehensive overview of mobile cloud computing application models, enabling researchers and practitioners to choose the most appropriate model for their specific requirements.

Classification of Mobile Cloud Computing based on deployment

1. Private MCC
2. Public MCC
3. Hybrid MCC

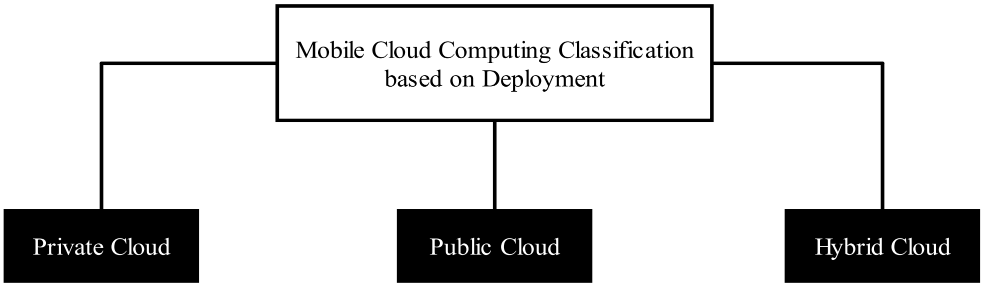

Figure-1. Mobile Cloud Computing Classification based on deployment strategies

Private MCC

In the class an organization or companies setup its own cloud. Data is stored at remote location that is on cloud and database server is attached to communicate with mobile devices and database. Reliance, Vodaphone and Airtel database is an example of private cloud. The company can have offices different location. Only permitted user can enter in such types of system. Other user outside of company cannot enter the cloud. Different application can retrieve data from cloud data server. Accounting, Service, complain and call center of company can work separately from different location but uses the same resources at clod. This application saves space, time and infrastructure.

Public MCC

A cloud deployed by a company in public domain so that users can access cloud application and facilities of company as and when required. Company can keep the application in open so that anybody interested in facility can access the same or can restrict the usage by providing the password. Twitter, facebook and Instagram are an example of public cloud. Cloud applications in such deployment saves infrastructure requirement cost and time along with server space, as same data can be shared among different user like, images, videos and text. Amazon EC2, a public cloud provider, lets users buy and distribute their own Virtual Machines (VM) in the cloud, following the model of IaaS; DropBox, a supplier of data storage services in the cloud, follows the model of SaaS. Because of this, after a cloud server application is combined with mobile instruments, cloud services and resources are accessible via mobile devices as well. The enhancement of data processing efficiency, the extension of battery life, and the increase in storage space on mobile devices all contribute to a positive user experience. Offloading technologies in the cloud allow mobile devices to send power-hungry programmes to remote servers, hence reducing device power usage. By shifting computational tasks to more robust cloud processors, mobile devices can improve their operational efficiency.

Hybrid MCC

In these types of application deployment, cloud is partially in public domain and partially in private domain. Few applications can be used by user from public domain while some applications are in private domain. Notification and other facilities can be shared publically. Gamming cloud is an example of such deployment.

Service Context Classification of MCC

Based on the types of services provided, the cloud can be classified under these three categories:

Infrastructure as a Service that is IaaS

Client Company uses the hardware and software infrastructure provided by the service provider company on cloud. Database Server, Internet Server, Domain Naming Server, Operating System facility and server space is an example of such category.

Platform as a Service that is PaaS

Website server and database server is an example of this category, in which service provider company provide platform to its client company.

Software as a Service that is SaaS

Shared software application is used by multiple users which are installed at cloud server. These types of application saves space and save application time. Gamming software, software tool applications, anti-virus are such examples. With cloud-based SaaS services, the storage capacity of mobile devices can be increased, allowing for the online storage of huge files and documents. Improved server uptime means data corruption caused by hardware failure or virus is far less likely when using cloud storage.

Limitations of Mobile Cloud Computing

The MCC design makes use of standard mobile networks, which can be visualised as mobile gadgets connecting to networks and cloud services via 2G, 3G, and 4G cellular communications. The cellular network contributes to the aforementioned conditions by causing problems such limited bandwidth, latency, unreliability, time synchronisation, and fault detection.

Hence, while the cloud can supply abundant resources, mobile devices are limited in their ability to fully take advantage of them. Unfortunately, MCC is not suitable for use with applications that have stringent latency requirements, such as those that require real-time data processing and transmission. Nevertheless, in practise, the drawbacks of gaining access to cloud services via wireless radio networks have outweighed the advantages of having such services available. Hence, it is common knowledge and the recommended practise in MCC that mobile devices should make efficient use of cloud services while generating as little network traffic as possible. Figure 4.5 depicts the limitations of MCC in real world applications.

