Mobile Cloud Database Security: Problems and Solutions

Mahmoud Ismail*, Naif El-Rashidy, Nabil M. Abdel-aziz

Faculty of computers and Informatics, Zagazig University, Zagazig, 44519, Egypt

Emails: mahsabe@zu.edu.eg; Naif.ElRashidy@gmail.com; NMoustafa2@zu.edu.eg

*Correspondence: mahsabe@yahoo.com; mahsabe@zu.edu.eg

Abstract

The rise in mobile Internet usage and increased reliance on cloud computing have led to increased fear of cloud database security. Mobile cloud computing has emerged as the only promising way of providing solutions for the mobile computing environment, including computation offloading and data binding. This paper discusses the overview of mobile cloud computing features and its prone computing security issues and how to walk over them with the most promising solutions. More specifically, it explores in detail a wide range of threats that may attack the mobile cloud-computing platform and the various devices and applications that work extremely well in supporting and mitigating the wide range of problems related to security issues in mobile applications. Moreover, this paper studies some of the ways to make mobile cloud computing more secure and productive no matter the intensity of the required computation. This study takes into consideration, the most common threats that affect the security issues of the mobile cloud database and its solutions. It is deemed necessary to note that, the duty of various cloud service providers is to keep all mobile cloud data safe. Consequently, they must come up with solutions to the problems affecting the day-to-day mobile-cloud database security.

Keywords: Cloud computing; Mobile cloud; Database; Internet; Security; offloading

1. Introduction

Due to advances in the technological world, the way people interact today is changing dramatically. Continuous technological developments provide fast, efficient, and stable information computing platforms for the world on board. Today, the world is experiencing major hardware advances and heightened capability in mobiles that ensure the effective use of many applications. Mobile cloud computing has emerged to make mobile devices more intensive in performing a variety of complex tasks.

Mobile Cloud Database provides users with the ability to use cloud infrastructure, services, and applications at a pocket-friendly cost. As such, most users have been able to use the resources of their choice easily with minimal management effort and interactions among cloud service providers. However, just like computers, mobile devices experience challenges in resource availability, communication, and security. As such, the mobile cloud database works extremely hard to address these challenges to ensure the user experience speedy mobile computing.

Mobile and cloud computing are integrated into Mobile Cloud Computing (MCC) to provide cloud services to mobile device users that have characteristic features such as on-demand self-service, resource pooling, rapid resilience, and large network access [4]. MCC typically uses mobile agents to reduce traffic on the network, reduce the amount of information exchanged, enable mobile code, reduce latency interaction, download new services, as well as improve capacity and performance [5, 6]. To ensure a flexible and more fruitful performance, the mobile cloud database should have a secure computing framework capable of making dynamic decisions and locating program partitions through the

DOI: https://doi.org/10.54216/FPA.070102

use of mobile agents [6]. In order to ensure better security of the mobile cloud databases, both mobile agents and frameworks must work together.

Cloud computing is most challenged by the complexities of mobile cloud database infrastructure which makes MCC, compared to traditional client-server, vulnerable to attackers who can access sensitive protocols [7]. For example, hackers may attack various aspects of vulnerable cloud management and maliciously alter and to the extreme, block the user from accessing cloud services.

This paper will focus on identifying and discussing various mobile cloud database issues/challenges and their possible solutions. More specifically, the main contributions of this paper are:

- A comprehensive survey of various security issues facing mobile-cloud databases.
- Challenges to address mobile-cloud database security.
- Factors that attribute to the challenges facing mobile cloud computing.
- Analysis of the wide range of security threats to mobile cloud computing.
- Solutions to current problems that are being faced by mobile cloud computing.

This paper could be navigated as follows. In Section 2, an overview of Mobile Cloud Computing along with its service model is discussed. Section 3 illustrates the impact of threats on the Mobile Cloud Computing paradigm. Section 4 discusses some of the Mobile Cloud Computing security solutions. Section 4 shows some of the challenges faced by mobile cloud applications and at last, and Section 5 presents the conclusion of the proposed study.

2. Mobile Cloud Computing

Mobile Cloud Computing (MCC) attracts industrialists as a commercially profitable alternative to reduce the costs of designing and operating mobile applications. Mobile computing supports a number of low-cost mobile services and green IT solutions [8]. Mobile cloud computing means a network or infrastructure in which both data processing and data storage outside of the mobile device is done. In which the mobile cloud systems transfer the data storage and processing capacity from mobile devices into the cloud, taking applications and mobile computing to a wider range of mobile subscribers as well as smartphone users. With mobile cloud computing, there are many benefits for both end-users and organizations of various sizes. The simple and important benefit is that consumers no longer have to think about the infrastructure or know about the construction and maintenance of the infrastructure. With respect to the mobile-cloud database, the main objective is to give users safe and fast access to data from the cloud anywhere, anytime through mobile devices. Figure 1 illustrates the architecture of the MCC. In this architecture, mobile devices are linked to the base stations of the mobile wireless network. These base stations include satellite and Basic Transceiver Station (BTE). The interface between mobile devices and the Internet provides a network connection. The user requests are transmitted over the wireless network to the Cloud Server (CS) by using the Authentication, Authorization, and Accounting (AAA) process. After user requests are sent to the cloud, the cloud controller process these requests to provide users with the appropriate cloud services.

