International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

Fundamental Study of Penetration Testing on Mobile Cloud Computing

Amilia BintiAbu Bakar [1], Mohd Saffuan bin Che Mansor [2], Mohd Shamshul Anuar bin Omar, Mohamad Fadli Bin Zolkipli[4]

Hospital Kulim, Kedah, Malaysia[1]
School of Computing, University Utara Malaysia, Sintok, Kedah,Malaysia[2]
School of Computing, University Utara Malaysia, Sintok, Kedah,Malaysia[3]
School of Computing, University Utara Malaysia, Sintok, Kedah,Malaysia[4]

Date of Submission: 15-02-2023 Date of Acceptance: 25-02-2023

ABSTRACT: Penetration testing, ethical hacking, and white hat hacking are all synonymous terms used to describe the activity of identifying and fixing flaws in a system. This study aims to provide a comprehensive overview of the current research on penetration testing in the context of mobile cloud computing. The study conducts a systematic literature review to gain insights into various approaches, tools, and best practices used in penetration testing for mobile cloud computing applications. The study also highlights the challenges and limitations in the field and proposes recommendations for future research. The insights gained from this study are valuable for researchers, practitioners, and students interested in mobile cloud computing security and penetration testing. Ultimately, this study contributes to the development of secure and reliable mobile cloud computing systems.

KEYWORDS: mobile cloud computing, penetration testing, mobile applications

I. INTRODUCTION

Mobile computing is a rapidly expanding business solution within Information and Communication Technology (ICT). The number of mobile users increasing, consequently due to improving hardware and software of mobile devices [1]. Currently, smartphones and tablets are utilized for various tasks such as emailing, chatting, browsing the internet, running applications, sharing files, editing or reading documents, and entertainment. However, these mobile devices alone may not have the capability to meet the computational demands of a large user base. To address this, mobile cloud computing (MCC) has been introduced, which refers to cloud computing services provided through mobile devices or embedded systems. The merging of mobile computing with cloud computing is due to the inherent characteristics of the cloud model, which include self-service on demand, virtualized resources, broad network access, rapid elasticity, and subscription-based services. The popularity of cloud computing is also increasing among mobile users because of the cloud-like services it offers. This study aims to provide a comprehensive review of the current research on penetration testing in the context of mobile cloud computing, highlighting various approaches, tools, and best practices used, as well as the challenges and limitations faced in this field. The insights gained from this study can be useful for researchers, practitioners, and students interested in developing secure and reliable mobile cloud computing systems.

Penetration testing, also known as "pen testing," is a vital aspect of mobile cloud computing (MCC) security. It involves simulating a real-world attack on the system to identify vulnerabilities and assess the effectiveness of existing security measures. Penetration testing is an essential tool for identifying security weaknesses in MCC before attackers can exploit them. Penetration testing should be conducted periodically by qualified professionals with in-depth knowledge of MCC and security protocols. Therefore, businesses can ensure that their mobile cloud computing systems remain secure and effective. We will present a paper on penetration testing on Mobile Cloud Computing by firstly define MCC definition, MCC architecture and overview of penetration testing. The rest of this article is structured as follows. In Section 2, the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

definition and types of Mobile Cloud Computing Security Threats are introduced. Section 3 provides an overview of the best practices for Mobile Cloud Computing Penetration Testing. In Section 4, the challenges and limitations of Penetration Testing in Mobile Cloud Computing are analysed. Section 6 concludes this article, followed by acknowledgments and references.

1.1 DEFINITION OF MOBILE CLOUD COMPUTING

Mobile cloud computing (MCC) is a hybrid computing model that combines mobile computing with cloud computing services delivered over the Internet [1]. With the rapid advancements in mobile technology, the need for faster processing and storage capabilities has become essential. MCC is the solution that brings the heavy lifting of processing and storage to cloud servers, providing users with more computing power, storage capacity, and data processing capabilities. MCC offers many advantages over traditional mobile computing models. For instance, mobile apps and services that are powered by cloud computing have greater processing power, increased data storage capacity, and enhanced features that were not previously available. This means that mobile apps that need a lot of power to do complicated tasks can now use a cloud server instead of the mobile device to do the work. This allows the app to function smoothly on a range of mobile devices, regardless of their hardware capabilities.

