AN EFFECTIVE AND EFFICIENT PRIVACY MODEL OF HEALTH BIG DATA IN CLOUD COMPUTING

G.Kavitha[1]

*[1]Departmentmet of Computer Science, Alagappa University,Karaikudi, Tamilnadu, gkaviajan@gmail.com [1]

Abstract— — Motivated by the privacy issues, curbing the adoption of electronic healthcare systems and the wild success of cloud service models, we propose to build privacy into mobile healthcare systems with the help of the private cloud. Our system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and audit ability for misusing health data. Specifically, we propose to integrate secure management from pseudorandom number generator for un linkability, a secure indexing method for privacypreserving keyword search which hides both search and access patterns based on redundancy, and integrate the concept of attribute based encryption with threshold signing for providing role-based access control with audit ability to prevent potential misbehavior, in both normal and emergency cases..

Keywords – cloud service models, role- based access control, encryption

I INTRODUCTION

Fast access to health data enables better healthcare service provisioning, improves quality of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life. Services supported by mobile devices, such as home care and remote monitoring, enable patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy, allowing patients with higher need of in-hospital treatment to be admitted. While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace.

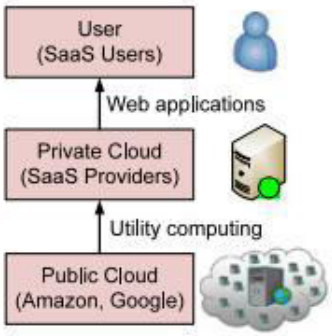

Fig: 1 Basic Structure of cloud system

While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace. According to the government website [1], around 8 million patients' health information was leaked in the past two years. There are good reasons for keeping medical data private and limiting the access. An employer may decide not to hire someone with certain diseases. An insurance company may refuse to provide life insurance knowing the disease history of a patient. Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information. Outsourcing data storage and computational tasks becomes a popular trend as we enter the cloud computing era. A wildly successful story is that the company's total claims capture and control (TC3) which provides claim management solutions for healthcare payers such as medicare payers, insurance companies, municipalities, and self-insured employer health plans. TC3 has been using Amazon's EC2 cloud to process the data their clients send in (tens of millions of claims daily) which contain sensitive health information. Outsourcing the computation to the cloud saves TC3 from buying and maintaining servers, and allows TC3 to take

advantage of Amazon's expertise to process and analyze data faster and more efficiently. The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm.

II RELATED WORK

Mobile cloud storage faces various security threats. Firstly, the cloud provider may be untrusted and want to profit from user information [23,24]. Secondly, several users share the same physical infrastructure in cloud storage, thus malicious users can obtain other user information through attacks such as unauthorized access, reverse control, and memory leaks [25]. Lots of privacy protection algorithms are proposed to resist the security risks caused by the untrusted cloud. Encrypted search schemes are one of the privacy protection algorithms. They can be categorized into two main classes: boolean keyword search and ranked keyword search. The former selects files only based on whether the keyword appears in the content of the file and is not concerned about any relevance of the files in the search result (e.g., [12–14,26]). The latter records the relevance scores to compare the relevance of files to the searched keyword and then replies with the top-k relevant files as a response (e.g., [11,15,16]). It greatly improves the efficiency of extracting useful information and accuracy. Therefore, it has been widely used by cloud storage and has attracted many researchers to develop it. Most of the latest studies about ranked keyword search focus on the cloud storage scenario. In [11], Swaminathan et al. developed a framework for a confidentially-preserving rank-ordered search. In this scheme, the computation task of the relevance scores is assigned to the client side, which increases the client's workload as a sacrifice to ensure the data security.

