WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Navigating Mobile Cloud Computing: Challenges and Protective Strategies

C. S. Manigandaa [a], V. Anush Kumar [b], Challapalli Manikantaa [c], Asiya Mariyam [d]

[a] *Panimalar Engineering College, Department of Artificial Intelligence and Data Science, Chennai*
[b] *Panimalar Engineering College, Department of Artificial Intelligence and Data Science, Chennai*
[c] *Panimalar Engineering College, Department of Artificial Intelligence and Data Science, Chennai*
[d] *Panimalar Engineering College, Department of Artificial Intelligence and Data Science, Chennai*
DOI: https://doi.org/10.55248/gengpi.4.823.51855

A B S T R A C T

The concept of Mobile Cloud Computing (MCC) has garnered substantial attention within the realm of information technology (IT) owing to its potential to enable ubiquitous access to information regardless of time and location. Mobile devices, specifically smartphones, have facilitated the emergence of immersive user interactions, predominantly governed by prominent entities such as Apple, Google, Facebook, and Amazon, who exert significant influence over the mobile industry. Nevertheless, the exponential expansion of mobile cloud computing technology has concurrently ushered in novel security vulnerabilities. Efforts are currently underway to improve the reliability and security of the cloud environment, as it contains significant amounts of valuable data. The exponential growth of Internet-capable mobile devices, including smartphones and tablets, has resulted in a surge of intricate web-centric malevolent hazards. Therefore, the preservation of data security emerges as a paramount concern within the context of the Mobile Cloud environment. This study delves into the principles of Mobile Cloud Computing (MCC) and examines numerous security challenges and proposed solutions put forth by researchers. The objective is to augment security and dependability within the Mobile Cloud environment.

Keywords: Mobile Cloud Computing (MCC), Ubiquitous access, Information technology (IT), Smartphones, Immersive user interactions

1. Introduction

The domain of Information Technology has experienced an unparalleled upsurge due to the expeditious expansion of Mobile Cloud Computing (MCC). In contemporary times, the imperative nature of guaranteeing data security in the realm of Mobile Cloud has become increasingly prominent, owing to the escalating prevalence of mobile devices equipped with internet connectivity. Smartphones, which occupy the highest position in the hierarchy of technological advancements, utilize mobile operating systems to facilitate sophisticated computational capabilities and accelerated connectivity, thereby distinguishing themselves from traditional mobile phones. As a result, the emergence of Mobile Cloud has been observed as a highly influential phenomenon, fundamentally altering the dynamics of enterprises and end-users alike. In the present day, mobile applications designed for use on portable devices have undergone a process of advancement, resulting in heightened levels of security and complexity. These developments have been specifically tailored to meet the requirements of both cloud users and enterprises. In 2012, the global revenue generated by mobile networks exceeded an astonishing $1,200 billion, thereby establishing a significant foundation for immense potential within the mobile cloud market. Based on projections, it is anticipated that the mobile cloud market, which serves both consumer and enterprise sectors, will surpass $45 billion by the year 2016. Mobile cloud computing, in essence, encompasses the amalgamation of cloud computing services within the mobile ecosystem, effectively integrating wireless networks with cloud infrastructure to provide users with exceptional services. Mobile devices utilize wireless connections to access centralized applications, wherein the interaction is facilitated through web browsers or thin native clients.

One notable aspect elucidated by researchers is that mobile cloud computing eliminates the necessity for robust mobile configurations, as intricate computations are transferred and executed in the cloud environment itself. The emergence of Smartphones has posed a significant challenge to the prevailing supremacy of Blackberry as the favored corporate Smartphone, as iPhones, Android devices, and Windows Phones have witnessed extensive adoption across various organizations.