MCC applications is unique, and it is difficult to test them due to the different ways in which each process is executed and where it occurs, which represent various offloading approaches. To ensure that all possible ways an MCC application can function are considered, each test instance must be created and run according to the device's state. As in MCC, cloud-based applications store and process data in the cloud, which is accessible to a wide range of mobile users. MCC is a powerful technology that combines the flexible resources of different clouds and networks to provide unrestricted functionality, storage, and mobility. It can be used on a wide range of mobile devices, anytime and anywhere via the internet, regardless of the various platforms and environments. With MCC, you pay only for what you use. MMC is a combination of mobile computing, cloud computing, and wireless technology that allows people who use mobile devices to access cloud services like how people who use computers access them [2].

1.1.1 MOBILE CLOUD COMPUTING ARCHITECTURE

Mobile Cloud Computing (MCC) is a relatively new technological advancement that arose from the integration of two broadly used technologies: mobile computing and cloud computing. Essentially, MCC transforms the capabilities of mobile devices by merging cloud storage and processing with mobile computing, resulting in enhanced optimization and operational performance, and enabling seamless and transparent access to cloud resources [3]. Architecture of mobile cloud computing is described by [4] comprise of three different layers as depicted in Figure 1:

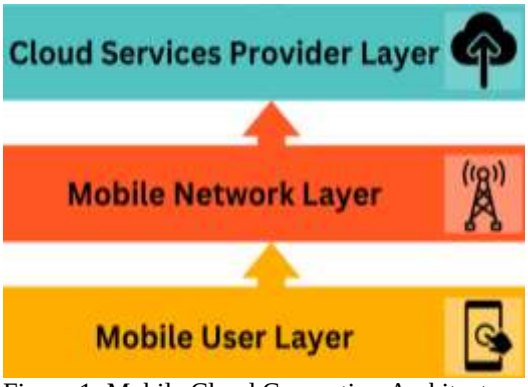

Figure 1: Mobile Cloud Computing Architecture

- Mobile User Layer

The Mobile Cloud Service Layer comprise of multiple customers who access cloud services through mobile devices such as smartphones and tablets. These devices are connected to the Mobile Network Layer via Base Transceiver Station (BTS), Wireless Access Points (WAPs), or satellite.

- Mobile Network Layer

This layer consists of various mobile network operators that handle requests from mobile users and distribute information via base stations. Following successful identification and permission, the operator forwards the requests of mobile users to a cloud over the Internet. The access for mobile user to corresponding cloud-based services is provided by the controllers.

- Cloud Services Provider Layer

The Cloud Service Provider Layer consists of numerous providers that offer all types of cloud computing services, such as IaaS, PaaS, and SaaS. These services are scalable and can be adjusted as per the requirements of their users. Cloud computing enables users, inclusive those with mobile devices, to access these services via the internet.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

1.2 OVERVIEW OF PENETRATION TESTING

A penetration test is an ethical cyber attack that with the aim to evaluate the level of security of an information system to identify and address vulnerabilities of system. It is a legitimate simulation of a cyberattack on a computer system that is used to assess the computer system. In order to try and break into a computer system, such as its system protocol, application protocol interfaces, servers, and databases, penetration testing can be used. An organisation needs penetration testing to reduce the likelihood of being hacked by cybercriminals. Due to the quick development of technology, it is necessary to continuously examine penetration testing standards and methodologies to make sure they are still applicable to the state of technology and capable of identifying any cyberattack techniques that could be harmful to the system [5]

The evolution of cyber-attack strategies has raised awareness among organisations, government agencies, and enterprises on the significance of protecting assets by performing cyber security. As a result, penetration testing is the action to imitate cyber-attacks on a computer system, networking, application, or website. The primary goal of penetration testing is to detect potential weakness in the current system so that security controls can be established to reduce such dangers before they are exploited by cyber criminals. According to [5], the advantages of implementing penetration testing in a business are listed below.

Advantages	Details
Identifying system vulnerabilities	Penetration testing might expose flaws in the target system as it's enabling the identification of actual cyber security vulnerabilities, allowing for improvements in software and hardware such as system architecture or network infrastructure to be explored to improve overall security implementation. The penetration testing findings report offers an overview of the system and can be utilised in analysis for the overall security architecture of the system.
Cyber-defence capability of the systemis being tested	Since penetration testing can assist uncover potential vulnerabilities and cyber-attack strategies, whenever an attack happens, the response time and appropriate action plans related to the attack can be estimated to reduce potential harm and losses to the organisation.
Maintain consumer trust and business continuity	A sensitive data breach could damage the organization's reputation and damage trust among stakeholders, customers, and employees. After the penetration testing is completed, the controls for cyber security can be improved for any vulnerabilities that have been found, enabling the company to react to the situation promptly and minimising the damage and losses caused by the cyber attack.

