2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA) | 978-1-6654-7709-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ETCEA57049.2022.10009662

Review of Security Challenges in Mobile Cloud Computing Applications

1st Majd Alqarqaz
dept. Computer Science
Philadelphia University
Amman, Jordan
majd_alqarqaz@yahoo.com

2nd Maram Bani Younes
dept. Cybersecurity and Information Security
Philadelphia University
Amman, Jordan
mbani047@uottawa.ca

***Abstract*—Mobiles and smartphones recently store huge amounts of valuable information such as personal information, financial transactions, social applications, and call records. These devices allow the transmission of data, by voice, text, or video, at anytime and everywhere. They enable easy access to the required information. The huge development of mobile devices has introduced the ability to use new and advanced applications. In several scenarios, the advanced applications require a connection to the cloud services. This affects the general environment, infrastructure, and security challenges of mobile applications. In this paper, we mainly aim to investigate the security challenges and issues of Mobile Cloud Computing (MCC) applications. First, we discuss the most popular applications of MCC. Then, we present an adversary and threat model that determines the main security challenges and issues in these applications. We summarize some security techniques, that have been used to tackle these challenges and determine their main requirements. Finally, clear recommendations regarding the directions and required research in this field are given in the paper.**

***Index Terms*—Mobile computing, Mobile cloud computing application, Security issues, Security attacks, Security techniques.**

I. Introduction

Mobile devices could be used while moving to finish a digital task or use a certain application. This requires connection to wireless internet services most of the time. Mobile devices could be cellular (i.e., smartphones), laptop computers, tablets, PDAs, or any other portable device. The popularity of mobile applications in modern society has increased due to the fast internet spreading and the advances in mobile technology. Mobile applications are simply software applications running on mobile devices [1]. Moreover, the term Mobile Computing is often used to describe the type of technology that combines wireless networks with computing on mobile devices. It is an interaction between humans and computers that enable text, voice, and video to be transmitted and processed.

Recently, mobile applications have been connecting to cloud servers due to the limited storage and capacity of mobile devices [2]. This requires a strong and sustainable connection to the internet [1]. We refer to the union between these two technologies by Mobile Cloud Computing (MCC). This is an ideal technology that enables people to access services in all circumstances and anywhere, it offers flexibility over physical mobility for the computing environment. Data information or other logical objects can be accessed from any device in the network. To make the mobile cloud computing environment ubiquitous, the transporter connections must be distributed through wired and wireless media [3].

However, this technology introduces several problems and challenges that should be tackled. The security conditions and privacy of users are the main issues to be considered here. Accessing emails, social media accounts, or bank accounts should be secure and safe over mobile devices [4]. Otherwise, no one would venture to use them. For example, smartphones collect sensitive information, which must be monitored to protect the privacy of the user and his information whether it is personal, financial, or others. Otherwise, all smartphones are preferred targets for attacks that can come from communications like SMS, MMS, or WIFI networks that these attacks exploit [5]. Mobile cloud computing has committed to developing mobile applications and meeting the security challenges of mobile devices with cloud computing [6]. This makes it a vital problem to secure mobile information and applications and the growth of mobile computer networks creates new security challenges [7].

In this work, we aim to investigate the most popular applications in mobile cloud computing. Develop an adversary and threat model that determines the main security challenges and/or threat to these applications. Summarize the previously proposed security and privacy solutions that aimed to tackle these issues and remark on the requirements, success, and gaps of these solutions. In general, the paper provides some directions for future studies in this field of research.

The rest of this paper is organized as follows: Section II illustrates previous studies that aimed to investigate security challenges in mobile cloud computing. Section III defines mobile cloud computing, the most popular applications in MCC, and their advantages. Section IV introduces an adversary model that determines the main security and privacy challenges in the applications of MCC. Section V summarizes some previous solutions that have been used to tackle the determined challenges. Section VI discuss and remarks on the previously proposed solutions and highlight the existing gaps. This should direct researchers towards open issues in this field of work. Finally, Section VII concludes the entire paper.

This work is supported by Philadelphia University.

II. Literature review

Several research studies have been introduced in the literature aiming to define the challenges and issues in the mobile cloud computing and its applications. Security and privacy issues are considered the main challenges that have been deeply investigated to encourage safe usability of applications on this environment [8], [9].

