The Cloud Computing Approach for Secured Health Maintenance Record of Patient's Using Attribute Vector Algorithm

Manasa k chigateri[1], Arun Kumar G[2]

[1]*M.Tech student, Electronics and Communication Engineering Department, STJIT College, Ranebennur, Haveri, Karnataka ,India*
[2] *Associate Professor, Electrical and Electronics Engineering Department, IBRICT, Oman*

---***---

Abstract- ***Nowadays, health is more important for every human life exits in earth for survival. Death rate grows increasing because of non-availability of hospitals in rural areas, not sufficient medical equipment and moreover doctors are not free to work in rural region. Hence in order to reduce death rate, cloud approaches are implemented to provide direct facility to the patients without going to clinics and take tablet in home itself. Branching tree, bilinear property and some cryptographic tools are effective to preserve the patient's record whenever it desired. Along with text, images are also used to indicate the description and symptoms of particular patients after fully loading image. Finally without loss of information, by generating secret keys then only information about healthcare is obtained.***

Keywords: *Data safety, Intellectual property, Maintenance record, IBE, MDRQ, provider, user, STA, SaaS.*

1. INTRODUCTION

In primary 20's, medicinal maintenance was brought by straight calls by surgeons at patient's home. Later, healthcare systems changed radically with the introduction of cloud computing. The "MediNet" is a project designed by the Microsoft to recognize remote observing on the health position of diabetes and cardiovascular diseases in remote areas in Caribbean nations [1]. PD indicator progression, a representing between dysphonia measures and UPDRS. PD is based on speech so that they are classified as daily living part and motor part. Some nerves are considered [2]. Worldwide health checking organization uses dissimilar illnesses connected incomes for tele-health. Wireless knowledge now occurs as an authenticity for calculating numerous illnesses and regulatory through diverse gadgets. 95% populates on earth are expending mobile phone to convey and obtain the info for specific facilities sources [3]. Computing approaches are progressed to offer not only secrecy but also harmless defense and care best of separate data. Reliability of statistics comprises together official and illegal statistics of patient's, though genuine statistics is more used to escape the fake records. Safety is a significant issue in all types of communication networks such as social broadcasting associated with different networks which all of it under several servers [7]. The digital world moves always around the profit and advantage of personally identified data which contains the stored detailed information. Collection of individual data increases day by day and more precautions are undertaking to create awareness. The person sample consists of their tallness, weightiness in terms of kg, blood categories, DNA profiles, and fingerprints. The more important information of the person is identified by the DNA samples and fingerprints. Re-isolating data is one which shows the difference between the two or more samples of the people [8]. CAM system architecture is efficient to build and maintaining and also controlling the records of patients by using private keys. Cloud serves as medicinal resource agent and saves various recent applications [9].

2. EXISTING METHODS

2.1 Anonymization Technique

Old-style privacy safety mechanisms by basically eradicating users' individual self-data or by using anonymization method flops as a current way in dealt with confidentiality of Health schemes due to the cumulative amount and variety of private recognizable info. Usually, the secrecy matter is commenced with anonymization technique that is *k*-anonymity or *l*-diversity. Nevertheless, it has been specified that these expositions might be inadequate to avoid re-identification incidence.

2.2 R e -encryption Algorithm

It is a process of transforming cipher text encrypted under sender's key to a different cipher text under recipient public key and also used for data sharing.

2.3 Cloud Computing Technique

" Cloud Computing is a ideal for empowering global, suitable, on request net admittance to a communal group of configurable calculating incomes that can be quickly provisioned and free with nominal association strength or provision supplier interface". The network of network provider's remote access to a set of distributed resources.it is a network storing space and consists of computer resource. There are three types of cloud providers namely:

a. Software as a Service (SaaS): A SaaS source offers subscribers contact together incomes and requests. SaaS makes it needless for you to have a physically copy of software to connect on your strategies. It also brands it easier to have the identical software on all of your strategies at once by retrieving it on the cloud.

b. Platform as a Service (PaaS): A PaaS provider gives subscribers access to the components that they require to progress and operate applications over the internet. A PaaS system goes a level above the Software as a Service setup.

c. Infrastructure as a Service (IaaS): In an IaaS contract, the subscriber totally contract out the storage and assets, such as hardware and software. It completely deals through computational organization.