In [10], Zerr et al. proposed the concept of r-confidentiality as the degree of information leaked from an index, and proposed a system that allows for tunable index confidentiality and efficiency. But it only allows the client to decrypt the posting list and perform a top-k relevant search. This kind of research all assigns a heavy workload to the client, so it is not suitable for mobile cloud storage which uses resource-constrained mobile devices to access the cloud service. Considering the resource constraints in a mobile device, Miettinen and Nurminen in [27] pointed out that offloading some computing intensive tasks onto a cloud could be an effective way of dealing with this issue. Wang et al. in [26] presented a secure ranked keyword search over encrypted cloud data which used one-to-many mapping Order Preserving Encryption to encrypt the index of the file set. This design allows an efficient server-side ranking which reduces the client-side workload. Li et al. in [14] used cloud computing to improve the encrypted data search performance. Bowers et al. [28] proposed a distributed cryptographic system where the safety and retrieval of stored files are proven by a set of cloud servers. Wang et al. [15] introduced a secure ranked keyword search over encrypted cloud data. However, information leakage relating to the relevance between keywords and documents exists in these schemes, which could result in untrusted cloud providers obtaining the major term of stored files. In the era of the Internet of Things, edge computing is rapidly emerging because edge servers build a bridge between resource-constrained mobile devices and the cloud. Since applications can access infrastructure and application services provided on-premises [29], and edge servers and mobile devices are usually in the same LAN, edge severs would be conductive for mobile devices to implement the necessary privacy protection algorithm and protocols efficiently with their relatively adequate resources when data owners want to outsource massive local data from mobile devices to the cloud. Wadood Abdul et al. [30] proposed implementing visual cryptography and zero-watermarking algorithms on edge servers to encrypt the face images that are to be uploaded to the cloud. This prevents the untrusted cloud from obtaining and abusing user biometrix content, and also ensures the image quality, which means that the result of face recognition is not affected by image encryption. Maher Jridi et al. [31] also offloaded the image compression and encryption tasks to the digital gateway on the edge of network. Manisha Jindal et al. [32] used a trustworthy edge server to implement a secure forward encryption algorithm to prevent data from being acquired by unauthenticated users and untrusted service providers. Therefore, edge servers can be a key component in the secure data processing framework for mobile cloud storage and resemble the cloud trusted domain which is introduced in [33].

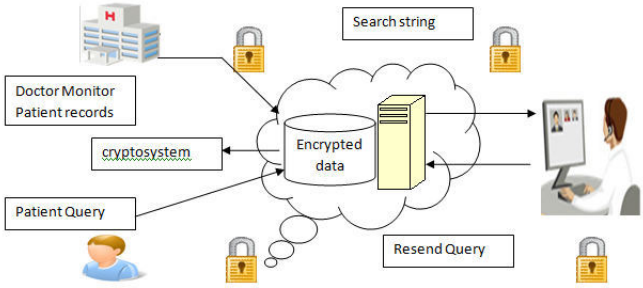

Fig: 2 Architecture of proposed work

III PROBLEM FORMULATION

EXISTING SYSTEM

In existing system, patient health monitoring and record maintenance are manipulated manually. It includes the use of paper entries/registers for the record maintenance, it is the tedious and very difficult process and it will take more time and increase human intervention. Despite efforts in managing these information systems, the healthcare data often result to be fragmented, redundant, prone to errors, and heterogeneous, making the task of finding useful information among such data very challenging

Disadvantages

- There may leakage of patient details
- Does not contain dispensary stock details
- There is no method for finding exact matching research matching patient matching requirements.
- Is a standalone system.
- There is no privacy security in patient records

PROPOSED SYSTEM

The drawbacks, which are faced during existing system, can be eradicated by using the proposed system. The development of this proposed system is PPRL methods is presented to five dimensions grouped into three categories: privacy guarantee, scalability, and linkage quality. EHR linkage, the same patient records may change over time; therefore, the temporal information has to be taken into account for designing effective linkage solutions.

Advantages

- The system can be used anytime and from anywhere by the doctor.
- It excludes the use of paper entries/registers.
- Doctors can view patient whenever needed in their application.
- Saves time and reduces human intervention.
- The system is flexible and secured to be used.
- The system can identify new details without affecting patient privacy by using unique no.

IV PROPOSED WORK IMPLEMENTATION

MODULES DESCRIPTION

In our project we are providing main 5 modules. They are as follows

- Record Linkage Approach
- Secret Key Generation
- Cryptosystem
- Stranger Blocking
- Monitoring Records

Modules Description

Record Linkage Approach

Admin module is the doctor module in this product software. Doctor module is used for maintaining and manipulating the patient's records. Doctor can add the patient's personal details and health details in the record. For secureness in patient's health record, doctor will generate a security key in each and every record and the patient's disease details are encrypted and then stored in the database. The patient records sending from admin then it is matched into the database using Record Linkage approach.

