Medical data Collection and Sharing in a Privacy and Secure way by using Cloudlet

[1]R.Sateesh, [2]K.Lavanya, [3]B.Harshitha, [4]G.GangaRajulu, [5]M.Bhavya.

[1]Assistant Professor, [2,3,4,5]B.Tech Final Year Students
Computer Science & engineering,
MTIET, Palamaner, India

***Abstract*— Now a day's sharing of medical data is a challenging issue, so people utilize cloud to store the data remotely. That data will retrieve easily anywhere at any cost of time. While storing into the cloud there is a communication energy consumption problem and cloud act as a third party so there is no privacy protection and there is no any IDS to avoid the intrusion. At that time the concept of cloudlet came into existence to overcome the drawbacks of direct storage of cloud. It will reduce the communication energy consumption. The data will be collected by using wearable device and stored to cloudlet and perform some operations and stored to cloud. 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. Cloudlet will provide one trust model to find similar patient to share disease information and communicate with each other.**

***Index Terms*— Cloudlet, Cloud, Collaborative IDS, Intrusion, Wearable device, Doctor, Patient.**

I. INTRODUCTION

Now a days people are busy with their jobs and daily activities, so they do not find enough time to go to hospitals and consult the doctors. With this point of concern this concept came into exist. By using this communication energy consumption will be reduced. The process of medical data includes the data collection which will be collected by wearable devices, data storage which uses the cloudlet and finally stored into the cloud. Finally, data sharing which will shared between the doctor and cloudlet, doctor and patient and among the similar disease patients with in the cloudlet, for this one trust model will develop by using similar disease based.

For the privacy protection of medical data which is a patient sensitive and disease information we utilize a algorithm called AES to encrypt the medical data and the doctor and patients will register first into cloudlet, so only authorized people can access the data by login into cloudlet. Then finally entire data will stores into the cloud server. The intrusion is the major problem now a day, to avoid those problems we utilize one intrusion detection system namely collaborative Intrusion Detection System, which will give one warning when intruder inject some data into cloudlet.

For the data sharing between cloudlet and doctor, doctor and patient, among the similar disease patients also, to discuss each other one trust model will be developed. Doctor see that data and will give some prescription also. Patients also will see the cloudlet data by getting doctor permission. Cloudlet is a collection of mobile devices, the data is store and share specifically.

II. EXISTING SYSTEM:

Existing system uses the cloud to store the data. But clouds have not been used widely due to some privacy and intrusion problems. This system utilizes the DES to encrypt the data, which uses keys size is very less so less privacy in this system. On the privacy protection of healthcare data, there exist some works like SPOC [Secure and Privacy Preserving Opportunistic computing framework] which is used to solve the storage problems of healthcare data and also used to address the privacy protection and security problems. Another system MRSE [Multi Keyword Ranked Search over Encrypted data in cloud computing] it provide rank for result encrypted data based on people interest. Finally PHDA [Priority based Health Data Aggregation] which is used to protect and aggregate the different types of health care data.

III. DRAWBACKS OF EXISTING SYSTEM:

There are some drawbacks are present in cloud based medical data storage and sharing. They are,

1. There is no trust in cloud based data storage and sharing.
2. Causes communication energy consumption in cloud data sharing.
3. There is no privacy protection in this system.
4. There is no any collaborative Intrusion Detection System to avoid intrusion.
5. Takes lot of time to store and retrieve the data from cloud.

IV. PROPOSED SYSTEM:

In the proposed system cloudlet is used as cache to store the data, it overcomes the draw backs of existing system. This novel healthcare system uses AES algorithm to encrypt the data which utilizes the keys in large size. Firstly the patient disease details will collect by wearable devices and stored to nearby cloudlet which will form by some mobile devices whose owners may store

or share the specific data. Then this data will be stores into remote cloud. In cloudlet privacy protection and intrusion avoidance are the main concerns, and we build a trust model to share the data among the patients who are alike.

