



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURING PATIENTS DATA STORAGE IN REAL WORLD CLOUD

RALLABANDI SRI LAKSHMI KAMESWARI ^{#1}, L. SOWJANYA ^{#2}

^{#1} MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

^{#2} Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT :

In current days cloud has gotten one of the entrancing area so as to store and recover all the information from the distant machines rather from the neighborhood machines. With the notoriety of wearable gadgets, alongside the improvement of mists and cloud hand held innovation, there is a colossal increment for the clinical consideration so as to store and access the data distantly. Because of the rising innovation every single clinical organization attempt to store and access data inside the cloud worker, which leaves a way for the gatecrasher to hack the information un-approved way. So in this paper we attempt to recognize the gatecrasher who attempt to change or adjust the patient data illicitly during information stockpiling.

KEYWORDS : emerging technology, cloud server, hack , unauthorized manner.

1. INTRODUCTION

With the improvement of human services large information and wearable innovation [1], just as distributed computing and correspondence advancements [2], cloud-helped social insurance enormous information processing gets basic to satisfy clients' evergrowing needs on wellbeing counsel [3]–[5]. Be that as it may, it is provoking issue to customize explicit social insurance information for different clients in a helpful style [6]. Past work recommended the blend of interpersonal organizations and social insurance administration to encourage [7] the hint of the infection treatment process for the recovery of realtime sickness data [8]. Human services social stage, for example, PatientsLikeMe [9], can get data from other comparable patients through information partaking as far as client's own discoveries. In spite of the fact that sharing clinical information on the interpersonal organization is valuable to the two patients and specialists, the delicate information may be spilled or taken, which causes protection and security issues [10] [11] without productive insurance for the mutual information [12]. Hence, how to offset security insurance with the comfort of clinical information sharing turns into a difficult issue. With the advances in distributed computing, a lot of information can be put away in different mists [13], including cloudlets [14] and far off mists [15], encouraging information sharing and serious calculations [16] [17]. In any case, cloud-based information sharing involves the accompanying major issues:

- 1) How to ensure the security of client's body information during its conveyance to a cloudlet?
- 2) How to ensure the information partaking in cloudlet won't cause protection issue?

As can be anticipated, with the expansion of electronic clinical records (EMR) and cloud-helped applications, an ever increasing number of considerations ought to be paid to the security issues in regards to a distant cloud containing human services enormous information. Instructions to make sure about the social insurance large information put away in a far off cloud?How to successfully shield the entire framework from malevolent assaults

2. LITERATURE SURVEY

Writing review is the most significant advance in programming improvement process. Before building up the device it is important to decide the time factor, economy n organization quality. When these things r fulfilled, ten subsequent stages are to figure out which working framework and language can be utilized for building up the apparatus. When the developers begin constructing the instrument the software engineers need parcel of outside help. This help can be gotten from senior developers, from book or from sites. Before building the framework the above thought r considered for building up the proposed framework.

1. Protecting your right: Attribute-based keyword search with fine-grained owner enforced search authorization in the cloud.

AUTHORS: W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li

Writing review is the most significant advance in programming improvement process. Before building up the device it is important to decide the time factor, economy n organization quality. When these things r fulfilled, ten subsequent stages are to figure out which working framework and language can be utilized for building up the apparatus. When the developers begin constructing the instrument the software engineers need parcel of outside help. This help can be gotten from senior developers, from book or from sites. Before building the framework the above thought r considered for building up the proposed framework

Achieving secure, scalable, and fine-grained data access control in cloud computing

AUTHORS: S. Yu, C. Wang, K. Ren, and W. Lou

Distributed computing is a developing figuring worldview in which assets of the registering foundation are given as administrations over the Internet. As promising as it seems to be, this worldview additionally delivers numerous new difficulties for information security and access control when clients re-appropriate delicate information for sharing on cloud workers, which are not inside a similar confided in space as information proprietors. To keep delicate client information classified against untrusted workers, existing arrangements as a rule apply cryptographic techniques by unveiling information decoding keys just to approved clients. Be that as it may, in doing as such, these arrangements definitely present an overwhelming calculation overhead on the information proprietor for key dispersion and information the executives when fine-grained information get to control is wanted, and therefore don't scale well. The issue of at the same time accomplishing fine-grainedness, adaptability, and information classification of access control in reality despite everything stays uncertain. This paper tends to this difficult open issue by, on one hand, characterizing and authorizing access arrangements dependent on information properties, and, then again, permitting the information proprietor to assign the vast majority of the calculation errands associated with fine-grained information get to control to untrusted cloud workers without revealing the hidden information substance. We accomplish this objective by misusing and extraordinarily consolidating strategies of quality based encryption (ABE), intermediary re-encryption, and lethargic re-encryption. Our proposed plot additionally has striking properties of client get to benefit classification and client mystery key responsibility. Broad investigation shows that our proposed conspire is profoundly proficient and provably secure under existing security models.

Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption

AUTHORS: M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou,

Individual wellbeing record (PHR) is a rising patient-driven model of wellbeing data trade, which is frequently redistributed to be put away at an outsider, for example, cloud suppliers. In any case, there have been wide protection worries as close to home wellbeing data could be presented to those outsider workers and to unapproved parties. To guarantee the patients' authority over access to their own PHRs, it is a promising strategy to encode the PHRs before redistributing. However, issues, for example, dangers of protection presentation, versatility in key administration, adaptable access, and proficient client renouncement, have remained the most significant difficulties toward accomplishing fine-grained, cryptographically authorized information get to control. In this paper, we propose a novel patient-driven structure and a set-up of instruments for information get to control to PHRs put away in semitrusted workers. To accomplish fine-grained and versatile information get to control for PHRs, we influence property based encryption (ABE) strategies to scramble every patient's PHR record. Unique in relation to past works in secure information redistributing, we center around the different information proprietor situation, and separation the clients in the PHR framework into various security areas that significantly lessens the key administration unpredictability for proprietors and clients. A serious extent of patient protection is ensured all the while by misusing multiauthority ABE. Our plan additionally empowers dynamic alteration of access strategies or document qualities, underpins productive on-request client/trait disavowal and break-glass access under crisis situations. Broad systematic and test results are introduced which show the security, versatility, and productivity of our proposed plot.

3. EXISTING SYSTEM

Till now there is no concept of cloud integrated in medical domain. So the following are the limitations which takes place in the existing cloud server. They are as follows:

LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They is as follows:

1. All the existing cloud servers try to store and access the data in a plain text manner .
2. There is no concept like integrating cloud in medical domain for storing and accessing the data to and from the cloud server.
3. There is no concept like intrusion detection system in the current cloud servers which leaves a way for the intruders to hack the sensitive data of the patients.

All the primitive cloud servers failed to achieve the principle of data integrity.

4. PROPOSED METHODOLOGY

The purpose of medical data sharing is to make better use of data between users. The paper proposed data sharing strategy among several clouds, which used encryption method based on attribute to realize data sharing under semi-trusted cloud environment. In the proposed system we try to use the cloud server for storing the medical data. Here we try to provide a communication between doctor and patient regarding the diseases and cure related information. In this proposed approach we try to use an intrusion detection system in which if any user who is not having any authorized profile creation, try to change any patient information. Then at that case the user account will be blocked and the same System IP address is blocked for permanently not to re-enter into the Account.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. It is an efficient authenticated structure.
2. It is the first practical proved its security in the field of medical domain
3. All the data is stored in an encrypted manner so if any patient or doctor want to view the request or response, they need to send request for the cloud admin and then they need to view the data.

There is a high level of security to block un-authorized user not to enter into the account.

5. MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed protocol. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server. The application is divided mainly into following 5 modules. They are as follows:

- 1) System Construction Module
- 2) Patient Module
- 3) Doctor Module
- 4) Cloud Server Module
- 5) Intrusion Detection Module

Now let us discuss about each and every module in detail as follows:

5.1 System Construction Module

The system construction module mainly contains the roles like single cloud server and multiple doctors and multiple patients. Here the doctor and patient need to be registered first in order to login into the system and once they are registered they will be authenticated by the cloud admin. Once the patient or doctors gets authorized by admin they can login into the system to perform the operations.

5.2 Patient Module

Here the patient is one who got registered into the application and once they get authorization from admin they can login into the system and perform some operations like request the files from doctor from the cloud server which is stored in an encrypted manner. Once if the cloud server approves then only they can view in a plain text manner

5.3 Doctor Module

Here the doctor is a person who initially register into the application and once they get authorized by admin they will login and add the patient details into the cloud in an encrypted manner. The doctors are one who can view the data about patients and they can give prescription for the patients.

