**A NOVEL BASED PRIVACY PROTECTION AND INTRUSION AVOIDANCE FOR CLOUDLET-BASED MEDICAL DATA SHARING**

\*Dr. C. Premila Rosy1,

Head & Assistant Professor,

PG & Dept., of CS,

Idhaya College for Women,

Kumbakonam,

Tamil Nadu, India

Mrs. R. Priyangagandhi2,

II – M.Sc., (CS),

Idhaya College for Women,

Kumbakonam,

Tamil Nadu, India.

Ms. T. Kaviyarasi3,

II – M.Sc., (CS),

Idhaya College for Women,

Kumbakonam,

Tamil Nadu, India.

Ms. M. Asha4,

II – M.Sc., (CS),

Idhaya College for Women,

Kumbakonam,

Tamil Nadu, India.

Ms. T. Nivetha5,

II – M.Sc., (CS),

Idhaya College for Women,

Kumbakonam,

Tamil Nadu, India.

Corresponding Author \*Dr. C. Premila Rosy – [premilarosy78@gmail.com](mailto:premilarosy78@gmail.com)

**ABSTRACT**

Now a day’s cloud has become one of the fascinating domains in order to store and retrieve all the data from the remote machines rather from the local machines. With the popularity of wearable devices, along with the development of clouds and cloud hand held technology, there is a tremendous increase for the medical care in order to store and access the information remotely. The data collected from patient through wearable devices (like heartbeat, blood pressure etc.) has to be passed to application running in cloud to implement various services like expert advice, emergency assistance etc. Then build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, first utilize Number Theory Research Unit (NTRU) method to encrypt user’s body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, 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 similar 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, then develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. The cloudlet act as a cache for cloud and it provide privacy for the data by encryption using AES algorithm and avoid the intrusion by using the Collaborative IDS. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. The experiments demonstrate the effectiveness of the proposed scheme.

**Keywords :** Healthcare System, Medical Data Store, Collaborative Intrusion Detection System (IDS).

**I. INTRODUCTION**

The medical data on the social network is beneficial to both patients and doctors. With the development of healthcare big data and wearable technology, as well as cloud computing and communication technologies, cloud-assisted healthcare big data computing becomes critical to meet users’ ever growing demands on health consultation. Healthcare social platform, such as Patients-Like Me, can obtain information from other similar patients through data sharing in terms of user’s own findings. Though sharing medical data on the social network 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. This paper proposes a cloudlet based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Those data are further delivered to the remote cloud where doctors can access for disease diagnosis. According to data delivery chain, separate the privacy protection into three stages. In the first stage, user’s vital signs collected by wearable devices are delivered to a closet gateway of cloudlet. During this stage, data privacy is the main concern. In the second stage, user’s data will be further delivered toward remote cloud through cloudlets. A cloudlet is formed by a certain number of mobile devices whose owners may require and/or share some specific data contents. Thus, both privacy protection and data sharing are considered in this stage. Especially, the user trust model to evaluate trust level between users to determine sharing data or not. Considering the users’ medical data are stored in remote cloud, here classify these medical data into different kinds and take the corresponding security policy. In addition to above three stages based data privacy protection, and also consider collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

**A. Collaborative IDS based on cloudlet mesh**

A number of prior works have studied different intrusion detection systems with quite some advances. For example, [4] proposed a behavior-rule specification-based technique for intrusion detection. The main contribution is the performance outperforms other methods of anomaly-based techniques. [5] Proposed a collaborative model for the cloud environment based on distributed IDS and IPS (intrusion prevention system). This model makes use of a hybrid detection technique to detect and take corresponding measures for any types of intrusion which harm the system, especially distributed intrusion. However, collaborative IDS based on the cloudlet mesh structure is a new kind of intrusion detection technique, which was first proposed in Shi et al. [6]. The authors demonstrated that the detection rate of the intrusion detection system established on the basis of a cloudlet mesh is relatively high. [7]Describes design space, attacks that evade CIDSs and attacks on the availability of the CIDSs, and introduces comparison of specific CIDS approaches. [5] Describes the IDS for privacy cloud. The authors give an overview of intrusion detection of cloud computing and provide a new idea for privacy cloud protection.

