Secure Data Sharing Using Bloom Filter in Cloudlet based Healthcare System

S. Srinivas[1], A.Neeharika[2]
[1]*Asst. Professor, Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, India*
[2]*M. Tech Student, Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, India*

Abstract- Healthcare social platform, together with Patients Like Me, can achieve data from other similar patients through data sharing in phrases of person's own findings. Though sharing scientific data on the social community is useful to both sufferers & doctors, the sensitive records is probably leaked or stolen, which reasons privacy & security issues without efficient protection for the shared data. In this paper, I increase a novel healthcare system through utilizing the power of cloudlet and also utilizing Bloom filter hashing for security. The functions of cloudlet consist of privacy protection, data sharing & intrusion detection. The body data accumulated via wearable gadgets are transmitted to the nearby cloudlet. Those data are in addition added to the remote cloud wherein medical doctors can get right of entry to sickness analysis.

Keyword- Cloudlet, Data Collection, Intrusion Detection

I. INTRODUCTION

Cloud computing is increasing a vital technology for coping with clinical health care data. With the growing demands on health consultation, it is challenging issue to customize unique healthcare data for diverse customers in a convenient fashion [1, 2]. Though the existing machine presents security of data by means of warding off intrusion [2], it is lagging in supplying statistics privacy. As healthcare data is taken into consideration to be the most sensitive information, it wishes a robust privacy even as sharing data between customers. Though sharing clinical information is beneficial to both patients & medical doctors, the sensitive statistics might be leaked or stolen, which causes privacy & protection issues without efficient safety for the shared information. Therefore, a way to balance privacy protection with the ease of medical records sharing becomes a tough trouble. At the time of importing of private health care statistics within the cloud the proprietor of data losses the bodily manage additionally[4] it is able to be hacked with the aid of attackers. Hence the supplying the security is a massive issue even as sharing personal health care data in cloud environment. This may be solved by means of the use of encryption mechanism on the time of records sharing[5] so one can growth the confidentiality of the records in addition to records safety within the third party storage server. By making use of several encryption techniques consumer can keep the statistics on cloud without disturbing approximately the security.

This clinical statistics on the social community is useful to both patients & doctors, the sensitive information might be leaked or stolen, which causes privacy & safety problems without efficient safety for the shared data. MRSE (multi-keyword ranked search over encrypted data in cloud computing)[3] privacy safety gadget became presented, which aims to provide customers with a multi-keyword technique for the cloud's encrypted statistics. Although this approach can provide result rating, wherein people are fascinated, the amount of calculation may be bulky. A priority based health data aggregation (PHDA) scheme turned into provided to shield & combination distinctive forms of healthcare date in cloud assisted wireless body area networks (WBANs)[4]. The article investigates protection & privacy problems in cell healthcare networks, along with the privacy safety for healthcare information aggregation, the security for statistics processing & misbehavior. Here, I describe a flexible protection model particularly for statistics centric programs in cloud computing based totally state of affairs to make certain data confidentiality, information integrity & best grained access manage to the software statistics.

With the advances in cloud computing, a large amount of data can be stored in diverse clouds, consisting of cloudlets & faraway clouds, facilitating data sharing & in depth computations. However, cloud-based totally data sharing includes the following essential issues: How to protect the security of consumer's body records throughout its shipping to a cloudlet? How to ensure the records sharing in cloudlet will now not cause privacy trouble? As can be anticipated, with the proliferation of digital clinical records (EMR)&cloud-assisted packages, more&more attentions should be paid to the security problems regarding to a far off cloud containing healthcare huge data. How to relax the healthcare large statistics saved in a far off cloud?

II. RELATED WORK

Cloud-Supported Cyber–Physical Localization (CCPLSs)[6] represented with the aid of M.Shamim Hossain&it's miles a unexpectedly evolving technique to affected person tracking,&feature many interesting opportunities in regards to verbal exchange (localization)&computation[6]. The design&improvement of such systems requires access to full-size sensor&user contextual records which might be stored in our on-line world. Ensuring dependable&real-time get right of entry to such information once in a while hindered by way of

the excessive latencies of extensive-region networks underlying the CCPLS infrastructure. To recognize those characteristics of localization structures, the workload have to be measured by way of deploying proposed localization approach over public cloud offerings along with Amazon's EC2 platform. Some of the workloads are measured.

