Security, Privacy Issues and Solutions of Mobile Cloud Computing

Mohammed Lawal Toro[1] Nuraddeen Ado Muhammad[2] Aliyu Rabiu Shu'aibu[3]
Muhammad Amin Garba[4] Abdulrazaq Abdulaziz[5] Kasim Musa[6]
[1,2]Dept. of Computer Science and Mathematics Nigeria Police Academy, Wudil, Kano, Nigeria
[3]Department. of Computer Science, Nile University of Nigeria, Abuja, Nigeria
[4]MIS/ICT Nigeria Police Academy, Wudil, Kano, Nigeria
[5]Department of Electrical and Electronics Engineering Usmanu Danfodiyo University, Sokoto, Sokoto, Nigeria
[6]Department of Procurement and Logistics, Thunder ICT Skills Ltd., Kaduna, Nigeria
Email: [1]molatoro@hotmail.com, [2]muhdnura@polac.edu.ng, [3]aliyurs@gmail.com, [4]aminugarba70@gmail.com, [5]abdulrazaq.abdulaziz@udusok.edu.ng and [6]send2musakasim@gmail.com

***Abstract* —** Simplicity usage, accessibility and the lack of internationally agreed overall service access / safety protocols allow the mobile cloud vulnerable to various forms of violence. The introduction of smartphones and the extensive usage of other technology such as smartphones has brought significant changes to cloud storage, providing a higher level of versatility in data access, and thus increasing the need for security protocols. Unlike many problems, when dealing with business goals, financial activity and health care, protection and confidentiality are critical. In this study, we discuss mobile cloud computing in detail, then the model and role of the whole technology. Finally, we dragged some solutions for the three-level security and privacy concerns.

***Keywords*—** Mobile cloud computing, Technology, privacy issues, security.

I. INTRODUCTION

Mobile cloud computing has become a buzzword since 2009 in the technology world. Statistical analysis from IDC's Worldwide Quarterly Cloud IT Infrastructure Tracker, International Data Corporation (IDC 2016) published a quarterly cloud revenue report for different clouds. This list demonstrates the number of servers, hard disks, and peripheral equipment installed in the cloud system. As shown by IDC in 2015, the cloud IT technology software provider's gross profit rose 21.9 percent every year to $29.0 billion [1]. It is a significant invention as the resource limitations like- memory shortage, battery, and processing power of the handful of devices are resolved. In the busy schedule of today's world, it is a great technology to keep users comfortable to work with useful data anytime from anywhere. As the area of wide-ranging wireless networking technology, including Wi-Fi, 5th-generation/advanced 5Gmm-wave connectivity is going to make for smartphone users to use cloud infrastructure easier than before. Also, mobile cloud computing has become an important trigger for the expanding popularity of mobile devices and cloud services. The different types of mobile cloud computing conducted by mobile gadgets include video play, voice video sharing, data storage, web surfing, networking sites. The cellular data traffic is anticipated to raise 30.6 Exabytes for every month (one Exabyte=1018 byte) at the CAGR (compound annual growth rate) of 53% between 2015 and 2020, as shown in the report published by Cisco (2016) [2]. However, no technology has only benefits and no issues at all. Similarly, the main challenge in mobile cloud computing today is still having privacy and security issues. In virtual business and healthcare technologies, these are extremely crucial and represented by confidential and lengthy transactions, which involve both the protection of data and confidentiality of the users [3]. A range of influences is behind this design thinking process. Initially, their extreme capacity limitation is a prominent problem of mobile platforms, because they may be made up of small detectors or chips which have restricted computing power and speed.

This makes it difficult to implement complex and dynamic encryption algorithms. In contrast to their cabled equivalents, implementing protection was often a serious hurdle because of their intrinsic storage and broadcasting distribution, and because of their system limitations. Secondly, unified traffic, unforeseeable shifts in topology, varying distributions in nodes, large network levels, and high bit error ratios dominate interaction across the mobile source and the network. Thirdly, the mistakes of a user using a cloud network to handle confidential and cost-effective data may result in a high risk for data robbery transmitted from the cloud to the tablet or smartphone. [4] The purpose of the study is to introduce the main challenges and privacy issues in mobile cloud computing that have become the main concern of every mobile cloud computing user and researchers. Focusing on the previous studies, here the

solutions are provided that may be effective to resolve the problem.