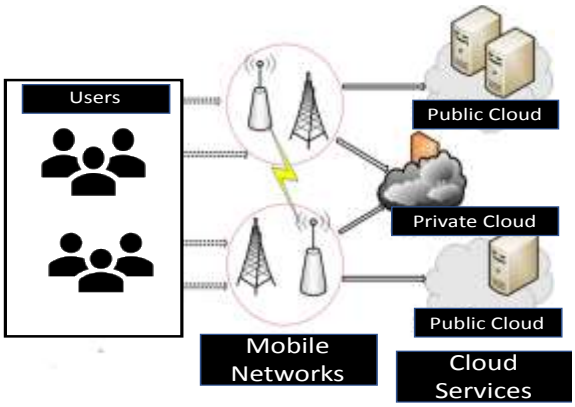

Figure 1: MCC Architecture

DOI: https://doi.org/10.54216/FPA.070102

Compared to a personal computer, the cloud can store and handle much more data. Using the cloud, infinite storage space and scalability are practically possible. Therefore, no further spending on technology or time spent adding new servers. It is possible to scale infrastructure to optimize investments. Cloud computing facilitates dynamic scalability with fluctuating demands. The cloud is not based on local hardware or software, so users gain new versatility when it comes to accessing the solution [8]. The cloud costs are based on the subscription model and can in some cases be paid for as you service, which fits well for the business model of the company. Cloud mobility supports access through a Web link anywhere. The cloud is everywhere, whether the development platform is owned or not. Cloud offers software that can be used wherever the end-user is. Most types of cloud computing providers provide complete, efficient, and scalable backup and retrieval solutions across service types and platforms. Cloud deployment is typically based on a very strong architecture, which provides its users with resilience and redundancy. Scalability is an integrated cloud deployment feature. The cloud instances are automatically deployed upon request and the users are therefore paying for the necessary applications and data storage only.

As mentioned above, mobile cloud computing is a technology that gives its adopters various benefits. It has, however, a number of problems and inefficiencies. Security is the most important problem because of the rising popularity of cloud computing, security is becoming very important and crucial. Security is one of the biggest issues in the cloud, particularly in the event of privacy and confidentiality, such as information about customers or credit cards. It is also very important to monitor the flow of information from or to the cloud since it is very important to maintain the security of data that flows from the cloud to the local users. It is really important to ensure the flow of information when measuring sensitive information in the cloud, where information such as credit card details, government intelligence, or personal health information has handled the cloud, the more sensitive it is to ensure that this information becomes confidential [7]. Compatibility is another problem. In the cloud, each current tool, software, and system should be Web-based, web-based, infrastructure, or platform compatible [8]. The cloud offers a significant advantage in hardware costs, but the price could ultimately be higher than anticipated. The implicit reliance on the provider is one of the major issues of cloud computing. In certain cases, it is difficult and even impossible to switch from a service provider after rolling out its services. The applications and services are therefore operating in a third-party virtual environment remotely, with little control by users and companies over the operation of the hardware and software used. In addition, the features of an application running locally are typically missing due to the remote applications used [8].

2.1 MCC Service Models

Mobile Cloud Computing is a rich mobile computer technology that draws on unified elastic resources from different clouds and network technologies to ensure unlimited functionality, storage, and mobility to serve a multitude of mobile devices everywhere, regardless of the heterogeneous environment and platforms that are pay-per-use. The definition of cloud computing is often divided into three separate service models.

Current Internet clouds for mobile have commonly been categorized into several category models: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaaS), software-as-a- service (SaaS), mobile data-as-a-service (MDaaS), mobile platform-as-a-service (MPaaS), mobile infrastructure-as-a-service (MIaaS) [6,8].

The MCC service models are however better suited for the classification according to the roles of computer entities within their service structure because of both Cyber-Physical System (CPS) and Cyber Virtual System (CVS) participation, where the classification of MCC service models may take advantage of roles and relationships between mobile companies and their cloud-based resource provisioning [7,8]. In this regard, current MCC services can be categorized into three main models: Mobile-as-a-service-consumer (MaaSC), Mobile-as-a-service-provider (MaaSP) and Mobile-as-a-service-broker (MaaSB).

DOI: https://doi.org/10.54216/FPA.070102

MaaSC comes from the conventional client-server paradigm with the initial implementation of virtualization, fine-grained access control, and other cloud-based technologies. Mobile devices should outsource their cloud computing and storage functions to boost performance and additional application ability. The infrastructure is one-way from cloud to mobile devices and mobile devices are service users in this architecture. This category includes most current MCC facilities.

MaaSP is different from MaaSC because the function of a mobile device is changed from a customer to a provider of services. For example, mobile devices can sensor data from devices and their neighboring environment using onboard sensors like GPS, camera, gyroscope, etc., and further distribution of sensing services to other mobile devices via the cloud [6-8]. Consumers offer both cloud-based and mobile-based services. The types of services offered by mobile devices depend on their capacity to sensor and process.

MaaSB can be seen as an extension to MaaSP, when MaaSB offers other mobile devices and sensing nodes networking and data transfer services. MaaSB is wanted in some cases because mobile devices typically have limited sensing capacity in contrast to sensors for specially built functionalities and sensing locations. For example, some sports enterprise does use mobile phones to capture the physical activities of users [2,8]. MaaSB expands the cloud bounds to wireless sensors and mobile devices. Via various connectivity approaches including 3/4G, Bluetooth, WiFi, etc a mobile device could be configurated as a gateway or a proxy providing networking services. In addition, the mobile proxy system will give its user the sensors security and privacy protection.

While the MCC tries to enhance the user's convenience, a lot of challenges still remain the main barriers to the realization of the main intentions of the mobile cloud database. Most of the challenges arise as a result of the reasons which are discussed in Section 3.

3. Mobile Cloud Computing Threats

Numerous research has indicated malicious threats which pose a challenge to the Mobile Cloud Computing paradigm. The following sub-section discusses some of the concerns related to this issue.

3.1 Scarcity of Resources

It is worth to be noted that the presence of technological advancement not only ensures fast communication, but also faces networking, computerization, power capabilities, and storage constraints compared to regular computers. The challenges inhibit mobile device performances and the ability to ensure optimum performance of vital security applications leaving them exposed to attackers. For example, applications like the intrusion detection tool may overuse the mobile's resources, thus shortening its lifespan. Such cases pose a challenge to security and performance pertaining to MCC [7].