Table 1: Advantages of Penetration Testing [5]

II. MOBILE CLOUD COMPUTING SECURITY THREATS

Mobile Cloud Computing (MCC) is a rapidly emerging technology as the number of mobile users grows by the day. Data privacy and security are key concerns because of the use of mobile devices. Any ordinary smartphone can benefit from MCC's infrastructure, computational capacity, software, and platform services. MCC security concerns include network security, web application security, data access, authentication, authorization, data confidentiality, and data breach. Because mobile devices lack sufficient storage and CPU performance, their data storage capacity is

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

limited. Security threats must be examined in order to build a secure MCC environment.

2.1 OVERVIEW OF MOBILE CLOUD COMPUTING THREATS

Mobile phones have become an integral component of human existence for communication. Cloud computing and mobile are two extraordinary approaches that have emerged in recent years. When cloud computing, mobile computing, and wireless networks are integrated to generate mobile cloud computing, extensive computational resources are made available to mobile users. Mobile cloud computing (MCC) is an infrastructure that stores and processes data outside of mobile devices. Mobile cloud apps transfer computational power and data storage from mobile devices and store it on powerful and centralised computing platforms hosted in clouds, which are then accessed via a thin native client over a wireless connection. In mobile cloud computing, resources are virtualized and deployed to a group of several distributed computers rather than local computers or servers. Numerous apps, such as Google's Gmail, mobile maps and navigation systems, voice search, and so on, are based on Mobile Cloud Computing. MCC's purpose is to improve the potential offered by mobile devices by leveraging the benefits of cloud computing; yet, it is still a relatively new area of research with many unanswered questions.

2.2 TYPES OF SECURITY THREATS IN MOBILE CLOUD COMPUTING

Security is an important concern in mobile cloud computing (MCC), as mobile devices are particularly vulnerable to security threats. MCC involves transmitting data between mobile devices and cloud servers, which can be intercepted and compromised by malicious actors. Therefore, it is crucial to implement appropriate security measures to protect the data and maintain the privacy of users. Mobile Cloud computing is usually regarded as a revival of the original mainframe client-server concept. Resources, on the other hand, are ubiquitous, scalable, and highly virtualized. It includes all the usual hazards as well as some newer ones. It may be useful in finding solutions to cloud computing security challenges to identify the problems and approaches in terms of control issues, a lack of trust, and multi-tenancy issues. According to [6] types of Mobile Cloud Computing Security Threats can be listed in Table 2:

MCC Security Threats	Details
Confidentiality	As cloud environment involves a large number of users to deliver services, the number of access points for mobile users and applications grows. Each user's data should be kept secure and private. Only authorised users have access to allowed data.
Privacy	A person's desire to control his or her personal information is referred to as privacy. Many possibilities, such as insider user risks, external attacker threats, data leakage, and so on, can jeopardise cloud users' privacy.
Multi-tenancy	Cloud multi-tenancy refers to a situation where a single program or application is shared by a group of users. In this context, the data of each mobile user is isolated and inaccessible to other mobile users.
Object reusability	This methodology enables the development of cloud-based applications that are highly reusable by accessing cloud component repository components using pattern matching algorithms and various retrieval techniques.
Data remanence compromised.	It is the remnant representation of data that have been nominally destroyed or erased. Due to data remanence, data confidentiality could be unintentionally
Software Confidentiality	It refers to the trust placed in a particular application or process to securely manage and handle the user's personal data.
Integrity	Integrity in the cloud refers to protection against unlawful deletion, modification, or theft. In other words, data integrity involves preserving the accuracy and consistency of data during transactions, such as transmission, retrieval, and storage. Both intentional and unintentional deletion and alteration can occur.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

Authorization	This is the technique by which a system determines what level of access a specific authenticated user should have to secure the system's resources.
Availability	Availability is a crucial factor that allows access to services, data, and tools at any time and from any location. Building systems with this level of dependability and availability has traditionally been associated with high expenditures for businesses.