In the paper Privacy Protection&Intrusion Avoidance for Cloudlet-primarily based Medical Data Sharing [1] build up a singular healthcare machine through utilizing the ability of cloudlet. The features of cloudlet encompass privacy protection, facts sharing&intrusion detection[7]. In information collection utilize Number Theory Research Unit (NTRU)[2] approach to encrypt consumer as body data gathered via wearable gadgets. Those records might be sent to nearby cloudlet in an energy efficient fashion. Then gift a new accept as true with model to assist customers to pick trustable partners who need to exchange stored records within the cloudlet. The trust version additionally enables equal patients to communicate with every other approximately their illnesses.&divide users clinical facts saved in remote cloud of hospital into 3 parts,&supply them proper protection. Finally, with a view to guard the healthcare device from malicious attacks, design a singular collaborative intrusion detection[7]system (IDS) technique rely on cloudlet mesh, that may effectively prevent the remote healthcare big information cloud from assaults.

In the paper A Secure & Privacy Preserving Opportunities Computing Framework for Mobile Health Care Emergency[4] proposed in wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare issue into a pervasive surroundings for better health monitoring ,They advise a secure & privacy-retaining opportunistic computing framework, referred to as SPOC, for mHealthcare emergency. The SPOC, clever telephone wealth along with computing power & power may be opportunistically gather to method the computing extensive private fitness records (PHI) for the duration of mHealthcare emergency with minimum privacy disclosure. In an efficient user-centric privacy get entry to manage in SPOC framework, which is primarily based on an attribute-based totally get right of entry to manage & a new privacy retaining scalar product computation (PPSPC) method, & allows a scientific person to come to a decision who can participate inside the opportunistic computing to assist in handing out his overwhelming PHI facts. I have additionally verified the proposed SPOC framework can stability the high-in depth PHI procedure & transmission & minimizing the PHI privacy disclosure in m-Healthcare emergency.

In the paper A Privacy Enhanced Search Approach for Cloud-Based Medical Data Sharing[5] This paper proposes a privacy stronger search approach for cloud-primarily based scientific statistics sharing. The proposed answer implements a hybrid search method, in which the quest process is carried out throughout plaintext&ciphertext. The stepped forward get entry to manage can ensure the privacy protection of cloud information. The statistics recipient utilizes the proposed approach to recognize the report-level clinical data get admission to, i.e., to discover one or a couple of involved EMRs within the shared clinical dataset. Since symmetric encryption algorithms are greater efficient than uneven algorithms, in my implementation, a combination of each is being used. The information is encrypted using efficient symmetric key cryptography. This key's in flip encrypted with the recipient's public-key so that it is able to most effective be used by the legal users through the records proprietor. This way the advantages of both algorithms can be used.

III. FRAMEWORK

A. Overview of Proposed System

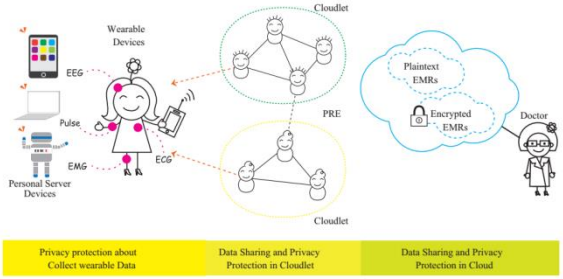


Fig.1: System Architecture

From the fig1, I describe about the proposed framework. The client's physiological data are first collected by wearable devices such as smart clothing.

In the proposed system, the body data gathered by means of wearable devices are transmitted to the nearby cloudlet. Those statistics are in addition added to the far cloud where doctors can get admission to for disease analysis. According to records delivery chain, we separate the privacy safety into 3 stages. In the primary stage, person's crucial signs collected by means of wearable gadgets are delivered to a closet gateway of cloudlet. During this level, records privacy is the principle subject. In the second level, person's records might be similarly delivered closer to far off cloud via cloudlets. A cloudlet is formed by way of a positive quantity of mobile gadgets whose owners may also require and/or share some particular records contents. Thus, both privacy safety & statistics sharing are considered on this degree. Especially, I use consider version to assess trust stage among users to decide sharing statistics or now not. Considering the customer's scientific facts are stored in faraway cloud, I classify these medical statistics into specific types & take the corresponding security policy. In addition to above three tiers based totally information privacy protection; I additionally keep in mind collaborative IDS based totally on cloudlet mesh to guard the cloud environment.