V. ADVANTAGES OF PROPOSED DATA:

The following are the advantages of proposed system by overcoming the drawbacks of existing system. These are as follows,

1. Proposed system uses the AES algorithm with large size of keys to encrypt the data which provide more privacy protection.
2. There is no communication energy consumption due to the cloudlet.
3. This system uses collaborative IDS to avoid intrusion.
4. In this we build one trust model to find trustable partner to share the disease data.

VI. SYSTEM ARCHITECTURE:

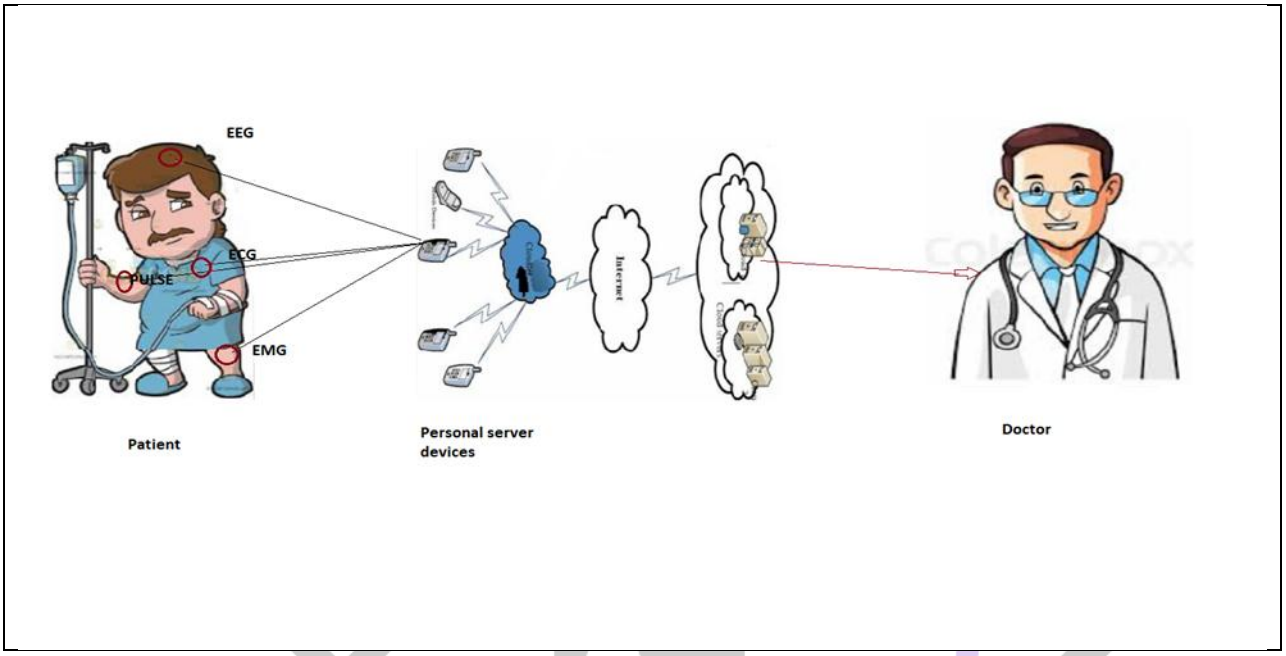


Fig: Medical data collection ,Storage and Sharing using Cloudlet

VII. MODULES:

The main modules present in this paper are as follows, these plays major roles in this system.

1. Wearable device
2. Cloudlet
3. Cloud server
4. Doctor
5. Patient
6. Intruder

1. Wearable Device:

With the development of clouds and cloudlet technology the popularity of wearable devices also increasing. The processing chain of medical health data mainly includes the data collection, data storage and data sharing. For the collection of disease data from patient's wearable devices plays a major role. Those data will stores into the nearby cloudlets for remote accessing. These data will access by doctors for further diagnosis and also accessed by patients with the permission of doctors. At the time of data collection itself we utilize the AES algorithm to encrypt the data for privacy preservation. These data will further stored into cloud server. Some of the wearable devices used in hospitals are ECG, EEG and EMG etc.

