International Journal of Science, Engineering and Technology
An Open Access Journal

Protection of Solitude and Encroachment on the Avoidance for Sharing the Medical Data Based on Cloudle

Uzma Tabassum, Sudarshan .N, Manuswani.V, Bhavya Javagal

Abstract

Using the clouds and cloudlet technology there are development of many wearable devices such as smart clothing, hand bands etc. Detects the pulse rate, amount of time a person sleeps etc. But it is very much necessary to give the better medical care. Processing of this data includes collection of data, storing and sharing of data etc. Sharing of medical data is usually risky and challenging. We make use of cloudlet to provide the healthcare system. We encrypt the user's body data by using the NUMBER THEORY (NT) method. In this the data of user is collected by wearable devices. The collected information Is further passed to the nearby cloudlet. Next ,we help users to communicate with the trusted partners who also share their data in the cloudlet using trust model .Trust model also helps the different users having similar diseases to communicate with each other. We then divide the user's medical data that is stored in the remote cloud of hospital into three sections and take various steps to protect them. Then at last to protect the health care systems from unexpected attacks from the intruder, we develop collaborative interruption detection system (InDS) based on cloudlet mesh to prevent from unexpected attacks.

Keywords: Data Encryption, Combinative intrusion detection system, healthcare, Data sharing.

Introduction

By making use of the different technologies such as wearable devices, health care big data, cloud computing etc the user can send his health data to the nearby doctor and an interaction can be built between doctor and a patient as shown in the below figure 1. But the delicate data can be leaked or taken over by the third person or the intruder and hence this causes protection problem. Via the cloud computing much of the information can be held in the clouds that include cloudlets and the secure clouds.

The major disadvantage here is the security and privacy from spiteful attacks. Taking consideration of above problem, this paper proposes a cloudlet based health care system (reference K. Hung) . The collected data from wearable devices are transmitted To the nearby cloudlets from where it is further transmitted to the secure clouds from where doctors will access the data and diagnose the disease.

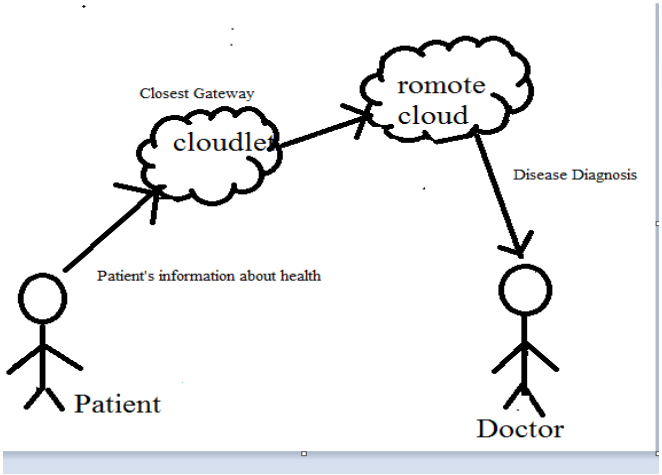


Figure 1:Encrypted data through cloudlet sent to doctor

In Figure. 2 the privacy protection is distributed into three stages .In the first stage the data of user's health collected via wearable devices is transmitted to the nearby cloudlets. Transmission of this health data needs to be secured a lot. Next, the data from the cloudlet is transmitted to the secure cloud where the third stage the data is divided into different types and corresponding security is provided. In order to provide the above stages we consider combinative InDS to protect cloud echo system.

RELATED WORKS

Privacy of data In the cloudlet:

In spite of the development of many platforms for sharing the data's via cloud, cloudlets etc, and these technologies are used much in health care data sharing because it requires lots of privacy and security.

There are many contributions towards the data security regarding the health care:

1. In Lu et al. [13], a system called SPOC (Secure and privacy preserving opportunistic computing framework).
This system was proposed to treat the storage problem of health care data and to address the problems of security and privacy protection under cloud environment.
2. In Cao et al. [14], MRSE (multi keyword ranked search over encrypted data in cloud computing)
The aim of this method is to provide the user with multi-keyword method for encrypted data of the cloud. People can make use of it but calculation could be a burden.
3. In Zhang et al. [15], PHDA Priority based health data aggregation.
This scheme was given to protect different types of healthcare data in a cloud.