Table 2: MCC Security Threats [6]

III. PENETRATION TESTING METHODOLOGIES FOR MOBILE CLOUD COMPUTING (MCC)

3.1 TYPES OF PENETRATION TESTING

Software testing requires huge number of resources to be executed successfully, and in the case of MCC, it requires high level complication compared to web application, mobile or even a cloud assessment and testing done separately. In certain developed programs, each segments require large-scale resources into assessment compared to the resources needed by MMC software testing. For example, MCC applications might require various deployment ways and contrasting sites of each task due to contrasting offloading deployment options, in the form of static or dynamic.

MCC application's offloading is a way of assigning processes to the cloud. Cloud offers various classification of services that can be ordered such as remote spreadsheet, remote programs, remote files and various application. MCC applications can be segmentized into client to server, virtualization, and mobile agents based on the offloading method [7]. MCC application's market using offloading is distinctive because it includes various type of mobile application such as gaming, healthcare, learning, mobile commerce and other useful applications [8]. For that reason, offloading characterizes the distinctivenessof MCC apps. It is a key attribute of MCC which has a critical impact on testing, since every produced test case requires an actual real device state to match every possibility [9] [10], that significantly raise the test cases produced.

The addition of this new attribute and specification has increased the complexity of penetration testing for MCC apps which simultaneously strengthened their safety measures. It is crucial to execute vulnerability test of MCC apps to detect any potential vulnerabilities across the mobile, web, and cloud principles. These triad eventually forms the base of MCC apps [11] [12]. According to [13], test models are predicated on several test methods; Penetration testing is of particular importance as it enables important security reviews and vulnerability assessment tests for mobile, cloud, applications, web and networks. In addition, penetration tests are ascendable, can run automatically, and can be scheduled to run without stopping operating systems.

3.2 STEPS IN PENETRATION TESTING FOR MOBILE CLOUD COMPUTING (MCC)

In MCC, the specifications are derived from penetration testing of mobile and cloud platforms, as well as other attributes unique to MCC applications [9] [12] [14]. To overcome MCC application penetration testing problems, the tests must be run via test models to address offloading and various platform tests. These test models can significantly simplify the complexity of penetration tests for MCC applications.

Phase	Details
Test case generation	Every test case will be designed to be deployed on both mobile and cloud platforms, with the necessary environment parameters.
Test case selection	To affirm every possibility of etiquette plans is thoroughly inspected. The environmental attributes utilization generated by both the mobile and cloud components is a must.
Test case execution	The test coordinator will capture every setting from various tests.

Table 3: MCC attributes, and the test phases it affects [15]

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

The implications of MCC properties, offloading, including numerous platforms on performing MCC apps pen testing are shown in Table 1. According to [16], it serves as an example of the impacts to the three key penetration stages (test case generation, selection, and execution). For example, while examining mobile or cloud apps, the test case creation phase generates test scenarios for either one of the platforms. However, during the assessment of MCC apps, this stage is required to produce test scenarios for each of them [17] [18]. The use of numerous platforms and offloading both have an impact on the choice of test cases for MCC applications. As a result, when choosing the test case sets, it must take offloading and numerous platforms into account. Due to the lack of offloading and the fact that both run on a single platform exclusively, neither of these two problems emerge while testing mobile or cloud applications [17] [18]. Offloading and various platforms will considerably enhance the path fill image.

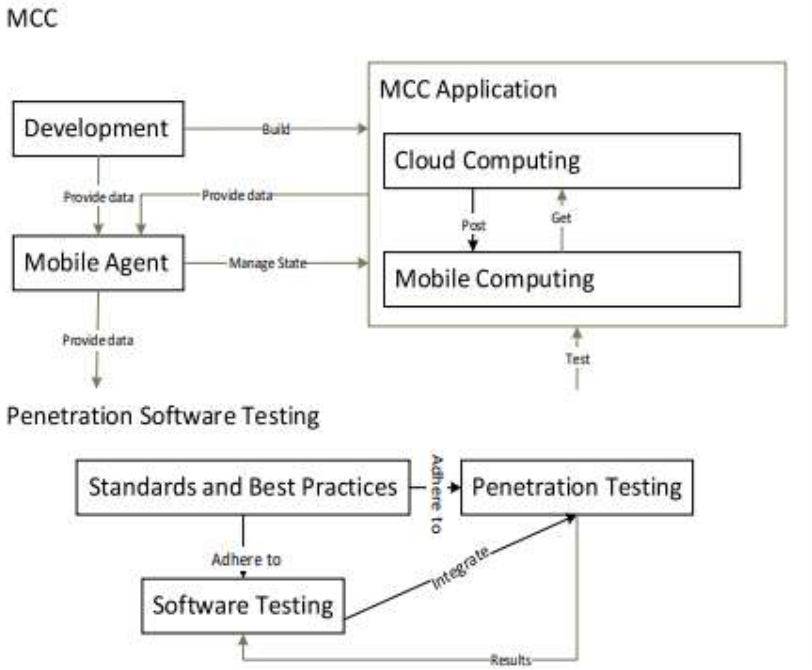

Figure 2: MCC Application Pen Testing Conceptual View [15]