Secret Key Generation

This module is used for maintaining the reception records of the hospitals. By using this module, receptionist can request the patient's records from the administrator for the patient's disease records request. For the receptionist request, admin will send the security key through the mail.By using that security key receptionist can get the patient's records from server.

Cryptosystem

This module is mainly used for the encryption and decryption of the patient's health records. This kind of encryption and decryption is called as cryptosystem. In this product, admin will maintain the health records in the server. For maintaining more secure on health records, the administrator will encrypt the records before storing into server and he will generate encrypted security key for every records.

- **Stranger Blocking**

Stranger blocking is used for security purpose in this product. As per the patient health records request, the receptionist will forward the request to admin and the receptionist can get the security key for the request. Now the receptionist have to give the correct security key to access the record, if the given key is mismatched then the user (i.e receptionist)is blocked automatically. If the receptionist would like to add in this product, it is possible only when the admin will add the receptionist.

- **Monitoring Records**

This module is used for overview the whole product software. By using this, admin can monitoring the receptionist activities and patients records request and security key generation for

records. Finally we can maintain the whole health record of the patient in printed form.

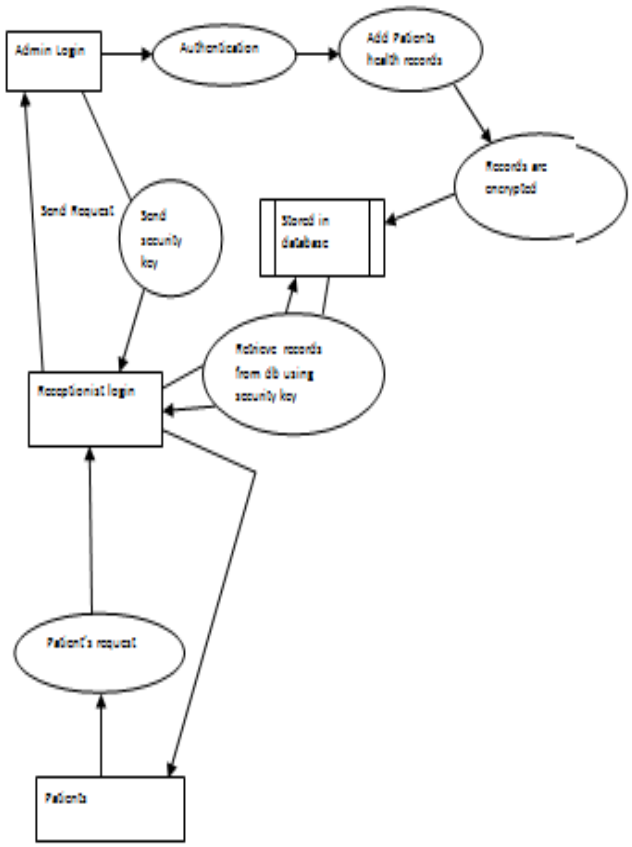

Fig:3 proposed work flow model structure

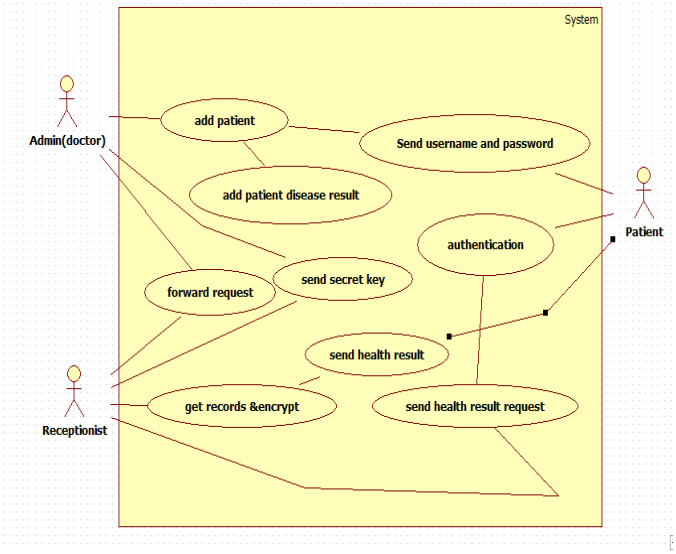

Fig: 4 Use case diagram for proposed work

