Online at: https://researchtrendsjournal.com ISSN No: 2584-282X

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 2; Issue 2; 2024; Page No. 165-170

Received: 02-12-2023
Accepted: 06-01-2024

Critical issues of data security and privacy of mobile cloud computing

[1]Suchit Kumar Vyas and [2]Dr. Satish Kumar

[1]Research Scholar, Department of Electronics & Communication Engineering, Himalayan University, Arunachal Pradesh, India
[2]Assistant Professor, Department of Electronics & Communication Engineering, Himalayan University, Arunachal Pradesh, India

DOI: https://doi.org/10.5281/zenodo.13118086

Corresponding Author: Suchit Kumar Vyas

Abstract

Cloud computing is a rapidly evolving technology that provides shared processing resources and data to computers and other devices on demand. Mobile computing, on the other hand, facilitates the transmission of data, voice, and video. The convergence of these technologies has given rise to Mobile Cloud Computing (MCC), a concept that not only addresses the limitations of mobile computing but also integrates cloud computing into mobile environments to tackle challenges related to performance, security, and resource constraints. MCC is gaining momentum as the number of mobile users continues to grow. Despite its advantages, data privacy and security remain significant concerns. MCC can deliver infrastructure, computational power, software, and platform services to even basic smartphones. However, several security issues need to be addressed, including network security, web application security, data access, authentication, authorization, data confidentiality, and data breaches. Given the limited storage and processing power of mobile devices, data capacity is constrained. To establish a secure MCC environment, it is essential to thoroughly study and analyze security threats. In this paper, we propose an algorithm designed to enhance the security of mobile cloud computing, ensuring data integrity and confidentiality. Additionally, we discuss the security threats present in MCC environments and propose solutions to address these challenges.

Keywords: Mobile Cloud Computing, Mobile devices, data, including network

Introduction

Cloud Computing (CC) is a coalesce of many computing fields and has gained much popularity in recent years (since 2007) [Khan *et al*., 2013] [2]. There is no consensual description on what a Cloud Computing or a Cloud Computing system is; dozens of developers and organizations describe it from different perspectives [Qi *et al*., 2012] [9]. Cloud Computing integrates various technologies to provides services, platforms and infrastructures to various users and business organizations. Mobile Cloud Computing (MCC) further combines cloud computing with mobile devices and wireless technologies distributed throughout the environment to enable continuous connectivity. With the rapid development of technology, more and more users upload various kinds of data on the cloud, which also includes the sensitive data. Data Security and privacy are the major concern when it comes to data sharing [Zhang, Yinghui, 2010] [3]. One way to ensure data security is by installing security software on the mobile device. Mobile devices are resource controlled; protecting them from the threats is very difficult. However, since mobile devices have processing and power limitations, protecting them from these threats could be more challenging compared to regular computers.

Mobile cloud computing

Cloud computing has a broad range of applications across various domains, and one area of significant interest today is mobile technology. This paper will explore how cloud computing environments can enhance mobile usage, focusing on the added value and improved functionality that cloud integration brings to mobile devices. According to Khan *et al.* (2013) [2], as illustrated in Figure 1, Mobile Cloud Computing (MCC) is a service that enables resource-

constrained mobile users to dynamically adjust their processing and storage capabilities. MCC achieves this by offloading computationally intensive and storage-demanding tasks to traditional cloud resources, thereby providing seamless wireless access and extending the capabilities of mobile devices.

