International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 26th May 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue= Spl Issue 04

DOI: 10.48047/IJIEMR/V11/SPL ISSUE 04/14

Title **ANALYSIS ON PRIVACY PROTECTION AND INTRUSION IN AVOIDANCE OF MEDICAL DATA SHARING**

Volume 11, SPL ISSUE 04, Pages: 128-132

Paper Authors
A.V Chandra Sekhar Reddy, M.Venkata Sai, I.Sai Gopinath, Dr.K.Parish Venkata Kumar

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ANALYSIS ON PRIVACY PROTECTION AND INTRUSION IN AVOIDANCE OF MEDICAL DATA SHARING

[1]**A.V Chandra Sekhar Reddy**, Pursuing III MCA, Department of Computer Applications, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India, 198w1f0005@vrsec.ac.in
[2]**M.Venkata Sai**, Pursuing III MCA, Department of Computer Applications, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India, 198w1f0040@vrsec.ac.in
[3]**I.Sai Gopinath** , Pursuing III MCA, Department of Computer Applications, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India, 198w1f0020@vrsec.ac.in
[4]**Dr.K.Parish Venkata Kumar**, Assistant Professor, Department of Computer Applications, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India, kpvk@vrsiddhartha.ac.in

ABSTRACT:

In order to maintain a healthy lifestyle in today's society, improved modern health care services are needed. Medical data monitoring is becoming increasingly important as the world's population ages and the prevalence of chronic diseases rises. Modern technology is assisting in every step of the process of providing sophisticated healthcare services. Specialized doctors are usually hard to come by and may be located far away from the patient in need of their services. Health care can't be provided in rural areas without the help of technology. Patients are frequently unable to get to the doctor's office because of their critical health issues. However, technology is coming to the rescue in a big manner in these situations. Using the latest technology, remote health care can be provided with the same level of quality as services provided by a local doctor. This technology's fundamental premise is to collect health data with the greatest precision feasible and to share it with clinicians who are not physically present. It is possible for wearable devices to collect the most accurate biological data and then transmit it to the cloud, where it may be accessed by doctors who are not physically there. The exchange of medical information, on the other hand, is a vital and problematic issue because medical information is comprised of the patient's important and highly personal data. Medical ethics, on the other hand, dictates that doctors must obtain the express permission of patients before sharing any information about their health with anybody else. In the cloud, such data would only be exchanged between authenticated users. Data collection, storage, and exchange form the bulk of the chain of processing. In this study, a cloudlet-based medical data sharing system is proposed. Three major issues with medical data exchange are discussed in this research. To begin, a cloudlet-based method for sharing medical data is offered. Number Theory Research Unit (NTRU) strategy used during data collection to encrypt user's physiological data gathered by wearable devices and subsequently transferred to adjacent cloudlet is the NTRU method. Second, a novel trust model is presented to help users find trustworthy cloudlet partners.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

1. INTRODUCTION

Patients and masters can both benefit from this relational linkage of medical data, but the delicate information could be leaked or stolen, posing a privacy and security risk if it is not adequately protected. Multi-watchword encryption in distributed computing (MRSE) was developed by Cao et al. to provide cloud clients with a multi-catchphrase approach [1]. To get an accurate estimate, we must take into account the fact that this methodology can be utilised to find out where individuals are most interested. To ensure and complete specific sorts of healthcare information in remote places, cloud-based health data collection (PHDA) was employed (WBANs). Convenient healthcare frameworks are reviewed in terms of security and privacy concerns, including the protection of healthcare data combination and the protection of personal data. This adaptable security solution for distributed computing-based applications ensures data privacy, data reliability, and fine-grained access control. The cloud-aided health mind structure delivers a precise composition analysis of privacy confirmation.

