[NC-Rase 18]
DOI: 10.5281/zenodo.1485432

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

DESIGN EFFECTIVE INTRUSION DETECTION SYSTEM FOR CLOUDLET-BASED MEDICAL DATA SHARING AND SECURE DATA TRANSMISSION BY USING 3DES HYBRID ALGORITHM.

Ms Mayuri S Taley[*1] & Prof A.P.Kankale[2]
[*1]ME Student, Rajashri Shahu College of Engineering, Buldana ,India
[2]Assist.Professor & Head , Dept. of Computer Science, Rajashri Shahu College of Engineering, Buldana, India

ABSTRACT

With the development of clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information .Practically, medical data sharing is a critical and challenging issue. In proposed System, design IDS to protect healthcare system by utilizing the flexibility of cloudlet Technology.In Proposed paper focus on design efficient E-healthcare system by using 3 DES hybrid algorithm.

Keywords: *Cloud Computing, E-Healthcare, EHR, etc .*

I. INTRODUCTION

In the current society, the transfer of information using internet is rapidly raising up, because it is easier and faster and has also proved security to transfer the data to destination. Security is a very important issue while transferring the sensitive data via internet because any unauthorized user can tamper the data and may make it useless or obtain the information unintended to him, especially in telemedicine. With the proliferation of patient's digital health records, and an increasing number of data breaches, protecting patient information is of utmost importance, with this respect lot of work has been done to secure medical data[1][2].

II. GOAL

- The goal of the project is to detecting attacks and preventing the system from attackers.
- We are providing a multistage detection to more precisely detect the possible attackers and a text-based Turing test with question generation module to challenge the suspected requesters who are detected by the detection module.
- When client attacks on server system our system detects that attack and blocks that client and that pattern of attack is stored at admin side.
- If another client attacks with same pattern then that client is detected and blocked. Admin performs Turing test for client by generating questions**.**

III. BACKGROUND

The Cloud Computing paradigm offers eHealth systems the opportunity to enhance the features and functionality that they offer. However, moving patients' medical information to the Cloud implies several risks in terms of the security and privacy of sensitive health records.

In this paper, the risks of hosting Electronic Health Records (EHRs) on the servers of third-party Cloud service providers are reviewed. To protect the confidentiality of patient information and facilitate the process, some suggestions for health care providers are made. Moreover, security issues that Cloud service providers should address in their platforms are considered[1][2].

IV. PROBLEM STATEMENT

The implementation of these systems has been growing rapidly. Purpose of guarding the privacy of sensitive patient information.

The patient's consent is required to manage and access this data, except in the case of an emergency where the patient's life is at risk.

EHRs, anyone working in a clinical practice could potentially access, view and copy protected health information without leaving a trace. On paper, illegal accessing of files are more difficult to spot.

V. PROPOSED SYSTEM

The proposed method is much stronger cryptosystem than the traditional methods. This work, presents an efficient approach to provide well-protected security for patients data. Unlike other healthcare solutions, this system utilizes paillier and homomorphic encryption of patient‟s health type thereby providing advanced security to the patient data. When comparing with the existing method, there is certain amount of overhead concerning the time required for individual health rate encryption computation but the overall outcome is satisfactory and precise[1][2]. However using this system, patient‟s sensitive health data are strongly secured and thereby not easily compromised. Hence this proposed scheme is very efficient both for doctors and medical researchers and they can view patient‟s records ubiquitously. Doctors are provided with highly secured and efficient storage of hospital data; hence patient‟s data are accessed securely. This method can solve the issue of protecting patient‟s private information against unauthorized viewers and provide high level of protection[7][8].

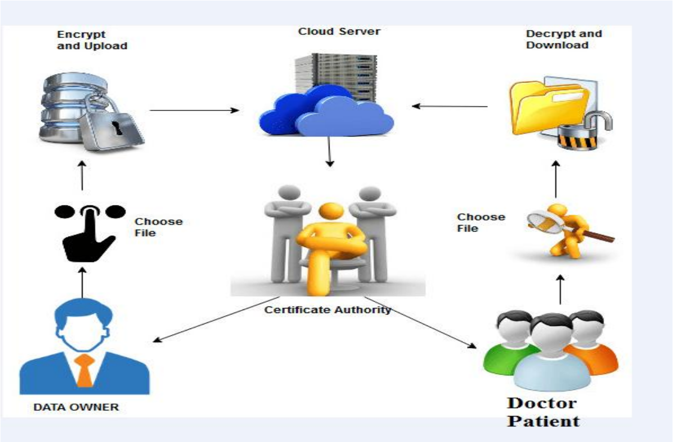
- There may be need of evaluating hospital performance based on its patients‟ health records, without disclosing the details of all patient records.
- Patient may want to use a web service that stores , maintains all his/her medical records in a centralized place.
- Cloud1, cloud2, doctor(user) login to access the data. Once the attacker attacker the data will not sent directly and bypass by intermediate cloud to send the data. Cloud1 and Cloud2 can share that sensitive data (doctor too)[1][4].