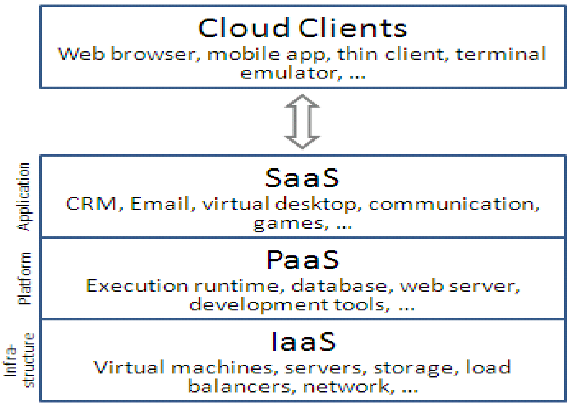

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig -1: SaaS, PaaS, IaaS outline.

3. SYSTEM ARCHITECTURE

Health checking system contains of four parts such as company, server, and client, finally STA (semi-trusted authority).Let us explain one by one.

a) Company: It is healthcare centre else hospital. It supplies the secret information and also all remedial records of operator every time it is needed; a client refers an enquiry to key server. Store is shifted in between company and server.

b) Server: Server offering as a cloud which preserves all the actions of demanded info from the client. Hence it is so-called healing storing assets. Query is recognised between the client and server.

c) STA: Secret keys are dispersed around clienteles and locating medicinal payment service area since client through some ideal (e.g. pay per use). Token are produced by means of these key, it is likely to access the statistics record. TokenGen is found in the mid of client and STA.

d) Client: Clients gets the deposited info from server through company and change those into attribute vectors. Code texts are reverted to client and original arrangement made among STA and company.

Roles of different phases

- **1st phase (setup):** Frist settings are done through setup which achieves the system concerns. This is accomplished by STA.
- **2nd phase (store):** After settings, company does Store procedure which assignments the result of cryptograph texts with the help of encoding function.
- **3rd phase (TokenGen):** Secret keys are made as attribute vector such as V = (v1, v2, v3...vn). Token are accepted to clients for safety so no loss of information.
- **4th phase (Query):** Queries are an enquiry which is led by the client to server. Then server reacts with the essential outcomes to demands.

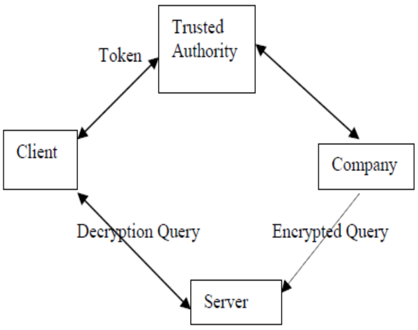


Fig -2: System Architecture.

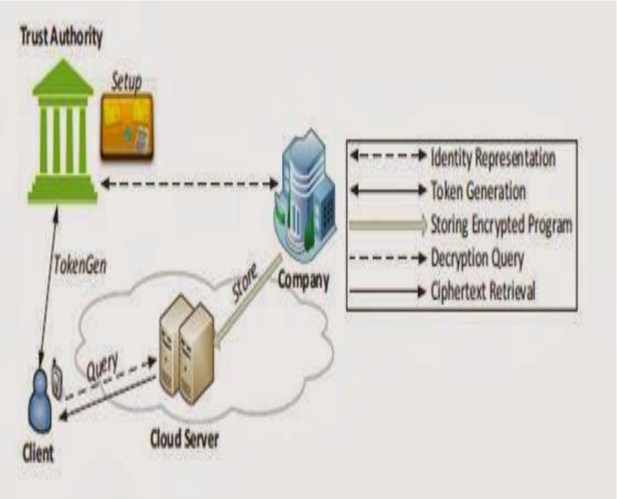


Fig -3: Block Diagram of client, server, company and STA.

3.1 Working

To meet the design aim, we need to review a few systems. Since that querying input to a diagnostic program frequently consists of a client's ID and attributes, we think the recently appeared attribute-based techniques derived to provide some feasible solutions. In this section, we discuss some of the security tools and offer the basic modifications to meet our design needs.

A. Splitting Sequencer

Frist demonstrate how a splitting tree performs. By scrutiny program announced in the MediNet plan to build a splitting database as shown in Fig.4. The MediNet drives to offer deliberate modified nursing provision for patients with diabetes or cardiovascular pollutions [1]. Customers entail of systolic blood pressure (BP) as contribution to database whether some of the patients do not remember to take every day tablets or have an uneven intake, and the energy intake of physical drive to the required conservation arrangement, then return a reference situations are established by trades which covers all the info.