3.2 Many Types of Storage Locations and Computations

The data stored on the cell phone are normally sent to the cloud, where it is stored and the majority of computations are downloaded from mobile devices and measured in the cloud. This leaves cloud data and codes vulnerable to attackers in a wide variety of places, including mobile devices, cloudlets, and cloud environments [11]. Mobile computations are also vulnerable, as attackers may target the links used to transfer data and codes. In other words, vulnerable attackers in the mobile cloud service chain are targeting important information or interfering with the computation process.

3.3 Mobility Between Cloud Services

Remote cloud computing is a cloud-based service for smartphones or laptops. It uses mobile and cloud networking technologies through the medium of network services and internet services providers as shown in Figure 2 [12]. The cloud structure maintains the cloud controller unit and the cloud storage database which are in turn connected to the application server. Due to a combination of mobile devices, cloud computing, and wireless communication, there is a wide range of challenges in MCC, including limited mobile resources, reliability challenges due to wireless network constraints, network connectivity costs at different times, elasticity challenges, bandwidth and security challenges.

DOI: https://doi.org/10.54216/FPA.070102

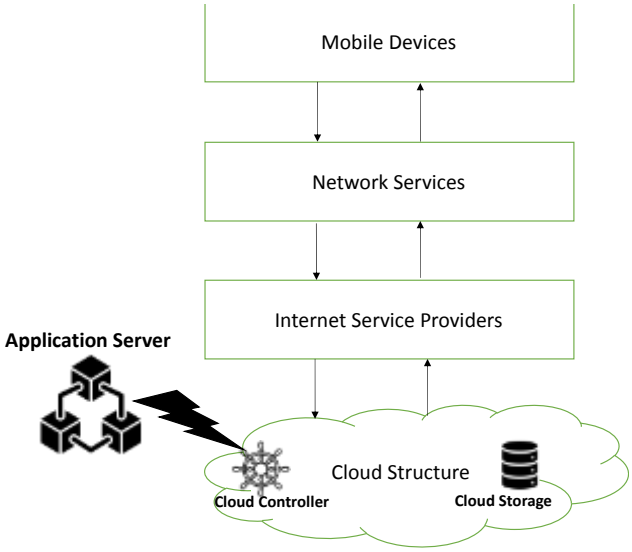

Figure 2: Connectivity of the mobile devices to the cloud structure

The subscribers to a mobile cloud database have unrestricted freedom to migrate data and computations from one public cloud to another depending on the security features of cloud service providers. This leaves the subscribers vulnerable because attackers may interfere with the cloud's specific parameters such as cloud topology and access subscribers' confidential information or maliciously alter the computation process [13].

The recommended way to address the security challenges in cloud computation is to ensure the cloud framework is secure and elastic enough to accommodate various challenges. This solution consists of four components, which are: secure code portioning; offloading; module authentication, and secure data management. These four security measures ensure the privacy of mobile computations in the cloud environment and utilize mobile features to make the whole cloud service secure and efficient. This section will discuss the three aspects in detail.

The proposed solution to ensuring secure code participation and offloading is a secure elastic framework. It contains four components, which include secure installation; secure migration between public clouds; module authentication; and permission authorization [14].

Secure installation components verify if the applications installed are from secure and genuine sources and that they have original hashes. Also, these components check the integrity of the applications and register them with elastic services after successful verification.

The module authentication component helps the installed application authenticate modules belonging to similar applications. Regardless of where the execution is taking place, dependent modules can be executed safely and securely in a sequence with the help of the module authentication component. Upon successful execution of the module, the application manager generates a pair of the session key and session secret that is associated with each module. Both the pair of the session key and the session secret in each module are used to secure and authenticate communication among modules.

A secure migration component makes sure that the migration process is secure by ensuring the module saves its state when migrating.

Permission authorization secures sensitive data by assigning permissions to the application modules. Different authorizations are used to secure modules because modules within an application differ in both functionality and locations. This security measure bases its approach on the argument that modules in the cloud environment should enquire credentials necessary to access sensitive data from the mobile device. Another argument is that modules in a cloud environment should ask the mobile user to finalize the authentication session and send end results to the application modules in the cloud. The following section discusses the impact on mobile devices due to cloud computing security issues.

DOI: https://doi.org/10.54216/FPA.070102

3.4 MCC Security Issue

Mobile devices store valuable information such as vital application data, including credit cards. When it falls into the wrong hands, attackers can get an opportunity to gain access to the important information of a mobile phone user through forensic analysis [15]. Today, there are many forensic tools available that can be used to perform malicious acts. For instance, the Joint Test Access Group was used by attackers to extract mobile users' personal information through the forensic process [15].

The most recent incident of malicious access to mobile users' information was the Carrier IQ software where smartphone users' personal data was illegally accessed and distributed to Carrier IQs subscribers without the knowledge and consent of the smartphone users [16].

Recently, malware attacks have threatened the privacy of most smartphone users through the exploitation of the mobile devices' operating systems. According to Portnoy, 2010 [17], through driven-by downloads, attackers can access and steal information from the iPhone 3GS SMS application. Ginger Master was another threat to android users [18]. This malware was bundled in legitimate applications running behind android phones and collecting mobile user information and submitting it without the permission of mobile users to a remote server.

Generally, if the attacker uses malware to get root permission to a mobile device, then they can interfere with the mobile's operating system as well as its computations. Malware with the capability of controlling the operating system also affects the functionality of other mobile applications and interferes with the integrity of the device computations. Also, wireless communication is prone to hackers such as hardware jammers who interfere with the device's capability of receiving the intended signals [19]. This is because mobiles use wireless communication which is prone to a wide range of attackers who may inhibit the ability of the wireless link to transmit the intended information between the mobile device and the router.