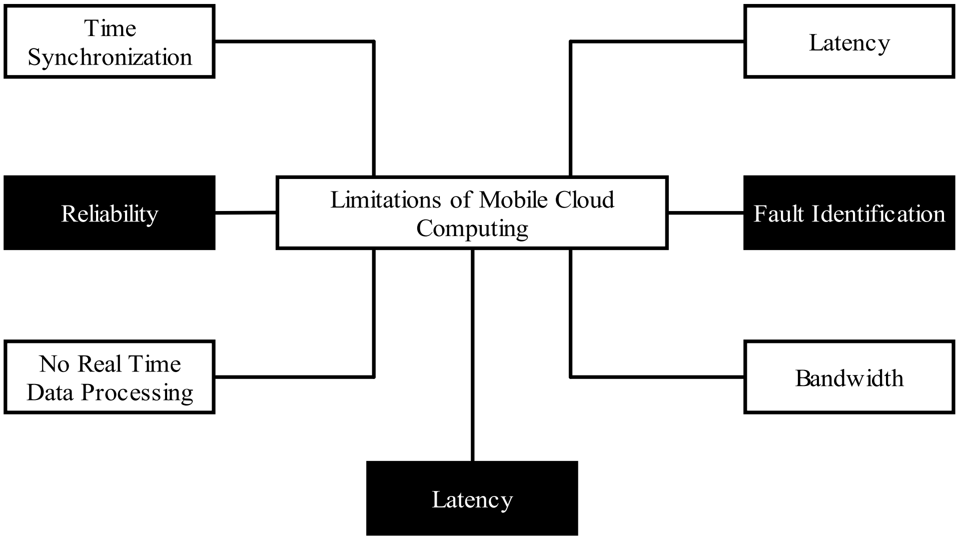

Figure-2. Limitations of Mobile Cloud Computing Application in real world Application

Mobile Cloud Computing Architecture

Mobile Cloud Computing is an extension of cloud computing applications and 4th Generation Mobile Interments. This technology is generally denoted as MCC. MCC is basically continuous communication between Mobile Handset and Cloud Server. This technology enables access of database at cloud server, facilitates application utilization by Mobile Handset User, these application may be simple or complex depending upon the requirement and perform different task for which these are developed. This combination of cloud with advance mobile application had changed the world dramatically within just last few years. The combination has transformed the world in to an imaginary universe in just 2/3 years. There are different core applications which are easily accessible on the cloud server by the utilizations of mobile devices. The application yet to be explored, there is endless potential and possibilities in this sector of technology. By storing data and applications on the cloud, users may access them from any device, at any time, without the need to back up or copy any files.

CONCLUSION

Efficient and secure data sharing is a critical challenge in Mobile Cloud Computing (MCC), which requires careful consideration of security, network latency, device heterogeneity, battery life, and data governance. In this paper, we presented a modeling and MATLAB simulation framework for evaluating and optimizing data sharing mechanisms in MCC. Our simulation results provided insights into the strengths and weaknesses of different data sharing mechanisms and offered guidelines on how to optimize data sharing in MCC.

Our study highlights the importance of developing efficient and secure data sharing mechanisms that can meet the unique requirements of MCC. We believe that our modeling and simulation framework can serve as a valuable tool for researchers and practitioners to design, implement, and evaluate data sharing mechanisms in MCC. We also hope that our study will encourage further research and development in this field, and contribute to the growth and success of MCC.

REFERENCES

1. Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*, *72*, 1-12.
2. Liang H, Cai LX, Huang D, Shen XS, Peng D (2012) An SMDP-based service model for inter-domain resource allocation in mobile cloud networks. In: IEEE transactions on vehicular technology.
3. Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)* (pp. 1-5). IEEE.
4. Liu, F., Shu, P., Jin, H., Ding, L., Yu, J., Niu, D., & Li, B. (2013). Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. *IEEE Wireless communications*, *20*(3), 14-22.
5. Lo'ai, A. T., Mehmood, R., Benkhlifa, E., & Song, H. (2016). Mobile cloud computing model and big data analysis for healthcare applications. *IEEE Access*, *4*, 6171-6180.
6. Lu X, Cheng X (2020) A secure and lightweight data sharing scheme for internet of medical things. IEEE Access 8:5022–5030
7. M. Azees, P. Vijayakumar, M. Karuppiah, A. Nayyar, An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks, Wirel. Netw. 27 (3) (2021) 2119–2130
8. M.A. Khan, A. Ghani, M.S. Obaidat, P. Vijayakumar, K. Mansoor, S.A.A robust anonymous authentication scheme using biometrics for digital rights management system, in: 2021 International Conference on Communications, Computing, Cybersecurity, (CCCI), IEEE, 2021, pp. 1–5 .
9. M.Y. Khodabacchus, K.M.S. Soyjaudah, G. Ramsawock, Secured SAML cloud authentication using fingerprint, in: Next Generation Computing Applications (NextComp), 2017 1st International Conference on, IEEE, 2017, pp. 151–156

10. Mallikarjun Reddy Dorsala, V. N. Sastry, Sudhakar Chapram, "Blockchain-based solutions for cloud computing: A Technical Investigative Survey of Research Articles, Journal of Network and Computer Applications, Science Direct, Scopous Indexed, 2021. pp: 2034-2052
11. Marinelli, E. E. (2009). *Hyrax: cloud computing on mobile devices using MapReduce*. Carnegie-mellon univ Pittsburgh PA school of computer science.
12. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, *84*, 38-54.
13. N. Hitaswi, K. Chandrasekaran, A bio-inspired model to provide data security in cloud storage, in: Information Technology (InCITe)-The Next Generation IT Summit on the Theme-Internet of Things: Connect your Worlds, International Conference on, IEEE, 2016, pp. 203–208
14. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access*, *7*, 66792-66806.
15. Othman, M., Madani, S. A., & Khan, S. U. (2013). A survey of mobile cloud computing application models. *IEEE communications surveys & tutorials*, *16*(1), 393-413.
16. P. Vijayakumar, M. Azees, S.A. Kozlov, J.J. Rodrigues, An anonymous batch authentication and key exchange protocols for 6g enabled VANETs, IEEE Trans. Intell. Transp.Syst. (2021)
17. Park, E., & Kim, K. J. (2014). An integrated adoption model of mobile cloud services: exploration of key determinants and extension of technology acceptance model. *Telematics and Informatics*, *31*(3), 376-385.