**II. RELATED WORK**

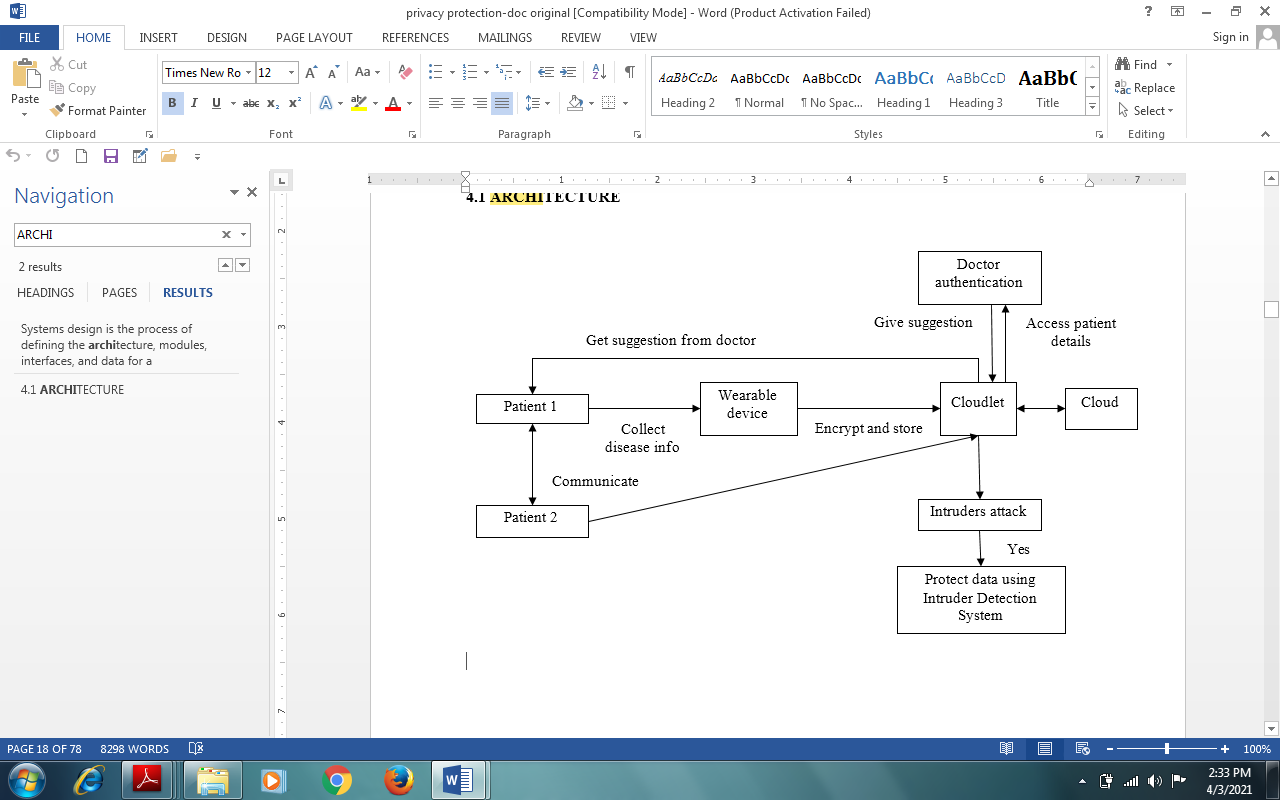
This section presents the prior work of the medical data sharing models. The author in [1] has demonstrated that authentication scheme may suffer from different attacks and may fail to provide several security characteristics. Later, proposed an authenticated key agreement scheme by applying “chaotic map-based cryptography” to solve these problems. This scheme realizes the protection of hospital data transmitted in the open channel and provides confidential protection during the remote diagnosing process, allowing the patient to enjoy the secure and convenient healthcare through the TMIS. Security analysis & performance analysis has been proved for various attacks and better performance and thus it’s more suitable for practical applications in TMIS environments.

In [2], considering the sensitive healthcare information in cloud environments, and proposed in a special data scrambling method for healthcare application, where a tiny part of data is used to scramble the remaining data for the purpose of encryption. This method improves in terms of security performance and practicability. ECG signals from both “MIT-BIH arrhythmia” database and “elf-collected” database are used. Conversion into decimal format is based on a quantization resolution of eight bits.

In [3], introduced a novel system for healthcare professionals to enhance their compliance with best practice and regulations using, Microsoft Kinect sensor‟ and smart devices’ while protecting patient privacy. A contribution for this study will be registration mechanism for a healthcare professional to explicitly give their system the permission to monitor his/her activities. Multiple Kinect sensors are used for improved tracking accuracy and better coverage for bigger workplaces.

