International Journal of Research in Engineering, Science and Management
Volume-2, Issue-11, November-2019
www.ijresm.com | ISSN (Online): 2581-5792

Secure Health Care System Based on Mobile Computing

M. Saravanan[1], J. Karthik[2], V. Rahul[3], T. Dhiliphan Raj Kumar[4]
[1,2,3]*Student, Department of Computer Science and Engineering, Kalasalingam University, Virudhunagar, India*
[4]*Professor, Department of Computer Science and Engineering, Kalasalingam University, Virudhunagar, India*

***Abstract*: Mobile Cloud Computing (MCC) allows mobile users to have on-demand access to cloud services. A mobile cloud model helps in analyzing the information regarding the patients' records and also in extracting recommendations in healthcare applications. In mobile cloud computing, a fine-grained level access control of multi-server cloud data is a pre-requisite for successful execution of end users applications. We proposed a Cloud-assisted Health monitoring system (CAM). We first identify the design problems on privacy preservation and then provide our solutions. To ease the understanding, we start with the basic scheme so that we can identify the possible privacy breaches. We then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the Health service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients decryption complexity, we incorporate the recently proposed outsourcing decryption technique into the underlying multi-dimensional range queries system to shift clients computational complexity to the cloud without revealing any information on either clients query input or the decrypted decision to the cloud. To relieve the computational complexity on the company's side, which is proportional to the number of clients, we propose a further improvement, leading to our final scheme. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud.**

***Keywords*: mobile computing**

1. Introduction

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

A "Secure health care system based on mobile computing" contains personal health record (PHR) makes it easy to collect and manage medical information in an accessible and secure location.

Personal health recording systems overcome this problem by making personal health records accessible at any time via a web-enabled device, such as a computer.

2. Technical feasibility

The Technical feasibility is the study of the software and how it is included in the study of our project. Regarding this there are some technical issues that should be noted they are as follows:

- Is the necessary technique available and how it is suggested and acquired?
- Will the system provide adequate response that is made by the requester at a periodic time interval?
- Can this system be expanded after this project development?
- Is there a technique guarantees of accuracy, reliability in case of access of data and security?

The technical issues are raised during the feasibility study of investigating our System. Thus, the technical consideration evaluates the hardware requirements, software etc. This system uses Java as front end and Oracle as back end. They also provide sufficient memory to hold and process the data. As the company is going to install all the process in the system it is the cheap and efficient technique.

This system technique accepts the entire request made by the user and the response is done without failure and delay. It is a study about the resources available and how they are achieved as an acceptable system. It is an essential process for analysis and definition of conducting a parallel assessment of technical feasibility.

Though storage and retrieval of information is enormous, it can be easily handled by Oracle. As the oracle can be run in any system and the operation does not differ from one to another. So, this is effective.

3. Existing system

In existing system, a PHR system model, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. But there is no security key to enter into cloud services for both clients and doctors. So that someone hack and modify the data in cloud easily.

Disadvantage:

- It poses a serious risk on both clients' privacy and intellectual property of monitoring service providers

- We could not deter the wide adoption of mHealth technology

4. Proposed system

In order to protect the personal health data stored on a semi trusted server, we adopt KP-ABE (Key Policy Attribute-Based Encryption) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. Whenever client enters into cloud services he has to give security key and which is generated based on KP-ABE and it is created freshly for every time login.

Advantages:

1. TA can be considered as a collaborator or a management agent for a company.
2. TA could collude to obtain private health data from client.

5. System architecture

A system architecture or systems architecture is the computational design that defines the structure and/or behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

6. UML diagram

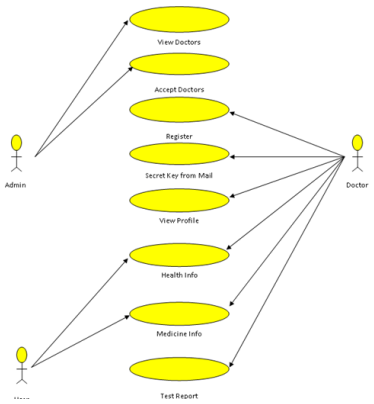

Fig. 1. Use case diagram

7. Modules description

Mobile User Module: In the mobile user module the user can login with their username and password if it is valid, it will be redirected to the another form. If the login id and password is not valid then mobile user cannot access the network operator. The user has to enter their details for disease prediction. After entering their details, it will show type and treatment to the user.

Network Operator Module: In this module all the mobile devices are connected to the network operator via the access point. Network Operator Module contains the CPU, Database, server. Database connected with the internet service provider to gather the required information to the mobile user from the cloud. CPU, Database, Server are connected together to access the data from the cloud via the internet connection.

Internet Module: Internet module act as a bridge between the network operator and application server module. It sends request to application server to collect the required information from the cloud. The application server module sends back the information to the user from the cloud data center to the Network operator.

Application Server Module: Incoming mobile user requests are distributed to the application servers that can most effectively process the requests in the cloud data centre. Application Server Module monitors the workload, performance, and behaviour of the application servers within our cloud database. The Application Server Module pulls logs and performance data from local and remote application servers.