B. Content Sharing & Privacy Protection

First, I introduce the encryption system for user's privacy statistics, which prevents the leakage or malicious use of customer's non-public facts for the duration of transmissions. Next, I present the identification management of customers who want to get right of entry to the health facility's healthcare statistics. Thus, I can assign one of a kind customers with exceptional ranges of permissions for information get right of entry to, at the same time as avoiding statistics get right of entry to beyond their permission degrees. Finally, we give an software of the use of customer's non-public data, that's beneficial to each users&doctors. Based at the healthcare big data stored inside the far flung cloud, a disorder prediction model is constructed based on choice tree. The predictions will be suggested to the users&medical doctors on call for.

C. Collaborative Intrusion Detection

In order to defend medical records, I also increase an intrusion [8][9] detection device on this paper. This phase presents a singular scheme to construct a collaborative IDS machine to discourage intruders. In the subsequent, I first recollect what occurs if the gadget is tormented by extraordinary attacks, whilst detection costs for character IDS range with the cloudlet servers.

D. Bloom Filter

Bloom filters have a robust area benefit over other information systems for representing sets[11], consisting of self-balancing binary search trees, hash tables, or simple arrays or linked lists of the entries. It is a space-efficient based totally data shape this is probabilistic in nature. Initially, this technique changed into used when the amount of facts for use was impractically big.

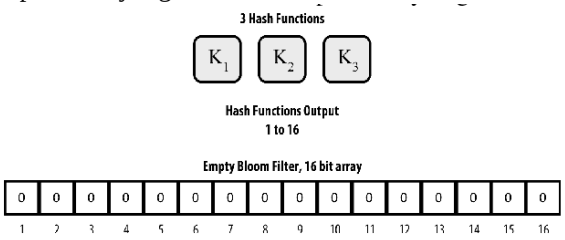


Fig.2: Bloom filter example

Bloom clear out is a probabilistic records shape which tells us that the given query key-word is both genuinely now not inside the set or can be in the set. The base data structure of a bloom filter is a Bit vector[11]. Each empty mobile in that desk represents a chunk and the quantity under it its index. To add a word to the Bloom filter, we without a doubt hash it some instances and set the bits within the bit vector at the index of these hashes to one. When a question keyword is fired through the person we actually hash the string with the same hash features see if those values are set within the bit vector. If those bits aren't set I can sincerely say that elements aren't inside the set.

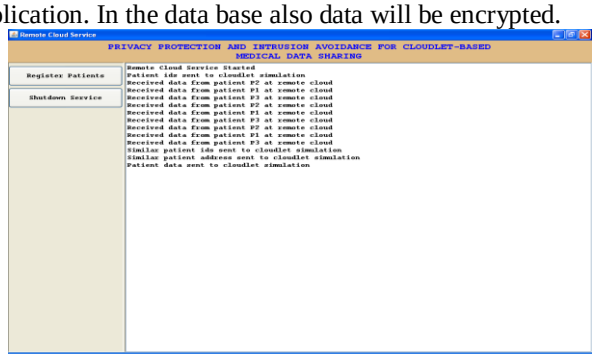
IV. EXPERIMENTAL RESULTS

In my experiment, I have to add some patients in the application by using registration process. After adding the users, I have to run the cloudlet simulation[2].