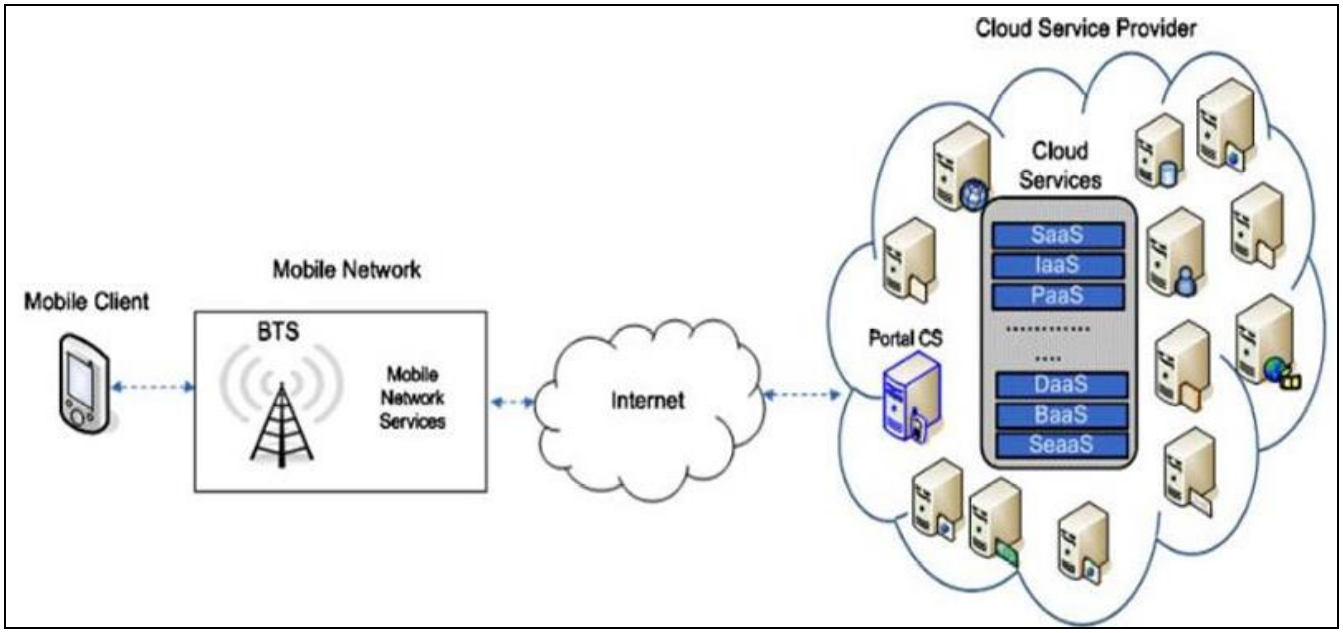

Fig 1: Mobile cloud computing architecture

Data security in mcc

The security architecture in a cloud environment is separated into three layers. The inner layer handles the various deployment models that were previously covered. Its layer is made up of many delivery models: The three main components of cloud architecture are SaaS, PaaS, and IaaS. As seen in the outer layer, these components include scalability, location dependency, on-demand self-service, and multi-tenancy. Cloud security is contingent upon the model of deployment and delivery that is employed, as well as the traits that it displays. Adopting virtualization and cloud computing presents fundamental security concerns that include data storage security, hardware security, software security, access control, data transmission security, application security, and security pertaining to external sources.

When moving to the cloud, the following are the primary queries that cross our minds

- How secure is the cloud for our data?
- On the cloud, where will our data be kept?
- Who can access the data we have placed in the cloud?
- To what extent may a customer trust the business or an outside party?
- Do cloud providers maintain client data that isn't accessible to other clients?

The challenge of assigning accountability for security measures and controls remains unresolved, impacting both CSPs and their clients. On the one hand, the service providers are in charge of developing features and services that adhere to privacy and data protection regulations; on the other hand, customers can customize and utilize such services in a manner that is appropriate for their area and industry. Customers must make use of these operational measures to stop unintentional data sharing, which can be established by service providers to safeguard their data on cloud servers. While clients must confirm that service providers' audit reports and certificates meet their organization's data privacy needs, service providers are in charge of getting certifications and signing SLAs.

Because it is unclear where these obligations end and where they begin, it is dependent upon the terms of the contract that the client and service providers sign, as well as the cloud service and deployment model that is employed. For instance, clients and PaaS and IaaS providers are equally accountable for security issues pertaining to anything above the virtual machine layer. However, with SaaS and cloud programs, the client bears greater responsibility for tasks like monitoring and access control. In a public cloud, consumers and CSPs share security duties, whereas in a private cloud, the customer has full responsibility for security. Applications and data installed on cloud platforms and services must be secured by the customer.

States of data

We must identify potential states in which the data may exist as well as the controls that are available for those states in order to secure data in the cloud.