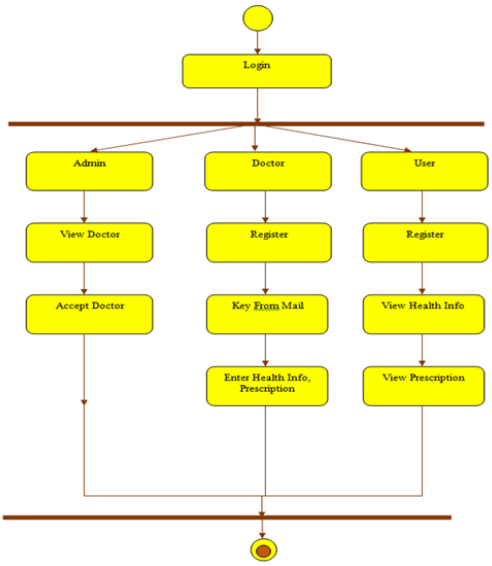

Fig. 2. Activity diagram

8. System implementation

Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the users, what it will work efficient and effectively. It involves careful planning, investing of the current system, and its constraints on implementation, design of methods to achieve the changeover methods. The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out in these plans; discussion has been made regarding the equipment, resources and how to test activities.

The coding step translates a detail design representation into

a programming language realization. Programming languages are vehicles for communication between human and computers programming language characteristics and coding style can profoundly affect software quality and maintainability. The coding is done with the following characteristics in mind.

- Ease of design to code translation.
- Code efficiency.
- Memory efficiency.
- Maintainability.

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

9. System testing

System Testing is an important stage in any system development life cycle. Testing is a process of executing a program with the intention of finding errors. The importance of software testing and its implications with respect to software quality cannot be overemphasized. Software testing is a critical element of software quality assurance and represents the ultimate review of specification, design and coding. A good test case is one that has a high probability of finding a yet undiscovered error.

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Testing is the set of activities that can be planned in advance and conducted systematically. Different test conditions should be thoroughly checked and the bugs detected should be fixed. The testing strategies formed by the user are performed to prove that the software is free and clear from errors. To do this, there are many ways of testing the system's reliability, completeness and maintainability.

The important phase of software development is concerned with translating the design specification into the error-free source code. Testing is carried out to ensure that the system does not fail, that it meets the specification and it satisfies the user. The system testing was carried out in a systematic manner with a test data containing all possible combinations of data to check the features of the system. A test data was prepared for each module, which took care of all the modules of the program.

System Testing is an important stage where the system developed is tested with duplicate or original data. It is a process of executing a program with the intent of finding an error. It is a critical process that can consume fifty percent of the development time.

The following are the attributes of good test:

- A good test is not redundant.
- A good test should be "best of breed".
- A good test should be neither simple nor too complex.
- *Unit Testing:* In the unit testing the analyst tests the program making up a system. The software units in a system are the modules and routines that are assembled and integrated to perform a specific function. In a large system, many modules on different levels are needed. Unit testing can be performed from the bottom up starting with the smallest and lowest level modules and proceeding one at a time. For each module in a bottom-up testing, a short program executes the module and provides the needed data.
- *Integration Testing:* Integration testing is a systematic technique for constructing the program structure while conducting test to uncover errors associate with interfacing. Objectives are used to take unit test modules and built program structure that has been directed by design. The integration testing is performed for this Multi Cloud when all the modules where to make it a complete system. After integration the project works successfully.
- *Validation Testing:* Validation testing can be defined in many ways, but a simple definition is that can be reasonably expected by the customer. After validation test has been conducted, one of two possible conditions exists.

1. The functions or performance characteristics confirm to specification and are accepted.
2. A deviation from specification is uncovered and a deficiency list is created.

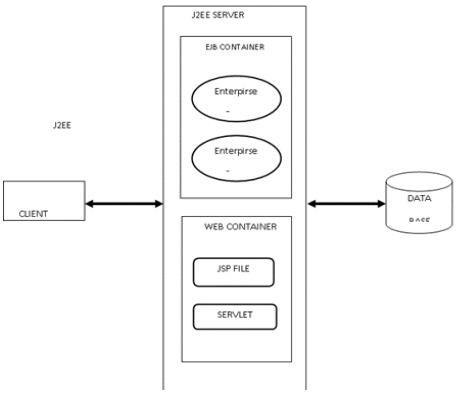

Fig. 3. Methodology

Proposed system under consideration has been tested by using validation testing and found to be working satisfactorily. For example, in this project validation testing is performed

against module. This module is tested with the following valid and invalid inputs for the field id.

- *Black Box Testing:* This method treats the coded module as a black box. The module runs with inputs that are likely to cause errors. Then the output is checked to see if any error occurred. This method cannot be used to test all errors, because some errors may depend on the code or algorithm used to implement the module.

10. Conclusion

We have implemented the formal and informal security analysis to show that the proposed scheme is secure against various known attacks. The widely-applied formal methods (for example, random oracle model) cannot capture some structural mistakes, and hence, ensuring the soundness of authentication protocols still remains an open issue. Due to this important observation, we also require the security analysis informally (non-mathematical) and formal security verification tool to ensure that the proposed scheme will be secure with high probability. So we have implemented in this J2EE project to prove the security of the system.