Combinative InDS Network:

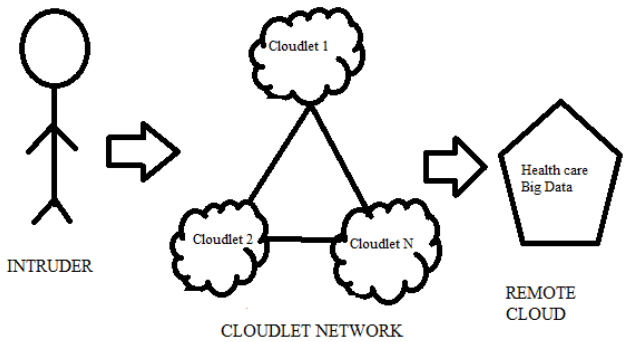
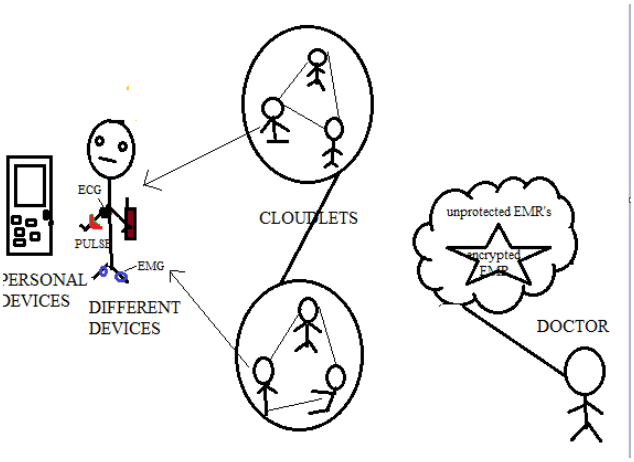


Figure .2.combinative InDS of the secure cloud.

1. When an attack by an intruder is detected, an alarm is fired. The finding rate of a Combinative InDS is better than a single InDS which ensures the security.

INTER-NETWORK COMMUNICATION.



Framework of the healthcare system is shown in the above figure. The user's data that is collected is delivered to the nearby cloudlet. During this transmission we suffer from two problems:
1. Privacy Protection.
2. To develop counter measures to prevent data from being stolen from outsiders. Privacy Protection of health care can be encrypted and shared as follows:

a. Client data encryption.
b. Cloudlet based data sharing.
c. Secure cloud privacy protection.
d. Combinative InDS based on cloudlet mesh.

SHARING OF DATA AND SECURITY

Here, we describe the problems that occur during transmission of the content from client to the doctor. We can provide each user with different Authority to access the data where the user can only access the data within his/her level and cannot go beyond the access rights.
We can provide an application to use the private data that is useful to both client as well as doctors, by making use of the healthcare big data.
Big data is present in some secure cloud, based on the details provided by the user; a disease prediction model is setup which is based on the concept of decision tree that is used to deduce the disease the user is suffering from and based on which doctor suggest the correct medication. The predictions obtained are sent to both client and Doctor.

Encryption at Client Edge And sharing Information on Network

The information's which are obtained from the various sensing devices that are attached to patient

are sent to the nearest cloudlet ensuring its protection. For instance, the average heart beat rate that is collected via the devices is passed on to the cloudlet in a secured manner, In order to establish the interaction between clients. The paper [10] proposed information sharing strategy among several clouds, depending on the attribute, the protection method is used. It doesn't consider users' social activities.

In [11], Fabian et al., Based on the discussion, during information sharing we give judgment that is as follows.

We set hospital for trusted authority (TA).Let us consider an example, Since Abhi wants to share the data with Akash, so he asks TA to check the information's of Akash. Then the TA work is divided into the following two stages:

1. We have to check for the data which is similar between Abhi and Akash this can be done using the data present in the TA. For example ECG's of two clients. Familiarities can be of three stages low, medium and high.
2. Analyze the trust level between Abhi and Akash. We should also consider the goodwill of the clients that consists of bad, average and good. We have to consider familiarities obtained in the previous step as an input data.

The information in the secure cloud is obtained from patients who are treated in hospital. The information of treatment and bills of patients are maintained in the form of files, and saved in cloud that can minimize cost and helpful to Doctors to give treatment and research on the diseases. The secured environment is created which ensure that the medical information sharing can be done without any interruption. We have to be careful will sharing such private information of clients.