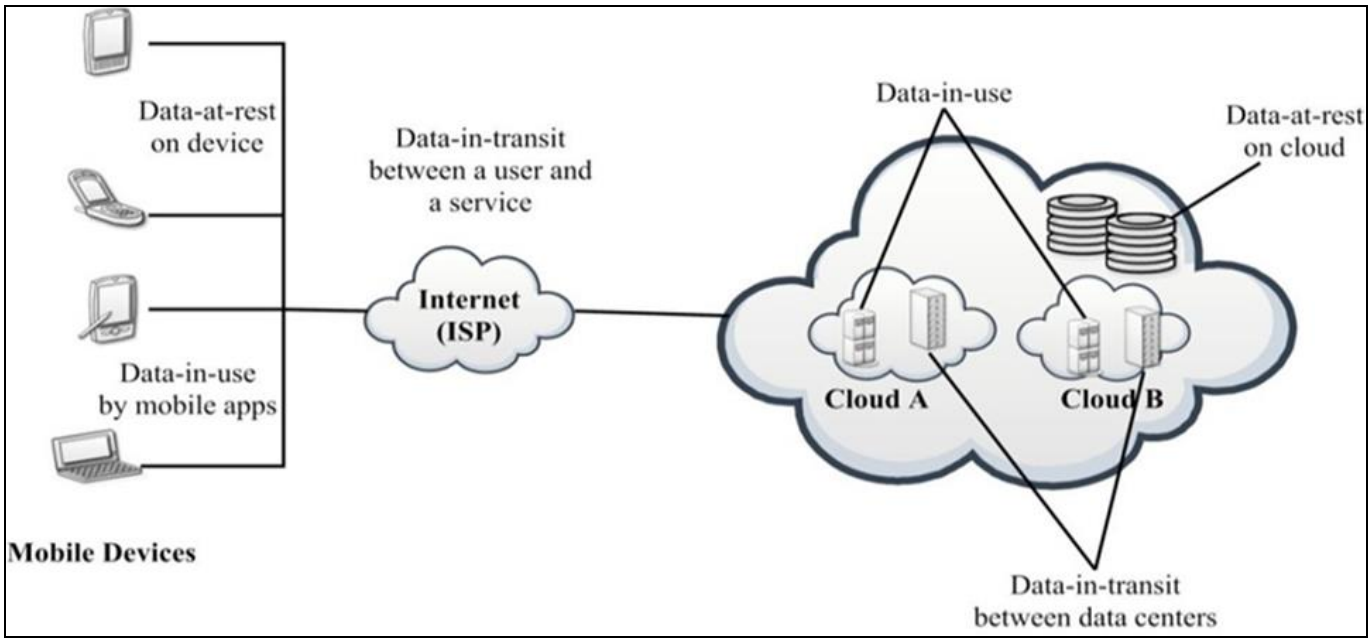

Fig 2: Possible states of data

Data-at-rest protection is now regarded as being just as vital as data-in-transit protection due to the rapid growth of the Internet and cloud computing. Cloud data is shielded by encryption from third-party disclosures, security lapses, and noncompliance. As seen in Figure 2, encryption is seen to be crucial for all three potential states of data: in-transit, at-rest, and in-use.

For any encryption policy to be successful, selecting robust encryption algorithms and a key management system is essential. Customers can choose to use their own key management infrastructure rather than the CSP's default key management infrastructure for increased security. According to a recent analysis by Skyhigh Networks Inc. of 12,000 cloud providers, 81.8% of CSP encrypt data while it is in transit, shielding it from MITM attacks as it travels over the Internet. However, only 9.4% of CSP encrypt data while it is at rest, leaving it open to data breaches, unauthorized access, and blind government subpoenas. Merely 1.1% of CSPs utilize encryption keys that are managed by the customer. The most widely used apps, including eBay, Linkedin, Facebook, Twitter, PayPal, Gmail, and Linkedin, save user passwords, bank account information, and credit card numbers in an unencrypted format. In 2014, Ebay experienced its largest data breach due to the theft of 145 million account credentials. The following are the possible states of the data:

- **Data-in-transit:** Information that is considered to be in motion when it leaves enterprise control and travels over a network or to the cloud, and vice versa, includes voice, video, text, and metadata. For this reason, encryption is essential. It entails communication across virtual networks in addition to connection with an external component of the cloud service. It must establish an encrypted and authenticated channel to prevent eavesdropping attacks using cryptographic protocols like TLS or SSL.
- **Data-at-rest:** This describes inactive data that is physically kept on file servers, NAS devices, SANs, databases, data warehouses, off-site backups, and so forth. To prevent assaults, robust access control procedures and data federation should be implemented in addition to encryption.
- **Data-in-use:** This term describes dynamic data that is kept in a non-persistent state, such as encryption keys or data that are kept in cache or main memory, or transactions in a message queue or data that is presently being handled by an application. For value-added operations like searching and data retrieval, these data are often in clear text format; however, the Cloud Security Alliance now advises encrypting data while it is being used for increased security. When using fully homomorphic encryption, calculations on ciphertext are permitted, and the outcomes, upon decryption, correspond to the calculations conducted on plaintext. Enclaves are used to protect data-in-use, which is information that is accessible as clear text inside the CPU but is stored in RAM in encrypted form.

Security principles

Any data security system must adhere to the fundamental security principles of confidentiality, integrity, authentication, and non-repudiation. Two further concepts are availability and access control, which are related to the system as a whole rather than to specific information or messages.

- **Confidentiality:** According to this principle, the message should only be accessible by the sender and the recipient(s). It stops illegal access to data, and when confidentiality is compromised, interception happens
- **Integrity:** It guarantees accurate and unaltered message delivery to the designated destination or recipients. A modification assault results from a loss of integrity.
- **Authentication:** This process aids in proving that the communicating node is who it says it is. A fabrication attack results from the lack of authentication measures.
- **Non-repudiation:** This concept ensures that the message's sender cannot subsequently retract having sent it.

- **Access control:** It guarantees that only authorized users can utilize the resources and services of the network. It serves as a link between sincerity, integrity, and confidentiality. After authentication, it determines who has "access" to what, with access encompassing both writing and reading of data (integrity and confidentiality).
- **Availability:** It guarantees that information may be accessed by authorized parties whenever needed. Information blocking results in denial-of-service attacks that prevent authorised users from accessing resources.

Classification of data security schemes

An enterprise or organization's data must be secured on the cloud to guarantee privacy and confidentiality, which makes effective key management strategies necessary when utilizing cloud SaaS. The data kept in the cloud is more vulnerable to malicious assault due to the rising use of advanced hacking tools. Thus, strong authentication protocols for cloud computing are also necessary to guarantee that only authorized and legitimate users can access data. Each and every user wanting to access the cloud system must have their identity confirmed by SaaS providers. The MCC categorizes its data security plans into:

The majority of systems in use today rely on password-based authentication, wherein a server keeps a database of passwords or their hashed values following salting. The first one-time password approach for remote authentication was proposed in 1981 by Lamport [2020] [10]. Although they are simple to install, an attacker can quickly take advantage of, guess, or alter the credentials kept on the server. It has scalability problems as well. A lightweight, flexible, and fine-grained system for access control (F2AC) in multiparty file sharing in a mobile cloud computing context was recently proposed by Ren *et al*. It allowed for dynamic actions like separating access authentication from system authentication, approving or rescinding member credentials transitively, and adding or removing people inside an ad hoc group. It was made up of two lists, one kept on the cloud and the other for user authentication and access control. The filename, users, privileges (read, update, edit, create), and conditions (location, MAC addresses, etc.) make up the Access Control List (ACL), whereas the user authentication list contains the username and associated token or password. Tokens were allocated and distributed by the file's creator to other users so they may share files. It is susceptible to replay attacks, password guessing, and impersonation. Password issues draw attention to the necessity of an additional user identification system.