11. Future Enhancement

The security verification can be done through the following method, which is popularly used for testing the vulnerability of a session key security. The coding may be designed to be done in three steps. First, we declare various keys, constants, channels etc. Second, we simulate the working process of the mobile users. Third, we simulate the working process of the cloud server. Finally, we execute the simulation code in the website and obtain the result. In future we can implement this method even though it is costlier than the proposed system.

References

[1] L. A. Tawalbeh, W. Bakhader, R. Mehmood, and H. Song, "Cloudlet Based Mobile Cloud Computing for Healthcare Applications," in IEEE Global Communications Conference (GLOBECOM'16), Washington, DC, USA, 2016, pp. 1–6.

[2] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services," IEEE Access, vol. 5, no. 1, pp. 25808–25825, 2017.

[3] H. Wang, D. He, Y. Sun, N. Kumar, and K.-K. R. Choo, "PAT: A precise reward scheme achieving anonymity and traceability for crowd computing in public clouds," Future Generation Computer Systems, vol. 79, pp. 262–270, 2018.

[4] L. Wu, B. Chen, K.-K. R. Choo, and D. He, "Efficient and secure searchable encryption protocol for cloud-based Internet of Things," Journal of Parallel and Distributed Computing, vol. 111, pp. 152–161, 2018.

[5] D. He, N. Kumar, H. Wang, L. Wang, and K.-K. R. Choo, "Privacy preserving certificate less provable data possession scheme for big data storage on cloud," Applied Mathematics and Computation, vol. 314, pp. 31–43, 2017.

[6] K. Ratchinsky, "Cloud today and tomorrow: Why hospitals are tripling the use of cloud services," 2016. http://www.healthcareitnews.com/blog/cloud-today-and-tomorrowwhy-hospitals-are-tripling-use-cloud-services. Accessed on November 2017.

[7] "Cloud Computing: Building a New Foundation for Healthcare," 2011,

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06), Alexandria, Virginia, USA, 2006, pp. 89–98.

[9] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 4, pp. 673–686, 2011.

[10] S. Chatterjee and S. Roy, "Cryptanalysis and Enhancement of a Distributed Fine-grained Access Control in Wireless Sensor Networks," in Proceedings of IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, India, 2014, pp. 2074–2083.

[11] C. C. Lee, P. S. Chung, and M. S. Hwang, "A Survey on Attribute based Encryption Schemes of Access Control in Cloud Environments," International Journal of Network Security, vol. 15, no. 4, pp. 231–240, 2013.

[12] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, A. G. Reddy, K. Park, and Y. Park, "On the Design of Fine Grained Access Control with User Authentication Scheme for Telecare Medicine Information Systems," IEEE Access, vol. 5, no. 1, pp. 7012–7030, 2017.

[13] J. L. Tsai and N. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," IEEE Systems Journal, vol. 9, no. 3, pp. 805–815, 2015.

[14] P. Gope and A. K. Das, "Robust anonymous mutual authentication scheme for n-times ubiquitous mobile cloud computing services," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1764–1772, 2017.

[15] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," Future Generation Computer Systems, vol. 68, pp. 74–88, 2017.

[16] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.

[17] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proceedings of 19th Annual International Cryptology Conference (CRYPTO'99), LNCS, vol. 1666, Santa Barbara, California, USA, 1999, pp. 388–397.

[18] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure Biometric-Based Authentication Scheme using Chebyshev Chaotic Map for Multi-Server Environment," IEEE Transactions on Dependable and Secure Computing, 2016.

[19] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," IEEE Transactions on Dependable and Secure Computing, 2017.

[20] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," IEEE Journal of Biomedical and Health Informatics, 2017.

[21] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in Proceedings of the Advances in Cryptology (Eurocrypt'04), Lecture Notes in Computer Science, vol. 3027, Interlaken, Switzerland, 2004, pp. 523–540.

[22] F. B. Hildebrand, Introduction to Numerical Analysis, 2nd ed. New York: Dover, 1974.

[23] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol. 5, no. 3, pp. 145–151, 2011.

[24] D. Wang, D. He, P. Wang, and C. H. Chu, "Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 428–442, 2015.

[25] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'05), Lecture Notes in Computer Science, vol. 3386, Les Diablerets, Switzerland, 2005, pp. 65–84.

[26] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic Map-based Anonymous User Authentication Scheme with

User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things," IEEE Internet of Things Journal, 2017.
[27] M. Ballare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS'93), Fairfox, VA, USA, 1993, pp. 62–73.
[28] V. Shoup, "Sequences of games: A tool for taming complexity in security proofs," cryptology ePrint archieve, Report 2004/332.
[29] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's Law in Passwords," IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2776–2791, Nov 2017.
[30] D. Pointcheval and S. Zimmer, "Multi-factor authenticated key exchange," in International Conference on Applied Cryptography and Network Security. New York, USA: Springer, 2008, pp. 277–295.