

# Seclusion Protection and Invasion Avoidance in Medical Data Sharing based on Cloudlet Technology

Ch. Hanumantha Rao<sup>1</sup>, V. Nagabhushanam<sup>2</sup>

<sup>1</sup>M.Tech. Student, Dept. of Computer Science and Engineering, Chirala Engineering College, Chirala, India

<sup>2</sup>Associate Professor, Dept. of Computer Science and Engineering, Chirala Engineering College, Chirala, India

**Abstract:** A variety of wearable devices are leading the market in now days. With development of cloud let technology and cloud based model for taking care of health. Medicines are treated as health hazards. As we know prevention is better than cure, before getting sufferer to the diseases, we have to take care of our health. For that work has done to take care data collection, data storage and sharing of data in variety ways also available. The mechanism followed here is a new healthcare system is implemented by using flexibility of cloud based system. The functions of cloudlet include seclusion protection, data sharing and invasion detection. In the stage of data collection, first thing done is utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Here collected data will be transmitted to nearby cloudlet in an energy efficient fashion. Second step to present a new trust model this help user to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. In Third step, users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. Lastly, in order to protect the healthcare system from malicious attacks, a new collaborative invasion detection system (IDS) method based on cloudlet mesh is implemented, which can effectively prevent the remote healthcare big data cloud from attacks.

**Keywords:** Health care System, NTRU, Cloudlet, Sharing data, Invasion detection system.

## 1. Introduction

Large storage available in cloud where all the types of resources can be shared and on demand devices can be used in internet. parallel computing, bigData processing are using together with cloud computing. Cloud technology is the one of the popular technology in IT that provides various services to the user via Internet. Cloud system authorize the information sharing system which gives the variety of services to the user. In this way sharing of data takes higher priority. This task plays an important role in any organization that causes productivity in the cloud environment. The cloud services shared are effectively available by the on-request, on-requirement network access service as well as it is adaptable and accessible at less cost. The health record of the person is trading technology in applications of medical that are utilized for creating, managing

as well as modifying the health data related to the patient in very required way. The health records of the personal has diversified data related to the patient. the data such as information sheet, problems, medical records, progress notes, consultation reports, lab reports, immunization records, consent forms, diagnosis reports, analysis reports imaging and x-ray reports etc. Such records information must be stored on the cloud for the sharing as well as getting mechanism that is utilized for controlling the activities of the patient. In the personal health record, sharing of the data is fine-grained access control, security, data confidentiality, authorization and authentication is crucial challenge while sharing the personal health records in the third party storage. At the time of uploading of personal health care data in the cloud the owner of data losses the physical control also it can be hacked by hackers. Hence the providing the security is a big issue while sharing personal health care data in cloud environment. This can be solved by using encryption mechanism at the time of data sharing that will increase the confidentiality of the data as well as information security in the third party storage service. By making use of several encryption techniques user can store the data on cloud without worrying about the security. In the next segment we will go through some of the researches provided the different authors on Medical Data Sharing Systems.

## 2. Literature review

In this paper [1], for the first time, define and solve the challenging issue of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE). They establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, they choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. They further use "inner product similarity" to quantitatively evaluate such similarity measure. First propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models.

Thorough study of inspecting privacy and efficiency guarantees of proposed schemes is given. In paper [2] author build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet consist of privacy protection, data sharing and intrusion detection. In the stage of data collection, firstly utilize Number Theory Research Unit (NTRU) method to encrypt user as body data collected by wearable devices. Those data will be end to nearby cloudlet in an energy efficient fashion. Secondly, 1538 resent a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps identical patients to communicate with each other about their diseases. Thirdly, divide users medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, design a novel collaborative intrusion detection system (IDS) method depend on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. This paper [3] first introduces the main aim of this special issue and gives a brief guideline. Then, the present situation of the adoption of EMRs is reviewed. After that, the emerging data technologies are presented which have a great impact on the healthcare provision. These include health sensing for medical data collection, medical data study and utilization for accurate detection and prediction. Next, cloud computing is discussed, as it may offer scalable and cost-effective delivery of healthcare services. In this paper [4], author developed a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources involving computing power and energy can be opportunistically collected to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in mHealthcare emergency, They introduce an efficient user-centric privacy access control in SPOC framework, which is depend on an attribute-based access control and a new privacy preserving scalar product computation (PPSPC) technique, and permits a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security study display that the proposed SPOC framework can efficiently achieve usercentric privacy access control in mHealthcare emergency. This paper [5] developed a practical solution for privacy preserving medical record sharing for cloud computing. On the basis of the classification of the attributes of medical records, they use vertical partition of medical dataset to achieve the consideration of distinct parts of medical information with different privacy concerns. It mainly consisting four components, i.e., (1) vertical data partition for medical information publishing, (2) data combining for medical dataset accessing, (3) integrity checking, and (4) hybrid search across plaintext and ciphertext, where the statistical analysis and cryptography are innovatively combined together to