Advantages of proposed system:

- 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[1][5].
- In order to share data in the cloudlet, we use users' similarity and reputation to build up trust model. Based on the measured users' trust level, the system determines whether data sharing is performed.
- 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.

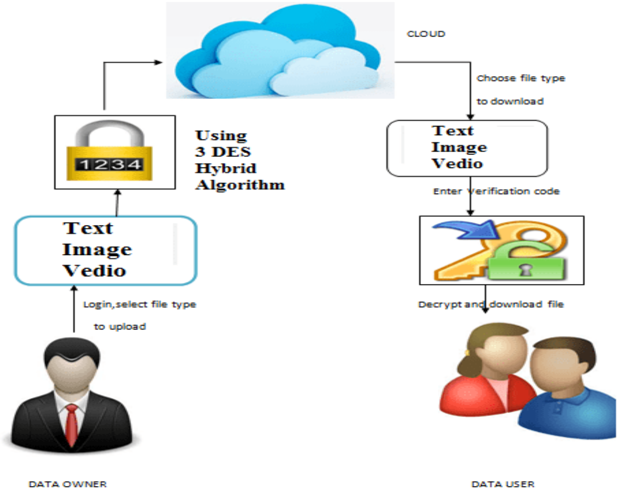
ISSN 2348 – 8034
Impact Factor- 5.070

VI. PROPOSED ARCHITECTURE



VII. PROPOSED METHODOLOGY

In hospitals, documents consisting of sensitive patient information, that is stored digitally and security of such documents are very much essential. Privacy of such sensitive information can only be guaranteed, if it is encrypted by the data owner before it is being stored in data centers. In this work, the high end security is provided for the patient‟s sensitive data thereby ensuring maximum privacy for the patients.[1][5][6]



The users of this system are doctors and researchers. For registration, doctor needs to provide his username and password. Thereafter doctor can either view or needs to enter the patient‟s details such as name, age, health type etc. The users should be able to perform the following functions using this system:

By Doctor Register to medical database

- Login using a user name and password
- View all the patients‟ record.
- Enter patients details [name, age, health type etc]

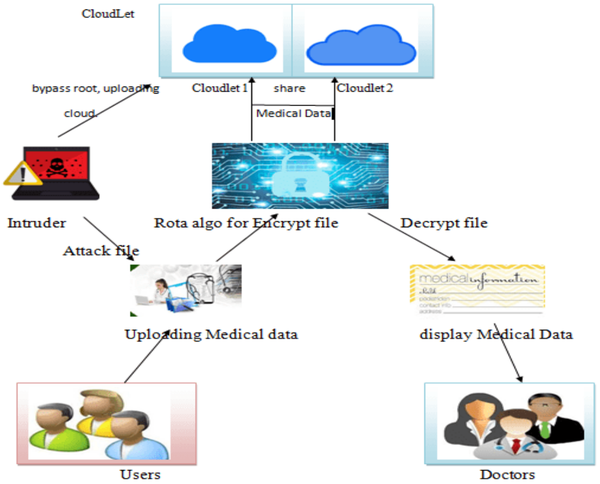
By Pathology Lab

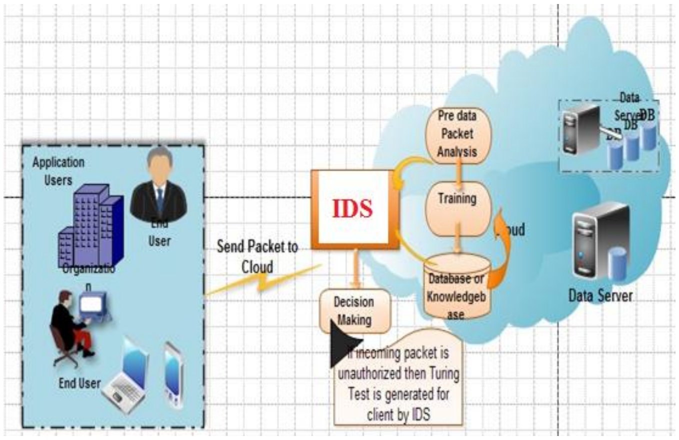
Register to medical database

- Login using a user name and password
- View his or her patients record based on required health type Add or delete patients record based on required health type