By taking a simple example, consider a hypertension patient gives an input as attribute vector consisting "BP: 145, (indicating he/she not took the medicine), Energy Spending: 870 kcal, salt consumption: 900 milligrams]". The reference returned from the checking program which specifies the client needs to "inform that adjust day to day diet, and take proper medicine, moreover intake of salt content is less.

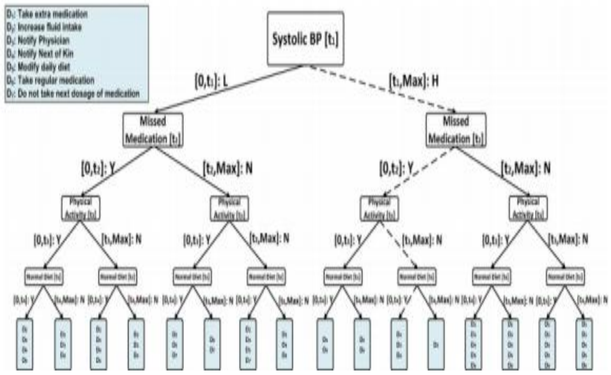


Fig -4: Splitting sequence.

B. Bilinear Mixture

Bilinear mixture is serious for project, which turns as the edifice block of the scheduled secure healthcare inspection system. Based on connection, Boneh and Franklin suggested the identity based encryption (IBE), which started an advanced research way in current years. A combination is an effectively calculated as E=G*G --→Gt, the bilinearity function: for all the finite field modulo Q, G and Gt are all multiplicative sets of prime rule generated by g and e (g, g) and, respectively. G- Generator polynomial, E- encryption.

C. Multidimensional Range Query Based on Anonymous IBE

As per verified previously, a Health watching database can be considered as a second resolution tree starting from the attribute vector planetary. So, an attribute vector can be exclusively matched to a binary minute slab per definite quantization of the restrained data, leading to a binary bit signified tree (second tree). Thus, the multidimensional range query (MDRQ) scheme can be useful to design our Healthcare Watching System. MDRQ was first suggested by Shiet al. and was additional improvement is done by us to model a reputation-based encryption scheme. The simple clue of MDRQ is as follows: a -level second tree is employed to denote the -bit data (or the range).

D. Module Description

Execution is the period of the mission when the speculative design is twisted out into a occupied system. Thus it can be measured to be the greatest serious period in realizing a prosperous innovative structure and in generous the user, assurance that the innovative structure will ready to employ and be operative.

The execution stage involves careful planning, examination of the existing system and it's restrictions on execution, designing of methods to achieve exchange and evaluation of changeover methods.

Modules:

- Provider
- Semi Trusted Authority
- User's

Provider: Provider/Doctor has to give brief description about the health and tell the precautions about the drugs and keep the information in cloud to get security.

Semi Trusted Authority: STA has to give security to the cloud by providing generated key so that authorized users who is having key has to view the information about the health.

User's: If user is having diseases he want to view information about the health so user will access those information from the cloud if the key is generated by STA, it means that user is authorized person. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy.

E. Software Design

- **Class diagram**

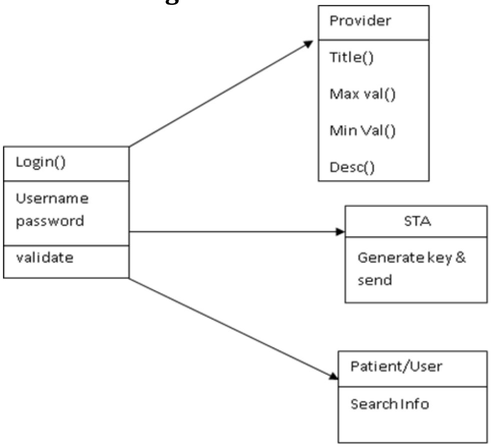


Fig -5: Class diagram.

Here in the above fig.5, the user, provider or STA can entered the login page by using username and password and checks for correct result. Provider includes max and min values, title of the diseases and also description.

F. Data flow diagram

The DFD is also known as bubble chart. It is a modest graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

Some of the software that use is listed as follows:-

- Java
- JavaDatabase Connectivity(JDBC)
- JDBC drivers
- Packages
- Swings.