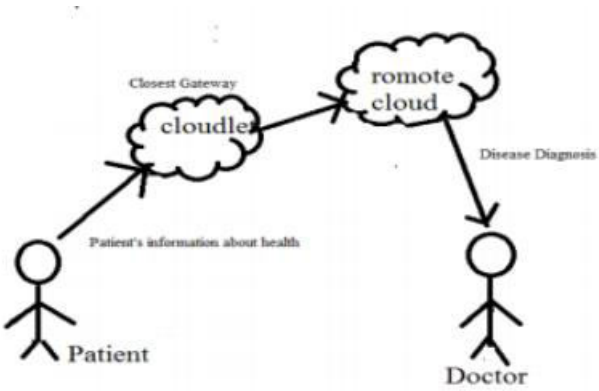

Fig 1: Encrypted data through cloudlet sent to doctor

Figure 1 shows how a patient's health data is transmitted to a nearby doctor via wearable devices, big data, distributed computing, etc., and a patient-professional relationship can be built as illustrated. No matter how careful you are, someone could still get their hands on important information, which could put your network at risk. Using distributed computing approaches, mists that connect cloudlets and protected mists may store a large amount of data. It's the ambush protection that's causing the real problem here. This research presents a cloudlet-based health mind system to address the aforementioned issue (reference K. Hung).

Figure 1 shows the three stages of privacy insurance.

Wearable gadgets transfer health data to nearby cloudlets in the primary part of the experiment. Transmitting sensitive medical information should be extremely safe. In the third stage, all of the cloudlet's data is sent to the safe cloud, where it is sorted and compared for security.

2. LITERATURE REVIEW

Using the flexibility of cloudlets, the author of paper [1] built a new healthcare organisation. The cloudlet's components include privacy protection, data sharing, and interference detection. First and foremost, use the NTRU (Number Theory Research Unit) technique to encode client data gathered by wearable devices as soon as possible. These data will be sent from one cloudlet to another in a time-sensitive manner. You should also display an additional confidence model to help clients select trustworthy partners with whom to exchange stored data in the cloudlet. As with any other form of trust demonstration, this encourages patients to open up to one another about their illnesses. It's also a good idea to divide the customer's medical information into three separate regions and ensure that it is adequately protected. A new beneficial intrusion ID system (IDS) method based on cloudlet work can reasonably protect the distant healthcare giant data cloud from attacks, keeping in mind the ultimate goal of protecting the healthcare structure from destructive strikes.

As if by magic, this work [2] depicts and illuminates the testing issue of privacy saving multi-catchphrase positioned search across encrypted cloud data (MRSE). They devised a strategy for securing cloud data in a way that ensured the highest level of privacy. Accordingly, they select "encourage organising" as a multi-watchword semantics, which is to say, a closeness fraction of "encourage organising, i.e., an acceptable number." Quantitative analysis of this equivalency is performed using a technique known as "interior thing likeness." To begin, present a main idea for the MRSE based on a secure internal thing estimation, and then provide two fundamentally enhanced MRSE plans to meet separate rigorous privacy requirements in two different threat scenarios. Surveying privacy and profitability assurances of suggested ideas are examined in depth.

This study [3] describes the SPOC architecture for m-Healthcare emergency as a spearheading processing platform that is both secure and private. To complete the registration of genuine individual health data (PHI) with minimal private disclosure, SPOC can be applied to innovatively acquire propelled cell resources such as calculating power and essentiality. As a result, SPOC provides the medical customer with the ability to choose who can share in the cunning processing of his enormous PHI and who can't, ensuring that the privacy of PHI is protected in mHealthcare emergency situations, as well as giving the medical customer control over who can share in the cunning processing of his enormous PHI and who can't. The SPOC paradigm can financially provide a customer-driven privacy control in a mHealth emergency, as illustrated by independent security considerations. This document [4] begins by outlining the issue's aim and providing a brief principle. The current state of EMR apportionment is examined at this point. Thereafter, new information is supplied that has a significant impact on the healthcare process. Medical data collection, medical data analysis, and the use of medical data for exact recognisable proof and desire are all part of the health identification. This is followed by a discussion of distributed computing because of its potential to provide flexible and cost-effective transportation of healthcare administrations.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3. PROPOSED SYSTEM