- Collect patient data and upload to cloudlet.
- View all patients collected data.

2. Cloudlet:

A cloudlet is formed by a certain number of mobile devices which will act as a cache for cloud server. Whose owners may store and or share the some specific data. In cloudlet privacy protection and data sharing are the main functionalities. To overcome the drawbacks of cloud as communication consumption the cloudlet introduced. The cloudlet uses a trust model to calculate the trust levels between users to find whether share data or not. We also consider collaborative IDS based on cloudlet to protect the cloud system.

- View all patients and authorize.
- View all doctors and authorize.

- View all patients' cloudlet data.
- View patient data access request and authorize.
- View all cloudlet intruder details.
- View no. of same symptoms in chart.
- View no. of patients referred same doctors in chart.

3. Cloud Server:

The Cloud server is a third party which is used to store and retrieve the large amount of data remotely. The cloud provide three types of services they are,

1. Platform as a service
2. Software as a service
3. Infrastructure as a service.

By using cloud we access the data and also store the large amount of data. The cloud has less privacy protection because it acts as third party to users.

4. Doctor:

In the processing chain of patients health care data doctor play the major role. The entire users sensitive data will be under the reference of doctor only. The doctor will access the data from the cloudlet and view the patient details and also give some prescription and suggestions to patients. For the authentication the doctor will register into the cloud let with that username and password only again he/she will login into the cloudlet.

5. Patient:

The entire conversation in this paper is related to the patient disease details only. So, the patient is the main module in this system. The patient disease information will collect by wearable device and stored to cloudlet. The patient first register into cloudlet and login into the cloudlet with doctor permission to view data, get suggestions and prescriptions. Patients will communicate with in the cloudlet to share views with similar disease patients. For this they utilize the trust model to find trust level of patients.

6. Intruder:

Intruder will act as hacker who wants to steal the health care data for some reasons. The intruder login into the cloudlet with patient's username. The intruder has rights to view only, if he/she inject any information into the cloudlet then the cloudlet will display one warning message. Intruder hack the information to spoil the image of certain hospital and also to modify the patient details etc.

