International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

PRIVACY GUARD AND INTRUSION A VERTING FOR CLOUDLET BASED MEDICAL RECORDS DISTRIBUTION

V.Hellan Surya [#1], R.Divya[*2] and T.C Vidhya [*3]

[#1]*Student, IT , Kings Engineering College, Iungattukottai, India*
[*2]*Student, IT , Kings Engineering College, Iungattukottai, India*
[*3]*Assistant Professor, IT , Kings Engineering College, Iungattukottai, India*

***Abstract*: The cloud storage system provides convenient file storage and sharing services for distributed clients. In order to solve the integrity, we present identity-based data outsourcing (IBDO), outsourcing and original auditing concerns about outsourced documents, The program is equipped with an ideal feature that facilitates existing recommendations to protect outsourcing data. First of all, our IBDO plan Allows the user to authorize the dedicated agent to upload the data to the cloud storage server (for example, the company can authorize) Some employees upload files to the company's cloud account in a controlled manner. The agent is identified and authorized Identifiable identity eliminates complex certificate management in conventional secure distributed computing systems. We Propose IBDO program is a comprehensive audit that our program not only allows for formal integrity audits in existing programs Used to protect the outsourced data, but also allows the review of external data sources, types and consistency information. Safety Analysis and experimental evaluation show that our IBDO solution provides strong safety and ideal efficiency. 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. Safety Analysis and experimental evaluation show that our IBDO solution provides strong safety and ideal efficiency.**

Key words: Bloom filter algorithm, Data Collaborative IDS

1. INTRODUCTION

Cloud Computing is a technology which depends on sharing of computing resources than having local servers or personal devices handle the applications. In Cloud Computing, the word "Cloud" means "The Internet", so Cloud Computing means a type of computing in which services are deliver through the internet. With the development of healthcare big data and wearable technology [1], as well as cloud computing and communication technologies [2], cloud-assisted healthcare big data computing becomes critical to meet users' ever-growing demands on health consultation [3]–[5]. However, it is challenging issue to personalize specific healthcare data for various users in a convenient fashion [6]. Previous work suggested 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 PatientsLikeMe [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. With the advances in cloud computing, a large amount of data can be stored in [8] various clouds [13], including cloudlets [14] and remote clouds [15], facilitating data sharing and intensive computations [16] [17]. However, cloud-based data sharing entails the following fundamental problems: How to protect the security of user's body data during its delivery to a cloudlet?How to make sure the data sharing in cloudlet will not cause privacy problem?As can be predicted, with the proliferation of electronic medical records (EMR) and cloud-assisted applications, more and more attentions should be paid to the security problems regarding to a remote cloud containing healthcare big data. How to secure the healthcare big data stored in a remote cloud?

• How to effectively protect the whole system from malicious attacks?

In terms of the above problems, 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,weusetrustmodeltoevaluatetrust

wireless local area networks) to generate, sense, analyze, and cognitive analysis for healthcare applications. C. Zhang, J. Sun, X. Zhu, and Y. Fang proposed the Privacy and security for online social networks: challenges and opportunities. In this paper present the unique security and privacy design challenges brought by the core functionalities of OSNs and highlight some opportunities of utilizing social network theory to mitigate these design conflicts.

3. Issues in cloud: In cloud computing the security maintenance is one of the main 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, users 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

levelbetweenusers 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.

2.Related work: K. Hung, Y. Zhang, and B. Tai proposed the Wearable medical devices for tele home healthcare. Aim of this project is to develop a tele-home healthcare system which utilizes wearable

devices, wireless communication technologies, and multisensory data fusion methods. M. S. Hossain proposed the Cloud-supported per–physical localization framework for patients monitoring. These systems integrate a large number of physical devices such as sensors with localization technologies

towards remote cloud through cloudlets. A cloudlet

4. System architecture:

The architecture aims to provide the high security for end users (patients).First hospital A doctor upload all the details of the patient in the cloud. There is one trust act like a aggregate authority. With their permission the doctor can upload the patient detail in cloud. Similarly hospital B doctor also upload the patient detail. On that time there is major chance to the hackers can hacked the patient detail. In this project we use IDS algorithm.