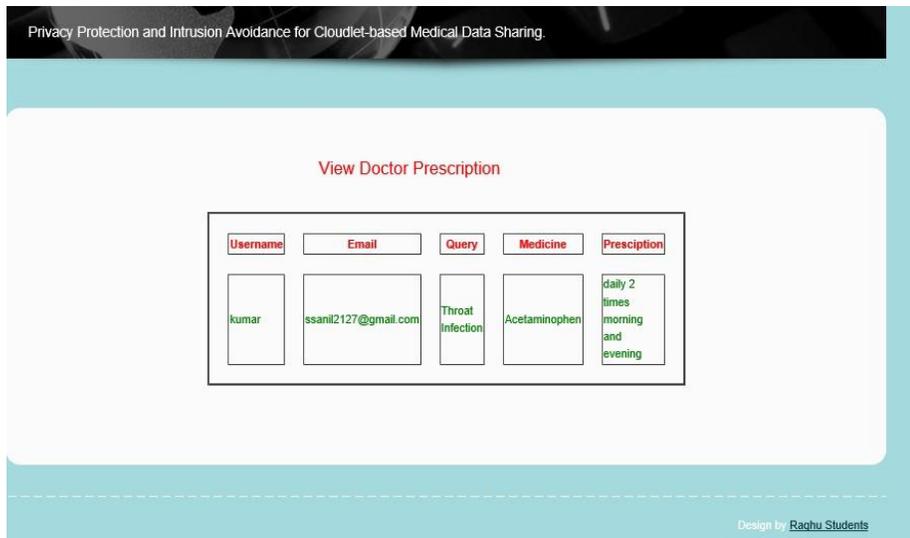
5.4 Cloud Server Module

Here cloud server module is one which can store all the information in an encrypted manner and this will give authorization for the end users. This will try to store all the data in a secure manner and try to store the data in a encrypted manner. This will verify the user identities and then try to download the data.

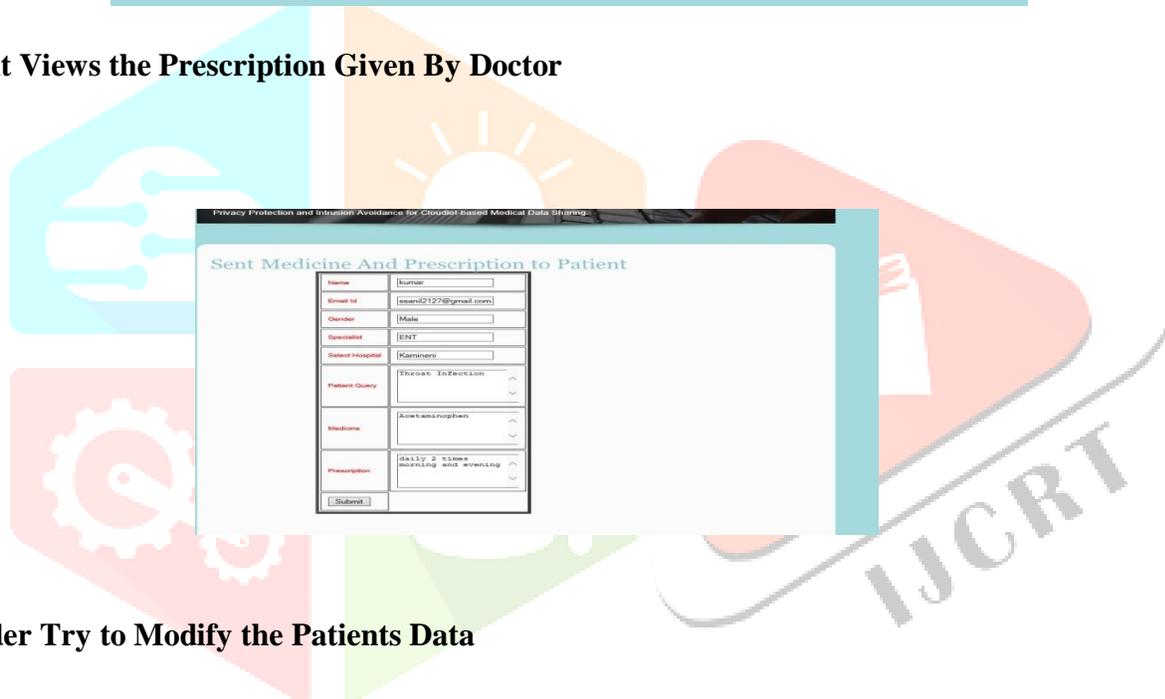
5.5 IDS Module

This module is used to identify the attacker who try to attack the data by editing the patients data. So if any intruder try to illegally enter and modify the patients data which is present in the cloud will be identified by this module.