Additionally, the attacker may sense that the mobile user is trying to install applications that may bar them from accessing the mobile device and send a large amount of malicious data that apply specific rules, as a result, overwhelming the resources. Also, malware that executes junk instructions targets availability by draining the power of the mobile device.

As the hacker attacks the mobile operating system (MOS), its associated hardware, software, and communication channel, then the only way to ensure storage security is by encryption of the mobile device and any stored data. One can ensure security by using an independent chip known as the Trusted Platform Module [20], which secures all functions conducted by the SIM card.

Besides SIM card security, the integrity of all mobile applications running in the cloud environment is of importance. One can ensure integrity by securing the mobile device operating system. The OS is secured by using kernel hardening to secure the Mobile Operating System (MOS). By doing so, one can be sure of secure updating and installation as well as controlling security over applications Moreover, Mandatory Access Control (MAC) can be of great benefit if introduced in MOS since it improves overall OS security. Although most modern MOS is designed to update or patch drivers and install both applications and OS modules, mobile users should disable unwanted privileges or allow permission at run time [21]. Another effective security measure is to track when the application accesses critical information or when it’s about to expose such information to untrusted entities [22].

When the data is submitted to the cloud to be stored or computed, it becomes vulnerable to malicious attacks [23]. This is because most cloud architectures create a clone of the mobile device on the cloud environment making it possible for execution to occur in the cloud. The integrity adopted in the cloud computation does great in protecting virtual information in the cloud but fails to protect the information in physical mobile devices. Most cloud technologies allow the users to upload their data and personal information virtually as Virtual Machines (VMs) for their execution in the cloud environment. Also, many virtual machines allow sharing of a single server to save resources, which results in a security mismatch.

Although a cloud's intention is to keep the data and information being executed confidential, the cloud environment does not guarantee the security of the data or code executed in the device. For example, the Dynamic Data Kernel rootkit can be used to target virtual data and interfere with the execution of data and code by most host mobile devices as a result of interfering with all running of virtual machines[24][25].

Also, certain malware may suspect their execution in the cloud and alter their behavior accordingly to pass the cloud's security gates [26].

DOI: https://doi.org/10.54216/FPA.070102

Besides the availability attacks that may affect access links to the cloud, there are other threats that may pose serious threats to the cloud. For instance, the attackers may target particular cloud links. Lastly, the mobility of computation between clouds paves way for attackers to interfere with the virtual data and computations [27].

During the literature review of the MCC frameworks listed in the previous section, we have been able to synthesize some of the major MCC problems and challenges that the authors have identified. These issues and challenges have been categorized and illustrated using **Figure 3.** Mobile cloud users have serious questions about cloud data protection. Data security is one of the greatest obstacles for users to transfer their data to the cloud. Some of the common cloud data issues have been outlined as follows [28][23][29].

1. Data fraud risk

2. Data protection is the responsibility of customers

3. Violation of rights to privacy

4. Threat mitigation failure

5. Encryption and decryption key handling

6. Digital computer stability and auditing problems

7. Standard lack to guarantee data integrity

8. Incompatibility of services because of different vendors

The cloud technology questions about the data life cycle that must also be standardized so that users can adopt and use cloud data services. Some of the points pertaining to this issue are highlighted as follows [22][30][31][13]:

1. Data generation

2. File transfer

3. Data usage and exchange

4. Archiving and loss

In addition to threats to data protection on the cloud side, certain attacks on mobile end users are also possible. These issues are highlighted as follows [28][27][32]:

1. Theft of device data

2. Attacks of viruses and malware via wireless devices

3. Misuse of freedom of access

DOI: https://doi.org/10.54216/FPA.070102

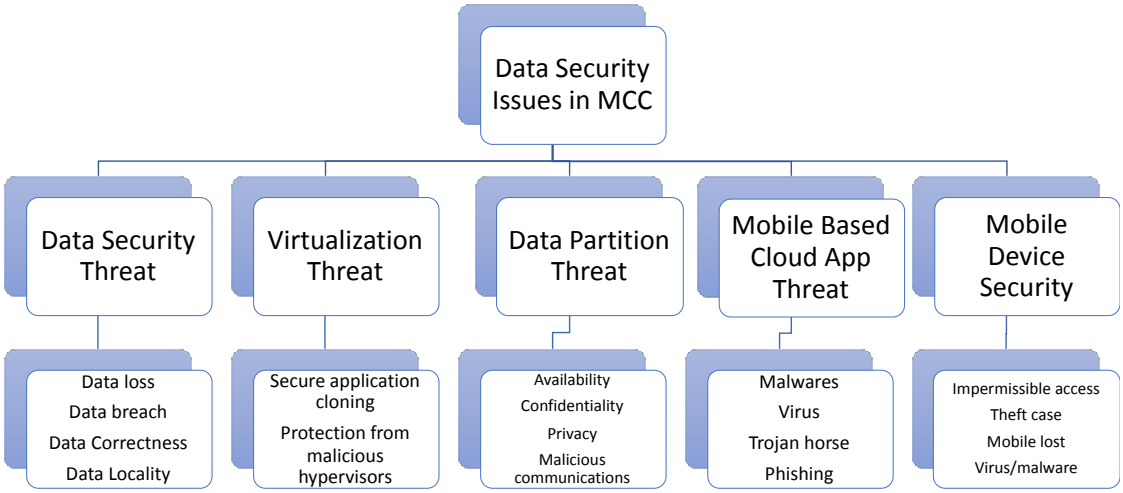

Figure 3: The hierarchal structure of data security issues in MCC

With respect to the information security associated with the cloud environment, some of the common security issues are highlighted as follows [14][32][33][13]:

1. Server and Database System Security

2. Protection of networking

3. Authentication of the consumer

4. Protection of data

5. Protection of device and storage

Considering the many threats targeting various components of a mobile cloud database, there are more than enough solutions that have been proposed to overcome these security issues. For heightened confidentiality, availability, and integrity of cloud computing, here are some trusted security measures that ensure mitigation of mobile cloud security challenges which are discussed in the following section.