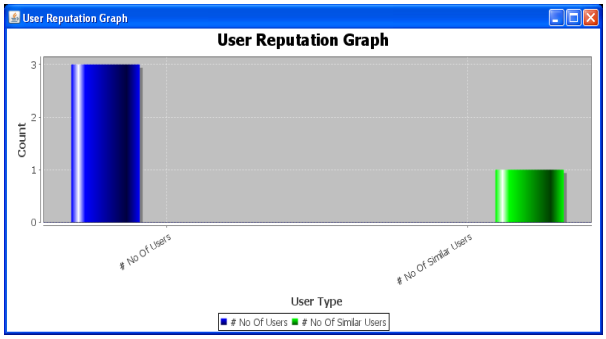
In this simulation I will get that many patients as I add at the remote cloud server. When I start the simulation, then sensor starts sending data to nearest cloudlet& can stop sending data to cloud let if it required.

Next, after sending data to the sensor, I can view the similar diseases patients&also can view the doctor shared data. But, here the data displayed in the form of encryption.

Here, the patients can login&they can access their data&these patient's data will be saved in the database of the proposed application. In the data base also data will be encrypted.



I can see the different operations done by the remote cloud server.



I observed that the user reputation graph to generate graph of total no of patients versus no of patients with similar disease.

V. CONCLUSION

In this paper, Ievolved a device which does no longer permit users to transmit information to the far off cloud in attention of secure collection of facts, as well as low communication cost. However, it does permit customers to transmit records to a cloudlet, which triggers the facts sharing problem in the cloudlet. Firstly, we will utilize wearable gadgets to acquire user's statistics. Secondly, for the reason of sharing records

inside the cloudlet, I use believe model to measure customer's consider level to choose whether to share personal information or not. Thirdly, for privacy-maintaining of far off cloud records, I partition the records stored within the faraway cloud & encrypt the statistics in one of a kind methods, if I want to now just make sure facts protection but additionally accelerate the efficiency of transmission and to increase the efficiency we also generating a Bloom filter hash code. Finally, I advocate collaborative IDS based on cloudlet mesh to defend the complete system.

VI. REFERENCES

[1]. Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao&Long Hu, "Privacy Protection&Intrusion Avoidance for Cloudlet-based Medical Data Sharing", DOI 10.1109/TCC.2016.2617382, IEEE Transactions on Cloud Computing

[2]. K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for tele-home healthcare," in

[3]. Engineering in Medicine and Biology Society, 2004.IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2.IEEE, 2004, pp. 5384–5387.

[4]. Ning CaoCong Wang, , Ming Li, Kui Ren,&Wenjing Lou," Privacy-Preserving Multi Keyword Ranked Search over Encrypted Cloud Data", IEEE transactions on parallel&distributed systems, vol. 25, no. 1, january 2014.

[5]. Rongxing Lu, Xiaodong Lin,and Xuemin (Sherman) Shen ," SPOC: A Secure&Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE transactions on parallel&distributed systems, vol. xx. 2012.

[6]. Lu Liu, Jingchao Sun, Jianqiang Li, Rong Li, Juan Li, Xi Meng, Huifang Li&Jijiang Yang," A Privacy Enhanced Search Approach for Cloud-Based Medical Data Sharing "Research Institute of Information Technology,2015 IEEE International Conference on Smart City/SocialCom/SustainCom together with DataCom 2015.

[7]. M. Shamim Hossain, "Cloud-Supported Cyber–Physical Localization Framework for Patients Monitoring", Article in IEEE Systems Journal · September 2015.

[8]. H. Mohamed, L. Adil, T. Saida,&M. Hicham, "A collaborative intrusion detection&prevention system in cloud computing," in AFRICON, 2013. IEEE, 2013, pp. 1–5.

[9]. Y. Shi, S. Abhilash,&K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions&network attacks," in The Third IEEE International Conference on Mobile Cloud Computing, Services,&Engineering,(Mobile Cloud 2015). IEEE, 2015.

[10]. E.Vasilomanolakis, S. Karuppayah, M. Muhlh auser,&M. Fischer, ¨ "Taxonomy&survey of collaborative intrusion detection," ACM Computing Surveys (CSUR), vol. 47, no. 4, p. 55, 2015.

[11]. P.K.Rajendran, B.Muthukumar,&G. Nagarajan, "Hybrid intrusion detection system for private cloud: a systematic approach," Procedia Computer Science, vol. 48, pp. 325–329, 2015.

[12]. One-hashing bloom filter, 2015 IEEE 23rd International Symposium on Quality of Service (IWQoS).