VI. EXPERIMENTAL RESULTS

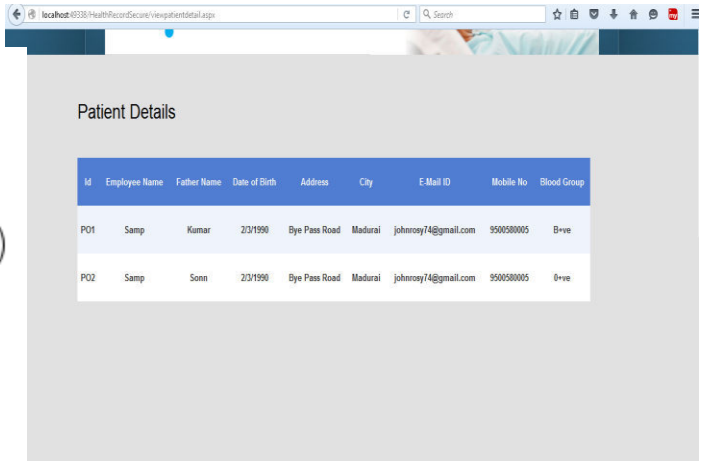

Fig: 5 Patient details in big data

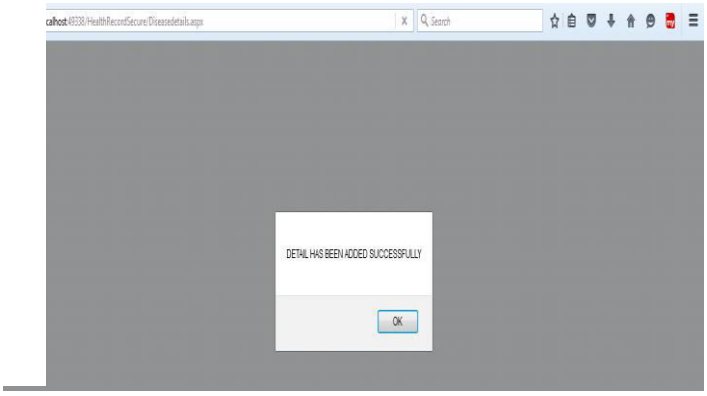

Fig: 6 Encrypted location of request file

V CONCLUSION

By this software package, records are transferred securely because of data mining concept and datas are transferred among the family members and friends. By using the analytical method we can forward the records.

FUTURE ENHANCEMENT

In future we may extend this software package with the following enhancements. They are

- Live supported implement this one as the software but in future we may extend this as android one
- Server based one

- Now we app.

REFERENCES

1. Tang, J.; Liu, A.; Zhang, J.; Xiong, N.N.; Zeng, Z.; Wang, T. A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks. Sensors 2018, 18, 751. [CrossRef] [PubMed]

2. Liu, A.; Huang, M.; Zhao, M.; Wang, T. A smart high-speed backbone path construction approach for energy and delay optimization in WSNS. IEEE Access 2018. [CrossRef]

3. Li, Y.; Cai, Z.; Xu, H. LLMP: Exploiting LLDP for Latency Measurement in Software-Defined Data Center Networks. J. Comput. Sci. Technol. 2018, 33, 277–285. [CrossRef]

4. Chun, B.G.; Ihm, S.; Maniatis, P.; Naik, M.; Patti, A. Clonecloud: Elastic execution between mobile device and cloud. In Proceedings of the 6th Conference on Computer systems, Salzburg, Austria, 10–13 April 2011; pp. 301–314.

5. Huang, D. Mobile cloud computing. In Proceedings of the 2011 10th IEEE/ACIS International Conference on Computer and Information Science, Sanya, China, 16–18 May 2011; p. 432.

6. Huang, D.; Zhang, X.; Kang, M.; Luo, J. Mobicloud: Building secure cloud framework for mobile computing and communication. In Proceedings of the IEEE International Symposium on Service Oriented System Engineering, Nanjing, China, 4–5 June 2010; pp. 27–34.