These issues are considered the obstacles that stop users from shifting their data into the cloud environment. Safely storing data on the cloud has to tackle the data integrity, loss of physical security, and the risk of data theft issues. Moreover, the architecture, infrastructure and communication channels of mobile cloud computing introduce serious challenges for security concerns. In general the security of MCC applications has been directly connected to the cloud data security as discussed by Abid and Mureed [10].

The security vulnerabilities in different mobile cloud frameworks have been investigated by Suleman et al., [11] and Vaishnavi et al., [12]. The general vulnerabilities are summarized by the mobility nature of connecting devices, heterogeneity of hardware setup, wireless access, platform integration, application functionalities and features, and a variety of client devices and specifications. Nikil and Aloysius [13] have summarized the security issues on the mobile cloud environment by the poor authorization, poor authentication, sensitive information disclosure, broken cryptography, free applications for transmission data, server-side controls, and client-side injection. The smartphone security problems are directly connected to the security of web applications and connecting network. It witness the same physical threats, vulnerabilities, Trojans, Botnet, Worms, and Rootkits.

Integrating the cloud computing and mobile computing has arisen several new challenges. That are summarized by identity privacy, data security, data privacy, security of mobile cloud applications, and security of mobile devices [8]. Indeed, the security of MCC has to maintain and involve new classes of challenges inherited from the combined use of new technologies. The combination of mobile devices and cloud environment becomes increasingly difficult to address the new challenges presented. For example data, application, virtualization and remote implementation are vulnerable in the absence of direct user control. Several problems are still open and must be resolved to ensure a secure MCC environment. A comprehensive and integrated security solution is needed to address these security and privacy requirements.

Using mobile phones for gaming, surfing the internet and money transfer introduce several vulnerabilities that attackers can exploit through unprotected mobile devices [14], [15]. Mobile applications should specify the security issues of using mobile phones, computers, and tablets. Algarni et al., [16] connected the mobility and security issues in order to ensure the privacy of users and secrecy of exchanged information. The user's mobility and data introduce problems regarding the secrecy and authenticity of the information exchanged between the users and between a user and a fixed host. Secure data transfer from databases at location nodes to other user profile information or parameters. All network-sensitive and transparent traffic must be kept safe and authentic for the nomadic user.

During developing the services and applications for mobile devices, every safety issue needs to be addressed. The most popular threats to mobile security include the complexity of technical solutions and illegal copying of internet programs, content and threats. Tong et al., [17] presented a comprehensive study regarding mobile computing environment security issues. In general, security risks confronted with mobile computing, infrastructure-based security risks of wireless local area networks (WLANs), and infrastructure-free ad-hoc network vulnerabilities. The designing and operating features of WLANs cause most of the security concerns. Mobility, power-restricted hosts that encourage mobility and portability have restricted physically and network bandwidth. However, securing WLANs has been partially tackled with numerous security solutions.

Furthermore, Naveen and Soniya [18] presented some challenges in terms of the physical, logical and network categories related to the safety of mobile devices. The confidentiality of stored data and storage units should be kept safe, to ensure they are not lost or stolen. Besides, the confidentiality of personal data like the bank account number and the ATM password stored on your mobile device should not be known to others if the device gets lost or stolen. Mobile devices support wireless connecting and remote control activities. This is often affected by the removal of confidential and sensitive information such as usernames and passwords. Malware that installed to mobile devices as a game, patch or other useful software applications for third parties. It is transferred to the mobile device as Trojans which appear to be featured but contain malicious insider attacks. As security policies are lacking in awareness, there have been many violations.

In this paper, the study uses the characteristic of the cloud frameworks to investigate the security challenges in mobile cloud computing. The responsibility of security depends on the cloud features, the operating system for mobile device, and the internet service provider (ISP) for the internet. We investigate some security solutions and remark on the open issues for developing in this field.