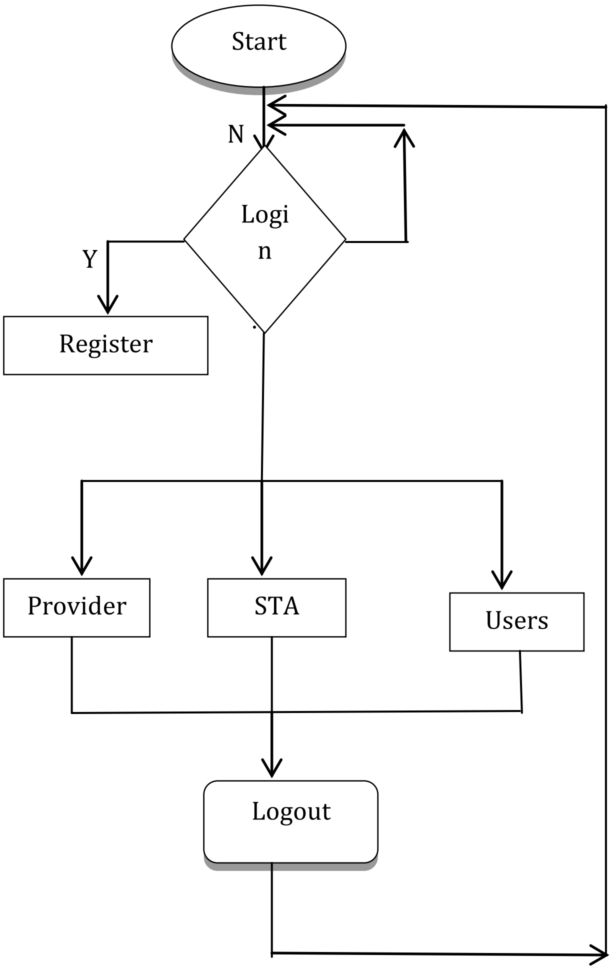


Fig -6: Program flow chart

4. RESULTS AND ANALYSIS

The yield form of an info system should complete one or more of the following objectives.

- ❖ Express info about former activities, up-to-date position or forecasts.
- ❖ Forthcoming indication.
- ❖ Indicator vital actions, occasions, difficulties, or notices.
- ❖ Generate an act.
- ❖ Approve an act.

System Evaluation Testing: Testing is a serious element which guarantees quality and effectiveness of the proposed system is satisfying in meeting its purposes. Testing is done at various stages in the System designing and operation process with an objective of evolving a clear, flexible and protected system. Testing is a primary part of software expansion. Testing is a process involves constructing of test cases, against the tested samples.

System Testing and Acceptance Testing: System testing is really a series of dissimilar tests whose major determination is to entirely use the computer-based system. Comprise saving from testing during smashes, security testing for illegal user, etc. Acceptance testing is occasionally achieved with realistic data of the client to exhibit that the software is working adequately. This testing in FDAC focuses on the exterior manners of the system.

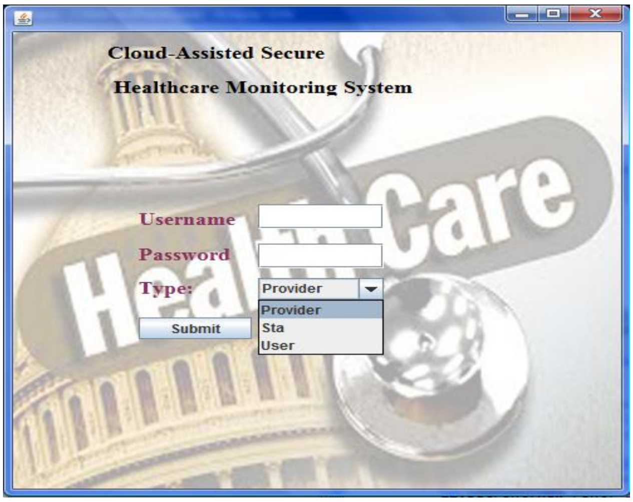


Fig -7: Front end JAVA Platform

Here, with reference to the above fig .9 Java software is used to implement the patient's record. It includes the username password and also types such as provider, STA and user. Submit button is used to accept the different types.