VII. AES ALGORITHM :

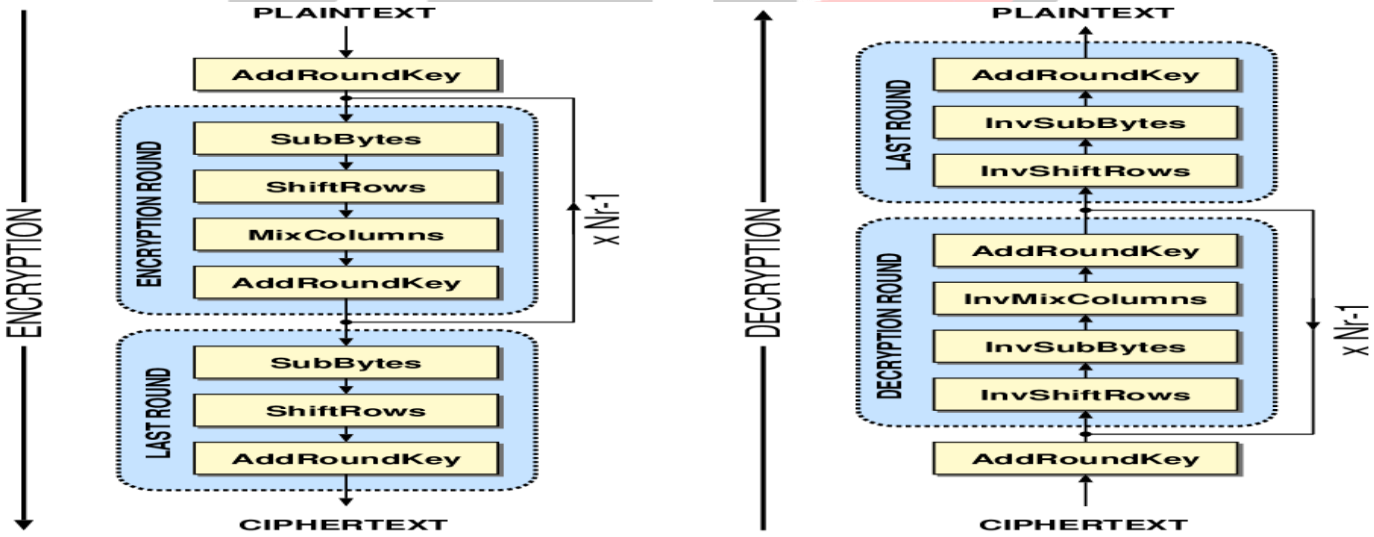
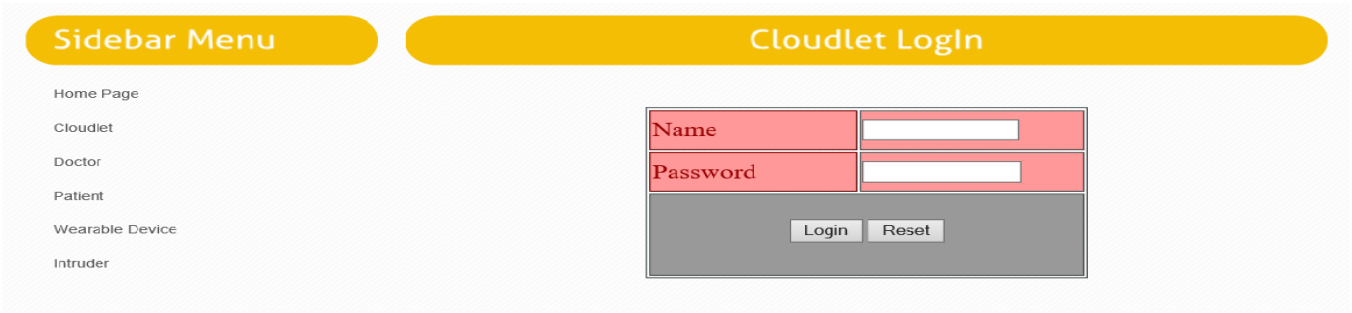


Fig: AES algorithm for Encryption and Decryption

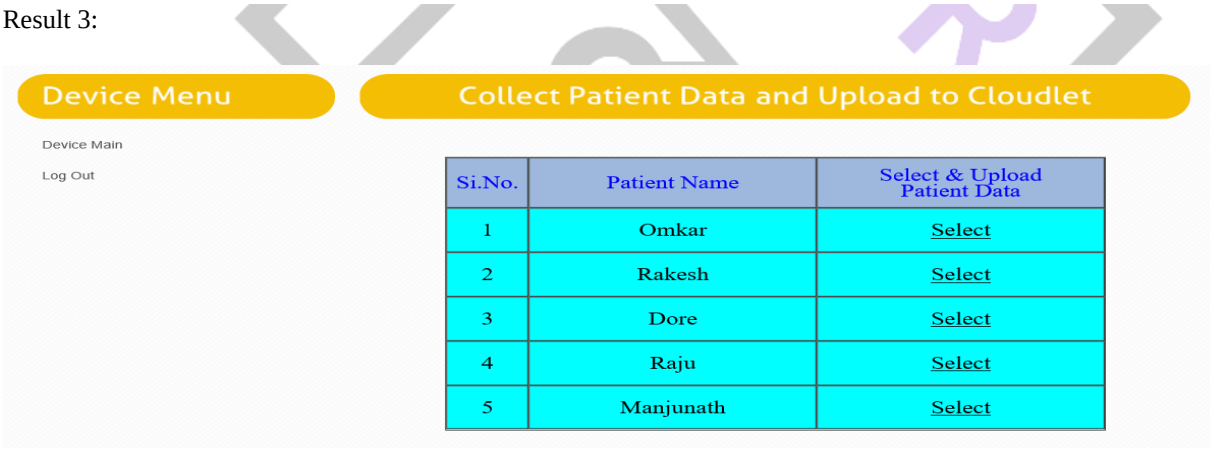
VII. RESULTS:

Result 1:

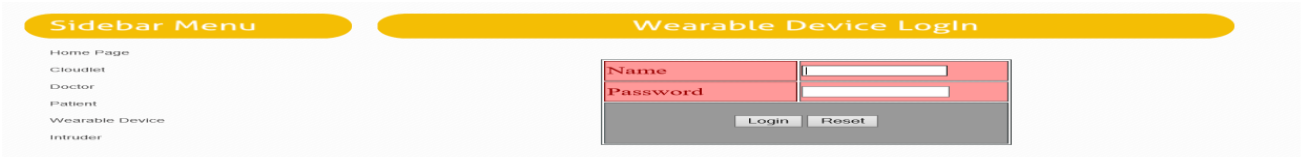


Result 2:

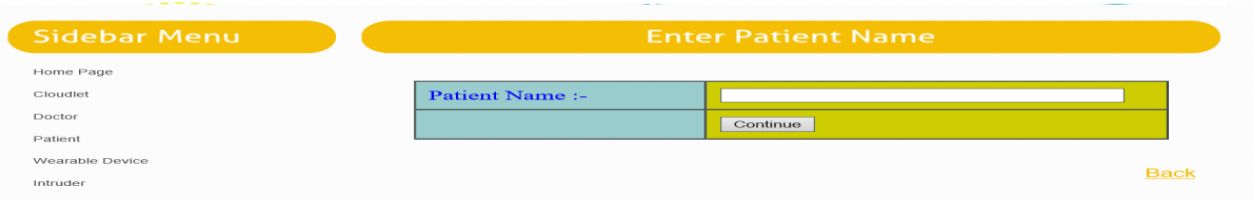
Result 3:



Result 4:



Result 5:



VIII. CONCLUSION:

In this paper we solved the privacy protection and sharing large amount of medical data problems in cloudlet and remote cloud. Firstly we utilize the wearable devices to collect patients' body details and also for protect users' privacy by encrypting the data by using AES algorithm. Secondly we build a trust model to make sure the transmission of users' data to cloudlet in security. Finally we use a Collaborative Intrusion Detection System [IDS] to protect the entire system.

REFERENCES:

[23] K. Rohloff and D. B. Cousins, "A scalable implementation of fully homomorphic encryption built on ntru," in Financial Cryptography and Data Security. Springer, 2014, pp. 221–234.
[24] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, "Phda: A priority basedhealthdataaggregationwithprivacypreservationforcloudassisted wbans," Information Sciences, vol. 284, pp. 130–141, 2014.
[25] 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.
[26] S. Saha, R. Das, S. Datta, and S. Neogy, "A cloud security framework for a data centric wsn application," in Proceedings of the 17th International Conference on Distributed Computing and Networking. ACM, 2016, p. 39.
[27] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," Journal of Medical Systems, vol. 40, no. 6, pp. 1–16, 2016.
[28] S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor node trust based intrusiondetectionsystemforwsn,"Procedia Computer Science,vol.63, pp. 183–188, 2015.
[29] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detectionforsafetycritical medicalcyberphysicalsystems,"Dependable and Secure Computing, IEEE Transactions on, vol. 12, no. 1, pp. 16–30, 2015.
[30] H. Mohamed, L. Adil, T. Saida, and M. Hicham, "A collaborative intrusion detection and prevention system in cloud computing," in AFRICON, 2013. IEEE, 2013, pp. 1–5.
[31] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015). IEEE, 2015.
[32] E. Vasilomanolakis, S. Karuppayah, M. M¨uhlh¨auser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," ACM Computing Surveys (CSUR), vol. 47, no. 4, p. 55, 2015.