The paper is structured in the following manner: Section 1 presents an introductory overview of MCC, emphasizing its inherent significance and the potential ramifications it may have. Section 2 expounds upon the underlying impetus for composing this manuscript, discerning the lacunae and domains of inquiry. Section 3 provides a comprehensive analysis of the underlying architecture of MCC, presenting valuable insights into its operational framework. Section 4 delves into the examination of several intricate matters within the realm of MCC, thereby illuminating the impediments encountered in this ever-evolving domain. Section 5 delves into a comprehensive examination of various security facets pertaining to Mobile Cloud Computing

(MCC), with a particular emphasis on the utmost importance of ensuring the protection and preservation of data and operational processes. In Section 6, a thorough examination is provided on the diverse methodologies utilized to guarantee data security within the Mobile Cloud environment. In conclusion, Section 7 serves as the final segment of the paper, wherein it provides a concise overview of the fundamental discoveries and presents a framework for potential future investigations within this rapidly expanding domain.

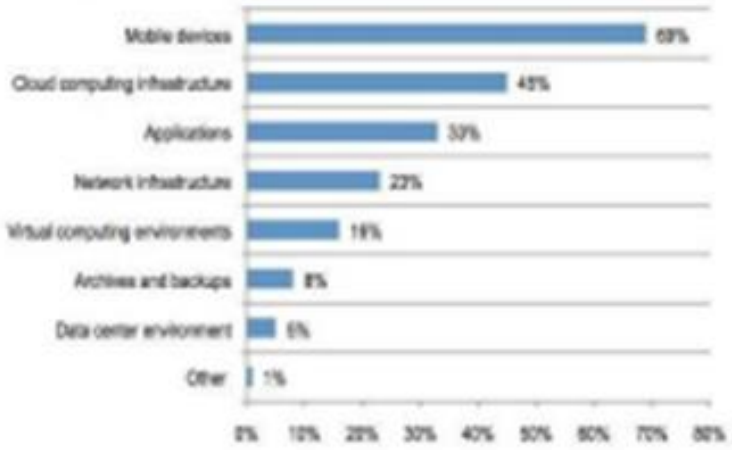

Fig 1.Data Protection Risks

II. MOTIVATION

Mobile Cloud Computing has effectively integrated mobile devices into cloud environments, thereby facilitating heightened productivity for individuals engaged in business-related activities. Customers are exhibiting a growing inclination towards Mobile Cloud Services to cater to their individual requirements, accentuating the distinctive benefits provided by mobile computing. The present topography exhibits a wide-ranging assortment of mobile cloud applications that cater to diverse domains. These domains encompass image processing, language processing, shared GPS, shared internet access, sensor data applications, querying, crowd computing, and multimedia search.

Nevertheless, notwithstanding the myriad advantages, specific obstacles necessitate diligent consideration and subsequent resolution. Figure 1 depicts the inherent vulnerabilities associated with knowledge protection, thereby emphasizing the criticality of preserving data within operational settings. The Mobile Cloud Computing environment necessitates careful consideration of crucial factors such as network dependency, data sharing, transactional applications, and security.

A significant obstacle encountered in the realm of Mobile Cloud Computing pertains to the irregularity and availability of networks. The impact of network connections on the optimal operation of mobile cloud applications and services is a significant factor that requires the implementation of effective resolutions to mitigate these issues.

III. WORKING OF MCC

Figure 1 illustrates the structural arrangement of Mobile Cloud Computing, wherein Mobile devices establish connections with mobile wireless network base stations, encompassing Satellite and Base Transceiver Station (BTE). The aforementioned base stations function as intermediary devices that facilitate the establishment of network connectivity between mobile devices and the internet. User requests are transmitted via wireless network and subsequently reach the cloud server, facilitated by the Authentication, Authorization, and Accounting (AAA) mechanism. Following the transmission of user requests to the cloud, cloud controllers engage in the processing of said requests in order to furnish users with the requisite cloud services.

