International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume – 3, ISSUE – 3 **ISSN (Online):2454- 1966**

Research Manuscript Title

A SURVEY ON PROVIDING ANONYMOUS PROTECTION AND SECURITY FOR MEDICAL DATA SHARING

K.Priyanga[1], B.Ananthi[2]

[1]PG Student, Vivekanandha College of Engineering for Women, Namakkal

[2]Assistant Professor, Vivekanandha College of Engineering for Women, Namakkal

E-Mail-ID: pritech18@gmail.com

Sep – 2017

www.istpublications.com

A SURVEY ON PROVIDING ANONYMOUS PROTECTION AND SECURITY FOR MEDICAL DATA SHARING

K.Priyanga[1], B.Ananthi[2]

[1]PG Student, Vivekanandha College of Engineering for Women, Namakkal

[2]Assistant Professor, Vivekanandha College of Engineering for Women, Namakkal

*E-Mail-ID:*pritech18@gmail.com

ABSTRACT

Cloud computing is the delivery of computing and storage space as a service to a diversified community of end users, it is necessary to develop a more privacy providing and secure storage system for sensitive medical data. This process includes data collection, data sharing and data storage. They need to provide privacy under data sharing mode and security under data storage model. A new healthcare system is proposed by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the phase of data collection, the first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data composed by wearable devices. The data is collected from wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. A trust model is developed to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to converse with each other about their diseases. As the data dealt is medical data, a more privacy model is required to share data, thus a anonymous techniques such as suppression and generalization of data is handled during data sharing phase. To shield the healthcare system from malicious attacks, intrusion detection system is designed, which can effectively prevent the healthcare data from cloud attacks.

Keywords - *Data collection, data sharing and data storage, trusted model, intrusion detection , healthcare.*

1. INTRODUCTION

Cloud computing is increasing an essential technology for handling medical health care data. With the growing demands on health consultation, it is challenging issue to personalize specific healthcare data for various users in a convenient fashion. Though the existing system provides security of data by avoiding intrusion, it is lagging in providing data privacy.

As health care data is considered to be the most sensitive data, it needs a strong privacy while sharing data between users. Though sharing medical data is beneficial to both patients and doctors, the sensitive data might be leaked or stolen, which causes privacy and security problems without efficient protection for the shared data. Therefore, how to balance privacy protection with the convenience of medical data sharing becomes a challenging issue. 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. Thus, we propose a strong privacy model to prevent data privacy, an anonymous technique such as data suppression and generalization is performed.

2. LITERATURE REVIEW

In [1] Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu in the paper **Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing** 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 data collection 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. Then present 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. And 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.

1n [2] Ning Cao, Member, Cong Wang, Member, Ming Li, Member, Kui Ren, Senior Member, and Wenjing Lou. **Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data** describe Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. It can be solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). For meeting the challenge of supporting multi-keyword semantic without privacy breaches, we propose a basic idea of MRSE using secure inner product computation. Then, give two improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Without providing the capability to compare concealed inner products, predicate encryption is not qualified for performing ranked search. Furthermore, most of these schemes are built upon the expensive evaluation of pairing operations on elliptic curves.We also investigate some further enhancements of our ranked search mechanism, including supporting more search semantics, i.e., TF *IDF, and dynamic data operations.

In [3] Rongxing Lu, Member, , Xiaodong Lin, Member, , and Xuemin (Sherman) Shen, in the paper **A Secure and Privacy Preserving Opportunities Computing Framework for Mobile Health Care Emergency** proposed in wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring ,They propose a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. The SPOC, smart phone wealth including computing power and energy can be opportunistically gather to process the computing intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure .In an efficient user-centric privacy access control in SPOC framework, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to make a decision who can participate in the opportunistic computing to assist in handing out his overwhelming PHI data. we have also demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency.

In [4] Lu Liu, Jingchao Sun, Jianqiang Li, Rong Li, Juan Li, Xi Meng, Huifang Li and Jijiang Yang in the paper **A Privacy Enhanced Search Approach for Cloud-Based Medical Data Sharing** This paper proposes a privacy enhanced search approach for cloud-based medical data sharing. The proposed solution implements a hybrid search approach, where the search process is conducted across plaintext and ciphertext.

The improved access control can ensure the privacy protection of cloud data. The empirical experiment show the effectiveness of our solution. To strengthen the utilization of encrypted cloud data, we propose a privacy enhanced search approach for cloud based medical data sharing These results validate again that the proposed hybrid search approach across ciphertext and plaintext can achieve similar performance to the pure plaintext search approach. The data recipient utilizes the proposed method to realize the record-level medical data access, i.e., to find one or multiple interested EMRs in the shared medical dataset. Since symmetric encryption algorithms are more efficient than asymmetric algorithms, in our implementation, a combination of both is being used. The data is encrypted using efficient symmetric key cryptography. This key is in turn encrypted with the recipient's public-key so that it can only be used by the authorized users by the data owner. This way the advantages of both algorithms can be used.