III. Mobile Cloud Computing and Its Applications

Mobile cloud computing (MCC) has evolved from two hot technological trends, mobility and cloud [6]. The development of cloud computing and the development of the mobile domain create the potential for a global, interconnected mobile cloud computing environment. This is to enhance the entire mobile ecosystem's services across several networks. Mobile cloud computing aims to overwrite mobile terminal limitations such as mobile devices, and Wi-Fi sensors. This is mainly due to the lack of computer resources (e.g., processing capacity, and

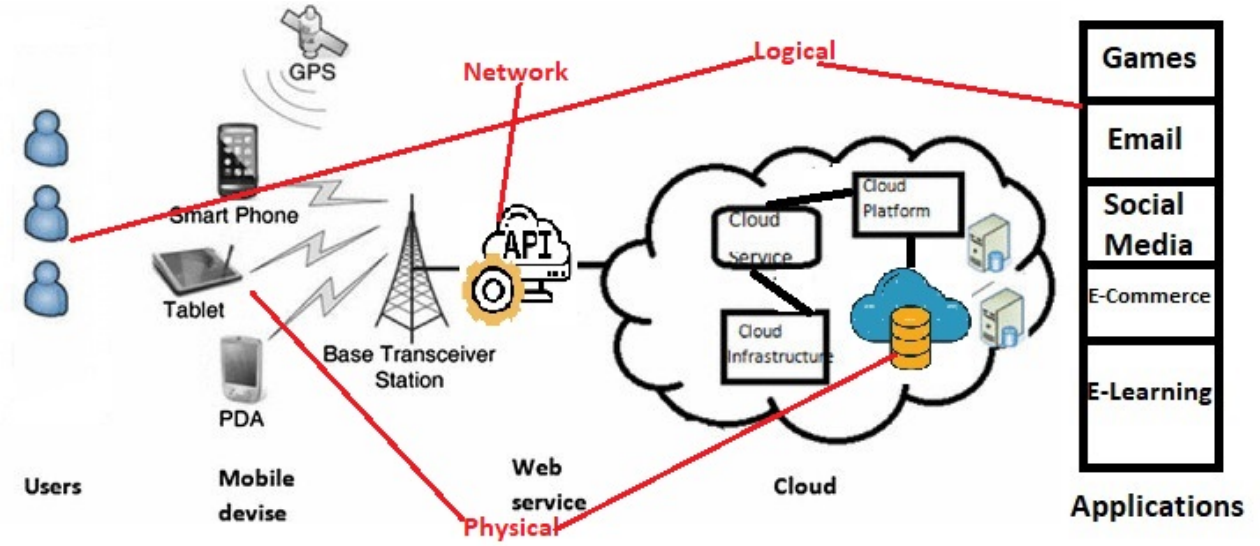

Fig. 1. MCC Architecture

data storage), communication (i.e., limited 3G and even 4G data rates), and power (i.e., battery life).

The ultimate aim of MCC is to make it possible to run high-mobile applications on many mobile devices. This requires a high level of user experience. MCC provides both mobile network operators and cloud suppliers with business opportunities. Mobile computing offers flexibility over physical mobility in the computer environment, enabling people to access services in any circumstance and anywhere. The evolution of mobile phones made various usages. This increased the new applications possibilities in mobile scenarios.

In general, the applications of MCC are as classified based on their purposes as follows: games, email applications, social media, E-commerce, and E-learning. In these applications, a graphical user interface appears on mobile devices for each application. However, all complex works and computations are sent to the cloud to protect the resources of a mobile device, such as battery and storage [19]. Figure 1 illustrates the general architecture of the MCC. The

- **Games** Kids, teenagers and even some adult are daily holding their mobile devices for hours playing online games. The technology of MCC allows a sophisticated interface on each mobile to control and run more complex computations and extensive work on the cloud [19].
- **Email applications** Gmail, Outlook, and Yahoo Mails are examples of email applications that have proposed a mobile version of their applications. Whenever the user inserts the the information of his/her email accounts using a mobile phone, they are transferred into mobile cloud technology [22].
- **Social Media** Twitter, Instagram, or Facebook, are important examples of social media that allow data sharing, users can store data and share videos with other users [20].
- **E-commerce** Banking and e-shop applications on mobile devices are examples of mobile E-commerce. They allow several money transactions like transferring money and bills payment. Moreover, they can use the e-shop applications to check orders for what they want to buy and ship using a mobile app [20].
- **E-Learning** E-learning allows educators to teach at or outside the classroom in places where learning takes place naturally. Zoom, MS Teams, and Google-class rooms are examples of using applications that allow teaching online without being limited by time or place [21].