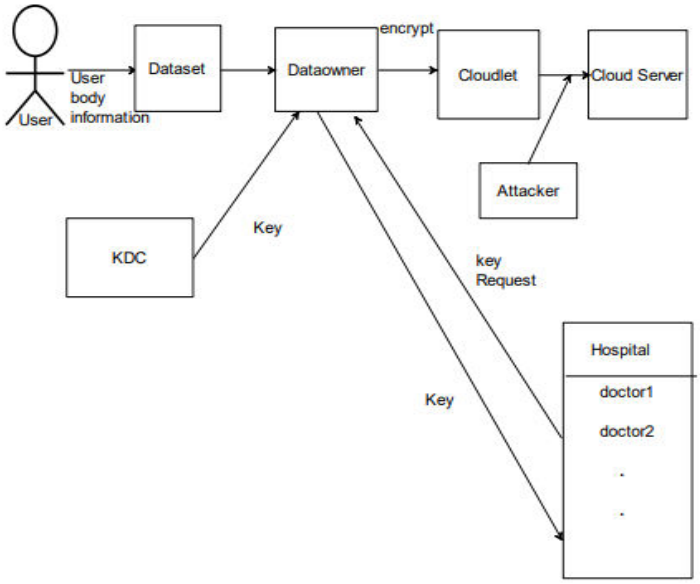

Fig: Block diagram

3.1 DESCRIPTION

The dataset is populated with the user's body data. An input dataset for a cloudlet-based system that secures data exchange. The cloudlet takes a dataset, encrypts it using the NTRU method, and stores it in the cloud. The Key Distribution Center (KDC) is used to minimise the danger of key exchange. In this case, the data owner and the authorised user were given the same key. While sharing, the cloudlet system stores the encrypted data provided by the data owner and uses a collaborative intrusion detection system mechanism to prevent any attacks. The user's encrypted data is stored on the cloud server, which can be accessed by an authenticated doctor in order to decode the data.

3.2 ADVANTAGES

- NTRU will protect all of the data that wearable devices send to the cloudlet.
- Patients can connect with others who have the same health issue and get answers to their questions. The trust model specifies whether or not data exchange can take place, and hence provides security for users.
- Encryption and classification are used to protect patient health records.

CONCLUSION

Proposed a safe data sharing system based on cloudlets. Data is transmitted in an encrypted form using this technology. Cooperative intrusion detection system (IDS) used by cloudlet to thwart an attack The new technology is safer and more reliable. Time and memory are also saved.

REFERENCES

1. J. Li, J.-J. Yang, Y. Zhao, and B. Liu, “A top-down approach for approximate Data anonymisation,” Enterprise

Information Systems, vol. 7, no. 3, pp. 272–302, 2013.

2. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222- 233, 2014.

3. 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.

4. 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.

5. Y. Wu, M. Su, W. Zheng, K. Hwang, and A. Y. Zomaya, "Associative big data sharing in community clouds: The meepo approach," IEEE Cloud Computing, vol. 2, no. 6, pp. 64–73, 2015.

6. K. A. Khan, Q. Wang, C. Luo, X. Wang, and C. Grecos, "Comparative Study of internet cloud and cloudlet over wireless mesh networks for realtime Applications," in SPIE Photonics Europe. International Society for Optics and Photonics, 2014, pp. 91 390K.

7. Rajendran, P. K., Muthukumar, B., &Nagarajan, G. "Hybrid Intrusion Detection System for Private Cloud": A Systematic Approach. Procedia Computer Science, 48,pp.325–329, (2015).

8. Raj Scholar, A. P., & Rani Assistant professor, S. M. "Behaviour Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems:A Review. International Journal of Computer Applications.

9.Dr. K. Parish Venkata Kumar, N. Raghavendra Sai, S. Sai Kumar, V. V. N. V. Phani Kumar & M. Jogendra Kumar "Concept Summarization of Uncertain Categorical Data Streams Based on Cluster Ensemble Approach"

[10] N. Srinivasarao, B. Lakshmi, N. Raghavendra Sai, K. Parish Venkata Kumar and K. Gurnadha Gupta, "A Spatiotemporal-Based Intrusion Detection Model," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, 2022, pp. 856-864, doi: 10.1109/ICEARS53579.2022.9752392.

[11] B. Lakshmi, S. S. Kumar, N. R. Sai, K. P. V. Kumar and G. S. C. Kumar, "WLAN Intrusion Detection System Based on SVM," *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 2022, pp. 1213-1219, doi: 10.1109/ICSCDS53736.2022.9760896.