In [5] Anders Andersen, Kassaye Yitbarek , Randi Karlsen in the paper **Privacy preserving health data processing** proposed The electronic health data from different sources for statistical analysis requires a toolset where the legal, security and privacy concerns have been taken into consideration. The health data are typically located at different general practices and hospitals the data shows that only one patient at that general practice is subscribed medication *a* that is typical for multiple sclerosis (MS) patients, and only one patient at that general practice has visible symptoms of MS. When such data is part of a computation or analyzing task, special care has to be taken to ensure the privacy of the patients. The outcome of SMC research will in combination with cryptography be used to address legal, security and privacy issues. To fulfill the requirements, a combination of SMC algorithms and careful usage of encryption and certificates are used. The approach is based on a coordinator that prepares the computation and a set of sub-processes (nodes) representing the parties in the multi-party computation. In this paper the focus is the combined usage of SMC algorithms and cryptography to achieve privacy.The constraints for SMC discussed in combined with a practical and efficient implementation are the basis for our work. It has been demonstrated that a combination of SMC, encryption and PKI can be used to perform privacy-preserving statistical analyses on distributed health data.

In [6] M. Shamim Hossain, Senior Member, in the paper **Cloud-Supported Cyber–Physical Localization Framework for Patients Monitoring** proposes a cloud-supported cyber–physical localization system for patient monitoring using smartphones to acquire voice and electroencephalogram signals in a scalable, real-time, and efficient manner. The proposed approach uses Gaussian mixture modeling for localization and is shown to outperform other similar methods in terms of error estimation. The accurate, stable, and reliable localization of patients is very important when responding to emergency situations. Incorrect location information could result in severe consequences in patient monitoring. It is helpful for caregivers to know the current status of the patient (location, biosignals such as heartbeat, and breathing) while the patient is on the move. Currently, doctors are overburdened by their patients, and the shortage of doctors and caregivers in hospitals means it is very difficult for doctors to physically check each patient's case. Some of the workloads are measured. In future work, we will conduct more workload measurements to record the resource utilization of CPU, memory, storage, and network bandwidth.

In [7] Rui Zhang and Ling Liu in the paper **Security Models and Requirements for Healthcare Application Clouds** described in the electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community. They describe an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud. Many healthcare providers and insurance company today include adopted some form of electronic medical record systems, though most of them store medical records in centralized databases in the form of electronic records. The interoperation and sharing among different EMRs has been extremely slow. Cost and poor usability have been cited as the biggest obstacles to adoption of health IT, especially Electronic Health Records (EHR) systems. It is widely recognized that cloud computing and open standards are important cornerstones to streamline healthcare

whether it is for maintaining health records, monitoring of patients, managing diseases and cares more efficiently and effectively, or collaboration with peers and analysis of data. records the access and sharing of EHRs should provide end-to-end source verification through signatures and certification process against blind subpoena and unauthorized change in healthcare critical data content and user agreements. Then we present an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud.The development of the projected Electronic Health Records security mention model through a use-case scenario and explain the corresponding security countermeasures and potential security techniques.

In [8] Mbarek Marwan, Ali Kartit and Hassan Ouahmane, **Applying Secure Multi-Party Computation to Improve Collaboration in Healthcare Cloud** we propose an approach based on Secure Multi-party Computation (SMC) protocols to ensure privacy-preserving in the collaborative systems. In this concept, different organizations collaborate to accomplish common goals without allowing any party to view and reveal another individual's private data. we propose a framework based on SMC for privacy preserving collaborative environment in the healthcare sector. we provide background information of Secure Multiparty Computation (SMC) protocols.They present and discuss different techniques and approaches used to implement the SMC protocols. this method allows multiple healthcare institutions to jointly compute a function over their private inputs without revealing patients' information to other parties Additionally, this concept is an appropriate solution to boost collaboration between healthcare organizations. Despite its multiple advantages, the migration to this paradigm faces security challenges. For this reason, secure multiparty computation (SMC) algorithms are used to ensure patients' privacy we intend to address issues concerning encryption key management for promoting collaboration in the healthcare sector.