provide multiple paradigms of balance among medical data utilization and privacy protection. A prototype system for the huge scale medical data access and distributing is implemented. The usage of electronic health data from distinct sources for statistical analysis requires a toolset where the legal, security and privacy concerns have been taken into consideration. The health data are typically placed at different general practices and hospitals. The data analysis includes of local processing at these locations, and the locations become nodes in a computing graph. To support the legal, security and privacy concerns, the proposed [6] toolset for statistical study of health data uses a combination of secure multi-party computation (SMC) algorithms, symmetric and public key encryption, and public key infrastructure (PKI) with certificates and a certificate authority (CA). The proposed toolset should cover a wide range of data analysis with different data distributions. To accomplish this, huge set of possible SMC algorithms and computing graphs have to be supported. In this paper [7], author propose a priority based health data aggregation (PHDA) scheme with privacy preservation for cloud assisted WBANs to improve the aggregation efficiency between different types of health data. Specifically, first explore social spots to help forward health data and enable users to select the optimal relay according to their social ties. According to distinct data priorities, the adjustable forwarding methods can be selected to forward the user as health data to the cloud servers with the reasonable communication overheads. The security analysis describes that the PHDA can achieve identity and data privacy preservation, and resists the forgery attacks. In this article [8], investigate security and privacy protection in MHNs from the perspective of QoP, which offers users adjustable security protections at finegrained levels. Specifically, first introduce the architecture of MHN, and point out the security and privacy limitations from the perspective of QoP. Then present some countermeasures for security and privacy protection in MHNs, consisting privacy-preserving health data aggregation, secure health data processing, and misbehavior detection.

#### A. Review report of various research titles

*Project title:* Privacy-preserving multi-keyword ranked search over encrypted cloud data

*Paper details:* Privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE).

*Method used:* coordinate matching

*Advantages:* Introduce low overhead on both computation and communication.

*Disadvantages:* Integrity of the rank order in the search result assuming the cloud server is untrusted.

*Project title:* Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing

*Paper details:* healthcare system by utilizing the flexibility of cloudlet

*Method used:* Number Theory Research Unit

*Advantages:* Effectively prevent the remote healthcare big data cloud from attacks.

*Project title:* Privacy preserving health data processing

*Paper details:* Proposed toolset for statistical study of health data uses a combination of secure multi-party computation (SMC) algorithms

*Method used:* a combination of secure multi-party computation

*Advantages:* Proposed method can be applied for a large number of statistical computations

*Project title:* Emerging information technologies for enhanced healthcare

*Paper details:* adoption of EMRs is reviewed

*Method used:* cloud computing is discussed

*Advantages:* Shown that the cloud can be used for medical health care records storage

*Disadvantages:* Does not cover all the aspects and applications

### 3. Conclusions

In this review we have considered the some of the effort done by the researchers on the medical data sharing in cloud specific, also listed some of advantages and disadvantages. By this knowledge we can bring to a close that there must be a coordination which will solve the trendy issues in the present systems.

### References

- [1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 222-233, 2014.
- [2] Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu, "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing", *IEEE Transactions on Cloud Computing*, 2016.
- [3] J. J. Yang, J. Li, J. Mulder, Y. Wang, S. Chen, H. Wu, Q. Wang, and H. Pan, "Emerging information technologies for enhanced healthcare," *Computers in Industry*, vol. 69, pp. 3-11, 2015.
- [4] R. Lu, X. Lin, and X. Shen, "Spoc: A secure and privacy preserving opportunistic computing framework for mobile-healthcare emergency," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 3, pp. 614- 624, 2013.
- [5] J. J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," *Future Generation Computer Systems*, vol. 43, pp. 74-86, 2015.
- [6] A. Andersen, K. Y. Yigzaw, and R. Karlsen, "Privacy preserving health data processing," in *e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on. IEEE*, 2014, pp. 225-230.
- [7] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, "Phda: A priority based health data aggregation with privacy preservation for cloud assisted wbans," *Information Sciences*, vol. 284, pp. 130-141, 2014.
- [8] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, "Security and privacy for mobile healthcare networks: from a quality of protection perspective," *Wireless Communications, IEEE*, vol. 22, no. 4, pp. 104-112, 2015.