7. Liu, F.; Li, T. A clustering k-anonymity privacy-preserving method for wearable IoT devices. Secur. Commun. Netw. 2018. [CrossRef]

8. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and Privacy in the Medical Internet of Things: A Review. Secur. Commun. Netw. 2018. [CrossRef]

9. Liu, Y.; Ota, K.; Zhang, K.; Ma, M.; Xiong, N.; Liu, A.; Long, J. QTSAC: An energy-efficient mac protocol for delay minimization in wireless sensor networks. IEEE Access 2018, 6, 8273–8291. [CrossRef]

10. Zerr, S.; Demidova, E.; Olmedilla, D.; Nejdl, W.; Winslett, M.; Mitra, S. Zerber: R-confidential indexing for distributed documents. In Proceedings of the International Conference on Extending Database Technology (EDBT 2008), Nantes, France, 25–29 March 2008; pp. 287–298.

11. Swaminathan, A.; Mao, Y.; Su, G.M.; Gou, H.; Varna, A.L.; He, S.; Wu, M.; Oard, D.W. Confidentiality-preserving rank-ordered search. In Proceedings of the 2007 ACM Workshop on Storage Security and Survivability, Alexandria, VA, USA, 29 October 2007; pp. 7–12.

12. Curtmola, R.; Garay, J.; Kamara, S.; Ostrovsky, R. Searchable symmetric encryption: Improved definitions and efficient constructions. J. Comput. Secur. 2011, 19, 895–934. [CrossRef]

13. Waters, B.R.; Balfanz, D.; Durfee, G.; Smetters, D.K. Building an encrypted and searchable audit log. Annu. Netw. Distrib. Syst. Secur. Symp. 2004, 4, 5–6.

14. Li, J.; Ma, R.; Guan, H. Tees: An efficient search scheme over encrypted data on mobile cloud. IEEE Trans. Cloud Comput. 2017, 5, 126–139. [CrossRef]

15. Wang, C.; Cao, N.; Li, J.; Ren, K.; Lou, W. Secure ranked keyword search over encrypted cloud data. In Proceedings of the IEEE International Conference on Distributed Computing Systems, Genova, Italy, 21–25 June 2010; pp. 253–262.

16. Zerr, S.; Olmedilla, D.; Nejdl, W.; Siberski, W. Zerber+r: Top-k retrieval from a confidential index. In Proceedings of the International Conference on Extending Database Technology: Advances in Database Technology, Saint-Petersburg, Russia, 23–26 March 2009; pp. 439–449.

17. Islam, M.S.; Kuzu, M.; Kantarcioglu, M. Access pattern disclosure on searchable encryption: Ramification, attack and mitigation. In Proceedings of the 19th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, 5–8 February 2012.

18. Cai, Z.; Wang, Z.; Zheng, K.; Cao, J. A distributed TCAM coprocessor architecture for integrated longest prefix matching, policy filtering, and content filtering. IEEE Trans. Comput. 2013, 62, 417–427. [CrossRef]

19. Zhang, H.; Cai, Z.; Liu, Q.; Xiao, Q.; Li, Y.; Chak, F.C. A survey on security-aware network measurement in SDN. Secur. Commun. Netw. 2018, 2018.

20. Satyanarayanan, M. The emergence of edge computing. Computer 2017, 50, 30–39. [CrossRef]

21. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. IEEE Internet Things J. 2016, 3, 637–646. [CrossRef]

22. Paradrop. Available online: https://www.paradrop.org/ (accessed on 2 January 2018).

23. Hung, S.H.; Shih, C.S.; Shieh, J.P.; Lee, C.P.; Huang, Y.H. An online migration environment for executing mobile applications on the cloud. In Proceedings of the Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Seoul, Korea, 30 June–2 July 2011; pp. 20–27.

24. Zou, P.; Wang, C.; Liu, Z.; Bao, D. Phosphor: A cloud based DRM scheme with sim card. In Proceedings of the 2010 12th International Asia-Pacific Web Conference, Busan, Korea, 6–8 April 2010; pp. 459–463.

25. Ristenpart, T.; Tromer, E.; Shacham, H.; Savage, S. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 199–212

G.Kavitha,,M.Sc(ComputerScience),M.Ed,M.Sc(Psychology).,PB.EdDSA., is working as Assistant Professor in Psychology, Puratchi Thalaivar Dr.MGR College of Education, Uchipuli, Ramanathapuram.