II. OVERVIEW OF MOBILE CLOUD COMPUTING

A. Mobile Cloud Computing

In brief, Mobile Cloud Computing is a combination of mobile computing and cloud computing. In this technology, data are kept in cloud repositories and the main operation in the cloud system is moved in such a way that even a mobile user is clear of practical limitations on current handheld devices. In addition, cloud computing services are used by wireless media for connectivity among mobile platforms and clouds. [5] The main three components for this technology are- mobile devices, wireless connection channels, and cloud. As the authors claim in their studies (Sanaei et al., 2012), Mobile Cloud Computing is an enriched mobile computer technology, which uses standardized flexible resources of various clouds and network infrastructure to provide unregulated connectivity, space and mobility and, irrespective of constrained systems and frameworks, serves numerously portable devices anywhere on Web [6].

B. Mobile Cloud Application

Since the skyrocketing growth of mobile devices, companies are developing emerging forms of application for these devices and many provide cloud-based services with robust usability. [7] Mobile users can gain enriched cloud solutions and services even on resource-limited devices from these apps.

Size-up or downgrade of these systems must be done immediately to meet both desktop and mobile device standards. The program needs to be split into mobile cloud applications and components by the specifications. Applications that involve local mobile tools, such as various sensors, need not be downloaded into the cloud. But the modules that are extremely resource-intensive must be discharged into the cloud.

These apps can thus be classified into three main categories, customer-based, customer-cloud based, and cloud-based models. [8] The main implementation of the app is on a mobile device in a customer- cloud-based model.

This customer-cloud based model on the application is divided into subsystems and portable devices and remote cloud run these subsystems. In the cloud models, however, the cloud is part of the app in which the app operates.

C. Mobile Cloud Computing Model

The traditional Mobile Cloud computing model consists of three main components- mobile devices, mobile networks, and the cloud. [9]

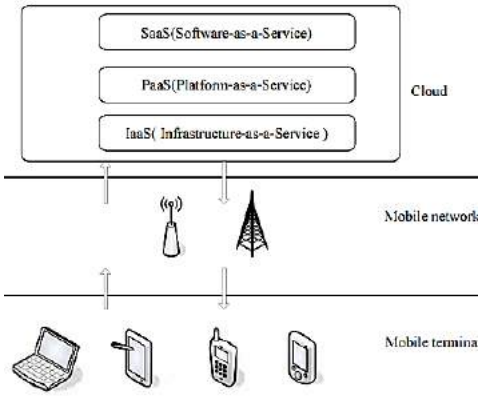

Fig. 1: Traditional Mobile Cloud Computing Model

Wireless devices for cloud connectivity, such as smartphones, laptops, computers, etc. are referred to as mobile devices. The protection and privacy concerns are covered with these three factors in the mobile cloud computing infrastructure.

- Mobile Network as a Service (MNaaS): This model provides the network infrastructure of network operators enables customers to access their connections, regulate the traffic and communicate to servers. [10] For example- OpenStack Network Service.
- Mobile Web as a service (MIaaS): The service providers provide cloud infrastructure and storage for mobile users in this service model. Examples of this are- the iCloud drive and Google drive for mobile users.
- Mobile Data as a service (MDaaS): The service providers offer database-related services in this model to allow mobile users to control their records, transactions, and other information-related activities. For instance- mobile cloud data from the service Oracle and cloud DB.
- Mobile App as a Service (MAppaaS): This system of service allows users in all wireless networks to enter, use and perform cloud-based mobile applications. Example: Google Play Store applications (www.play.google.com / store / apps).
- Mobile Multimedia as a Service (MMaaaS): In here users can manage and control multimedia applications, such as tv shows or game consoles, in rich devices via the cellular network.

- Mobile community as a Service (MCaaS): A mobile user team can construct and maintain a mobile social network or a group, in which the usages of social networks or community programs can be obtained to the user.[11]

D. Advantages of Mobile Cloud Computing

Increasingly people enjoy internet access via portable devices such as mobile phones and laptop computers. In reality, however, the mobile device storage space is reduced to ensure the used resources acquired are lower. So, in comparison with a PC, the calculation capacity of mobile devices is small and the longevity of batteries and the sharing of information with a Computer are low. Mobile cloud computing prevails for all these purposes and solves those problems.