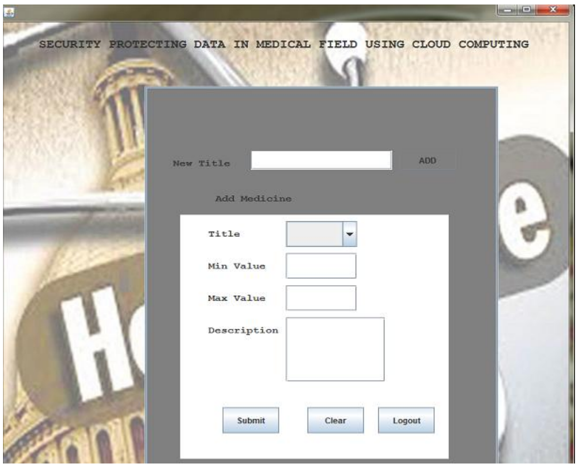
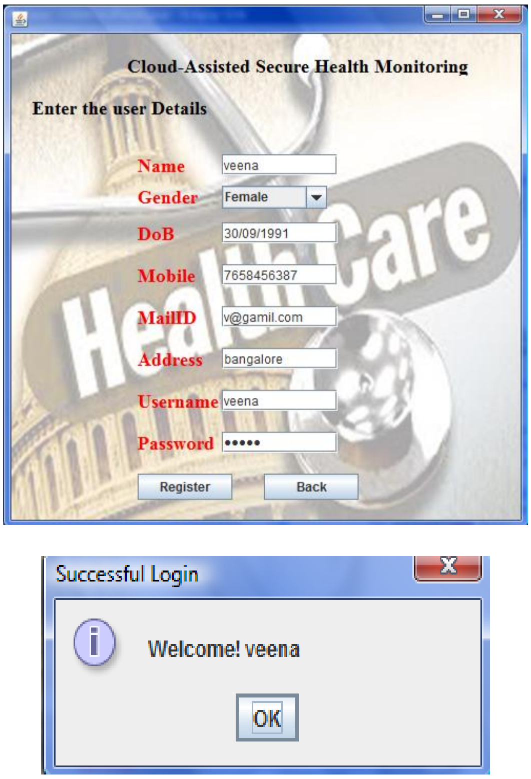


Fig -8: Provider's Module JAVA Platform

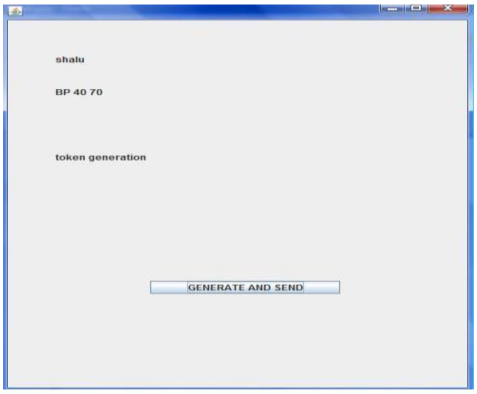


Name veena
Gender Female
DoB 30/09/1991
Mobile 7658456387
MailID v@gamil.com
Address bangalore
Username veena
Password •••••

Welcome! veena

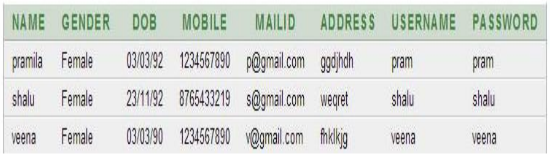
Fig -9: User Details Entry JAVA platform

Here, from all the above fig(8,9) provider gives the information about the which disease and then enters the min and max values of that disease.it includes clear button to refersh the perious data, submitt button to save the particular information and finally logout button to come out of the provider.s page. User data entry consists of name,gender,DOB,address,cell number,email-id,username and password.These contains are entered and used for futher purpose.To provide securecy password are kept confidentiality.