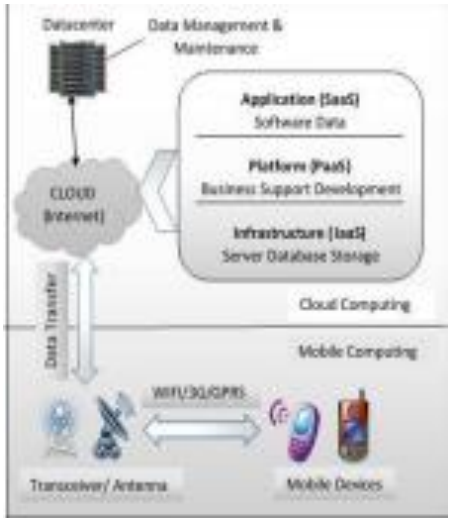

Fig2: Simple MCC Architecture

In Figure 2, a simplified MCC architecture is depicted, showcasing the development of cloud services through the utilization of Virtualization, Service-Oriented Architecture (SOA), and Utility Computing principles. A pivotal element within this architectural framework is the cloud controller, which enables the initiation, surveillance, and administration of the wireless network. The users have the capability to transmit two separate networks, with one being identified as the "private" network and the other as the "public" network. In order to facilitate the coexistence of multiple operating systems on a singular server or machine, the utilization of a hypervisor, alternatively referred to as a Virtual Machine Manager (VMM), is implemented. The hypervisor confers benefits in terms of application utilization and maintenance.

A. Characteristics of MCC:

Mobile Cloud Computing (MCC) possesses several key characteristics that define its operational framework and benefits:

Reliability: MCC ensures consistent and dependable access to cloud services and data, irrespective of the user's location or device.

Scalability: The architecture of MCC allows for seamless expansion to accommodate increasing demands, ensuring efficient performance even during peak usage.

Security: MCC emphasizes robust security measures to safeguard sensitive data and transactions, addressing potential vulnerabilities inherent in mobile and cloud environments.

Agility: MCC enables rapid deployment of services and applications, facilitating quick responses to changing business needs and user requirements.

Device Independence: Users can access cloud services and applications from various devices, promoting a seamless and consistent user experience.

Reduced Cost: MCC offers cost-saving advantages by eliminating the need for high-end mobile device configurations and centralized infrastructure management.

Reduced Maintenance: Users benefit from reduced maintenance efforts as cloud service providers handle the infrastructure and software updates.

B. Service Models in Cloud:

As per the National Institute of Standards and Technology (NIST), Cloud Computing services are categorized into three layered service models, often referred to as the SPI model, representing Software, Platform, and Infrastructure.

Software as a Service (SaaS): SaaS is commonly utilized by business users who access complete applications provided by the service provider. These applications are customizable within certain limits, catering to specific business tasks and end-user requirements.

Platform as a Service (PaaS): PaaS offers pre-built application components, such as APIs, aimed at developers and deployers. Developers can create and deploy higher-level applications, while the service provider manages the underlying operating systems and databases.

Infrastructure as a Service (IaaS): IaaS is predominantly used by system managers, as it eliminates the need to purchase physical server hardware and manage data center equipment, such as storage and networking. Managers can create platforms for service, utilizing the provider's infrastructure.

In addition to these primary service models, other service models exist, including Business Process as a Service (BPaaS), Network as a Service (NaaS), Anything as a Service (XaaS), and Disaster Recovery as a Service (DRaaS).

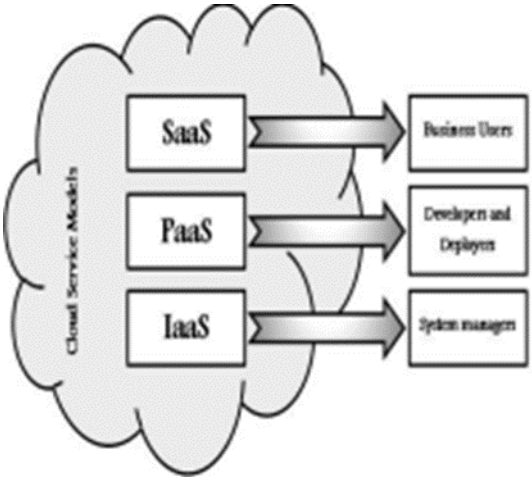

Fig3: Service Models in Cloud Computing

C. Mobile Military Intelligence Section 5 Layers

The security services in the mobile scheme are categorized into three distinct layers:

1. Backbone Layer: The backbone layer is responsible for ensuring the security and surveillance of the cloud's physical systems. It involves monitoring the servers and machines within the cloud infrastructure. This layer is vital in detecting potential threats and vulnerabilities in the physical components of the cloud.
2. Infrastructure Layer: The infrastructure layer focuses on monitoring the virtual machines (VMs) within the cloud environment. It carries out various activities to enhance cloud host services' security, including storage verification, VM migration, cloud service monitoring, VM isolation, risk analysis, and audits. These measures are crucial to maintaining the integrity and security of the cloud's virtualized resources.
3. Application and Platform Layer: The application and platform layer deals with securing the upper-level services and functionalities in the cloud. It encompasses essential activities such as user management, key management, authentication, authorization, encryption, and data integration. By implementing robust security measures at this layer, cloud service providers (CSPs) can address privacy and security concerns, thereby attracting more customers to their highly secure environments.