Three main general advantages can be easily extracted for MCC:

- **Flexibility:** Applications of MCC can easily be built and updated with cloud services. They can be accessed using several platforms. This is due to the fact these applications are supported by the most popular operating systems (Android, iOS, Windows). They also provide access to data simultaneously [23].
- **Shared Resources** These applications use fewer device resources because they are cloud-supported. The storage and processing capacity of mobile applications on the cloud is not restricted to certain types of device.
- **Reliability** The storage of data on clouds or applications is an effective way of increasing reliability. This reduces the risk that mobile devices lose data and applications. Users can store their data as and if they like and save it in the cloud. Moreover, they can back up the data to the cloud whenever they like [24].

IV. Adversary and Threats Model of MCC Applications

In this section, we investigate the ability to control all communication between the main contents involved in MCC. The possible attacks are observable and modifiable in all

Impacts	Active Attack	Passive Attack
Packet Modification	Modified	Unmodified
Danger	Integrity and Availability	Confidentiality
Impact on Application	Harmful to the system	Not harmful to the system
Accesses to resources	Physically control	Observation and no physically control
Detected Attack	Easily detected	Difficult to be detected
Types of attacks	Masquerade, Session Replay,Denial of Service	Release of a message, Traffic analysis

TABLE I
DIFFERENCES BETWEEN ACTIVE ATTACK AND PASSIVE ATTACK.

messages produced by the considered parties. In other words, this section investigates some communications protocol attacks in networking security. Security control is required over the services provider or users' public identities registry. For example, whenever the attackers obtain a private IP address of any entity in the system, they have access to that company or organization. Thus, they can easily retrieve confidential data and reach the protected system. In general, there are many challenges that an enterprise could face primarily when cloud computing services are not implemented locally. Mobile users need to connect to the Internet for using these MCC applications. This is due to the fact that these applications require Internet access to reach the cloud. Security is one of the main problems when using the MCC applications [23]. Here, we discuss the main security issues related to MCC applications. Then, we investigate some attack techniques.

A. *Security Issues of MCC Applications*

Three main issues are discussed in this section regarding security in MCC applications. Figure III points to the location of each security issue on the MCC architecture.

1) ***Physical Issues****:* Losing a mobile device causes to loss of the confidentiality of the stored data. If the device is found by the owner or another person, the integrity could be lost after a while. This is because of the fact that there is no guarantee of who changes the stored or accessed data. Spyware can be installed or a physical bug is added to the device that can cause the system to be impaired. Moreover, the secondary storage (e.g. flash memory) of the mobile devices should be protected from attackers. Sensitive information such as passwords, PINs, credentials, or corporate data like a customer list could be stored in it. Besides, the physical protection of these devices, the only way to protect the sensitive data is by encryption [18].

2) ***Logical Issues*** *:* Only authorized people should be able to read or modify the personal or corporate data stored on mobile devices. Otherwise, the stored data on these devices lose its confidentiality and/or integrity. Bank account numbers, mobile device ATM passwords, and sensitive business data, such as customer lists and phone numbers are usually stored on mobile devices. However, nobody would like to share this data with others. If attackers can see or access these data, the owner will lose his/her privacy. [18].

3) ***Network Issues****:* Security issues of wireless transmission are not always encrypted. The majority of wireless local area networks (WLANs) depend on private networks managed by others. A wireless device can create a denial of service attack by flooding other wireless clients with bogus packets to consume its limited energy and resources. Hackers can also intercept the radio signals by the wireless receiver and listen to all transmitted packets [1], [25].

Furthermore, other malicious software such as Viruses, Trojans, and Adware can be used to attack a victim's operating system. This is in a sequence of harmful operations. This includes system disruption, the deletion or alteration of data, the collection of sensitive data and information, unauthorized access to the computer system, or the illegal operations of the system, to mention a few [26].

B. *Attack Techniques in MCC Applications*

In general, all types attacks on the MCC applications can be classified into passive and active attacks. This is according to the used techniques and purposes of the attacker.