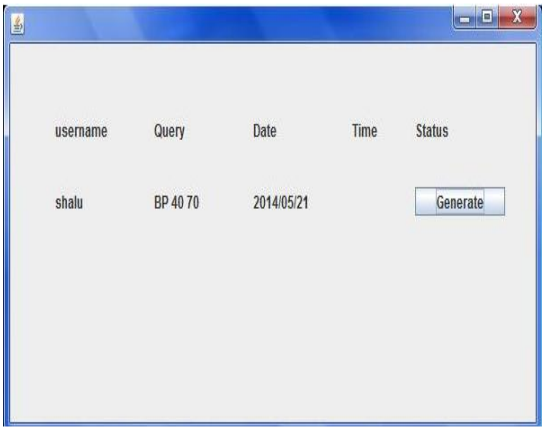

shalu

BP 40 70

token generation

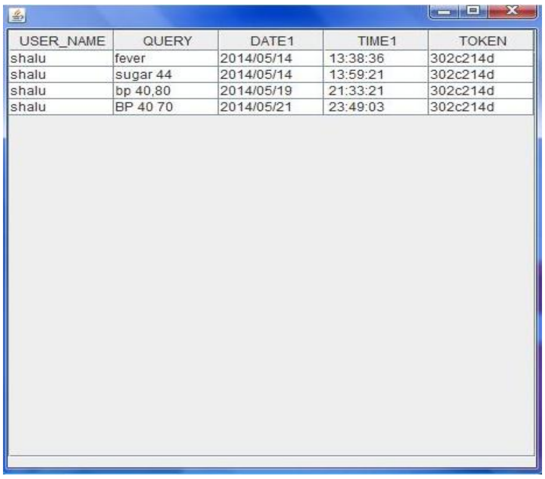


NAME	GENDER	DOB	MOBILE	MAILID	ADDRESS	USERNAME	PASSWORD
pramila	Female	03/03/92	1234567890	p@gmail.com	ggdjhdh	pram	pram
shalu	Female	23/11/92	8765433219	s@gmail.com	weqret	shalu	shalu
veena	Female	03/03/90	1234567890	v@gmail.com	fhklkjg	veena	veena



username	Query	Date	Time	Status
shalu	BP 40 70	2014/05/21		Generate

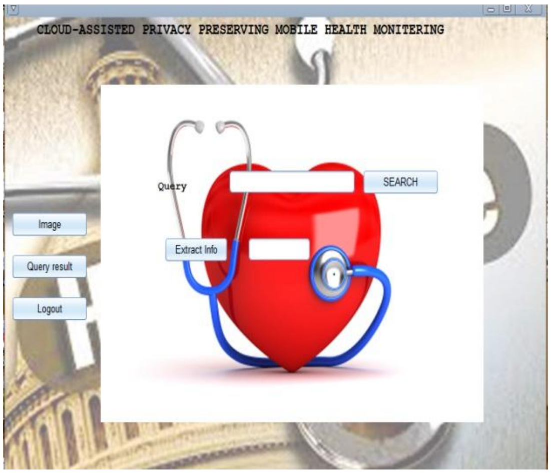
Fig -10: Generated key and sending schme.



USER_NAME	QUERY	DATE1	TIME1	TOKEN
shalu	fever	2014/05/14	13:38:36	302c214d
shalu	sugar 44	2014/05/14	13:59:21	302c214d
shalu	bp 40,80	2014/05/19	21:33:21	302c214d
shalu	BP 40 70	2014/05/21	23:49:03	302c214d

Fig -11: Output of query table.

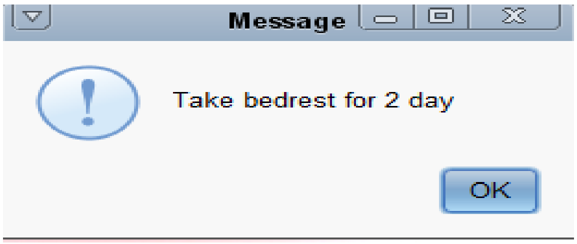
Fig.11 shows the key generation and sending scheme method for entered data to check out appropriate disease.Moreover, key is kept secret so no matter of leaking of information thus safe the data. Token is generated and used for removing data. It also displays the qurey,date,time.



CLOUD-ASSISTED PRIVACY PRESERVING MOBILE HEALTH MONITERING

Fig -12: Image loading frame.

Here you can load your query or image

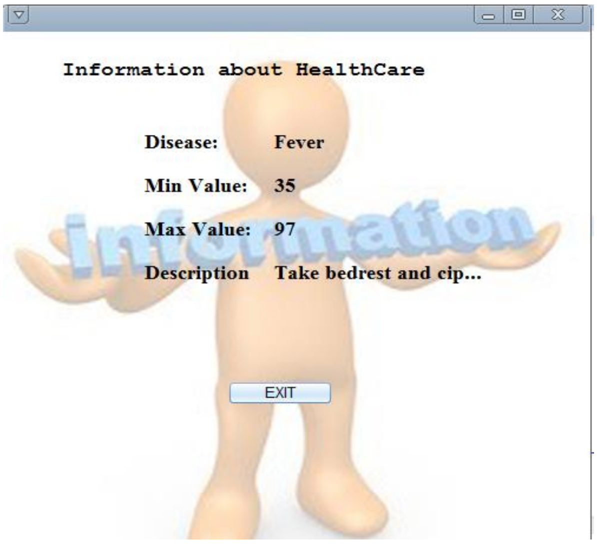


Message

Take bedrest for 2 day

Fig -13: Output of fever disease image.

