

A MOBILE CLOUD SECURITY TECHNIQUES AND CHALLENGES IN HEALTHCARE MANAGEMENT

E.S.Madhan M.E.(Ph.D)¹ , Dr. J. Sreedhar., M.Tech., Ph.D² & P.Jayaram., M.Tech³

Abstract-With the increasing and popularity of Mobile devices, integration of Mobile computing and Cloud Computing has become an imperative to develop their potential assets and helps in solving health care implications. The Mobile Cloud Computing (MCC) offers modern approach to service a patient's care. Moreover MCC gives solutions for reducing energy consumption, reduce cost, maintenance and low computing ability. However, security is a major concern when dealing with Mobile Cloud and Healthcare systems. In this paper, investigate and discuss the Mobile Cloud security challenges and issue present in the Health care management. The assurance development and motivation of Mobile Cloud Security are need flexible for mobility and ubiquity to future generations.

Keywords: Cloud Computing, Healthcare, Mobile Cloud Computing, Mobile Cloud Security.

1. INTRODUCTION

The rapid growth of usage in Cloud computing is increase as per demand services by the user. The main characteristics of Cloud computing is scalability, agility, reliability, security, reduction in cost and reduce maintenance. Security is a complex research issue in Cloud Computing. [8] The development and Scalable use of Cloud usage is directly or indirectly depends on important factor of security concern. There are many applications are deploy through the Cloud Computing such as medical, industry and educations.

In healthcare industry are used Cloud environment for storing, retrieve and analysis of healthcare data for emergency for future use. The easiest way of communication is handheld devices such as Mobile. A mobile data is stored through the Cloud have possess as biggest challenge as Cloud trust environment.

The MCC Security issues are follows as:

1. Data Loss.
2. Data steal by Malware softwares
3. Data Leakage.
4. Network Access.
5. Insecure market softwares.

The remainder of the paper organized follows as: In section2, we discuss about the related words of clouds security. In section3 presents the architecture of Mobile Cloud computing model, In section 4 represents an analysis of various cloud security models. In section4 we discuss the conclusion and future scope.

2. RELATED WORKS

In medical Healthcare systems frequently use the information security systems to store and process the patient information as well as hospital information.[1] authors presents that Cloud computing and mobile computing plays a major vital role in the recent trends. The communication between the mobile and the cloud providers to assure of user mobility. i.e. Mobile health(m-health) technology system. Greater data about the individual patients will able to store in the cloud for the Predictive analysis. [2,3] to widespread of the market approach to enabling the mobile cloud is easy way to access the information. [4] A security of MCC divided into two types of categories. They are mobile user levels and the Data security. a.) Mobile user's Security: Nowadays, Mobile phone and other smart devices [5] are increase, so exposure of various attacks is more possible with different kinds of malware codes such as Virus and Trojans. b.) Cloud Data Security: storing on Cloud providers has various benefits but dealing with secure data should be careful. The privacy can be authentication, Integrity and right privileges.

3. CLOUD SECURITY CHALLENGES

A.) Identification and Access Management

Many Existing methods in Identity and Authentication models are may not adopt to implement in Cloud. [6] The

¹ Department of Computer Science and Engineering, SVEC Autonomous-Tirupati, INDIA.

² Department of Computer Science and Engineering, SVEC Autonomous-Tirupati, INDIA.

³ Department of Computer Science and Engineering, SVEC Autonomous-Tirupati, INDIA.

username and passwords are weakening in process of security chain. The implementation of Identity and Access management (IAM) in cloud become a main key mechanism in the Cloud adoption.

B.) Cloud Data Protection

The Data protection in the Cloud is another major challenge which resides on the multi-renter environment. The Healthcare data have more personal and possessive data that must be trusted in cloud. The Cloud data protection is also depends on the Potential failure mechanism and also memory, storage.

C.) Data Compliance

Data Compliance is complicated issue in Cloud Computing. The Laws and Regulations are normally differs from various types of Cloud providers. For example, the European countries never allow sharing health care data to another's country. To restrict and complement a strict level data security requires better cloud infrastructure.

D.) Data Trust

Data Trust is a fundamental element aspect of Cloud computing. Data from various sources such as medical data shows the average trust of the different policies. So trust in the policies is high majority on provide the services of the Cloud computing.

E.) Cloud Secure Architecture

A cloud platform basically supports security features such as authentication support, Denial of service attack, Firewall policy management, Log Files handling and so on. But in Virtual environment of the cloud need higher level of Hybrid platform of security that facilitates greater level of platform architecture.