- **Based on smart cards:** An embedded chip in smart cards contains encrypted information relating to an individual's identity. Identity theft is reduced via on-chip defensive mechanisms. It is possible to configure a single smart card for several purposes, such as banking or health benefits. However, it is possible to access the data kept on smart cards. An opponent can corrupt a smart card, which also compromises the user. An effective remote user authentication system that works in multi-server environments and is based on dynamic identification using smart cards was proposed by Jangirala *et al*. The protocol developed by Halevi and Krawezyk is a password-based, one-way authentication system. The password and symmetric key shared by each client are stored by the server in two distinct tables, while the client stores the symmetric key on a smart card. Password-based authentication replaces the previous one-way authentication mechanism mutual authentication and key exchange protocol (PWAKE), which makes use of pseudorandom functions and collision-resistant hash functions to further improve to two-factor smart card-based, password mutual authentication and key exchange protocol. A smart card-based authentication system based on the ElGamal public cryptosystem was proposed by Hwang and Li. However, it only offers one-way authentication.
- **Cryptography-based:** This is a traditional method of protecting user identity and data privacy across an unsecured network. Access to encrypted data is granted to an individual or group of users who have the relevant cryptographic key. It can be used for user authentication in addition to safeguarding data against loss or tampering. In, a concise categorization of the many cryptography-based data security mechanisms in MCC is provided.
- **Biometric-based:** An attacker can gain keys for cryptography-based systems illegally and pose as a legitimate user. Using biometric attributes, which identify users by their physiological and behavioral characteristics, is a very dependable and natural way to stop such attacks. Your voice, fingers, and eyes are always with you and cannot be copied or taken over by someone else. However, it is feasible that a bad person obtains biometric templates, like a fingerprint, covertly and uses them. Numerous cloud-based biometric recognition solutions are on the market. A recent study by a New York-based company predicts that by 2015, 240 million consumers or organizations will still use cloud services via mobile devices, bringing the total income from mobile cloud computing to $5.2 billion.
- **Multi-factor authentication schemes:** Designed to offer more effective data protection and authentication, these schemes combine two or more methods. Even while some multifactor authentication techniques use passwords to protect biometric information, there is always a chance that the password will be cracked. Integrating biometrics with cryptographic infrastructure is a doable endeavor.
- **When it comes to remote authentication over open networks:** Biometric authentication is similarly susceptible to assaults, while seeming like a more dependable solution than other conventional authentication methods.
- **Based on intrusion detection:** Cryptographic solutions are proactive and need a lot of processing power. They hold up well against known and expected attacks, but they could fail against unforeseen and unexpected ones. The growing prevalence of smartphones due to their sophisticated processing capabilities has resulted in the emergence of malware unique to smartphones, such as viruses, Trojan horses, and worms, as well as malware that is general and can attack Bluetooth interfaces or speech recognition techniques. Therefore, in order to identify and report anomalous activity, we require an intrusion detection system as a second line of

protection. All malware signatures should be saved in the phone by an efficient intrusion detection system, but this will require a significant amount of processing power and memory on mobile devices. Secloud is a cloud-based, lightweight smartphone security solution created by Zonouz *et al*. [2019] [11]. It uses the device's network connections and inputs to continuously transfer data to the cloud, simulating a smartphone and maintaining synchronization. Three main components make up this system: a proxy server that mirrors network traffic between smartphones and Secloud's replica; a lightweight client agent that runs on smartphones to gather user and sensor inputs and pass them to an emulated replica on the cloud; and an emulator that runs a variety of host-based and network-based security solutions, including snort, file integrity checkers, network-based intrusion detection systems, and virus scanners. Mobile devices use less energy and processing power since it conducts security analysis on an emulated replica rather than the actual device utilizing intrusion detection techniques.

Critical issues for m-government applications

Privacy and Security: The open nature of the Internet means that all traffic is vulnerable to interception, and some hackers are able to spy on corporate wireless networks from outside buildings, accessing emails and documents. Wireless networks, which broadcast signals over public airwaves, are particularly susceptible to security breaches. Addressing privacy and security issues during the planning phase is crucial, as these considerations can affect the timing and choice of wireless services. Specific programs, such as AirSnort and WEPCrack, have been developed to exploit vulnerabilities in the Wired Equivalent Privacy (WEP) encryption system used in 802.11b networks, allowing unauthorized access to passwords and sensitive data. To combat these threats, additional security protocols are being developed for 802.11 networks, and some vendors are offering enhanced security features in their products.