According to [9][8],we can divide EMR table into the following three types:

(1)UID: The properties which can recognize the user's personal information. E.g.name, contact number, mail id, home address and so on.

(2)PID: The property which enables us to identify the user's in the cloudlet. E.g., zip code, DOB and gender.

(3)The medical details of the patients are shared in a secured manner so that the doctor and the patients suffering from similar disease can access the information provided UID and PID are encrypted.

Table.1 Input values which ensures the trust level.

Input Parameters	Quality Level	Threshold
Good will of clients c1	Bad Average Good	[0,0.2] (0.2,0.6] (0.6,1]
Familiarity between the c1 and c2	Low Middle High	[0,0.2] (0.2,0.6] (0.6,1]

Combination of Interruption Detection

Interruption detection system is used to protect medical data .If there is any suspicious attack, the system automatically alerts by an alarm. It helps in easy determination of the interrupters .Next step is to determine the detection standard in combinative InDS. We can look after that cloudlet network can be implemented with the estimated cost .The number of InDS to be to be present in the network is determined by arbitration structure. The main aim is to achieve a higher detection rate of the fake alarm also ensuring that it is cost minimizing system

Combinative InDS

In Combinative InDS let us consider n InDS I1, I2……., In which enhance detection level and reduce the fake alarm. Before moving the data to a secured cloud we have to perform combinative interruption detection on cloudlet network inorder to complete the task of interruption detection where each of InDS can determine interruption of individually.

Simulation Study

First we describe the transfer ratio to compare user data encryption method with encryption method of secure cloud we show the relation between InDS id's, amount spent and level of detection.

Enforcement level of data encryption

Inorder to secure the information about the user, we make use of encryption algorithm for the data encryption. We also have to measure the effectiveness of the algorithm .We draw graph by considering the variation in transfer ratio of user data encryption method with encryption method of secure cloud with increasing intervals. According to the graph it looks like both the curves provide a good transfer ratio but encrypted data sent by the

secure cloud seems to have good enforcement than encrypted data sent by the user.

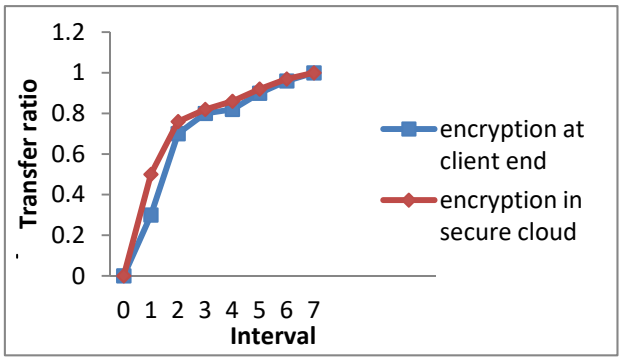


Figure 3.Compare the transfer ratio of the encryption method of secure cloud and client end.

We have to first determine the trust level before sharing the information on the cloudlet for this purpose it is necessary to know the good-will of the user on the network which can be ranged between [0,1] has specified in Table1. If the good wiliness of clients seems to be low, a likeness of the user is poor. The resulting model is not so trustworthy. In these conditions the users hesitate to share the data on such model as it is not safe. As there is increase in good-will and alikeness the model becomes more trusted and encourages sharing their data on the network.

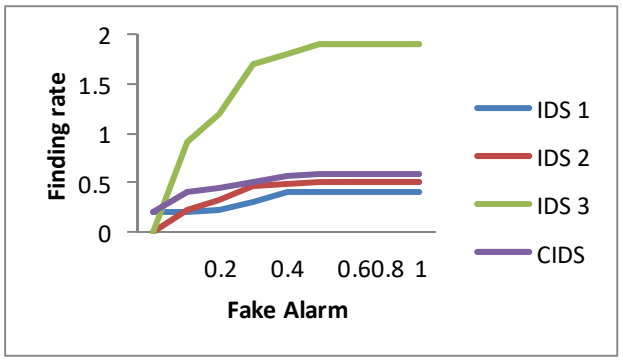


Figure 4.comparison between detection rate of a single INDS and combinative InDS

Combinative InDS's Enforcement

The cloudlet mesh simulator [12] to obtain a high level security in the mesh. There are 3 InDS and two types of interruption are required in our experiment. the probabilities of two interruption are p1=0.001 and p2=0.0015.In figure 4 we plot the finding rate of different InDS's used verses the fake alarm from the graph we can infer that the finding ratio of single interruption detection system less than combination interruption detection system i.e., for single interruption detection system It is of the range 20-25% but for CInDS it is 50-60% which is comparatively high.