4 Mobile Cloud Computing Security Solutions

The primary objective of MCC is the ability for users to easily and conveniently access the data from the cloud with their mobile devices. While improving user convenience, several issues still exist and remain in MCC implementation. When it comes to mobile devices that use cloud computing, the first thing to look at is to secure data transactions and threat-free implementation of cloud-based applications. The following sub-sections discuss some of the solutions to overcome the aforesaid security issues in MCC framework.

4.1 Security Guest Systems

One can control access to the mobile device by enforcing security policies that only authorize specific parties to access data and applications. Since the user cannot secure data stored in the cloud from cloud administrators if the data is stored without security measures. One promising solution is to use cryptographic security to encrypt cloud data. Cryptographic is the most secure solution because it's hemimorphic encryption that secures cloud data and computations. Full hemimorphic encryption ensures computations are performed directly over encrypted data and results are encrypted too and only the mobile device user can decrypt the results [34].

DOI: https://doi.org/10.54216/FPA.070102

Another way of securing data stored in the cloud is encrypting as cryptographic commitments [35]. This way informs the user of all processes in the cloud and notifies the user when a computation needs to be processed physically from the user's end. Once all computations have been completed, results are sent alongside commitments and zero-knowledge proof back to the cloud Then the cloud takes the initiative to review the results submitted with a commitment to ensure that all measurements are integral.

4.2 Virtual Machine Managers (VMM)

This is another way of ensuring mobile-cloud database security because it controls a wide variety of guest systems in the cloud. VMM secures multiple guest systems by ensuring another guest shall not endanger another guest system [36]. In other words, VMM ensures a guest performs their own computation as expected without interfering with other guests' computations. VMM achieves this security mechanism by creating boundaries between guests' computation resources [37]. VMM boundaries host each guest machine by machine in specific locations. The shortcoming of VMM is that guest system sharing the same computer share resources such as caches and memory CPU cores which makes it difficult to isolate guests. Resources such as cache are almost isolatable because it's situated in the CPU and not directly controlled by QoS provision VMM [38].

The proposed solution to this problem is grouping cores in the same Logical Link Control (LLC) and assigning the groups to a particular guest system. As such, each guest will have its own cache. The only shortcoming to this process is that if resources are underutilized at the group level, then they can be assigned to the other immediate guest system.

Additionally, further integrity check on the guest system is necessary because it may become prone to attacks when accessing the internet. As such, it's important for the user to ensure the guest system is secure from malware interferences during execution Through introspecting the virtual machine, the user can protect the device. Virtual machine introspection tracks the current status of mobile device modules, including processors, and internal storage to detect any disruptive activities[15]. Checking the execution of the code in the guest system is the second security check that ensures heightened security in mobile device components Entire solutions must be stored in the VMM, so they have the access to the guest system's actions and thus compare the predicted behavior.

Further, the user-control security measure is another challenge that targets mobile-cloud databases because the user creates, uploads, and retrieves virtual memory images and their dimensions which may make personal information vulnerable to attacks. One may download malicious data from the cloud because the primary task of the cloud is not to choose data that is secure or not but to store users' data and allow downloads for authorized users. As such, it's necessary for the mobile device user to securely manage data in the cloud. One can manage data in the cloud using Mirage; this is a virtual machine image management system with four components. Mirage manages virtual machine data through a framework that controls and regulates the retrieval of virtual machine data/images by filtering and removing or denying access to vital/sensitive data while sharing data in the cloud. Also, it acts as a tracking machine that tracks the data history including when the data was received and when the user generates new data [39]. Lastly, the component of Mirage involves repository maintenance that acts as a detector that fixes any present issue that makes images or data vulnerable [29].

The mobile cloud allows the user to customize communication among groups and set up different security levels that enhance mobile cloud data security. However, this might put sensitive information at risk because the cloud infrastructure is complex. To enhance the security of the user's information, it's important to enhance the end-user security through configurations to ensure an uninterrupted flow of information from one point to another.

4.3 Ad Hoc Mobile Clouds

Ad Hoc Mobile clouds threats arise from code distribution mechanisms that allow specific users' codes to be executed by multiple parties including mobile users, a hybrid, or cloudlet components. Some mobile applications are executed through code segments with the help of nearby devices because their execution on a single device is not feasible [40]. Some of the reasons that limit the capability of a single device to execute a whole application are limited battery power, since some mobile devices may have a limited battery life to execute an application to completion; limited access to the server, the mobile device may have limited capability to access the server infrastructure e.g., when the device in dead zones.

The reliance on the distribution mechanism to execute an application exposes the executing code segment to malicious interferences. Malicious nodes may collude to reverse engineering code segments exposing the functionality and code's capability. If a mobile server uses a nearby server to execute a code segment on its behalf, they are likely to experience

DOI: https://doi.org/10.54216/FPA.070102

non-responding computations or get incorrect results. The results from the distribution mechanism cannot be verified to be true unless the results are compared to the results from another device executing the same code segment. Ad Hoc Mobile Clouds challenges result from mobile nodes links attacks such as Jamming, and Dos may interfere with the code distribution modules. These attacks prevent the requesting mobile device from getting accurate results, add work on the redistribution segment and lead to latencies Moreover, there can be a threat to availability as a result of malicious attacks which cause the mobile device to drain its energy. Such malware requires a great deal of CPU computing and communication which leads to increased energy consumption.

It is deemed necessary to note that only with a powerful encryption algorithm, a reliable and powerful communication structure can be guaranteed to achieve integrity and confidentiality. Encryption algorithm prevents attacks such as eavesdropping because it ensures that once the data is sent to the cloud it cannot be altered in any way by either the sender or a malicious code [41].