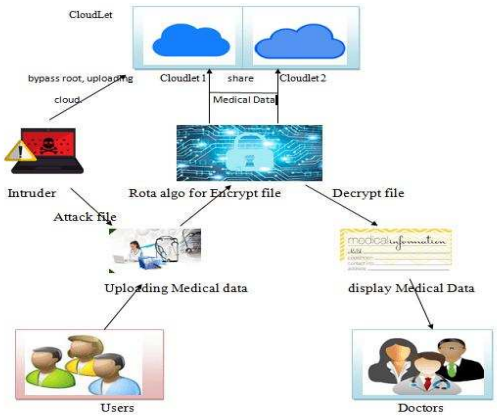

Fig 1.Architecture

Through this algorithm the trust can block the patient's detail page. So the intruder cannot visit this page. Now the hospital A doctor send the request to hospital B doctor if they need for something like particular blood, operational equipment in encrypted format. Then hospital B doctors decrypt the request using OTP message. Then they response the request.

5. Module Description:

5.1 Hospital A: Hospital A authority register activate by the trust. After activate enter login then if A need to view hospital B details they need Key hospital or view details.

Every time need key while authority login All details are view only in encrypt format Authority only added the medical data's & Patient details into the cloud If hospital A needs any details from hospital B they search based on identity then they give request. After accept request by the cloud & trust authority they send on secret key to hospital B authority mail id. Then only that particular data view in decrypt format.

5.2 Hospital B: Hospital B authority register activate by the trust. After activate enter login then if hospital B need to view hospital A. A details they need Key for view details.

Every time need key while authority login. All details are view only in encrypt format. Authority only added the medical data's & Patient details into the cloud. If hospital B needs any details from hospital A they search based on identity then they give request.

5.3 Cloud Service: Login by id and password. Then the doctor can get the OTP number after that they can access their request. Next the cloud activated the register user.

5.4 Intruder: When the doctor upload the patient's detail on that time there is many change to the hacker can hacked the page. Through the IDS algorithm we can block the page. Now it is not activated by the intruder.

6. Algorithm:

6.1 Bloom Filter Algorithm: A Bloom filter is a space-efficient probabilistic data structures conceived Burton Howard Bloom in 1970, that is used to test whether an element is a member of a set. False positive matches are possible, but false negatives are not – in other words, a query returns either "possibly in set" or "definitely not in set". Elements can be added to the set, but not removed (though this can be addressed with a "counting" filter); the more elements that are added to the set, the larger the probability of false positives.

1.Data holders A and B agree on a bit array length l, on k hash function and a common secret key k. 2.For every string i in Sa , A performs then following steps. (a) A converts string I into the set of its q- grams. (b)A stores the resulting q-gram set in a bloom filter bf of length l using the key hash function with a key k.3. A stores the resulting Na bloom filters and a randomly generated unique ID number id in a list BF.4. A removes any identifiers in DB, replacing them by id 5. A sends DB to D. 6.For string j in S. B performs the following steps. (a) B converts string j into the set of its q-grams. (b) B stores the resulting q-gram set in a bloom filter Bf of length l using the key k hash function with the key K. This protocol is intended to match string attributes only. However as outline above there are various protocol for matching attributes exactly in a privacy preserving manner. These protocol can be used for the

comparison of numerical attributes in combination.

Algorithm

```
B empty Bloom filter of size m
T hash table
for all reads & do
for all k- means x in &do
      x min (x,revcomp(x))//x is the
canonical k – mere for x
       if Xrep  B then
       if Xrep  T then
            T[x] 0
       Else
            add x to B
 for all reads & do
 for all k- means x in & do x
      min (x,revcomp(x)) if
      Xrep T then
    T[x] T[x]+1
  For all   x T do
If T[x]=1 then
Remove x from T
```

6.2 Collaborative IDS

Collaborative IDS based on the cloudlet mesh structure is used to screen any visit to the database as a protection border. If the detection shows a malicious intrusion in advance, the collaborative IDS will fire an alarm and block the visit, and vice-versa. In order to protect medical data, we also develop an intrusion detection system in thispaper.Onceamaliciousattackisdetected,t he system will fire and alarm .