1) ***Passive attack****:* A passive attack exploits open ports and defects of the system by monitoring and scanning it. The aim is simply to obtain information regarding the targeted entity, no data is changed. Mainly active recognition and passive recognition to exploit the gathered data are required. For example, mapping the access point, and possibly exploiting wireless connections. The intruder detects vulnerable Wi-Fi internet networks by monitoring communication channels for gathering a range of information, passwords, location, and encryption types. The attacker can then use this information to enable covered entry into a system or network [1]. The attacker obtains a copy of all transmitted packets among legal ends.

2) ***Active Attack****:* In the active attack, the hacker modifies the sent data before forwarding it to the receiver. For example, the masquerade attack relates to a person who relies on a false identity to acquire or modify information. The intruder tries to be a particular or legal user of a system to do an attack that gains access or escalates privileges than is permitted. On the other hand, in the replay attack, the intruder robs a network packet and transfers that packet to a service or application at a different time. It looks as if it were the user that originally sent the packet, because it contains all real parameters of the sender except the time [1], in Table I show summary of differences between Active Attack and Passive Attack.

V. SECURITY TECHNIQUES

A security framework cloud-based mobile application is named Secure Mobile Cloud (SMC). Security components are installed on the cloud and mobile device ends to ensure the

integrity and confidentiality of applications. First, to verify the application's completeness, the existence of the application is verified by the application stores searching for its name. The application signature is then compared to the original signature found in the application store. If you find both signatures identical, the application should not contain any malicious codes [8]. In the rest of this section, we investigate the security techniques used for protecting against security threats in physical, logical, and network aspects. Then, we present some security techniques to avoid passive and active attacks. Figure 2 represents the main security techniques that are used to secure the MCC applications.

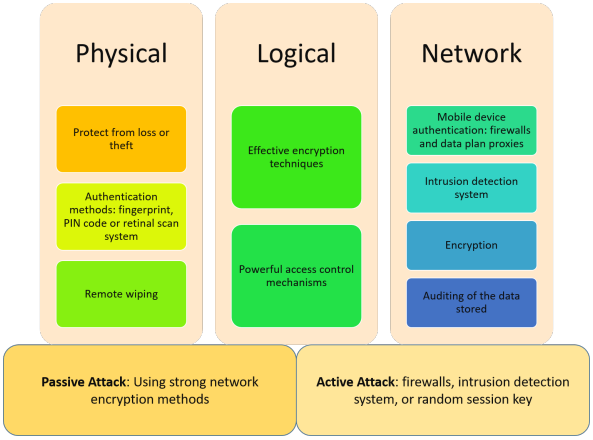

Fig. 2. Secure Mobile Cloud Framework

A. *Protecting Physical Threats*

Physically protecting the mobile device's applications and data begins with the user himself. This is by preserving his/her device from loss or theft. Besides the device should be protected in the event of being stolen or lost through fingerprint or PIN code or retinal scan system authentication methods. This is an obstacle to the theft of the device to obtain personal data fast and easily. These techniques enhance the device encryption system by enabling integrated in-built device encryption techniques; such as USB drive encryption in the secondary storage, memory sticks, data card and removable enable strong password encryption of mobile devices.

Owners should immediately report lost or stolen of their devices. They should ensure that mobile devices are enabled with Bluetooth, Wi-Fi, etc., and are disabled when they are not in use. Secure browsers, encrypted e-mail access, and trust technologies are all used for protecting sensitive and personal data. These techniques are required to be included in the settings of mobile devices [1] [18].

B. *Protecting Logical Threats*

Effective encryption techniques and powerful access control mechanisms can help to keep mobile data confidential. Moreover, maintaining the privacy of the user's information by securing all important information and stopping sharing them with anyone. For example, the banks never ask their clients over the phone or email to send their pin numbers or passwords of their E-Banking accounts. Users should not send any sensitive information by e-mail or call to who acts as a representative of a certain side they deal with.

C. *Protecting Network Threats*

There should be the proper implication of strong network services like mobile device authentication, firewalls and data plan proxies. This requires properly implementing the intrusion detection system, encryption, and auditing of the data stored on mobile devices. Multiple security applications for mobile devices with different functions such as mobile malware detection and prevention, unauthorized access control, and privacy protection are available, installation of Anti-Virus software, such as Kaspersky Mobile Security all help to stop the malware threat coming from the connecting network [8].