In [9] Larry A. Dunning, *Member, IEEE*, and Ray Kresman in the **paper Privacy Preserving Data Sharing With Anonymous ID Assignment** describe anonymous sharing of private data Among N parties is developed. This technique is used iteratively to assign these nodes ID numbers ranging from 1 to N . This assignment is anonymous in that the identities received are unknown to the other members of the group. The new algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for distributed solution of certain polynomials over finite fields enhances the scalability of the algorithms. Another form of anonymity, as used in secure multiparty computation, allows multiple parties on a network to jointly carry out a global computation that depends on data from each party while the data held by each party remains unknown to the other parties However, very little is known with respect to methods allowing agencies to opt-out of a secure computation based on the results of the analysis, should they feel that those results are too informative about their data The application of Sturm's theorem requires use of an ordered field resulting in large polynomial coefficients. Unfortunately, we do not currently know of a computationally reasonable analog of this result which is usable over a finite field. However, some results in this direction are available The communications requirements of the algorithms depend heavily on the underlying implementation of the chosen secure sum algorithm. In some cases, merging the two layers could result in reduced overhead. Our use of the Newton identities greatly decreases communication overhead. This can enable the use of a larger number of "slots" with a consequent reduction in the number of rounds required. The solution of a polynomial can be avoided at some expense by using Sturm's theorem. The development of a result similar to the Sturm's method over a finite field is an enticing possibility.

In [10] Thwe Thwe Ngwe, Su Wai Phy **Digital Envelope System Based on Optimized NTRU (Number Theory Research Unit) and RC6 Algorithm** This work proposes digital envelope system in order to meet the security requirement such as confidentiality. To create digital envelope system, the original message is encrypted by using Rivest Cipher-6(RC6) with the help of secret key. Then, that secret key is encrypted by using the ONTRU (Optimized Number Theory Research Unit) with the help of Receiver's public key. Many research areas proposed digital envelope systems in order to overcome the security

problems. Most of these systems focused on the combination of asymmetric key algorithm and symmetric key algorithm. Digital envelopes usually use public-key cryptography to encrypt the secret key. It effectively provides confidentiality (privacy). In proposed scheme, RC6 symmetric key algorithm and ONTRU (Optimized Number Theory Research Unit) are used. The usage of RC6 symmetric algorithm and optimized NTRU public key algorithm gives the security requirement such as confidentiality. The prime requirements for network and data communication security are privacy, authentication, integrity, maintenance and Non-Repudiation. The RSA algorithm is used for key exchange and authentication . This research developed a digital envelope in java by combining the methodologies of symmetric and asymmetric techniques. As further extension, various files such as image, audio, video files can be added for information security in the hybrid system and new methods can be developed based on the other public key algorithms in order to obtain more efficient system.

3. ANALYSIS

S. NO	TITLE	PAPER DETAILS	METHOD USED	ADVANTAGES	DISADVANTAGES
1.	Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing	Healthcare system by utilizing the flexibility of cloudlet	Number Theory Research Unit	Effectively prevent the remote healthcare big data cloud from attacks.	Lagging in providing data privacy
2.	Privacy-preserving multi-keyword ranked search over encrypted cloud data	Privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE).	Coordinate matching	Introduce low overhead on both computation and communication.	Integrity of the rank order in the search result assuming the cloud server is untrusted.
3.	Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency	developed a secure and privacy-preserving opportunistic computing framework, called SPOC	Attribute-based access control	Develop user-centric privacy access control to minimize the PHI privacy disclosure.	Very low sufficient to support the high-intensive PHI process and transmission framework.

4.	A Privacy Enhanced Search Approach for Cloud-Based Medical Data Sharing	The enhanced access control can ensure the privacy protection of cloud data.	Symmetric encryption algorithms are more efficient than asymmetric algorithms	The medical information from the original table T and construct the plaintext	Large amount of concurrences of medical data sharing and accessing.
5.	Privacy preserving health data processing	Proposed toolset for statistical study of health data uses a combination of secure multi-party computation (SMC) algorithms	A combination of secure multi-party computation	Proposed method can be applied for a large number of statistical computations	No trusted third part human or machine is part of the process.
6.	Cloud-Supported Cyber–Physical Localization Framework for Patients Monitoring	The potential of cloud-supported cyber–physical systems (CCPSs)	Gaussian mixture modeling for localization and is shown to outperform other similar methods	There is a need for new adaptable and scalable techniques for seamless localization in the cloud.	To conduct more Workload measurements to record the resource utilization of CPU, memory, storage, and network bandwidth.
7.	Security Models and Requirements for Healthcare Application Clouds	EHR sharing and integration in healthcare clouds and analyze the arising security and privacy issues	The corresponding EMR with appropriate signature algorithm.	EHR is ability to offer fine-grained authorization and access control.	The number of nodes in the attribute-based hierarchy of a composite EHR is large
8.	Applying Secure Multi-Party Computation to Improve Collaboration in Healthcare	Healthcare organizations are interested in adopting collaborative systems to	The field of data processing in the encrypted domain, i.e. Paillier and RSA. secure multiparty	The Paillier algorithm to prove its homomorphic properties and to demonstrate the benefits of the solution	Not use fully homomorphic algorithms for data encryption.