Controller (Admin): Controller is the administrator who is the owner of this system. The administrator is responsible for maintaining medical database. Admin will assign user name and password. The administrator can perform the following functions:

- Register genuine doctor and researchers
- Maintains patients database





Intrusion Detection System Architecture

The system architecture consists of intrusion detection, alert clustering, threshold check, intrusion response and blocking and cooperative agent. In case of intrusion detection, it drops attacker packet, then sends alert message about the attack detected by itself to other region. Alert clustering module collects alert produced by other regions. The decision about alert whether it is true or false is identified after calculating severity of collected alerts. This approach is suitable for preventing Cloud system from single point of failure caused by DDoS attack. However, the computational effort is

Increased[4][6][7].

Intrusion Detection Module

1) Checking source

In this module we are checking the source of attack. We are providing authentication for client for login. If client attacks with some pattern then by identifying that clients IP address we finding its source.

2) Counting

In this module we are recording the source address destination address and the time at which client performs login test. After login successful the counting module is reset. It will be enable by the Attack Detection module when there are some suspected traffic been detected.

3) Turing Test Module

In this module the client is provided with some CAPTCHA code which client will input through keyboard, doing this admin will understand that the client is a human not a machine.

4) Question Generation Module

In this module if client fails to perform Login then admin will ask some questions which client has to answer perfectly. The question will be stored by admin at the time of client registration.

System requirements

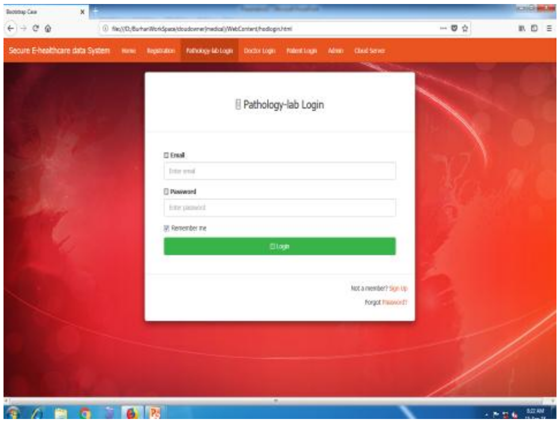
Hardware requirements:

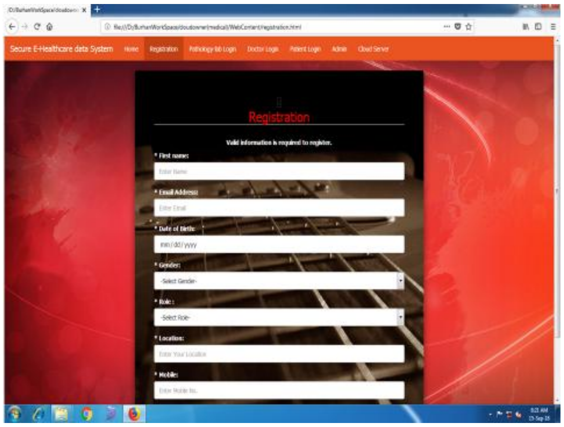
- Processor : i3
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

Software requirementss

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

VIII. OUTPUT SCREEN




/D:/BurhanWorkSpace/cloudown
file:///D:/BurhanWorkSpace/cloudowner(medical)/WebContent/registration.html
Secure E-Healthcare data System
Home
Registration
Pathology-lab Login
Doctor Login
Patient Login
Admin
Cloud Server
8:21 AM
15-Sep-18

Registration

Valid information is required to register.

* First name:
Enter Name

* Email Address:
Enter Email

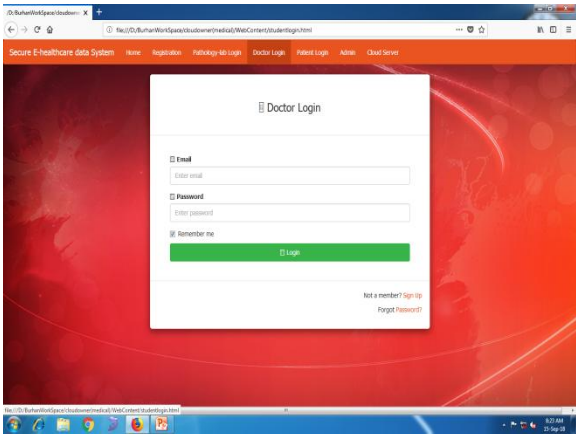
* Date of Birth:
mm/dd/yyyy

* Gender:
-Select Gender-

* Role :
-Select Role-

* Location:
Enter Your Location

* Mobile:
Enter Mobile No.