A recent survey revealed that 73% of IT executives and CEOs are hesitant to adopt cloud services due to associated risks concerning privacy and security. To overcome this reluctance and build trust with customers, CSPs must prioritize and address all security issues comprehensively, ensuring a highly secure and reliable cloud environment.

IV. CHALLENGING ISSUES IN MOBILE CLOUD COMPUTING

Mobile Cloud Computing (MCC) offers significant computational power through cloud resources, but the inherent limitations of mobile devices give rise to several challenges in achieving a balanced integration of the two. The implementation of cloud computing in mobile devices faces various issues related to restricted resources, network constraints, and security concerns. The following problems are explained in detail:

4.1 Restricted Resources: Mobile devices have limited computing power, battery life, and display capabilities, making it challenging to effectively utilize cloud computing. These restricted resources pose obstacles to seamless cloud integration and efficient mobile cloud applications.

4.2 Network-Related Problems: The entire process in MCC is dependent on the network, leading to several network-related challenges. These challenges include bandwidth constraints, latency issues, network availability, and non-uniformity. These network limitations can hinder the performance and user experience of mobile cloud services.

4.3 Security: Mobile devices, similar to PCs, face numerous security and privacy issues. Although threat detection services are performed in the cloud, they also encounter significant challenges. Security problems in MCC involve device security, mobile user privacy, and data security on the cloud. Threats such as viruses, hacking, and Trojan horses can compromise mobile devices' security. Additionally, the use of Global Positioning System (GPS) in mobile devices raises privacy concerns.

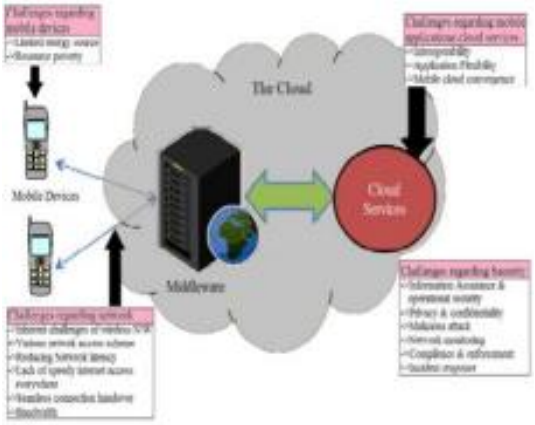

Fig. 3. Challenges Relating to Implementation of Cloud Computing in Mobile Applications

4.4 Low Bandwidth: Bandwidth scarcity is a major issue in MCC, as wireless networks have limited radio resources compared to traditional wired networks. One approach to address limited bandwidth is through cooperative data sharing among mobile users in the same vicinity, such as a workplace, station, or stadium. However, this approach may not consider fairness and distribution policies among users, leading to challenges in balancing contributions to a coalition.

4.5 Availability: Service availability becomes a critical concern in MCC, surpassing that of cloud computing with wired networks. Mobile users may face difficulties connecting to the cloud due to traffic congestion, network failures, and signal outages.

V. SECURITY IN MOBILE CLOUD COMPUTING

5.1 Security Framework in Mobile Cloud Computing:

Mobile cloud computing has gained significant popularity due to the growing adoption of cloud computing and mobile devices. Researchers are actively exploring this technology, but it comes with several challenges arising from the limitations of mobile devices, such as low battery power, restricted storage capacity, and limited bandwidth. As such, security becomes a critical concern in mobile cloud computing, and it can be generally classified into two frameworks.

