ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Design and Implementation of Medical Data Sharing For Safeguard and Intrusion Prevention in Cloudlet

Dr.K. Praveen Kumar

Associate Professor, Dept. of CSE, Chaitanya Institute of Technology and Science, Warangal, Telangana, India

ABSTRACT: Health Record of an individual personal is a vital way that can be utilized for keeping track of patient data in accurate, reliable as well as complete manner. For all intents and purposes, restorative information sharing is a basic and testing issue. 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 cloud let mesh, which can effectively prevent the remote health care big data cloud from attacks.

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

I. INTRODUCTION

With the expansion of healthcare big data and wearable technology [1], as well as cloud computing and communication technologies [2], cloud-assisted healthcare big data computing converts critical to meet users' ever-growing anxieties on health consultation [3]–[5]. Nevertheless, it is thought-provoking issue to personalize specific healthcare data for numerous users in a suitable fashion [6]. Aforementioned work recommended the combination of social networks and healthcare service to facilitate [7] the trace of the disease treatment process for the retrieval of real-time disease information [8]. Healthcare social platform, such as Patients Like Me [9], 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 [10] [11] without efficient protection for the shared data [12]. Therefore, how to balance privacy protection with the convenience of medical data sharing becomes a challenging issue.

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.

II. RELATED WORK

The system is privacy-assured where cloud sees neither the original samples nor underlying data. It handles well sparse and general data, and data tampered with noise.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Advantages:

1. We have proposed a privacy-aware cloud assisted healthcare monitoring system via compressive sensing.
2. The random mapping based protection ensures no sensitive samples would leave the sensor in unprotected form.

Disadvantages:

1. Wireless sensors are being increasingly used to monitor/collect information in healthcare medical systems.
2. Despite the increasing popularity, how to effectively process the ever-growing healthcare data and simultaneously protect data privacy, while maintaining low overhead at sensors, remains challenging.

[2] "Behaviour rule specification-based intrusion detection for safety critical medical cyber physical systems".
We demonstrate that our intrusion detection technique can effectively trade false positives off for a high detection probability to cope with more sophisticated and hidden attackers to support ultra-safe and secure MCPS applications.

Advantages:

1. For safety-critical MCPSs, being able to detect attackers while limiting the false alarm probability to protect the welfare of patients is of utmost importance
2. 2. We plan to analyze the overheads of our detection techniques such as the various distance-based methods in comparison with contemporary approaches.

Disadvantages:
We propose and analyze a behaviour-rule specification-based technique for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) in which the patient's safety is of the utmost importance.

[3] "Cloudlet mesh for securing mobile clouds from intrusions and network attacks".
We have specified a sequence of authentication, authorization, and encryption protocols for securing communications among mobile devices, cloudlet servers, and distance clouds.

Advantages:

1. Securing mobile cloud services is the major barrier to the integration of BTOD (bring your own devices) and BYOC (bring your own cloud) in our daily applications.
2. We use the cloudlet mesh to perform collaborative intrusion detection among multiple cloudlets.

Disadvantages:

1. Network attacks are a serious matter that confronts both cloud providers and massive number of mobile users who access distance clouds in our daily-life operations.
2. We extend their work to support security functionalities in offloading the distance clouds.

[4] "Cloud-supported cyber–physical localization framework for patients monitoring".
The proposed approach uses Gaussian mixture modelling for localization and is shown to outperform other similar methods in terms of error estimation.

Advantages:

1. The design and development of such systems requires access to substantial sensor and user contextual data that are stored in cyberspace.
2. We will conduct more workload measurements to record the resource utilization of CPU, memory, storage, and network bandwidth.

Disadvantages:

This enables a range of emerging applications or systems such as patient or health monitoring, which require patient locations to be tracked.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

[5] "Cloudlet-based efficient data collection in wireless body area networks".
The proposed work also attempts to minimize the end-to-end packet delay by choosing dynamically a neighbour cloudlet, so that the overall delay is minimized.

III.SYSTEM DESIGN

User provides the user body information to dataset. Data set 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.

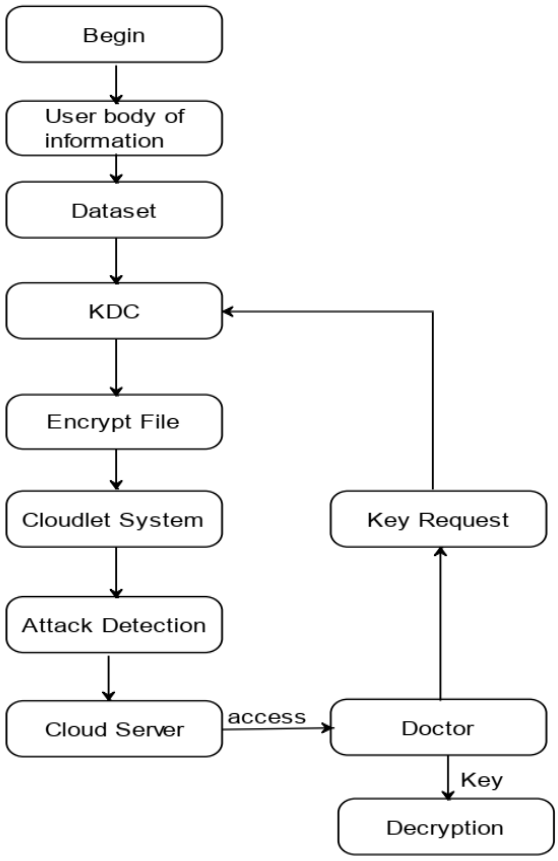

Fig.1: Flowchart of the process

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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

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 privatekeys, respectively.

For BAN:

Compute secret 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 demand for each HAN by g()-g()=forecastingfunction

-For all HAN in BAN cluster,

-Aggregate 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 demandand current price of all HAN stores in BANsdatabase.

-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, withsigning and encrypting electricity amount x

-CC accepts request

-Assign electricity amount

-Encrypt and send to BAN.

-At BAN decrypt and message and knowsapproximately expected bill.

Exchange Message phase:

At BAN

-Provides electricity share to each HAN

-Compute current payment for each HAN by:

$B_i = x_i * p * T_j$,

Where ,b_i=current payment

Xi=electricity share

P=current electricity price

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Tj=time period that HAN consumes its shareBilling 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.

IV. CONCLUSION

In this paper, we explored the issue of security assurance and sharing expansive medical information in cloudlets and the remote cloud. We built up a frame work which does not enable clients to transmit information to the remote cloud in light of secure gathering of information, and in addition low correspondence cost. 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] 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] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, "A security framework in g-hadoop for big data computing across distributed cloud data centers," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.
[4] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internetof 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 healthcareapplication clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rdInternational 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 WearableMicro and Nano Technologies for Personalized Health (pHealth), 20096th International Workshop on. IEEE, 2009, pp. 75–78.
[8] W. Xiang, G. Wang, M. Pickering, and Y. Zhang, "Big video data forlight-field-based 3d telemedicine," IEEE Network, vol. 30, no. 3, pp. 30–38, 2016.
[9] https://www.patientslikeme.com/.
[10] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for onlinesocial networks: challenges and opportunities," Network, IEEE, vol. 24,no. 4, pp. 13–18, 2010.
[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preservingmulti-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233,2014.
[12] K. T. Pickard and M. Swan, "Big desire to share big health data: A shiftin consumer attitudes toward personal health information," in 2014 AAAISpring Symposium Series, 2014.