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

\*Dr. C. Premila Rosy1,

Head & Assistant Professor,

 PG & Research 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

**ABSTRACT**

Currently, cloud is one of the interesting domains to store and retrieve information from the remote machine compared to the local machines. As the development of cloud technology, storing and accessing information is quite easy, especially in the medical field. With the help of apparel devices, data has been collected from the patients and send to the application which is running in the cloud to provide services like expert advice, emergency assistance etc. A novel healthcare system is then built up by using the adjustability of cloudlet. The cloudlet consists of privacy protection, data sharing and intrusion detection functionalities. In the data collection phase, mainly use the method of Number Theory Research Unit (NTRU) to encrypt user’s body data collected by apparel devices. This information will be transmitted to the neighbor cloudlet in an energy efficient fashion. Then, to help users by introduce a new trust model for selecting a trustable partners who need to share the data already stored in the cloudlet. Also that model helps the patients who are alike, to make a communication with each other. Next, users’ medical data stored in remote cloud is stored into three parts, and give them proper conservation. At last, to protect the health care system from the threats, develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, to prevent the remote healthcare big data cloud from attacks effectively. The cloudlet behave as a temporary memory and offers privacy for encrypted data using AES algorithm and the intrusion is avoided with the help of Collaborative IDS. The processing chain is primarily consists of data collection, data storage and data sharing, etc. The experiments reveal the success of the submitted scheme.

 **Keywords :** Cloudlet, Data Share, Intrusion System.

**I. INTRODUCTION**

The medical information on social platform is useful to both doctors and patients. Evolution of healthcare big data and wearable, also cloud computing and communication technologies, big data becomes judgmental to reach user’s increasing request on medical checkup. Healthcare social media, especially Patients-Like Me, can get data from patients are alike via information sharing in respect of user them. As the advantage mentioned above, confidential information might be exude, which leads to security threats with any protection. Thus privacy of medical information sharing becomes a burden. This paper explores a cloudlet installed healthcare system. The gathered data by wearable devices are sending to the close by cloudlet. Those information further submitted to the distant cloud to diagnosis the disease by the doctors. In proposition to data delivery chain, divide the privacy protection into three phases. At first, wearable devices collects the user’s key signs are conveyed to the closet entrance of cloudlet. In this phase, data privacy is the primary cover. In the second phase, user’s information will be again conveyed to the remote cloud via cloudlets. A cloudlet is built by a definite number of mobile phones and its owners may need some particular contents. Therefore, both privacy policy and information sharing are examined in this phase. Particularly, the user trust model to assess the trust level between end users to decide sharing information or not. In the view of user’s medical information, now segregate this information into various kinds and setup the respective security policy. Along with the above three phases based data privacy policy and also consider collaborative IDS based cloudlet mesh to secure the cloud ecosystem.

**A. Collaborative IS based on cloudlet**

Earlier works have studied various intrusion detection with some improvements. The primary endowment is the act beats other methods of anomaly-based techniques. Presented a co-operative model for cloud environment with the help of distributed IDS and IPS (Intrusion Prevented System). This models uses the hybrid detection technique to determine and grab the corresponding measures for different types of intrusion which distress the system, mainly distributed intrusion. Although, cloudlet mesh structure based collaborative IDS is a updated intrusion detection technique, which was first proposed in Shi et al. [6]. The authors illustrated that the detection rate of the intrusion detection system initiated because of the cloudlet mesh is moderately high. [7] Reports design space, attacks that elude CIDSs and attacks on the accessibility of the CIDSs, and initiates differentiation of parricular CIDS approaches. [5] Reports the IDS for privacy cloud. The authors provide an outline of intrusion detection of cloud computing and fresh idea for privacy cloud security.