Accessibility: As government entities aim to provide access to m-Government information and services via wireless devices, it is important to ensure that this information remains accessible to all citizens through various communication technologies. The development of the Voice Extensible Markup Language (Voice XML) protocol is a key advancement, enabling web information to be accessible by telephone for users with disabilities. This technology allows users to interact with web content through voice commands. The World Wide Web Consortium's draft Voice XML 2.0 standard further integrates markup languages for common dialogs, grammar, speech synthesis, and natural language processing to enhance accessibility.

The key illustrative areas of proposed research are

- Preparation of semantic data for security parameters
- Cloud Security attributes
- Mobile Security features and respective parameters
- Security protocols under different security requirements
- Platform Independent Security Architecture.

Security and privacy issues in mobile cloud computing

There are three main security issues determined in MCC: Mobile terminal, mobile network and mobile cloud. In mobile terminal there is malware which can be prevented by CloudAV. Software vulnerabilities also exist in the applications and operating systems which can be prevented by installing system patches and checking software legitimacy and integrity. Few other issues include lack of security awareness or mis-operation which can be prevented by regulating user's behavior. In mobile network, there may be an information leakage or any malicious attack which can be prevented by a strong security protocol or some good data encryption. In mobile cloud, there are issues such as platform reliability, data and privacy protection which can be prevented by integrating the current security technologies, key management, data encryption, authentication, access control, privacy and data protection [Suo, Hui, 2013] [12].

Conclusion

This paper conducts a literature review of various approaches for the effective deployment of secure mobile cloud computing paradigms. We outline the challenges and potential solutions while exploring and characterizing a flexible and dynamic framework that offers a configurable security interface at the application layer. Issues related to the validation and testing of the proposed solutions are also addressed, aiming to establish reliable testing and benchmarking methods for security firmware in the context of mobile cloud computing. The outcomes of this research are anticipated to benefit both e-governance and e-commerce applications. Given the numerous challenges in this evolving field, our research will proceed in phases. The first phase will focus on formally characterizing the problem and proposing a lightweight mobile interface with limited dynamic capabilities. Subsequent phases will aim to expand on these objectives and address additional aspects of the problem.

References

1. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Network Comput Appl. 2011;34(1):1–11.
2. Khan AN, Kiah MM, Khan SU, Madani SA. Towards secure mobile cloud computing: A survey. Future generation computer systems. 2013;29(5):1278-1299.
3. Huan D, Zhang X, Kang M, Luo J. MobiCloud: building a secure cloud framework for mobile computing and communication. In: Proceedings of the 5th IEEE International Symposium on Service Oriented System Engineering; c2010. p. 27-34.
4. Chow R, Jakobsson M, Masuoka R, Molina J, Niu Y, Shi E, Song Z. Authentication in the clouds: a framework and its application to mobile users. InProceedings of the 2010 ACM workshop on Cloud computing security workshop; c2010. p. 1-6.
5. Jia W, Zhu H, Cao Z, Wei L, Lin X. SDSM: a secure data service mechanism in mobile cloud computing. In2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS); c2011. p. 1060-1065. IEEE.

6. Yang J, Wang H, Wang J, Tan C, Yu D. Provable data possession of resource constrained mobile devices in cloud computing. J Networks. 2011;6(7):1033–1040.
7. Ren W, Yu L, Gao R, Xiong F. Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing. J Tsinghua Sci Technol. 2011;16(5):520–528.
8. Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing. In2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualiztion management (svm); c2012. p. 37-45. IEEE.
9. Qi Y, Zhu J, Fu Q, Hu H, Rong X, Huang Q. Characterization and Cu sorption properties of humic acid from the decomposition of rice straw. Environmental Science and Pollution Research. 2017;24:23744-23752.
10. Lamport DJ, Christodoulou E, Achilleos C. Beneficial effects of dark chocolate for episodic memory in healthy young adults: A parallel-groups acute intervention with a white chocolate control. Nutrients. 2020;12(2):483.
11. Khalili Zonouz H. The reconstruction of Zonouz historical bazaar: A case study. Journal of Urban Regeneration & Renewal. 2019;13(2):199-211.
12. Suo H, Liu Z, Wan J, Zhou K. Security and privacy in mobile cloud computing. In2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC); c2013. p. 655-659. IEEE.