It leads to the system loss/failure if InDS doesn't generate an alarm when there is an interruption. Along with all these modification using CInDS's we should also look after whether the detection can be done in the lower investment .If we consider six InDS's are used in this experiment whose finding ratio is described in figure 5. Finally we can infer that the find rate will be beyond 65-70% and fake alarm will be below 3.4-3.5% last but not the least we need to construct a effective CInDS at a minimize cost. Since the single InDS have below 30% of finding ratio, Collaboration of system enhances the finding rate at a low cost. We have to select InDS such that it works effectively and yield a optimal solution and it's cooperative

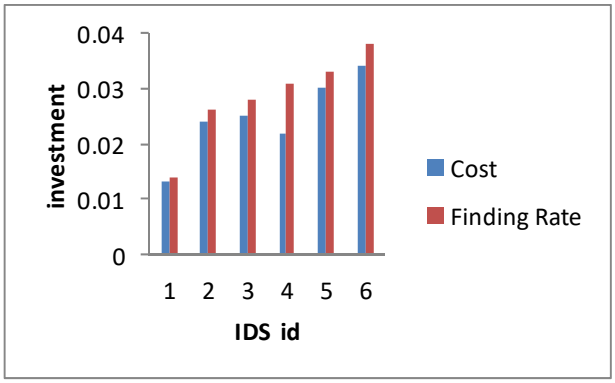


Figure5. Finding rate and the cost of six InDS's , it shows the forth InDS's seems to have good finding rate at minimum investment.

Conclusion

In this paper we analyze about the security to the private information of the user, sharing of medical details of clients to the cloudlets and secure cloud. it enables the users to transfer the information to cloudlet and also ensures the data shared in the network are secured and safe from interrupters.

Initially, we use wearable materials which gather the details of the user .In order to ensure protection to the data transmitted to cloudlet we make use of a NT methodology that encrypts the data before sending to cloudlet. Second the data on the cloudlet can be shared among user based on their confidence level, which show whether the data can be shared or not. Third, the protection level of the secure cloud, the information will be preserved in the secure cloud and encrypt the client information not just to ensure the security but enhance the transmission efficiency. Final stage, where CInDS on cloudlet network for the

security of data .The scheme is evaluated with simulation and experiments.

References

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome Healthcare," in Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[2] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," 2015.

[3] Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing Min Chen, Senior Member, IEEE, Shiwen Mao, Senior Member, Long Hu.

[4] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192–202, 2016.

[5] R. Zhang and L. Liu, "Security models and requirements for healthcare Application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.

[6] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," 2016.

[7] L. Griffin and E. De Leastar, "Social networking healthcare," in Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on . IEEE, 2009, pp. 75–78.

[8] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 43, pp. 74–86,2015.

Systems vol.40, no.6, pp. 1–16,2016. [9] 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.

[10] B. Fabian, T. Ermakova, and P. Junghanns, "Combinative and secure Sharing of healthcare data in multi-clouds," Information Systems, vol. 48, pp. 132–150, 2015.

[11] 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.

[12] 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

[13] 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.

[14] 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.

[15] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, "Phda: A priority Based health data aggregation with privacy preservation for cloud assiste Wbans," Information Sciences, vol. 284, pp. 130–141, 2014.

Author's details

1. Uzma Tabassum Student, Computer Science Engineering, T.John Institute Of Technology, Karnataka, India, uzma.3397@gmail.com.

2. Sudarshan.N Student, Computer Science Engineering, T.John Institute of Technology, Karnataka,India, sudhisudarshan1996@gmail.com.

3. Manuswani.V Student, Computer Science Engineering, T.John Institute of Technology, Karnataka, India, manju.manu17125@gmail.com.

4. Bhavya Javagal Asst. Professor, Computer Science Engineering, T.John Institute Of Technology, Karnataka, India, Bhavdec @gmail.com.