**III. CLOUD BASED PRIVACY PRESERVATION**

In a cloudlet based healthcare system, initially, the patient’s data was collected through wearable devices and further transmitted the nearest cloudlet. Now from this cloudlet the data is sent to the remote cloud where the doctors will have the authenticity to access the patient’s information and give suggestions to them. Here in the data delivery chain, the privacy is provided to the whole process where protection is classified into three phases. In the initial phase, the patient’s information gathered through wearable devices are transferred to the nearest gateway of cloudlet. In this stage, the main concern is on data privacy. In the second phase, the patient’s information from cloudlets are further transferred to the remote cloud. Here, cloudlet is formed with only a few mobile devices and the owners have authority either to share particular data contents with other people. So, in this stage, both data sharing and securing privacy are considered as the main task. A trust model is being used in this phase in order to compute the trust level among the different patients either to share the information with them or not. Now, in the third phase, the medical information stored in the cloud is categorized into different kinds and accordingly security policies are applied. Apart from all these three phases security, further this study used collaborative IDS (Iintrusion Detection System) based on cloudlet mesh in order to secure the cloud ecosystem. Until now the secured process is carried out between the wearable device and doctor in a secured manner. So, this research further proposed a hybrid cryptographic scheme where it merges both NTRU (Number Theory Research Unit) and AES(Advanced Encryption Standard).



**Figure 1 : Architecture**

**IV. EVALUATION OF RESULT**

User’s data can be made secure in the cloud using AES encryption.

• A user decides to use cloud services and transfer his data to the cloud.

•User then submits his service requirements to the Cloud Service Provider (CSP). She/he chooses the provider offering best services.

• When migration of data to the chosen CSP takes place and whenever an application uploads any data to the cloud, the data is encrypted and then sent. This encryption is done using AES algorithm.

• Any requests to read the data will happen after it is decrypted on the users end. Therefore plain text data can then be read by the requesting application.

The plain text data is never written anywhere on cloud. The key is never stored next to the encrypted data since it may compromise the key. To store the keys, a physical key management server is installed in the user’s location. This encryption method protects the data and the encryption keys and guarantees that they remain under users control and are never exposed in storage or in transit.

**V. CONCLUSION**

This project investigated the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud. Here developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost. However, it does allow users to send data to a cloudlet, which triggers the data sharing problem in the cloudlet. Firstly, utilize wearable devices to collect users’ data, and in order to protect user’s privacy, here use cloudlet mechanism to make sure the transmission of users’ data to cloudlet in security. Secondly, for the purpose of sharing data in the cloudlet, here use trust model to measure users’ trust level to judge whether to share data or not. Thirdly, for privacy preserving of remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission. Finally, we propose collaborative IDS based on cloudlet mesh to protect the whole system. User asks the question to the doctor online and doctor give the answer to user. In future use the concept of Elliptic Curve Digital Signature Algorithm ECDSA in specific for achieving non-repudiation in the healthcare cloud systems

**REFERENCES**

[1]. M. Quwaider and Y. Jararweh, “Cloudlet-basedefficient data collection in wireless body areanetworks,” Simulation Modelling Practice andTheory, vol. 50, pp. 57–71, 2015.

[2]. J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R.Ranjan, J. Kołodziej, A. Streit, and D.Georgakopoulos, Journal of Computer and SystemSciences, vol. 80, no. 5, pp. 994–1007, 2014.

[3]. Tadapaneni, N. R. (2018). Cloud Computing:Opportunities and Challenges. International Journalof Technical Research and Applications.

[4] M. Abousharkh and H. Mouftah, “Service oriented architecture-based framework for WBAN-enabled patient monitoring system,” in Proceedings of the Second Kuwait Conference on e-Services and eSystems, New York, NY, USA, 2011, pp. 18:1–18:4.

[5] T. Soyata, R. Muraleedharan, C. Funai, M. Kwon, and W. Heinzelman, “Cloud-Vision: Real-time face recognition using a mobile-cloudlet-cloud acceleration architecture”

[6] D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia. Commun. Tech. Comm. MMTC E-Lett., vol. 6, no. 10, pp. 27–31, 2011.

[7] D. Fesehaye, Y. Gao, K. Nahrstedt, and G. Wang, “Impact of Cloudlets on Interactive Mobile Cloud Applications,” in Enterprise Distributed Object Computing Conference (EDOC), 2012 IEEE 16th International, 2012, pp. 123–132.

[8]. R. Zhang and L. Liu, “Security models andrequirements for healthcare application clouds,” in Cloud Computing (CLOUD), 2010 IEEE.

[9]. K. Hung, Y. Zhang, and B. Tai, “Wearable medical devices for tele-home healthcare,” in Engineering in Medicine and Biology Society, 2004. IEMBS’04.26th Annual International Conference of theIEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[10]. Guiwu, W. Y. (2018, June). Research on Genetic Algorithm for Resource Scheduling in Cloud Computing Based on User Satisfaction. In 5th International Conference on Electrical & Electronics Engineering and Computer Science (ICEEECS 2018) (Vol. 5).

[11]. Patel, A., & Tiwari, P. (2018). Cloud Computing Security, Privacy Improvements Using Virtualized High Trust Zone. International Journal of Modern Trends in Engineering and Science, 3(12).