5.1.1 Security of Data/Files: A primary concern when using mobile cloud computing is ensuring the security of data and files belonging to mobile users stored on the cloud. The data and files are highly sensitive, and unauthorized access or modifications can lead to severe consequences. Thus, cloud service providers must prioritize data/file security, as it is crucial for the data owner to protect their valuable information.

5.1.2 Security of Mobile Applications or Application Models: Securing mobile applications or application models is equally important, as these applications utilize cloud resources to enhance mobile device capabilities. Ensuring the security of these applications is essential for delivering reliable and secure services to mobile users.

5.2 The Necessity of Knowledge Storage Security:

The data of the owner is stored on the cloud server, meaning that the owner does not have direct control over this data on their own device. Consequently, there is a significant risk associated with data security and confidentiality. Unauthorized access or disclosure of the data to unauthorized individuals can be detrimental to the owner. Before discussing the necessity of knowledge storage security, it is essential to understand the security threats to data stored on the cloud, such as:

Integrity Threats: Unauthorized modifications to another person's data can compromise the integrity of the information.

Confidentiality Threats: Unauthorized access to someone else's data can breach its confidentiality, leading to privacy concerns.

Authentication: Proper user authentication is crucial to verify the identity of the file creator and prevent unauthorized access.

Ensuring knowledge storage security is vital to safeguard sensitive data and maintain the trust of data owners in the mobile cloud computing environment.

VI. VARIOUS METHODOLOGIES FOR DATA SECURITY IN MOBILE CLOUD COMPUTING

In recent years, Mobile Cloud Computing (MCC) has garnered significant research interest due to its potential and increasing usage of mobile devices. However, limited surveys exist in various domains of MCC, particularly in securing data storage. This paper focuses on securing data storage in MCC and explores different methodologies for information security. Various researchers have made efforts to develop secure MCC solutions. This section discusses three methodologies for data security in MCC:

5.1 Energy-Efficient Framework for Integrity Verification: Itani et al. proposed an energy-efficient framework for integrity verification of storage services using progressive cryptography and trusted computing. The framework aims to ensure data integrity for information stored on cloud servers. The system involves three main entities: Mobile User (MU), Cloud Service Provider (CSP), and Trusted Third Party (TTP). The MU utilizes storage services provided by CSP, while TTP installs coprocessors on remote clouds associated with registered MUs. The coprocessor provides a secret key (SEK) to the MU and generates a message authentication code (MAC) for the mobile client. The framework involves various operations such as updating files on the cloud, inserting or deleting data blocks, and integrity verification. It ensures the integrity of data stored on the cloud and enables secure data management for mobile users.

5.2 Identity-Based Proxy Re-Encryption for Confidentiality and Access Control: Jia et al. propose a secure data service mechanism through Identity-Based Proxy Re-Encryption (IB-PRE). This mechanism provides confidentiality and fine-grained access control for data stored in the cloud by outsourcing data security management to the mobile cloud. The protocol ensures that only authorized sharers can access the data while unauthorized participants gain no knowledge of the content. The protocol utilizes identity-based encryption and linear pairing to achieve secure data sharing and access control. The entities involved are Data Owner (DO), Data Sharer (DS), and Cloud Servers (CSs). DO and DS utilize data storage services, while CSs provide services to mobile clients. The protocol goes through phases such as setup, key generation, and encryption, and it enables secure data sharing and storage in the mobile cloud environment.

5.3 Privacy Preserving Ciphertext Policy Attribute-Based Encryption: Zhou et al. propose a scheme for efficient and secure data storage operations by introducing Privacy Preserving Ciphertext Policy Attribute-Based Encryption (PP-CP-ABE) and Attribute-Based Data Storage (ABDS) system. PP-CP-ABE allows lightweight devices to securely outsource encryption/decryption operations to the Cloud Service Provider (CSP). The entities involved in this scheme include Data Owner (DO), Trust Authority (TA), Encryption Service Provider (ESP), Decryption Service Provider (DSP), and Storage Service Provider (SSP). DO uses CSP's storage service, TA distributes cryptographic keys, ESP encrypts files without knowing the actual encryption key, DSP provides decryption service to DO, and SSP offers storage services to clients. The scheme ensures privacy-preserving data storage and efficient data operations in the mobile cloud environment.