D. *Avoid Passive/Active Attacks*

Using strong network encryption methods to prevent passive attack. The original sent message should be well encrypted at the end of the sender into an unintelligible language and decrypted to an understandable language at the end of the receiver.

On the other hand, to prevent active attack technicians should use firewalls or intrusion detection system. Moreover, random session key (i.e., a temporary key) that is used to encrypt data transmitted between two parties in a communication session can be used. This key should be discarded after the session ends. This provides security, as the keys are valid only for a certain period of time, which means, after the session is finished, no one can access the data.

VI. Discussion and Remarks

Through the solution techniques that were mentioned previously in Section V, it is clear that the infrastructure of cloud computing and the mobile cloud must work together to protect the information and its confidentiality from modification or theft. The task of the cloud is not limited only to making sure that the applications that can be downloaded from the application store are authenticated.

There must be a clear mechanism to prevent the installation of any unsafe and unreliable version from the store. Users should verify the identity of the developers for each application and monitor fake advertisements that accompany downloading the application on mobile devices. This should ensure the reliability of the installed applications. Clear rules should be announced for developers and advertisers of these mobile applications to ensure reliability. Thus, the responsibility for saving data from modifying, stealing, or any other threat depends on the infrastructure of cloud computing. The operating systems in which mobile devices operate must provide their users with adequate support for securing their information applications. Such as bank applications or online shopping, which requires the customer's credit card number. They should protect this collected data from theft or fraud. This is by

sharing security tasks with the cloud and developing a strategy for clear and high security. Aiming to prevent intrusions or spying on them using the firewall or any other security system as mentioned in Section V.

As previously mentioned that there are methods of authentication such as fingerprint or retina scanning systems to improve device encryption. However, this feature or method is not supported by all mobile operating systems. Here it must be noted the importance that all operating system environments should support strong authentication methods and protection systems. This brings us back to the necessity of coordinated and integrated work between Cloud Computing and Mobile Cloud. There is a huge number of mobile applications and some of them are very large in size and require sufficient storage space. This is where we need the infrastructure of the cloud to ensure the work of applications on our mobile devices with the least space possible. Moreover, the availability of mobile applications in these varieties in the store supported by the cloud can be a major reason for the lack of the required security for users. This is considered a loophole in the protection system of the cloud and mobile cloud applications.

VII. Conclusion

Mobile computing technology provides users with a combination of wireless networking and mobility to access at any time and anywhere. Several services generate various new mobile applications and services. However, mobile computing is more susceptible to different risks than conventional networks. This is because of the inherent characteristics of wireless communication and the demand for mobility and portability. Mobile computing is crucial for viable applications to be developed. This paper provides possible solutions to the security problems of mobile devices. However, there is still a need to find innovative techniques, methods, or approaches to stop the threats and security issues. We believe that the user should also be aware of security problems and not simply download any application on his Smartphone. In addition, users should not ignore system security warnings that provide many security measures to avoid attacks. Users need to be informed of these problems to protect their devices because of the constant development of malicious software.

References

[1] G.Kaarthic ,M.Arfath and R.Divya ,Data Attacks and Security Techniques in Mobile Computing,International Journal of Scientific and Engineering Research, vol.8, pp. 129–135, April-2017.

[2] B.Abhishek ,N.Shivangi,A Study on the Techniques of Computational Offloading from Mobile Devices to Cloud ,Advances in Computational Sciences and Technology ,vol.10, pp. 2037–2060, 2017.

[3] P.Krishna ,Balachandra Security Issues in Mobile Computing, International Journal of Computer Science and Engineering Survey (IJCSES), Vol.6, PP.129–135, April 2015.

[4] C.Kevin,Vivian.M and H.Declan, Mobile device security,Int. J. Information and Computer Security,vol.7, pp. 1–14, Jan-2015.

[5] S.Javed,Mobile Computing: Wireless Networking Security Issues, International Journal of Grid and Distributed Computing, Vol. 9, pp.273–282, 2016.

[6] T.Daniel,Z.Saman and J.James,Mobile Cloud Computing and Its Security, Privacy and Trust Management Challenges, IGI Global, vol.3, pp. 384–407, September-2013.

[7] T.Chithambaram,M. DuraiRaj, Networks Security on Mobile Computing – A Survey, International Journal of Computer Science and Engineering Technology (IJCSET), Vol.6, pp.168–174, 2015.