The conceptual flow chart of the penetration testing model is referred to as in Figure 2 in order to comprehend the specifics of each step in the MCC penetration test. The MCC and penetration software testing are the two main parts that make up the concept [10]. There are three parts to each module. Standards and best practises, software testing plus pen testing modules make up penetration software testing. Additionally divided into three submodules, MCC consists of the MCC application, the mobile agent, and development.

Pentest preparation is the first step in the pen testing process. It entails creating a test strategy that specifies the target application, a budget, and a timeline. The identification and list of vulnerabilities are then checked. The data lists are then transformed into lists of test cases, which are then chosen and executed, before a test report is generated. The software testing item, which abides to standards and best practises, provides inputs to the pen testing component. Mobile agent and state manager are also producing an output for the software testing item. This model creates and sends the offloading data to the pen testing item in MCC application. Next, the pen testers would process developer inputs further by inspecting the programmes, either manually or with the aid of tools. However, unless explicitly stated in the programme manual pages, the developers must provide the offloading settings, which will be covered in a moment.

Now that all related activities related to test case generation, test case selection, and test case execution are ready to be implemented. The process of creating test cases will begin by iteratively going through every possible attack. Another inner loop will iterate over the settings, conditions including variants of information specified in every incoming by apps builders and analysts for each possibility. The variables indicate test cases that were generated when combined. Right after this, test case selection

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

must be carried out because offloading has resulted in a lot of generated test cases. When doing MCC pen testing, test case selection criteria are used to correspond with the mechanism chosen to produce test cases.

Finally, the test case execution process begins by running each test case listed in chosen test cases. Every test case's outcome is captured and sent to the analysts and report generators when all procedure is completed. Depending on the findings and the testers', developers', or clients' feedback, this pen testing procedure might be executed several times.

IV. BEST PRACTICES FOR MOBILE CLOUD COMPUTING PENETRATION TESTING

As mentioned earlier, penetration testing is the way to identify any vulnerabilities in any IT environment. One of the technics and method is OWASP stands for Open Web Application Security Project [18]. The MCC paradigm is where mobile and cloud computing intersect, as illustrated in Figure 2. While it shares similarities with both technologies, it also has distinctive features that set it apart from either paradigm.

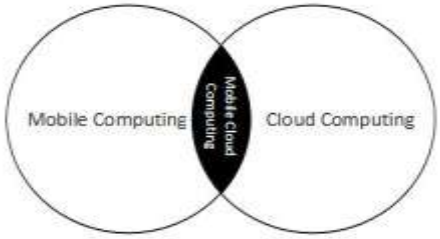

Figure 3: MCC in a Nutshell [1]

From the systematic literature review by [1], most of the authors found that an assessment model or method is the best way or best practices in cloud security. The significance of distinguishing between a penetration test and a vulnerability assessment is increasing within the field of penetration testing. It is common for some testers to label themselves as penetration testers when in fact they are only capable of performing vulnerability assessments. A company that is not familiar with the process may be misled into believing that their networked system has been fully evaluated, when in fact it has not, due to this confusion [5]. According to the study by [20] identify that the practice of penetration testing promotes an essential level of awareness of information security throughout an organization.

By proactively identifying security vulnerabilities, penetration testing enables these loopholes to be addressed and remediated, ultimately helping to prevent security breaches. A study by [21] mention that risk assessment metrics comprise various factors, such as the effectiveness of red and blue teaming, vulnerability assessments, penetration testing, and intelligence-driven defence. Penetration testing in cloud computing and mobile cloud computing share many similarities, as both environments rely heavily on network communication and the use of shared resources. However, there are also some key differences between the two that affect how penetration testing is conducted as listed Table 4:

	Cloud Computing	Mobile Cloud Computing
Infrastructure	Centralized infrastructure hosted by a third-party provider, typically accessed remotely over the internet.	The infrastructure is distributed, with resources shared between the mobile device and the cloud server.
Attack Surface	Typically, a larger attack surface, encompassing multiple virtual machines, storage systems, and network devices.	Often limited to a single mobile device and its associated cloud server.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 839-849 www.ijaem.net ISSN: 2395-5252

Network Complexity	Highly complex network infrastructure, involving multiple virtual and physical devices.	Simpler network architecture, as resources are primarily shared between the mobile device and cloud server.
Testing Focus	Focus may be on the cloud infrastructure, as well as the network traffic and data storage systems.	The focus could be on both the mobile device and the network traffic that flows between it and the cloud server.
Testing Tools	May use standard testing tools and techniques for network and system testing.	May require specialized testing tools and techniques to account for the unique challenges posed by mobile devices.
Key Considerations	It is essential to consider the security of both data at rest and in transit, as well as the security of the cloud infrastructure itself.	Must consider the security of the mobile device and its interaction with the cloud server, as well as the security of the cloud infrastructure.

Table 4: Differences Of Mobile Cloud And Cloud Computing In Penetration Testing

Penetration testing on mobile cloud involves assessing the security of cloud-based mobile applications. Here are some best practices for penetration testing on mobile cloud according to OWASP, NIST and NCSC model and guidelines.

1. Understand the Mobile Cloud Environment: Prior to commencing any penetration testing, it is crucial to acquire a thorough comprehension of the mobile cloud environment. This includes the types of devices, operating systems, and cloud platforms being used [22]
2. Automated and Manual Techniques: A combination of automated and manual techniques should be used to ensure comprehensive testing [23]. Automated tools can help to identify vulnerabilities quickly, while manual techniques are better suited to identifying complex vulnerabilities that may be missed by automated tools.
3. Test from the Perspective of an Attacker: To ensure that all vulnerabilities are identified, it is important to test from the perspective of an attacker [24]. This means thinking like an attacker and trying to identify vulnerabilities that could be exploited to gain unauthorized access to sensitive information.
4. Perform Regular Testing: Penetration testing should be performed regularly to ensure that any new vulnerabilities are identified and addressed quickly [23].
5. Document Findings and Remediation: It is important to document all findings and remediation efforts to ensure that vulnerabilities are addressed effectively and to provide a record of testing efforts [5].

V. CHALLENGES AND LIMITATIONS OF PEN TESTING IN MOBILE CLOUD COMPUTING

From the standpoint of applied cryptography, [25] analysed the security and privacy threats associated with the MCC's problems. Mobile user identification, data validity tests, safe data distribution, data search, dangerous pattern tracing, and offloaded data calculation were several issues that MCC faced. Additionally, [2] examined, contrasted, and suggested an answer to the safety issues associated with MCC.

5.1 OVERVIEW OF CHALLENGES AND COUNTERMEASURES

a) Authentication for Mobile Clients

For MCC deployment, a variety of authentication techniques are available. The three categories into which the methodologies are divided are as follows:

- The knowledge-based approach, which is typically applied to username and password authentication. In the mobile scenario, several of these functions are already present. Unfortunately, because to the limitations of human information processing, passwords may

have some flaws. People often make the mistake of choosing passwords based on unique and personal information, such as their hometown and pet's name, making it simple for hackers to guess the passwords once they have access to the data.

- Possession-based authentication gives mobile users a key they can keep with them to authenticate their identities. The disadvantage is that hackers might obtain the device and utilise it for their own purposes in the future.
- The biometric-based authentication used the user's bio-distinctives, for examples face structure, eyes, fingerprint and pitch of voice to provide a characteristic including method of user mobile identification. The secret processing and storing of biometric data are a serious privacy risk. Because personal biometric data is so unique, one's privacy would be seriously jeopardised if hackers were able to obtain it through unauthorised access to a user's mobile device.

To obtain the best authentication security in all three authentication methods, multi-factor authentication (MFA) systems were suggested for mobile cloud parameter. With MFA, two or more bases can be deployed on identity confirmation. A mobile unit and a server inside the cloud shared secret key as a prerequisite to next authentication, MFA enhanced the complexity of hacking the verification. During their attempt, hackers will jeopardize all factors to achieve their malicious intention.

b) Data Secrecy Protection and Data Integrity Check

The highest priority on the priority list needs to be confidentiality and MCC integrity. The method for preventing tampering with or theft of transmitted and mobile data is encryption. Local storage of the encryption/decryption key allows mobile clients to continue accessing their data in the future. The keys will be at risk if the mobile devices are hacked. Information can be retrieved from it by hackers. Finally, the requirement that we depend on the programmes and platforms we use created a possible security concern. Our personal information won't be guaranteed if reliable services are breached.

