Medical Data Sharing For Protection and Intrusion Avoidance in Cloudlet

Sonali Bodkhe[1], Aishwarya Gadkar[2], Sarika Mane[3] , Priyanka Pol [4], Jyoti Tarange[5], Prof.Nalawade T.B.[6]

[1,2,3,4]Student, Department of Computer Science and Engineering, SMSMPITR, Akluj, Maharashtra, India,
[5]Assistant Professor, Department of Computer science and Engineering, SMSMPITR, Akluj, Maharashtra, India.

Abstract*:* Sharing personal health data is essential to create next generation healthcare services. To acknowledge preventive and personalized medicine, extensive quantities of consumers must pool health data to make dataset that can be analyzed for wellness and disease trends. Consequently in this paper, we develop a novel human services framework by using the adaptability of cloudlet. The elements of cloudlet incorporate security insurance, information sharing and interruption location. In this paper, we 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, we 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, we 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, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. In order to protect the healthcare system from malicious attacks, we 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.
This paper proposed a protected cloudlet based medical data sharing. In this framework information proprietor encode the information by using encryption algorithm and store it cloudlet. For KDC give a key to the information proprietor.

Key Words: privacy protection, data sharing, Cloudlet, collaborative intrusion detection system (IDS), NTRU, KDC.

1. INTRODUCTION

This 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' evergrowing demands on health consultation. Healthcare social platform, such as Patients-LikeMe, 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, we 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, we use trust model to evaluate trust level between users to determine sharing data or not. Considering the users' medical data are stored in remote cloud, we classify these medical data into different kinds and take the corresponding security policy. In addition to above three stages based data privacy protection, we also consider collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

3. PROPOSED SYSTEM

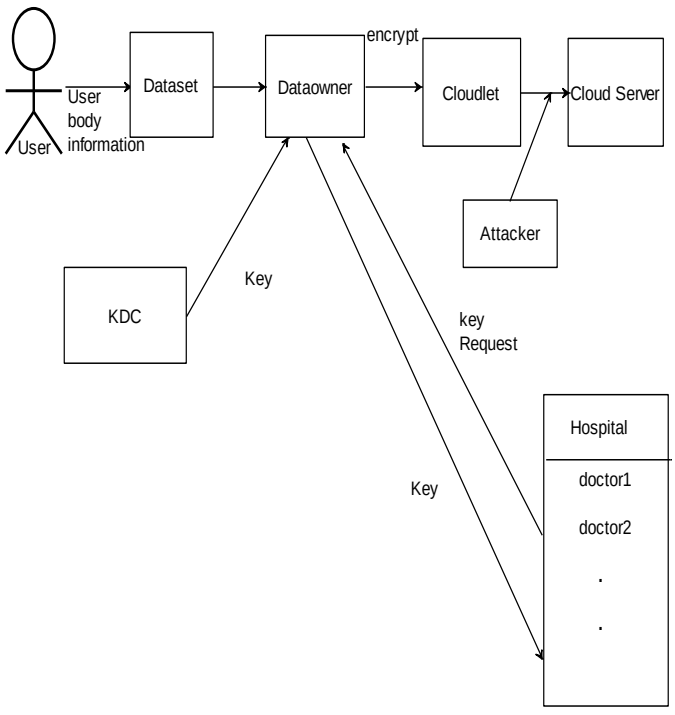

Fig: Block diagram

3.1 DISCRIPTION

User provides the user body information to dataset. Dataset as an input for securely sharing in cloudlet based system. Owner can be any person to access the information, it taking a dataset encrypt it using NTRU algorithm and store it cloudlet. The KDC is used to reduce the risk of key exchanging. It distributed the key among data owner and authenticated user. The cloudlet system store the encrypted data provided by data owner, while sharing if any attack found then it prevent it using collaborative intrusion detection system method. The cloud server is used to store the user encrypted data, if any authenticated doctor want to access the data then it can be access from the cloud for decrypt the data.

3.2 ADVANTAGES

- NTRU will secure the whole information that is being transferred to cloudlet from wearable devices.
- Patients can share their information or queries with other people who also suffer from a same health problem. Security is provided to users through trust model where it identifies whether the data sharing can be performed or not.
- Patient's health records are highly secured by classifying them and making use of encryption mechanism.