**II. RELATED WORK**

This part hand over the previous work of the medical data sharing models. The author [1] has proved that authentication scheme may failed to provide several security characteristics because of different attacks. To solve this kind of problem the author put forward an authenticated key agreement scheme by applying “chaotic map-based cryptography “.This scheme concluded that the patient enjoying the secure and convenient health care by the protection of hospital data transmitted in the open channel and provide confidential protection during the remote diagnosing process through the TMIS. Security analysis and performance analysis suggested by the author to protect the medical data from various attacks and provide better performance and thus it’s more suitable for practical applications in TMIS environments.

In [2], taking to consideration the sensitive health care information in cloud environments, and proposed in a special data scrambling method for health care application, where the small part of data is used to scramble and the remaining data for the purpose of encryption. This method develops the security performance and practicability. Both elf-collected database and MIT-BIH arrhythmia database are used in ECG signal. A quantization resolution of eight bits is the basis to convert the decimal format.

In [3], for protecting patient privacy the author introduced a novel system for health care professionals to intensity their compliance with infect sensor and smart devices. A contribution for this study will be registration mechanism for a health care professional to explicitly give their system the permission to monitor his/ her activities. For improved taking accuracy and better coverage for bigger workplaces uses multiple kinect sensors.

**III. CLOUD BASED PRIVACY PRESERVATION**

Now from this cloudlet the data is dispatched to the remote cloud where the medical doctors will have the authenticity to get right of entry to the patients data and give suggestions to them. Here in the data deliver chain, and private is supplied to the whole process where protection is categorized into three phases. In the preliminary phase, the patients information gathered via wearable devices are transferred to the nearest gateway of cloudlet. In this stage, the important issue is on data privacy. In the second phase, the patient’s statistics from cloudlets are similarly transferred to the remote cloud. In the second phase, cloudlet is formed with only a few mobile devices were decided by the owner. So, in this stage, both data sharing and security privacy are regarded as the essential mission. To calculate the trust level among the several patients either to allocate the information with them or not is used by the trust model in this phase. Now, in the third phase, the clinical records are saved in the cloud is labeled into distinctive sorts and hence security policies are applied. In order to secure the cloudlet ecosystem it uses collaborative IDS (Intrusion Detection System) based on cloudlet mesh instead of using these three phases security. Until now the secured technique is carried out between the wearable system 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**

By using the AES encryption, user’s data can be protected in the cloud. A user chooses to send his data to the cloud by using cloud services. In the Cloud Service Provider (CSP), the user submits all his service needs. She / He select the provider which gives the finest services. The data then sent in the encrypted form when the transfer of data occurs in the chosen CSP and also an application uploads any data to the cloud. That encryption can be achieved by using AES algorithm. Once after the data is decrypted on the user’s end, all of any requests are allowed to read the data. So, the requesting application then allowed to read the plain text data. Those plain text data can never find anywhere in the cloud. Because the plain text nowhere written in the cloud. Similarly, the key never stored next to the encrypted data. A physical key management server is installed to store the key in the user’s location. The data can be protected by the encryption method and make sure that they remain under user’s control by not revel in storage as well as in transit.

**V. CONCLUSION**

This paper explored the privacy protection problem and also sharing enormous medical data in cloudlets as well as in remote cloud. Here, the system is generated for secure the collected data by not allowing the users to transmits data to the remote cloud and also ensuring low communication cost. Yet it provoke the data sharing problem in the cloudlet for does not allow the users to send the data to a cloudlet. Primarily, exploit wearable devices to collect user’s data and to safe the user’s privacy. In order to secure the transmission of user’s data to cloudlet, the cloudlet mechanism is used. Next trust model is used to measure the user’s trust level to make sure that the data should share or not for the function of sharing data in cloudlet. Further, we divide the data stored in the remote cloud and encrypt the data in various ways privacy secure of remote cloud data. So that it made sure the data is protected and also it stepped up the transmission efficacy. Finally, to protect the entire system, we recommend collaborative IDS based on cloudlet mesh. The doctor provides the answer for the user’s queries through online. Use the Elliptic Curve Digital Signature Algorithm (ECDSA) concept in future for accomplishing non-repudiation in the health care 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).