Firstly, it is to cross the constraints of the hardware. Mobile cloud computing allows complicated data analysis and big data storage in the cloud. [12] The workload of computation and processing on mobile devices is therefore lessened. Secondly, it is smarter for load balancing and electricity saving. Thus, mobile cloud computing can fix the issues of battery maintenance and enhance the power consumption of mobile devices. Thirdly, this technology enables efficient access to data. Fourthly, it reduces the cost of maintenance by self-service.

III. SECURITY AND PRIVACY CHALLENGES

Privacy and confidentiality are key concerns in mobile cloud formulation and construction. The main challenges of security and privacy issues are discussed below-

A. Mobile nodes

Mobile terminals usually have basic specifications like- free operating system, third-party app support; "personalization;" wireless Internet access wherever or whenever. That's why mobile terminal security problems are very severe. The following will discuss malware, security problems of software, and other applications.

- Malware: The mobile terminal's accessibility and flexibility always capture the ire of hackers. A lot of malware, along with helpful programs and systems, can instantly be downloaded and brought unidentified to the user. This allows the malware to have unauthorized entry, control the flow, and charge automatically without the user operating. This will cause users to suffer economically from the mobile terminal impact or the spillage of data. Some security providers have built up virus protection for mobile devices to target malware [13].
- Application software: The key mobile device is the smartphone. And most cell phone users use the mobile managerial system to run the telephone by handling mobile telephone data via content syncing between the phone and the computer. This method normally involves the FTP (File Transfer Protocol). The username and password of FTP are transmitted through the network and saved in clear text in the config file. [14] In the end, unethical access on mobile phones via FTP will lead to the leakage of personal data and unauthorized disclosure by deliberate deletion and harmful activities from computer systems on the same network.
- Operating system: The Operating system is responsible for hardware and software resources management and operation. And the program is so complicated that programming bugs are eliminated. Such vulnerabilities are used in certain cases to harm useful data by hackers.
- Misoperate by the Users: Sometimes the security issues in mobile terminals are caused by users. The users are unaware of the security of cell phones and misoperate the device.

B. Network Security

Compared with the existing network, the mobile network improves the versatility of the network node and its connectivity. The network node can be expanded to include mobile devices such as smart telephones, tablets, etc.; mobile devices can access the system in a wide range of ways such as smartphone users using telephone and short messaging apps or other Internet services through 3G/4G/5G networks. Moreover, on a smartphone, it can also access the network via Bluetooth and Wi-Fi. This will lead to greater security threats like a responsive leak of data or harmful activities.

For example, different types of social spaces (for example, cafeteria, restaurants, hotel) offer free Wi-Fi, and many individuals have a laptop and free Wi-Fi internet access. In this scenario, the likely disclosure of data will occur. In addition to this public Wi-Fi system, even private Wi-Fi faces security hazards because of the vulnerability of the Wi-Fi encryption and decryption process. [15] The interaction also occurs through various platforms among mobile devices and cloud service companies which are increasing security risks every moment.

C. Mobile Cloud

The cloud infrastructure is vulnerable to exploitation due to its high volume of user data resources. The goal of the cybercriminal is to snatch useful information or services. Attacks can arise from fraudulent foreign,

illegal cloud computing users or inside cloud operators' employees. On the other hand, a malicious assailant has the intention of closing the cloud platform. For example- DOS attacks would break connectivity to the network and disable the cloud service. [16] When clients supply the cloud service providers with all their details without choosing a costly backup and restoration service, they face an accident and poses the risks of data loss. Such events occurred over and over in recent years in cloud providers. That's why, The cloud supplier has to incorporate the existing security technology to make sure that the service is accessible and also, the customers should not rely too much on the cloud supplier.

The proprietorship and control of the information are isolated in the cloud and users are thus made a major barrier to the rising popularity of mobile cloud computing by their worries about their information infrastructure. The user information is also a random manner placed in the shared infrastructure around the world and consumers do not realize where their data is kept. This increases the risk of sensitivity to personal information from users. So, a single method is not adequate to establish a secure connection. A complete security solution is only workable in this case.

IV. ADVANCED STEPS FOR SECURITY AND PRIVACY

In the modern era, different steps are taken to secure Mobile Cloud Computing. The latest protection taken for this technology is discussed here.