This section presents a novel scheme to build a collaborative IDS system to deter intruders. In the following.wefirst consider what happens if the system is suffering from different attacks, while detection rates for individual IDS vary with the cloudlet servers. We will plot the detection rate and false alarm rate as the receiver operating characteristic (ROC) curves.

Next, we evaluate the collaborative detection rate and estimate the expectedcostof implementation in the cloudlet mesh. We apply a decision tree to choose the optimal number of IDS's to be deployed on the mesh.

The goal is to achieve a prescribed detection accuracy against the false alarm rate under the premise of minimizing the system cost. when the intrusion behavior is not detected by the system, but IDS generates an alarm, the system will prevent the transmission of this user's data, which will affect the normal use of the healthcare system by the user, and may lead to decrease of the system's reliability.

The cost at this moment is denoted as Cα; • when the system suffers from intrusion Ii, 1 ≤i≤ K, but the IDS does not generate an alarm, the system will allow this intrusive behavior, which will break the healthcare big data.The cost in other scenarios is marked as 0.

Algorithm

```
Most Fit max()
If Most Fit members>1
Begin
    For Each Most Fit Members
Begin
    Most Counter Max(Counter) Best
detector DA most counter End
Else
    Best Detector DA most fit End
    Judgment-set={}
    Until Judgment-set Members=n For
    Each Detector Agent(DA)
Begin
    Count Random Number
    If Counter>=Count
    Begin
    Judgment-set Judgement-set+DA End
 End
End
```

VII.CONTENT SHARING AND PRIVACY PROTECTION:

In this section, we address the problem of protection and data sharing. First, we introduce the encryption process for users' privacy data, which prevents the leakage or malicious use of users' private data during transmissions. Next, we present the identity management of users who want to access to the hospital's healthcare data. Thus, we can assign different users with different levels of permissions for data access, while avoiding data access beyond their permission levels. Finally, we give an application of using users' private data, which is beneficial to both users and doctors. Based on the healthcare big data stored in the remote cloud, a disease prediction model is built based on decision tree. The predictions will be reported to the users and doctors on demand.

7.1 Medical Data Privacy Guard in the Cloudlet:
A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiency of data transmissions are our main concern. We use NTRU for data protection during data transmissions to the cloudlet. In order to share data in the cloudlet, we use user's similarity and reputation to build up trust model. Based on the measured users' trust level, the system determines whether data sharing is performed. 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' ever growing demands on health consultation . However, it is challenging issue to personalize specific healthcare data for various users in a convenient fashion. We investigated the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud. We developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost. However, it does allow users to transmit data to a cloudlet, which triggers the data sharing problem in the cloudlet. A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiency of data transmissions are our main concern. In order to share data in the cloudlet, we use users' similarity and reputation to build up trust model. We divide data in remote cloud into different kinds and utilize encryption mechanism to protect them respectively. We propose collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

VIII.CONCLUSION

Nowadays Cloud computing is the trending and emerging technology. The one of the main issue in cloud computing is Security problem. We investigated the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud. We developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost. However, it does allow users to transmit data to a cloudlet, which triggers the data sharing problem in the cloudlet.

IV.REFERENCES:

[1]Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical

Hwang, Fellow, IEEE, Shiwen Mao, Senior Member, Long Hu,2017

[2] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telephone 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.

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

[4] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Rajang, J. Kołodziej, A. Streit, and

Georgeakopoulos , "A security framework in g-hadoop for big data computing across distributed cloud data centres," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 994–1007, 2014.

[5] 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.

[6] 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.

[7]L.GriffinandE.DeLeastar,"Socialnetwor

kinghealthcare,"inWearable Micro and Nano Technologies for Personalized Health

(pHealth), 2009 6th International Workshop on. IEEE, 2009.

[8] W. Xiang, G. Wang, M. Pickering, and

Y. Zhang, "Big video data for light-field-

based 3d telemedicine," IEEE Network, vol. 30, no. 3, pp. 30–38, 2016.

[9] 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.

[10] 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.

[11] K. T. Pickard and M. Swan, "Big desire to share big health data: A shift in consumer attitudes toward personal health information," in 2014 AAAI Spring Symposium Series, 2014.