4. METHODOLOGY

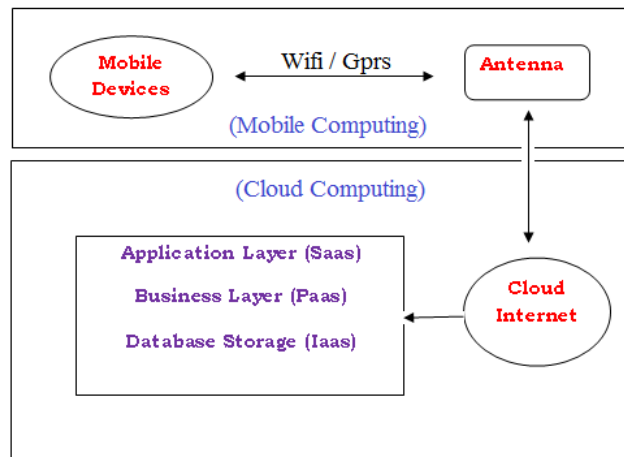


Fig-1: Mobile Cloud Architecture

Fig-1 explains that Mobile Cloud Architecture of Security. The mobile devices are connected through the wifi or GPRS communication and passes through the Antenna. This action carries out in Mobile computing, Then the Antenna is transfer over the Cloud environment again through the wifi signals that is carried out in the Cloud computing block. In the Cloud internet have the security solving mechanisms. A three important layers that facilitate in Cloud as i.) Appliation Layer, ii.) Business Layer and, iii.) Database Storage Layer. According to needs for data services every layer must have the end to end level of security function should be embedded in the Cloud Infrastructure.

5. CONCLUSION

In order to attain a better level of security and increase the reliability of MCC. Data security and privacy is an import mechanism for providing services to the Cloud computing that needs to be address and specified in security plan and also develop End to end security in cloud computing is important concern services are running on cloud must follow the different types of security policies and Principle of least privileges.

6. REFERENCES

- [1] B. Corona, M. Nakano, H. Pérez, "Adaptive Watermarking Algorithm for Binary Image Watermarks", Lecture Notes in Computer Science, Springer, pp. 207-215, 2004.
- [2] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognition Letters, vol. 26, pp. 1019-1027, 2005.
- [3] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," Vision, Image and Signal Processing, IEE Proceedings -, vol. 152, pp. 561-574, 2005.
- [4] F. Gonzalez and J. Hernandez, "A tutorial on Digital Watermarking", In IEEE annual Carnahan conference on security technology, Spain, 1999.
- [5] D. Kunder, "Multi-resolution Digital Watermarking Algorithms and Implications for Multimedia Signals", Ph.D. thesis, university of Toronto, Canada, 2001.
- [6] J. Eggers, J. Su and B. Girod, "Robustness of a Blind Image Watermarking Scheme", Proc. IEEE Int. Conf. on Image Proc., Vancouver, 2000.
- [7] Barni M., Bartolini F., Piva A., Multichannel watermarking of color images, IEEE Transaction on Circuits and Systems of Video Technology 12(3) (2002) 142-156.
- [8] Kundur D., Hatzinakos D., Towards robust logo watermarking using multiresolution image fusion, IEEE Transactions on Multimedia 6 (2004) 185-197.
- [9] C.S. Lu, H.Y.M Liao, "Multipurpose watermarking for image authentication and protection," IEEE Transaction on Image Processing, vol. 10, pp. 1579-1592, Oct. 2001.
- [10] L. Ghouti, A. Bouridane, M.K. Ibrahim, and S. Boussakta, "Digital image watermarking using balanced multiwavelets", IEEE Trans. Signal Process., 2006, Vol. 54, No. 4, pp. 1519-1536.
- [11] P. Tay and J. Havlicek, "Image Watermarking Using Wavelets", in Proceedings of the 2002 IEEE, pp. II.258 – II.261, 2002.
- [12] P. Kumswat, Ki. Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", IEEE Transactions on Signal Processing, Vol. 53, No. 12, pp. 4707-4719, December, 2005.
- [13] H. Daren, L. Jifuen, H. Jiwu, and L. Hongmei, "A DWT-Based Image Watermarking Algorithm", in Proceedings of the IEEE International Conference on Multimedia and Expo, pp. 429-432, 2001.
- [14] C. Hsu and J. Wu, "Multi-resolution Watermarking for Digital Images", IEEE Transactions on Circuits and Systems- II, Vol. 45, No. 8, pp. 1097-1101, August 1998.
- [15] R. Meul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", in Proceedings of the 2003 IEEE TENCON, pp. 935-938, 2003.