Sandboxing technique is another security measure that separates the device task processes from the host. Sandboxing restricts the host resources and prevents any impacts on the host due to the processing of tasks from other devices [42].

Antivirus software is another measure that can protect against threats in the ad-hoc cloud. Antivirus software protects the device from malicious attacks and can be used in the ad-hop cloud to ensure the trustful sharing of services [28]. In addition, security can be accomplished in an ad-hoc cloud through two approaches that protect a Mobile Ad-hoc Network (MANET)[43]. MANET provides multi hoc connectivity through distributed protocols in both the links and the server using a proactive approach and a reactive approach. The proactive approach attempts to prevent security threats while the reactive approach detects attacks and takes actions accordingly to prevent their harm. Using either of these approaches can be helpful in fighting threats in the ad-hoc mobile cloud [44]. However, it's advisable to use the two approaches together because the two incorporate three components, that is prevent, detect and react to malicious nodes [45]. The prevention component deters the attacker by creating prevention measures that make it difficult for malicious ware to penetrate the system. However, it's obvious that malicious nodes always find a way of penetrating prevention walls no matter the prevention component put in place. As such, it is recommendable to use the next component which is the reaction component. The reaction component detects the intrusions and takes the necessary actions to prevent adverse effects to the whole system detection component detects ongoing malicious activity by identifying abnormal behaviors of an application as a result of malicious nodes.

Typically, malicious behavior shows in an end-to-end manner or through overhearing the channel and achieving collaborative consensus. As soon as the malicious node is detected, the reaction component takes action in the routing operations. These actions include preventing the node from affecting the route section and keeping the node off the network.

5 Mobile Cloud Application Challenges

The most common attackers in a cloud-based mobile application are viruses, worms, Trojan, etc. These attackers interfere with the integrity and confidentiality of the application processes. This malware usually hides in fancy applications and the mobile user may install them without knowing. As a result, they alter the performance of mobile cloud applications.

From an overall perspective, attackers inject malicious codes into a target application and republish them to the mobile user application to download and run them on their system/device. A secure and stable mobile cloud is the proposed solution to this security threat[46]. A secure and stable mobile cloud ensures data computing protection in all mobile device application components and in the cloud environment. Also, it ensures the integrity of the mobile application whenever the user installs a new application to the mobile device [30]. This security measure verifies the existence of an application by searching the name of the application on the application stores and comparing the signature of the application with similar applications found in the app store. If the signature matches, then there is no malicious ware attached to the application. This security measure includes four framework managers, they are cloud security; mobile device security; optimization; policy [33].

The mobile device manager framework gathers all the events happening on the mobile device and sends them to the other concerned manager. The mobile security framework confirms that the mobile device security is present whereas the optimization manager framework gathers information from the mobile application and sends them to the appropriate manager [47]. Additionally, while the application manager verifies the integrity of installed applications, the policy manager defines the security measure to take to solve security threats [48].

DOI: https://doi.org/10.54216/FPA.070102

The hybrid attribute and protocol protection-based re-encryption[49][50] is another approach to this security problem. This security protocol uses re-encryption techniques and group keys to ensure that the attribute-based encryption is checked and that the key-generation responsibility is shared between a mobile device and a trusted entity[49]. The group key mechanism has the responsibility of providing added security by providing a group key security that is shared among trusted users. Typically, encryption involves data encryption to keep data secure [49].

One of the security measures proposed by Habak et al.,[51] is the edge-based elastic mobile application security. This security measure secures communication, authentication, and migration within components both in the mobile device and cloud. It has three parts; mobile application elasticity manager, application manager, and cloud manager. The device elasticity manager locates the components of the application and accordingly chooses a secure and stable communication path. The cloud manager controls resources and computations, bandwidth, and storage information of components running in the cloud environment [52]. Finally, the cloud manager allows the installation and launching of application components in different cloud nodes.

As a safeguard to ensure the deployment of untrusted mobile applications in the cloud world, Tan et al[53][54] suggested a Strict, Observable, Verifiable Data(STOVE) approach. STOVE works by isolating the untrusted application from the genuine ones and does not access any unauthorized data. However, if the mobile user still needs to install an untrusted application, STOVE verifies the untrusted application and executed all data access in favor of the application, and makes all data access observable [32]

Additionally, Mobile Application Assessment Cloud Architecture (MAACA) is another proposed mobile-cloud database security measure. It conducts the security duties through components such as frontier interface, service data center, analysis engine, and service manager [55]. All these components are implemented in the cloud environment and each component is assigned a particular duty. The frontier interface uploads mobile applications for assessment and sends the assessment report to the user. After authentication, the service manager sends assessments with device user information to the analysis engine. Service data center stores all necessary data for assessment. Lastly, the analysis engine assesses all the uploaded applications and then sends the assessment report to the service data center for safe keeping [56].

The security solution illustration can be taken into consideration by MCC company to provide better secure and reliable features to their customers. This will not only make the MCC company sustainable but will also generate substantial revenue for them to grow more and more. As, the final segment, the following section marks the conclusion of this review study.