A novel designed proof of retrievability-based (POR) architecture is developed that simultaneously ensures data protection, integrity check, and data recovery in order to guarantee encryption and data integrity. Unfortunately, POR made use of complicated computation and communication, which drains computing power. It will undoubtedly be expensive and may not be a good solution to the efficiency problem to optimise a third party to handle most of the computationally intensive tasks.

c) Mobile Cloud Data Search

Mobile clients need security when searching for and retrieving their cloud-stored data. To guarantee data confidentiality and search privacy, searchable encryption technologies have been developed. The reason why public key systems have low search efficiency is because systems typically use pairs computation as a matching test. In order to transfer the burden to a third party, it is assumed that party can be trusted and that it will be given access to confidential data search information that belongs to the data owner. Since the attackers can fully get the search ability once the party has been hacked, this trust assumption does not scale effectively in reality.

It is incredibly difficult to design an "all-around" system that supports safe data search, sharing, and computing. To the best of our knowledge, no cryptographic system now in use can fully do the task. Recently, two intriguing studies that provide search and share functions have been proposed. On top of attribute-based and identity-based encryption, respectively, [26] [27] are constructed.

VI. CONCLUSION

6.1 SUMMARY OF THE FUNDAMENTAL STUDY

In conclusion, mobile cloud computing is an important area of technology that brings new challenges in terms of security and vulnerability management. Penetration testing is a crucial aspect of ensuring the security of mobile cloud systems, allowing organizations to identify potential security risks and plug security loopholes before they can be exploited by malicious actors. Through a systematic literature review of relevant research, this study has identified best practices for penetration testing on mobile cloud computing, including conducting a thorough risk assessment, using specialized tools and techniques, and regularly updating and patching the system to address known vulnerabilities. By following these best practices, organizations can help ensure the security and integrity of their mobile cloud systems and protect their sensitive data from potential threats.

6.2 FUTURE RESEARCH DIRECTIONS.

There are several potential avenues for future research in penetration testing on mobile cloud computing. One promising area is the development of new tools and techniques specifically designed for mobile cloud environments, which can help improve the accuracy and effectiveness of penetration testing efforts. Another important area for future research is the exploration of how emerging technologies such as artificial intelligence and machine learning can be applied to improve penetration testing capabilities and identify potential vulnerabilities more quickly and accurately. Additionally, there is a need for further research on the specific risks and vulnerabilities associated with different types of mobile cloud applications, as well as best practices for securing these applications against potential threats. Finally, more research is needed to better understand the human factors that can impact the effectiveness of penetration testing efforts, such as the role of employee training and awareness in identifying potential security risks. Overall, these areas of research have the potential to significantly improve the security and resilience of mobile cloud systems, and help organizations better protect their sensitive data and assets from potential threats.

ACKNOWLEDGEMENT

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1]. Ahmad, A. S., Kahtan, H., Hujainah, F., & Jalab, H. A. (2019). Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications. IEEE Access, 7, 173524–173540. https://doi.org/10.1109/ACCESS.2019.2956770

[2]. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, 84, 38-54.

[3]. Anwar, M. A. (2018). Data security issues in the realm of mobile cloud computing: A survey (No. e27050v1). PeerJ Preprints.

[4]. Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Mobile cloud computing: Challenges and future research directions. Journal of Network and Computer Applications, 115, 70-85.

[5]. Tan, W. H., Ismail, S. A., & Abas, H. (2022). Penetration Testing Process: A Preliminary Study. Open International Journal of Informatics, 10(1), 37-46.

[6]. Yadav, D. S., & Doke, K. (2016). Mobile cloud computing issues and solution framework. Int. Res. J. Eng. Technol, 3(11), 1115-1118.

[7]. Fernando, N., Loke, S.W. and Rahayu, W. (2013) 'Mobile cloud computing: a survey', Future Generation Computer Systems, Vol. 29, No. 1, pp.84–106.

[8]. Dinh, H.T., Lee, C., Niyato, D. and Wang, P. (2013) 'A survey of mobile cloud computing: architecture, applications, and approaches', Wireless Communications and Mobile Computing, Vol. 13, No. 18, pp.1587–1611

[9]. Kirubakaran, B. and Karthikeyani, V. (2013) 'Mobile application testing – challenges and solution approach through automation', International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), Tamilnadu Salem, India, IEEE, pp.79–84.