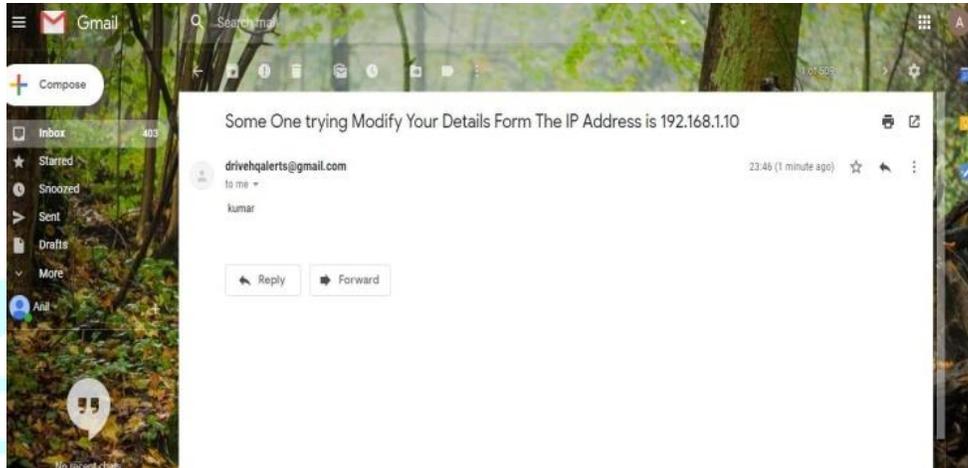
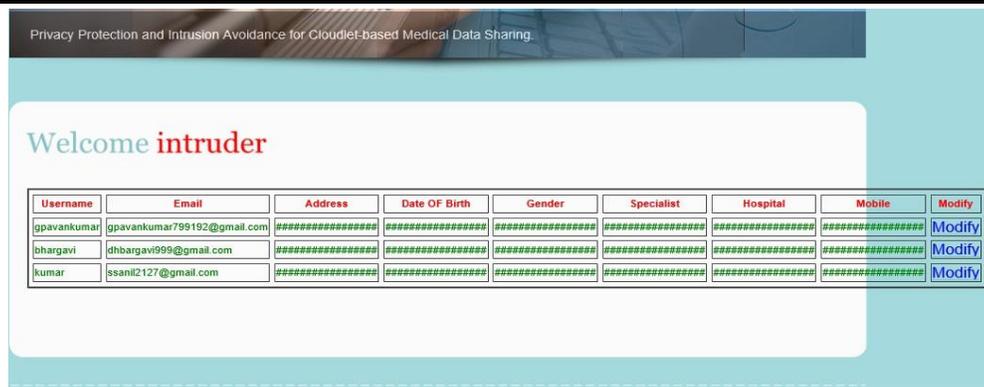
6. RESULTS WITH SCREEN SHOTS



Patient Views the Prescription Given By Doctor



Intruder Try to Modify the Patients Data



7. CONCLUSION

In this project, we examined the issue of security insurance and sharing huge clinical information in cloudlets and the distant cloud. We built up a framework which doesn't permit clients to send information to the distant cloud with regards to make sure about assortment of information, just as low correspondence cost. Here we can distinguish the gatecrasher who attempts to make assault on the delicate information of one patient who don't approach alter the substance. This application can ready to distinguish such a things in exact way

8. 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 centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.
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. 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. "https://www.patientslikeme.com/."
10. 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.
11. 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.
12. 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, 2014.2168-7161 (c) 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
13. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2016.2617382, IEEE Transactions on Cloud Computing
14. T. Xu, W. Xiang, Q. Guo, and L. Mo, "Mining cloud 3d video data for interactive video services," Mobile Networks and Applications, vol. 20, no. 3, pp. 320–327, 2015.
15. M. Quwaider and Y. Jararweh, "Cloudlet-based efficient data collection in wireless body area networks," Simulation Modelling Practice and Theory, vol. 50, pp. 57–71, 2015.
16. K. Dongre, R. S. Thakur, A. Abraham et al., "Secure cloud storage of data," in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.
17. M. S. Hossain, G. Muhammad, M. F. Alhamid, B. Song, and K. Al-Mutib, "Audio-visual emotion recognition using big data towards 5g," Mobile Networks and Applications, pp. 1–11, 2016.