	Cloud	improve the quality of medical services.	computation (SMC) algorithms are used to ensure patients' privacy.		
9.	Privacy Preserving Data Sharing With Anonymous ID Assignment	This technique is used iteratively to assign these nodes ID numbers ranging from 1 to N	anonymous IDs are examined with respect to trade-offs between communication and computational requirements.	Faith in the current generation of optimizing compilers has been slightly diminished.	Arises in that the nodes do not need to solve the Newton polynomial.
10.	Digital Envelope System Based on Optimized NTRU (Number Theory Research Unit) and RC6 Algorithm	Encrypted by using Rivest Cipher-6(RC6) with the help of secret key. Then, that secret key is encrypted by using the ONTRU (Optimized Number Theory Research Unit) with the help of Receiver's public key.	Cryptographic algorithms are analyzed and optimized to evaluate better performance according to their requirements.	The optimized NTRU, this system also fulfils to get faster execution speed than that of original NTRU	Intended not to take longer execution time when the larger file sizes are used for encryption/decryption process.

4. POSSIBLE SOLUTION

Cloud computing introduces risks to any sensitive data it touches. These risks largely arise from the need to entrust data protection to a third party cloud provider. Different nodes in the environment may be controlled or administered by different untrusted parties, and could be vulnerable to attacks fromother cloud tenants, malicious insiders or external adversaries. When data owners release control of their data to a cloud environment, they require guarantees that their data remains appropriately protected.

As the timed release data is considered to be time sensitive data, it is necessary to introduce an effective scheme, which will not release the data access privilege to intended users until reaching predefined time points. An efficient solution is needed to let data owners manually release the time-sensitive data: The owner uploads the encrypted data under different policies at each releasing time such that the intended users cannot access the data until the corresponding time arrives.

5. CONCLUSION

In this survey we have studied the some of the work can be done by the medical data sharing in cloud in detail, also listed some their advantages and disadvantages The problem of privacy protection and sharing large medical data in cloudlets and the remote cloud is studied. A system which securely shares data between users to the remote cloud in consideration of secure collection of data, as well as low communication cost. It does allow users to transmit data to a cloudlet, which triggers the data sharing problem in the cloudlet. Users' data privacy is also considered. For the purpose of sharing data in the cloudlet, trust model is used. For privacy-preserving data sharing, we use anonymous techniques like generalization and suppression. Collaborative IDS based on cloudlet mesh is developed to protect unauthorized access to cloud data.

REFERENCES

[1] . Min Chen,Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, *Senior Member*, Long Hu "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing," IEEE transactions on cloud computing.

[2] . Ning CaoCong Wang, , Ming Li, Kui Ren, and Wenjing Lou," Privacy-Preserving Multi Keyword Ranked Search over Encrypted Cloud Data", IEEE transactions on parallel and distributed systems, vol. 25, no. 1, january 2014.

[3] . Rongxing Lu ,Xiaodong Lin,and Xuemin (Sherman) Shen, ," SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE transactions on parallel and distributed systems, vol. xx. 2012.

[4] . Lu Liu, Jingchao Sun, Jianqiang Li, Rong Li, Juan Li, Xi Meng, Huifang Li and Jijiang Yang," A Privacy Enhanced Search Approach for Cloud-Based Medical Data Sharing "Research Institute of Information Technology,2015 IEEE International Conference on Smart City/SocialCom/SustainCom together with DataCom 2015 .

[5] . Anders Andersen, Kassaye Yitbarek Yigzaw, Randi Karlsen,"Privacy preserving health data processing" 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom).

[6] . M. shamim hossain, *senior member, ieee,"* cloud-supported cyber–physical localization framework for patients monitoring" ieee systems journal.

[7] . Rui Zhang , and Ling Liu, "Security Models and Requirements for Healthcare Application Clouds" 2010 IEEE 3rd International Conference on Cloud Computing.

[8] . Mbarek Marwan, Ali Kartit and Hassan Ouahmane," Applying Secure Multi-Party Computation to Improve Collaboration in Healthcare Cloud", University Chouaïb Doukkali –El Jadida, Laboratory LTI, ENSAJ.

[9] . Larry a. dunning, *member*, *ieee*, and ray kresman," privacy preserving data sharing with Anonymous id assignment", ieee transactions on information forensics and security, vol. 8, no. 2, february 2013.

[10] . Thwe Thwe Ngwea, Su Wai Phyob ," Digital Envelope System Based on Optimized NTRU (Number Theory Research Unit) and RC6 Algorithm", International Journal of Computer (IJC) ISSN 2307-4523.