A. Mobile Node Security

- Protection from Malware: There are two factors to do with malware for the mobile node. The one is for malware identification and deletion. We should switch the malware detection to the cloud to resolve the resource constraints on mobile terminals. With this, the identification rate can be increased and reduce mobile terminal resource usage. So if malware is found, it is possible to delegate legal software from the cloud to the mobile terminal to delete the malware. This legal app allows for authentication, certification, and restoration in the mobile device. CloudA V is an example of anti-malware. CloudA V is a new concept for mobile device malware detection focused on virus protection as an in-cloud network application. [17] CloudA V offers several important advantages: improved malicious software detection; reduction of antivirus vulnerability impacts; cumulative holder identification; advanced data analysis; enriched deployment and management skills. And it contains the cross-platform host operator and the network support with antivirus programs and two cognitive monitoring systems.
- Software issues: To maintain software issues, it is needed to careful when updating and installing any software on the mobile. Also, the user should be looking for the validation and authenticity of the third-party software while installing and downloading.
- Maintaining user awareness: At present most cybercrime or hacking occurs due to the carelessness of the users. To prevent the attacks the user should avoid misoperating the connections. [18] For example- avoid the unexplained links to ignore fishing. Also, turn off the Bluetooth after use and it is better not to use the public Wi-Fi or data security. It is also important to be careful about transmitting data from stranger devices. These can reduce malware spreading vastly.

B. Mobile Network Security

There are mainly two facts to secure a mobile network. The first is the encryption of data. Due to the best way that communication systems navigate the mobile network is relatively safe to transmit information is that the network is encrypted. Proper encryption and decryption are essential to maintain data security in the network connection. [19] The second is the procedure on defence. Protection protocol work is the secret to reducing various stances across all sorts of accessibility methods.

C. Mobile Cloud Security

The performance and reliability of the mobile cloud computing infrastructure are important for both users and service companies. First of all, cloud services can incorporate existing security solutions including VPN technology, authentication and authorization, encryption, and other technical means, and include the continuous service available towards various threats such as DOS attacks and information theft. [20] Secondly, cloud providers can provide a full backup and disaster recovery method to restore data from the users when severe attacks occur. Through this, cloud hosting will boost service value and improve the morale of the users.

Throughout the expected lifespan from storage to transmitting, the confidential data require encryption techniques. To avoid any leakage of sensitive information, the data should be stored in the cloud in the cipher text. Nevertheless, encryption would reduce the data usage rate, so the emphasis is shifted to the efficient processing and analysis of the cipher text. The latest

work on the encoding of cipher text is the algorithm for privacy. [21] Strict key management is another critical function for business users.

Once users complete the transition of data to the cloud, network security should have a significant part to play. There are two sorts of systems for network access. The owner is allocating the connection authorization to the account level and all occupants consider sharing this assigned account. The other one is to pre-assign access privileges to relevant tenant systems using the method of the Access Control List (ACL) [22].

V. CONCLUSION

When the technology of this nature expands, it raises business organizations' interest and draws several people, including critics, which poses a significant threat to any nature of confidential information. Safety and privacy are key issues in mobile cloud computing, particularly when implemented for confidential flows of information, such as medical records, financial statements and corporate strategy. [23]

Mobile cloud computing may be impacted if a service interruption or security issue occurs in mobile devices, cloud facilities, or in publicity. A wide strand of research demonstrates various forms of security and privacy problems in cloud computing and mobile cloud computing. There is no simple, uniform solution, however, that could be applied to the method. Cloud infrastructure is composed of diverse systems and technologies which renders implementation of a standard security mechanism or system complicated. Cloud infrastructure is composed of diverse technologies and services that implement a secure authentication mechanism or system challenging. The lack of a cloud computing security framework leaves cloud services susceptible to various kinds of security and privacy risks, such as VM-to-VM attacks, malicious command injection, unwanted access, data loss, and data corruption. [24]

Furthermore, mobile cloud computing struggles from the question and authority of information privacy which is national issues. Intra-cloud connectivity providers are a major issue that restricts users from switching between providers of cloud services. In this article, we coherently discussed mobile cloud computing benefits and models and explored security and privacy problems through three levels, that are mobile devices, mobile networks, and mobile cloud. Then, we provided suitable systems, such as anti-malware, privacy security, network distribution and encryption, access control, etc., as per the problems. Hopefully, with the updating of the latest technologies, mobile cloud computing will be more reliable with the increasing security and privacy system.