[8] M.Mollah ,MD.Azad and A.Vasilakos, Security and Privacy Challenges in Mobile Cloud Computing: Survey and Way Ahead, Journal of Network and Computer Applications,vol.84, pp. 34–54, April-2017.

[9] A.Ahmed , A.Hanan , K.Omprakash , M.Hamid , U.Mohammed ,A.Abubakar and T.Muhammad, Mobile Cloud Computing: Taxonomy and Challenges, Journal of Computer Networks and Communications, Vol. 2020,pp.1–23, Jun-2020.

[10] S.Abid,H.Mureed, Security Issues and Challenges of Mobile Cloud Computing, International Journal of Grid and Distributed Computing,vol.6, pp. 37–50,2013.

[11] K.Suleman,S.Muhammad,B.Laleh,G.Abdullah,K.Muhammad, Towards port-knocking authentication methods for mobile cloud computing, Journal of Network and Computer Applications,vol.97, pp. 66–78, 2017.

[12] M.Vaishnavi ,V.Revathi and T.Rama, Security and privacy attacks during data communication in Software Defined Mobile Clouds, Computer Communications, Vol.153, pp. 515–526,2020.

[13] T.Nikil,A.Aloysius, A Survey on Mobile Computing Security, International Journal of Research and Analytical Reviews,vol.6, pp. 645–649,Jun-2019.

[14] MM.Rajhashayamala,T.Anusha,AB.Vaishnavi, The Survey on Mobile Computing and its Applications, International Research Journal on Engineering and Technology (IRJET), Vol.4, pp. 1259– 1262,2017

[15] Z.Syed,S.Munam,K.Muhammad,Z.Sijing,A Survey on Security for Smartphone Device, International Journal of Advanced Computer Science and Applications, Vol.7,pp. 206–219,2016.

[16] Algarni, Mona, Munirah Alkhelaiwi, and Abdelrahman Karrar. "Internet of Things Security: A Review of Enabled Application Challenges and Solutions." International Journal of Advanced Computer Science and Applications 12, no. 3 (2021).

[17] Tong, Wei, Wenjie Chen, Bingbing Jiang, Fengyuan Xu, Qun Li, and Sheng Zhong. "Privacy-Preserving Data Integrity Verification for Secure Mobile Edge Storage." IEEE Transactions on Mobile Computing (2022).

[18] K.Naveen,V.Soniya, Security Issues and Solutions in Mobile Computing, International Journal of Scientific and Engineering Research, Vol.8,pp. 93–96,May-2017.

[19] S.Shahab,F.Mahdis,C.Anthony,M.Antonio, Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues, Journal of Information Security and Applications, Vol.55, pp.102–582, 2020.

[20] K.Jan, What Is Mobile Cloud Computing (MCC), Available:https://www.netguru.com/blog/mobile-cloud-computing ,Apr 28, 2021, [Online; accessed ,8 Jun 2021].

[21] Z.Janet,W. Zachary, Mobile apps for science learning: Review of research,Computers and Education, Vol.94, pp. 1–17, 2016.

[22] C.Arun,K.Prabu, Applications of Mobile Cloud Computing: A Survey, International Conference on Intelligent Computing and Control Systems ICICCS, pp.1037–1041, 2017.

[23] N.Hamid,G.Varun,S.Rajiv, Why Do Users Continue to Use Mobile Cloud Computing Applications? A Security-Privacy Investigation, Conference: The 13th Pre-ICIS Workshop on Information Security and PrivacyAt: San Fransisco, CA,pp.1–20,December-2018 .

[24] ME.Anup,R.Prabhaker, Mobile Cloud Computing the Necessity of Future with its Architecture, Advantages and Applications,International Journal on Recent and Innovation Trends in Computing and Communication, Vol.2, pp. 703–708,March-2014.

[25] S.Venus, Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications, Information Resources Management Association,USA,,Vol.4, pp. 1925–1939,2016.

[26] A.Sara,A.Mariam ,O.Fatimah ,W.Wei,A.Zeyar, Security in Mobile Computing: Attack Vectors, Solutions, and Challenges, Lecture Notes of the Institute for Computer Sciences,Vol. 191, pp. 177–191, JAN- 2017