6 Conclusion

This paper has compiled a comprehensive and extensive study on various security issues pertaining to the mobile-cloud database and its solutions. The initial segment of the manuscript introduced a mobile cloud database followed by various factors that attribute to the challenges currently being faced by the mobile cloud computing industry. Then, a later segment of the manuscript discussed a wide range of security threats related to mobile clouding computing architectures and showcased that attackers can use various ways to exploit a wider range of mobile cloud database environment resources. At last with the advent of this review, a new corridor can be opened for the researchers to enhance MCC to secure data, computations, and information stored in the cloud environment.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] K.-Y. Chung, J. Yoo, and K. J. Kim, “Recent trends on mobile computing and future networks.” Springer, 2014. https://doi.org/10.1007/s00779-013-0682-y

[2] L. Zhong, B. Wang, and H. Wei, “Cloud computing applied in the mobile internet,” in *2012 7th International Conference on Computer Science & Education (ICCSE)*, 2012, pp. 218–221. doi: 10.1109/ICCSE.2012.6295061

[3] E. Hossain and M. Hasan, “5G cellular: key enabling technologies and research challenges,” *IEEE Instrum. Meas. Mag.*, vol. 18, no. 3, pp. 11–21, 2015. doi: 10.1109/MIM.2015.7108393

DOI: https://doi.org/10.54216/FPA.070102

[4] T. Olokunde, S. Misra, and A. Adewumi, "Quality model for evaluating platform as a service in cloud computing," in *International Conference on Information and Software Technologies*, 2017, pp. 280–291.

[5] S. Bhardwaj, L. Jain, and S. Jain, "An approach for investigating perspective of cloud Software-as-a-Service (SaaS)," *Int. J. Comput. Appl.*, vol. 10, no. 2, pp. 40–43, 2010. https://doi.org/10.1007/978-3-319-67642-5_23

[6] S. Satyanarayana, "Cloud computing: SAAS," *Comput. Sci. Telecommun.*, no. 4, pp. 76–79, 2012.

[7] Ahmed Alzahrani, Nasser Alalwan, and Mohamed Sarrab. 2014. Mobile cloud computing: advantage, disadvantage and open challenge. *In Proceedings of the 7th Euro American Conference on Telematics and Information Systems (EATIS '14). Association for Computing Machinery, New York, NY, USA,* Article 21, 1–4. DOI:https://doi.org/10.1145/2590651.2590670

[8] M. Gopichand, "A survey on service models in mobile cloud computing," *International Journal of Computer Sciences and Engineering,* vol. 7 (5), pp. 1666-1671, 2019.DOI: https://doi.org/10.26438/ijcse/v7i5.16661671

[9] S. S. Manvi and G. K. Shyam, "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey," *J. Netw. Comput. Appl.*, vol. 41, pp. 424–440, 2014. https://doi.org/10.1016/j.jnca.2013.10.004

[10] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These aren't the droids you're looking for: retrofitting android to protect data from imperious applications," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 639– 652. https://doi.org/10.1145/2046707.2046780

[11] T. Verbelen, P. Simoens, F. De Turck, and B. Dhoedt, "Cloudlets: Bringing the cloud to the mobile user," in *Proceedings of the third ACM workshop on Mobile cloud computing and services*, 2012, pp. 29–36.

[12] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme*, vol. 20, no. 9. Stanford university Stanford, 2009.

[13] H. Liu, "A new form of DOS attack in a cloud and its avoidance mechanism," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, 2010, pp. 65–76.

[14] S. He, L. Guo, and Y. Guo, "Elastic application container," in *2011 IEEE/ACM 12th International Conference on Grid Computing*, 2011, pp. 216–217.

[15] B. Taubmann and H. P. Reiser, "Bringing Memory Forensics and Virtual Machine Introspection to Production Environments," 2018.

[16] K. Rosenfeld and R. Karri, "Attacks and Defenses for JTAG," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 36–47, 2010.

[17] A. Portnoy, "Pwn2Own wrap up and analysis," *Netw. Secur.*, vol. 2010, no. 4, pp. 4–5, 2010.

[18] F. Zou, S. Zhang, T. Wan, and L. Pan, "A survey of android mobile platform security," 2014.

[19] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 127–134.https://doi.org/10.1145/1655008.1655026

[20] R. N. Akram, K. Markantonakis, and K. Mayes, "An introduction to the trusted platform module and mobile trusted module," in *Secure Smart Embedded Devices, Platforms and Applications*, Springer, 2014, pp. 71–93.

[21] W. J. Buchanan, S. Chiale, and R. Macfarlane, "A methodology for the security evaluation within third-party Android Marketplaces," *Digit. Investig.*, vol. 23, pp. 88–98, 2017.

[22] Y. Liao, Y. He, F. Li, and S. Zhou, "Analysis of a mobile payment protocol with outsourced verification in cloud

DOI: https://doi.org/10.54216/FPA.070102

server and the improvement," *Comput. Stand. Interfaces*, vol. 56, pp. 101–106, 2018. https://doi.org/10.1016/j.csi.2017.09.008

[23] V. Moorthy, R. Venkataraman, and T. R. Rao, "Security and privacy attacks during data communication in Software Defined Mobile Clouds," *Comput. Commun.*, vol. 153, pp. 515–526, 2020. https://doi.org/10.1016/j.comcom.2020.02.030

[24] A. Druffel and K. Heid, "DaVinci: Android App Analysis Beyond Frida via Dynamic System Call Instrumentation," in *International Conference on Applied Cryptography and Network Security*, 2020, pp. 473–489. https://doi.org/10.1007/978-3-030-61638-0_26

[25] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," *Futur. Gener. Comput. Syst.*, vol. 89, pp. 525–538, 2018.https://doi.org/10.1016/j.future.2018.06.053

[26] J. Zhang, B. Wang, F. Xhafa, X. A. Wang, and C. Li, "Energy-efficient secure outsourcing decryption of attribute based encryption for mobile device in cloud computation," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 2, pp. 429–438, 2019. https://doi.org/10.1007/s12652-017-0658-2

[27] P. Kulkarni, R. Khanai, and G. Bindagi, "Security frameworks for mobile cloud computing: A survey," in *2016 international conference on electrical, electronics, and optimization techniques (ICEEOT)*, 2016, pp. 2507–2511.