[10]. Chandane, S.H. and Bartere, P.M.M. (2013) 'New computing paradigm: software testing in cloud, issues, challenges and need of cloud testing', Today's World International Journal of Emerging Research in Management & Technology, Vol. 50, No. 8, pp.68–75.

[11]. Mohata, V.B., Dakhane, D.M. and Pardhi, R.L. (2013) 'Cloud based testing: need of testing in cloud platforms', International Journal of Application or Innovation in Engineering and Management, Vol. 2, No. 3, pp.369–373.

[12]. Pundhir, Y.S. (2013) 'Cloud computing applications and their testing methodology', Bookman International.

[13]. Mainka, C., Somorovsky, J. and Schwenk, J. (2012) 'Penetration testing tool for web services security', 8th IEEE World Congress on Services, Honolulu, Hawaii, USA, IEEE, pp.163–170.

[14]. Amalfitano, D., Fasolino, A.R., Tramontana, P. and Amatucci, N. (2013) 'Considering context events in event- based testing of mobile applications', International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Luxembourg, IEEE, pp.126–133.

[15]. Ahmad, S. A., Aljunid, S. A., and Ismail, N. K. (2020) Mobile cloud computing applications penetration testing model design. , International Journal of Information and Computer Security, 13(2), 210. doi:10.1504/ijics.2020.108849

[16]. Färnlycke, I. (2013) An Approach to Automating Mobile Application Testing on Symbian Smartphones: Functional Testing through Log File Analysis of Test Cases Developed from Use Cases, Master thesis, KTH Royal Institute of Technology.

[17]. Labarge, R. and Mcguire, T. (2013) 'Cloud penetration testing', International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol. 2, No. 6, pp.43–62.

[18]. Jadhav, S., Oh, T., Kim, Y.H. and Kim, J.N. (2015) 'Mobile device penetration testing framework and platform for the mobile device security course', 17th IEEE International Conference on Advanced Communications Technology, Pyeongchang, South Korea, IEEE, pp.675–680.

[19]. Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020). Mobile Application Security Penetration Testing Based on OWASP. IOP Conference Series: Materials Science and Engineering, 846(1), 012036. https://doi.org/10.1088/1757-899X/846/1/012036

[20]. Mukherjee, S., Chatterjee, P., Roy, S., & Bose, R. (2021). A Systematic Analysis of the Attack Pattern in Penetration Testing. 2(1).

[21]. M. Sunil Kumar, B. Siddardha, A. Hitesh Reddy, Ch.V.Sainath Reddy, Abdul Bari Shaik, & D. Ganesh. (2022). APPLYING THE MODULAR ENCRYPTION STANDARD TO MOBILE CLOUD COMPUTING TO IMPROVE THE SAFETY OF HEALTH DATA. Journal of Pharmaceutical Negative Results, 1911–1917. https://doi.org/10.47750/pnr.2022.13.S08.231

[22]. Hassan, M. A., Shukur, Z., & Mohd, M. (2022). A Penetration Testing on Malaysia Popular e-Wallets and m-Banking Apps. International Journal of Advanced Computer Science and Applications, 13(5). https://doi.org/10.14569/IJACSA.2022.0130580

[23]. Ravindran, U., & Potukuchi, R. V. (2022). A Review on Web Application Vulnerability Assessment and Penetration Testing. Review of Computer Engineering Studies, 9(1), 1–22. https://doi.org/10.18280/rces.090101

[24]. Rencelj Ling, E., Urrea Cabus, J. E., Butun, I., Lagerström, R., & Olegard, J. (2022). Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis. Proceedings of the 17th International Conference on Availability, Reliability and Security, 1–7. https://doi.org/10.1145/3538969.3544483

[25]. Au, M. H., Liang, K., Liu, J. K., Lu, R., & Ning, J. (2018). Privacy-preserving personal data operation on mobile cloud—Chances and challenges over advanced persistent threat. Future Generation Computer Systems, 337–349.

[26]. Liang, K., & Susilo, W. (2015). Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Trans. on Information Forensics and Security , 1981-1992.

[27]. Liang, K., Su, C., Chen, J., & Liu, J. K. (2016). Efficient multi-function data sharing and searching mechanism for cloud-based encrypted data, in:. AsiaCCS '16, ACM, 83-94.