these methodologies aim to enhance data security in mobile cloud computing, addressing confidentiality, integrity, and access control concerns. Implementing these methodologies can lead to a more secure and reliable mobile cloud environment, encouraging further adoption and usage of mobile cloud computing services

VII.CONCLUSION

This paper presents an investigation into the concepts of Mobile Cloud Computing (MCC), addressing challenging issues, and exploring various methodologies to enhance security in the Mobile Cloud Environment. The existing frameworks often overlook crucial aspects such as user data privacy, data storage, and energy-efficient data sharing, which pose significant challenges. User data privacy and secure mobile application deployment utilizing cloud services are recognized as particularly demanding aspects. To achieve higher security levels in the mobile cloud environment, it is imperative to thoroughly study and address potential threats. Developing a comprehensive data security plan that mitigates security risks, reduces costs, and simplifies the adoption of cloud computing in mobile environments is vital. In designing future frameworks, emphasis should be placed on cost-effectiveness, while ensuring superior security and performance.

REFERENCE

1.RNewswire.org, http://www.reportlinker.com/, 2012.

2.Preston A. Coz, "Mobile Cloud Computing: Devices, trends, issues & enabling technologies", 2012.

3.Schneider, "Essential characteristics of Mobile Cloud Computing", Marquette University, United States, 2012.

4. Professor Kun Yang, Dr. Shumao Ou, Professor Hai Jin, Huazhong, and Professor Amiya Nayak, "Mobile Cloud Computing and Networking", Proceedings of IEEE conference, 2013.

5. M. Rajendra Prasad, Jayadev Gyani, and P. R. K. Murti, "Mobile Cloud Computing: Implications and Challenges, Journal of Information Engineering and Applications", Vol.2, No.7, 2012, Print ISSN 2224-5782, pp.7-15.

6. Ronnie D. Caytiles and Sunguk Lee, "Security Considerations for Public Mobile Cloud Computing", International Journal of Advanced Science and Technology, Vol.44, July 2012.

7. Soeung-Kon Victor Ko, Jung-Hoon Le, and Sung Woo Kim, "Mobile Cloud Computing Security Considerations", April 30, 2012.

8. Anand Surendra Shimpi and R. Chander, "Secure Framework in Data Processing for Mobile Cloud Computing", International Journal of Computer & Communication Technology, ISSN (Print) 0975-7449, vol.3, Iss.3, 2012.

9. Jibitesh Mishra, Sanjit Kumar Dash, and Sweta Dash, "Mobile Cloud Computing: A Secure Framework of Cloud Computing for Mobile Application", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, pp.347-356.

10. Itani et al., "Towards secure mobile cloud: A survey", Proceedings of Analyses paper, 2012.

11. Eugene E. Marinelli, "Hyrax: Cloud Computing on Mobile Devices", Dissertation of Thesis, Carnegie Mellon University, Pittsburgh, 2009.

12. Xiaojun Yu and Qiaoyan Wen, "Design of Security Solution to Mobile Cloud Storage", Knowledge Discovery and Data Mining, AISC, Springer-Verlag Berlin Heidelberg H. Tan (Ed.), 2012, pp.255-263.

13. Robert Lemos, "Cloud's Future Security Depends on Mobile", Proceedings of RSA Conference, February 2012.

14. V.L. Divya, "Mobile Applications with Cloud Computing", International Journal of Scientific and Research, Vol.2, Issue 4, April 2012, ISSN 2250-3153.

15. Han Qian and Abdullah Gani, "Research on Mobile Cloud Computing: Trends, Review, and Perspectives", Proceedings of Analyses paper, University of Malaya, Malaysia, 2012.

16. S. Chetan, Gautam Kumar, K. Dinesh, Mathew K., and Abhimanyu M.A., "Cloud Computing for Mobile World", Proceedings of Analyses paper, National Institute of Technology, Calicut, 2010.

17. Jon Oberheide and Evan Cooke, "Virtualized in-cloud security services for mobile devices", Proceedings of the First Workshop on Virtualization in Mobile Computing, ACM, New York, USA, 2008, pp.31-35.