Getting output here as take rest for 2days after uploading image as fever disease.



Information about HealthCare

Disease: Fever

Min Value: 35

Max Value: 97

Description Take bedrest and cip...

Fig -14: Result of fever query.

Here getting the outcome of image by loading which appropriate solution to the user. It shows that not only texts but also considered the images and provide the actual solutions to the desired requirements.

5. CONCLUSIONS

Among the various encryption methods IBE encryption is important and more powerful compare to other methods. Good results can be obtained from the cloud computing technique. Including both texts and images are enhanced to achieve the desired objective. Java platform assures the best workspace for evaluation and testing of any technical issues. Finally improvements in the health care maintenance record of user are accomplished through confidentiality. It was noticed from the study that health checking system provides maximum amount of advantages regarding maintenance of patients' record, regular precautions and medicines are taken at correct time. In rural region, there is no proper availability of doctors at that time they have makes use of this strategy. They have little awareness about the body health and not able to get proper diagnosis, moreover unaware of cleanliness.

6. SCOPE OF ENHANCEMENT

In future we can use encryption and decryption techniques for uploading the data into the cloud and compare it with existing system. By this comparison we can find the accuracy which one gives more privacy in cloud storage. We have proposed secure cloud architecture to address the user privacy problem in a cloud. It also uses images and videos of patient have to provide proper treating to particular diseases. Now Videos are also added in order to encapsulate the information about the patient's condition and giving satisfactory treatments at particular time basis.

Acknowledgement

I greatly acknowledge my project guide, Mr. Arun Kumar G, Associate Professor, Department of Electronics and Communication Engineering, Sri Taralabalu Jagadguru Institute of Technology, Ranebennur and for providing the required impetus and helping me for carrying out this project work successfully.

REFERENCES

[1] P. Mohan, D. Marin, S. Sultan, and A. Deen, "Medinet: Personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony", in Proc. 30th Ann. Int. Conf. IEEE Engineering in Medicine and Biology Society, 2008 (EMBS 2008), 2008, pp. 755–758.

[2] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests", IEEE Trans. Biomed. Eng., vol. 57, no. 4, pp. 884–893, Apr. 2010.

[3] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine", Ann. Rev. Medicine, vol. 63, pp. 479–492, 2012.

[4] L. Ponemon Institute, Americans' Opinions on Healthcare Privacy, 2010 [Online]. Available: http://tinyurl.com/4atsdlj.

[5] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, and P. D. Stefanis, "End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust", in Proc. Pervasive Health,2011, pp. 478–484.

[6] M. Delgado, "The evolution of health care it: Are current U.S. privacy policies ready for the clouds?", in Proc. SERVICES, 2011, pp. 371–378.

[7] E. B. Fernandez, "Security in data intensive computing systems", in Handbook of Data Intensive Computing. NewYork,NY,USA: Springer, 2011, pp. 447–466.

[8] X. Zhou, B. Peng, Y. Li, Y. Chen, H. Tang, and X. Wang, "To release or not to release: Evaluating information leaks in aggregate human-genome data", Computer Security-ESORICS 2011, pp. 607–627, 2011.

[9] H. Lin, J. Shao, C. Zhang, and Y. Fang, "CAM: Cloud-Assisted Privacy PreservingMobile Health Monitoring", 2013 [Online].Available:http://www.fang.ece.ufl.edu/drafts/cam.pdf.

BIOGRAPHIES

Manasa k chigateri has completed her B.E in E&CE discipline from Visvesvaraya Technological University at UBDTCE. She is recently completed M.Tech in Digital Communication and Networking from Visvesvaraya Technological University at STJIT. Ranebennur,Haveri,Katnataka, India.

Arun kumar G has completed his B.E in ECE discipline at Visvesvaraya University and M.Tech in Digital Communication & Networking at kuvempu University. He is recently working as Associate Professor in Dept. of EEE at IBRICT, Oman.