REFERENCES

[1] IDC 2016, 'Worldwide Cloud IT Infrastructure Spend Grew 21.9% to $29.0 Billion in 2015', Press release, Framingham, viewed May 2016, http://www.idc.com/getdoc.jsp?containerId=prUS41176716

[2] Cisco 2016, 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020', Cisco Systems, pp. 5. viewed Jun 2016, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visualnetworking-index-vni/mobile-white-paper-c11-520862.htm

[3] Akhil Behl 2011, 'Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation', 2011 World Congress on Information and Communication Technologies, pp. 217-222, December

[4] Talukdar, A. K. (2010). Mobile Computing, 2E. Tata McGraw-Hill Education.

[5] Stojmenovic, I. (2002). Handbook of wireless networks and mobile computing. New York: Wiley.

[6] Sanaei, Z., Abolfazli, S., Gani, A., Shiraz, M., 2012. SAMI: service-based arbitrated multitier infrastructure for mobile cloud computing, in Communications in China Workshops (ICCC), 2012. In: Proceedings of the 1st IEEE International Conference on, pp. 14–19.

[7] Bahrami, M., Singhal, M., 2015. A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing, in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015. In: Proceedings of the 3rd IEEE International Conference on, pp. 189–198.

[8] Flores, H., Srirama, S. N., & Paniagua, C. (2012). Towards mobile cloud applications. International Journal of Pervasive Computing and Communications.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[9] Mishra, J., Dash, S. K., & Dash, S. (2012, January). Mobile-cloud: A framework of cloud computing for mobile application. In International Conference on Computer Science and Information Technology (pp. 347-356). Springer, Berlin, Heidelberg.

[10] Yin, Z., Yu, F. R., & Bu, S. (2014, December). Joint cloud computing and wireless networks operations: a game theoretic approach. In 2014 IEEE Global

Communications Conference (pp. 4977-4982). IEEE.

[11] Sharifloo, A. M., & Metzger, A. (2017). Mcaas: Model checking in the cloud for assurances of adaptive systems. In Software Engineering for Self-Adaptive Systems III. Assurances (pp. 137-153). Springer, Cham.

[12] Song, W., & Su, X. (2011, May). Review of mobile cloud computing. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 1-4). IEEE.

[13] Kumar, R., & Rajalakshmi, S. (2013, December). Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems. In 2013 International Conference on Computer Sciences and Applications (pp. 663-669). IEEE.

[14] Vikas, S. S., Pawan, K., Gurudatt, A. K., & Shyam, G. (2014, February). Mobile cloud computing: Security threats. In 2014 international conference on electronics and communication systems (ICECS) (pp. 1-4). IEEE.

[15] Jo, M., Maksymyuk, T., Strykhalyuk, B., & Cho, C. H. (2015). Device-to-device-based heterogeneous radio access network architecture for mobile cloud computing. IEEE Wireless Communications, 22(3), 50-58.

[16] Yan, Q., & Yu, F. R. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 53(4), 52-59.

[17] Liu, F., Shu, P., Jin, H., Ding, L., Yu, J., Niu, D., & Li, B. (2013). Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. IEEE Wireless Communications, 20(3), 14-22.

[18] Hussain, R. G., & Khan, M. F. SECURITY ISSUES IN MOBILE CLOUD (PLATFORM RELIABILITY, DATA PRI.

[19] Li, H., Shou, G., Hu, Y., & Guo, Z. (2016, March). Mobile edge computing: Progress and challenges. In 2016 4th IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud) (pp. 83-84). IEEE.

[20] Koe, A. S. V., & Lin, Y. (2019). Offline privacy-preserving proxy re-encryption in mobile cloud computing. Pervasive and Mobile Computing, 59, 101081.

[21] Jiang, X., Kong, W., Jin, X., & Shen, J. (2019, September). A Cooperative Placement Method for Machine Learning Workflows and Meteorological Big Data Security Protection in Cloud Computing. In International Conference on Machine Learning for Cyber Security (pp. 94-111). Springer, Cham.

[22] Sookhak, M., Yu, F. R., Khan, M. K., Xiang, Y., & Buyya, R. (2017). Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. Future Generation Computer Systems, 72, 273-287.

[23] Li, H., Shou, G., Hu, Y., & Guo, Z. (2016, March). Mobile edge computing: Progress and challenges. In 2016 4th IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud) (pp. 83-84). IEEE.

[24] Xing, T., Liang, H., Huang, D., & Cai, L. X. (2012, June). Geographic-based service request scheduling model for mobile cloud computing. In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 1446-1453). IEEE.