[28] T. McGill and N. Thompson, "Old risks, new challenges: exploring differences in security between home computer and mobile device use," *Behav. Inf. Technol.*, vol. 36, no. 11, pp. 1111–1124, 2017.

[29] L. Bordoni, M. Conti, and R. Spolaor, "Mirage: Toward a stealthier and modular malware analysis sandbox for android," in *European Symposium on Research in Computer Security*, 2017, pp. 278–296.

[30] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. P. C. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Ind. Informatics*, vol. 15, no. 1, pp. 457–468, 2018.doi: 10.1109/TII.2018.2824815

[31] M. Satyanarayanan, "Mobile computing," *ACM Trans. Comput. Syst.*, vol. 10, p. 1, 1992.

[32] S. Kumar, M. Tyagi, A. Khanna, and V. Fore, "A survey of mobile computation offloading: applications, approaches and challenges," in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2018, pp. 51–58.

[33] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Futur. Gener. Comput. Syst.*, vol. 68, pp. 74–88, 2017. https://doi.org/10.1016/j.future.2016.09.009

[34] W. Magonga, "A Secure end to end verifiable e-voting system using cryptography: a case of Independent Electoral and Boundaries Commission of Kenya." Strathmore University, 2019.

[35] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, 2019.

[36] S. M. N. Islam and M. M. Rahman, "Securing virtual machine images of cloud by encryption through Kerberos," in *2017 2nd International Conference for Convergence in Technology (I2CT)*, 2017, pp. 1074–1079.

[37] D. Xu, C. Fu, G. Li, D. Zou, H. Zhang, and X.-Y. Liu, "Virtualization of the encryption card for trust access in cloud computing," *IEEE Access*, vol. 5, pp. 20652–20667, 2017.

[38] M. S. Rahman, I. Khalil, A. Alabdulatif, and X. Yi, "Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform," *Knowledge-Based Syst.*, vol. 180, pp. 104–115, 2019.

DOI: https://doi.org/10.54216/FPA.070102

[39] R. Spolaor, "Security and Privacy Threats on Mobile Devices through Side-Channels Analysis," 2018.

[40] A. J. Ferrer, J. M. Marquès, and J. Jorba, "Towards the decentralised cloud: Survey on approaches and challenges for mobile, ad hoc, and edge computing," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–36, 2019. https://doi.org/10.1145/3243929

[41] T. H. Noor, S. Zeadally, A. Alfazi, and Q. Z. Sheng, "Mobile cloud computing: Challenges and future research directions," *J. Netw. Comput. Appl.*, vol. 115, pp. 70–85, 2018.

[42] S. Narain and G. Noubir, "Mitigating location privacy attacks on mobile devices using dynamic app sandboxing," *Proc. Priv. Enhancing Technol.*, vol. 2019, no. 2, pp. 66–87, 2019.

[43] S. Kausar *et al.*, "Secure and efficient data transfer using spreading and assimilation in MANET," *Softw. Pract. Exp.*, vol. 50, no. 11, pp. 2095–2109, 2020.https://doi.org/10.1002/spe.2782

[44] A. Al-Omary, "A Secure Framework for Mobile Cloud Computing," in *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2019, pp. 1–6.

[45] A. M. Desai and R. H. Jhaveri, "Secure routing in mobile ad hoc networks: a predictive approach," *Int. J. Inf. Technol.*, vol. 11, no. 2, pp. 345–356, 2019. https://doi.org/10.1007/s41870-018-0188-y

[46] S. Al_Janabi and N. Y. Hussein, "The reality and future of the secure mobile cloud computing (SMCC): survey," in *International Conference on big data and networks technologies*, 2019, pp. 231–261.

[47] R. Neware, K. Ulabhaje, G. Karemore, H. Lokhande, and V. Dandige, "Survey on Security Issues in Mobile Cloud Computing and Preventive Measures," in *Smart Computing Paradigms: New Progresses and Challenges*, Springer, 2020, pp. 89–100.

[48] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, 2017.

[49] N. Mahakalkar and V. Sahare, "Implementation of re-encryption based security mechanism to authenticate shared access in cloud computing," in *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, 2017, pp. 547–550. doi: 10.1109/ICOEI.2017.8300719

[50] A. S. V. Koe and Y. Lin, "Offline privacy preserving proxy re-encryption in mobile cloud computing," *Pervasive Mob. Comput.*, vol. 59, p. 101081, 2019.

[51] K. Habak, C. Shi, E. W. Zegura, K. A. Harras, and M. Ammar, "Elastic mobile device clouds: Leveraging mobile devices to provide cloud computing services at the edge," *Fog 5G IoT*, p. 159, 2017.

[52] H.-Y. Lee and N.-J. Wang, "Cloud-based enterprise resource planning with elastic model–view–controller architecture for Internet realization," *Comput. Stand. Interfaces*, vol. 64, pp. 11–23, 2019. https://doi.org/10.1016/j.csi.2018.11.005

[53] J. Tan, R. Gandhi, and P. Narasimhan, "STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications," in *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, 2014, pp. 644–649.

[54] O. M. Alofe and K. Fatema, "Trustworthy Cloud Computing," in *Data Privacy and Trust in Cloud Computing*, Springer, 2020, pp. 129–145. https://doi.org/10.1007/978-3-030-54660-1_7

[55] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and M. Abdelhag, "Mobile cloud computing: challenges and future research directions," in *2017 10th international conference on developments in esystems engineering (DeSE)*, 2017, pp. 62–67.

[56] K. Habak, E. W. Zegura, M. Ammar, and K. A. Harras, "Workload management for dynamic mobile device clusters in edge femtoclouds," in *Proceedings of the second ACM/IEEE symposium on edge computing*, 2017, pp.

DOI: https://doi.org/10.54216/FPA.070102

1–14.https://doi.org/10.1145/3132211.3134455

DOI: https://doi.org/10.54216/FPA.070102