/D:/BurhanWorkSpace/cloudown
file:///D:/BurhanWorkSpace/cloudowner(medical)/WebContent/studentlogin.html
Secure E-healthcare data System
Home
Registration
Pathology-lab Login
Doctor Login
Patient Login
Admin
Cloud Server
file:///D:/BurhanWorkSpace/cloudowner(medical)/WebContent/studentlogin.html
8:23 AM
15-Sep-18

Doctor Login

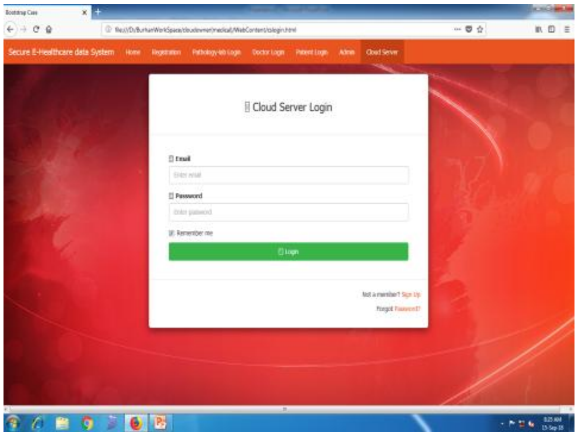
Email
Enter email

Password
Enter password

☑ Remember me

Login

Not a member? Sign Up
Forgot Password?



Cloud Server Login

Email
Enter email

Password
Enter password

☑ Remember me

Login

Not a member? Sign Up
Forgot Password?

.

IX. CONCLUSION

- The proposed method is much stronger cryptosystem than the traditional methods. This work, presents an efficient approach to provide well-protected security for patients data.
- Finally this method can be improved by distributing encrypted data by using 3 DES Algorithm to different data servers without being compromised even if any one of the data server gets attacked.
- Proposed collaborative IDS can achieve a detection rate of 95%, which is a considerable improvement over the single IDS approach

X. FUTURE ENHANCEMENT

Future enhancement is IoT base remote cloud system where doctors can access data for disease diagnosis. A cloudlet based healthcare system.

REFERENCES

1. *Min Chen, Senior Member, IEEE, Yongfeng Qian, Jing Chen, Kai Hwang, Fellow, IEEE, Shiwen Mao, Senior Member, Long Hu, “Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing”, IEEE Transactions on Cloud Computing, 2017.*
2. *Ms Mayuri S Taley, Prof A.P.Kankale “A Survey on Cloudlet-based Medical Data Sharingand Secure Data Transmission “, International Journal of Ongoing Research in Science and Engineering (IJORSE)Volume 2 Issue 9 SEPT 2018,ISSN 2456-8481.*
3. *Liping Zhang, Shaohui Zhu, and Shanyu Tang, “Privacy protection for Telecare Medicine Information Systems Using a Chaotic Map-Based Three-Factor Authenticated Key Agreement Scheme”, IEEE Journal of Biomedical and health informatics, Vol. 21, No. 2, March 2017.*
4. *Shu-Di Bao, Meng Chen, Guang-Zhong Yang, “A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications”, IEEE, DOI 10.1109/JBHI.2017.2679979, 2017.*
5. *Wenbing Zhao, RoannaLun, Connor Gordon, Abou-BakarFofana, Deborah D. Espy, M. Ann Reinthal, Beth Ekelman, and Glenn Goodman, Joan Niederriter, ChaominLuo, XiongLuo, “A Privacy-Aware Kinect-Based System for Healthcare Professionals ”, IEEE, February 2016.*
6. *Lingjia Liu, RachadAtat and Yang Yi, “Privacy Protection Scheme for eHealth Systems: A Stochastic Geometry Approach”, IEEE, September 2016.*
7. *Abdelali El Bouchti, Samir Bahsani, TarikNahhal, ”Encryption as a Service for Data Healthcare Cloud Security”, IEEE 5th International Conference on Future Generation Communication Technologies, July 2016.*
8. *Tzu-Wei Tseng, Cheng-Yi Yang, Chien-Tsai Liu, “Designing Privacy Information Protection of Electronic Medical Records”, IEEE2016 International Conference on Computational Science and Computational Intelligence, April 2016.*
9. *Jisha S, Mintu Philip, “RFID based Security Platform for IOT in Health Care Environment”, IEEE Online International Conference on Green Engineering and Technologies ,(IC-GET) 978-1-5090-4556-3/16 , 2016*