4. FLOWCHART

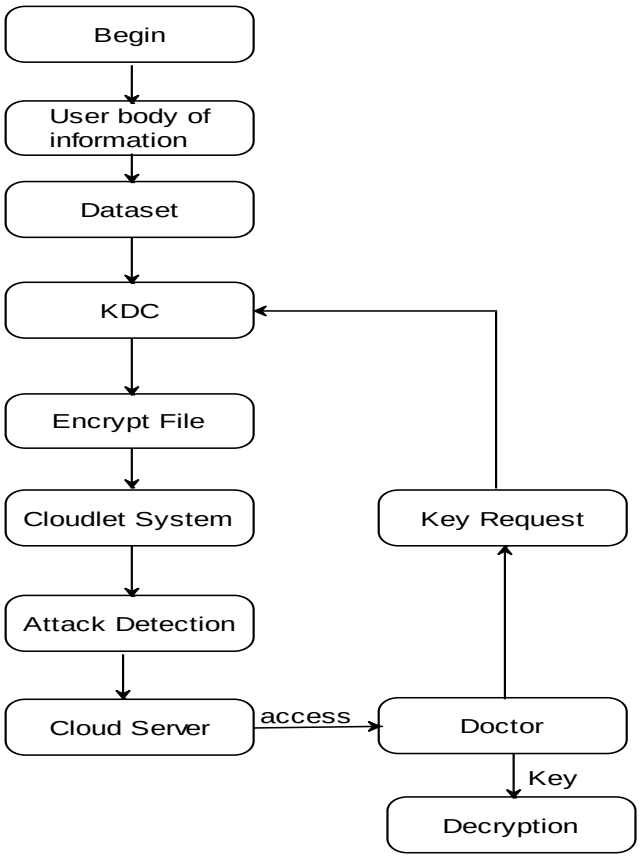

Fig: Flowchart

5. ALGORITHM

Initialization Phase:

1. Key Generation:

In existing system NTRU uses only static values for decryption .Because, in dynamic value scenario, decryption does not work if values are exceeded .so proposed system overcome this limitation by using dynamic public parameter for decryption, which have to satisfy following condition,

$$Q>(6d+1)*p$$

Create two pairs of keys for CC and BAN gateway as follows.

Key Generation:

- Encryption Keys:

  For CC:

  Compute secret key fcc as:

  Fcc=p.fcc+1,

  Compute hcc as:

  Hcc=p. gcc / fcc.

  (fcc, hcc) is pair of encryption public and private keys, respectively.

  For BAN:

  Compute serect key fban as:

  Fban=p.fban+1,

  Compute hcc as:

  Hban=p. gban/ban.

  (fban, hban) is pair of encryption public and private keys, respectively.

- Signing Key:

  Choose polynomial of f and g.

  Compute public key for all users.

  Compute small polynomials (F,G)

  Generate signing key for CC as:

  Skcc=(fcc,gcc,Fcc,Gcc)

  Generate signing keys for BAN as:

  SKban=(fban,gban,Fban,Gban)

2. Demand Forecast:-Calculate approximate electricity electricity demand for each HAN by g()-g()=forecasting function

-For all HAN in BAN cluster,

-Aggrgate electricity consumption such as,

Xi=g(HANi)

X=amount of HAN

N=the number of HANs in BAN region.

-Store ID, Corresponding pair of electricity demand and current price of all HAN stores in BANs database.

-Aggregate the total demand for all smart meters

-Compute total required energy amount for BAN

3. Agreement request message:

-x=BANs fixed demand per month.

-Accomplish agreement with CC

-Send agreement request message to CC, with signing and encrypting electricity amount x

-CC accepts request

-Assign electricity amount

-Encrypt and send to BAN.

-At BAN decrypt and message and knows approximetly expected bill.

Exchange Message phase:

At BAN

-Provides electricity share to each HAN

-Compute current payment for each HAN by:

Bi=xi*p* Tj ,

Where ,bi=current payment

Xi=electricity share

P=current electricity price

Tj=time period that HAN consumes its share

Billing Process

At BAN

-Compute total bill for each HAN

-Aggregate regions total bill – S

-Sign billing message by private key of BAN

-Encrypt it using CCs public key

-Hashing of S

-Send billing message to CC

At CC

-Decrypt message

-Verify signature of BAN on massage

-Check validity of timestamp

-Accept the message.

7. CONCLUSION

Proposed a secure cloudlet-based data sharing system. This system share data in encrypted format. Attack prevented by the cloudlet using collaborative intrusion detection system (IDS) method. Proposed system is more secure and trustable. Also saves the time and memory.

REFERENCES

[1] Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu, "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing", IEEE Transactions on Cloud Computing, 2016.

[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] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," *Network, IEEE*, vol. 24, no. 4, pp. 13–18, 2010.