SECURITY AND PRIVACY IN SMART HEALTH: USING ABE AND AES

Aarti Kalshetti

Marathwada Mitra Mandal's College of Engineering, Karvenagar, Pune.

Manasi Patil

Marathwada Mitra Mandal's College of Engineering, Karvenagar, Pune.

Pranjali Nehe

Marathwada Mitra Mandal's College of Engineering, Karvenagar, Pune.

Ajinkya Shimpi

Marathwada Mitra Mandal's College of Engineering, Karvenagar, Pune.

Prof. Swapnil Shinde

Marathwada Mitra Mandal's College of Engineering, Karvenagar, Pune.

ABSTRACT:

SMART health (s-health) is the context-aware augmentation of mobile health in smart cities, and it provides an opportunity for accurate and efficient prevention of various diseases and accidents. As a kind of fundamental technologies in smart cities, the Internet has been widely applied to interconnect available medical resources and provide reliable and effective s-health services to the elderly and patients. Cloud-based s-health is expected to provide desirable health care in the near future. We will use Amazon EC2 cloud for storing our confidential data. However, s-health is still in its early stages and many concerns remain to be solved for practical applications. According to symptoms intensity system will suggest to go emergency department and showing nearest hospitals. In particular, data security and privacy issues have become the biggest concerns of people in s-health. For example, Usually, a patient expects his s-health documents (SHRs), such as blood pressure and pulse rate, to be accessible only through approved professional health care-givers. Whereas, either data security is breached or only coarse-grained access policies are permitted if traditional access control methods are adopted. The system is used by any Doctor, Patient and Pathology laboratories to obtain patient information and then store it for future use. The current system in use is a paper-based system. It is too moderate and can't give refreshed arrangements of patients inside a sensible time allotment. The expectations of the framework are to decrease over-time pay and increment the number of patients that can be dealt with precisely. Necessities proclamations in this record are both utilitarian and non-useful. This system will provide security and privacy to the patient history. To provide privacy for patient Treatment in this System we'll use CP-ABE and DES algorithm for encryption and decryption.

Keyword: Cloud computing, Data Security, Data privacy, Attribute-based encryption, AES.

I. INTRODUCTION

A health-care aim is to create a patient portfolio management scheme capable of tracking the medical history of their patients. This system is to facilitate the middle to retrieve, update, and report the patient information expeditiously, assisting physicians in turn to create timely, efficient diagnoses. At the same moment, to monitor their medical and financial management, the center can use this scheme. Currently, completely different departments within the aid center have their own separated systems resulting in the dearth of communications and also the inefficient information sharing. In the clinic department, Doctors must write down patient prescriptions and maintain paper records, as well as have no data on insurance plans for patients, the drugs department has got to keep the prescription and inventory records on their own system. While every system serves a particular purpose, there is no coordinating, assimilating and representing of data. The systems might have duplicate information that could be a waste of space.

The completely different systems might have different application programs that cause incompatible files. Due to these disadvantages of the present system, a health-care management system is proposed. Health-care management system is a database management system (DBMS), which is based on computer networks, using the advanced database technology to construct, maintain, and manipulate various kinds of data in a database system (DBS). We are also using cloud architecture. For this architecture we will using Amazons EC2 cloud. The major benefits of the software system square measure straightforward to retrieve and update info, efficient data sharing and communication, and reliable backup and security. Scheduling the appointment of patient with doctors to create it convenient for each. This system is easy to handle. If intensity of symptoms is high, then we suggest emergency appointment and also showing the nearest hospital [1].

II. LITERATURE SURVEY

Yinghui Zhanget.al. [1] stated related data in the encoded s-wellbeing records (SHRs). For another, it as a rule bolsters little quality universe, which places a bothersome impediment on viable arrangements of CP-ABE on the grounds that the measure of its open parameters develops directly with the span of the universe. To address these issues, we present PASH, a security-conscious s-wellbeing access control framework in which an expansive CP-ABE universe with incompletely covered access strategies is the primary solution. PASH covers ownership estimates of access agreements in encoded SHRs and uncovers only property names. To tell the truth, estate estimates transmit much more sensitive data in specific, PASH acknowledges an effective SHR decoding test requiring few bi-linear pairings. The universe of quality can be exponentially expanding and the scope of open parameters is small and coherent. Our safety inquiry shows that in the standard model, PASH is totally safe. Execution examinations and exploratory results demonstrate that PASH is more proficient and expressive than past plans.

Prachi Garg et.al.[2] proposed distributed computing is one of the quickly developing fields in the present situation. It tends to be characterized as virtual pooled servers that give application, foundation, and stage based application and different offices. The real point of this figuring innovation is that the customers utilize just what they need and pay as per their utilization. Be that as it may, a lot of information, of people and associations are situated at the cloud server; security for information is the significant worry in distributed computing condition. In this paper we work upon various cloud security properties for example respectability, secrecy, security to make the framework sufficiently secure on the two sides for example customer and server side. By applying every one of these properties on information we proposed a framework on two distinct conventions for example AES and DES and look at the outcomes on the two conventions.

Hossam Ahmed et.al. [3] States the eHealth associations are a noteworthy focus for programmers as they hold abundance of data. Current digital security answers for eHealth associations are not extensive and just ensure certain security layer. Along these lines; the requirement for a next age digital security arrangement is expanding, an answer that is keen, versatile and adoptable to challenges. The wide spread of security instruments and propelling innovation have given the required foundation to make an exhaustive eHealth security arrangement. Associating the correct security apparatuses together to guarantee the general security without influencing the system execution what's more, client efficiency is hard and requires uncommon setup. The arrange layer is a noteworthy focus for any eHealth association, this investigate has demonstrated a few system security measurements that need to be viewed as when planning and overseeing system security for an eHealth association. A definitive objective of this examination is to recognize the restrictions in the current eHealth association digital security arrangements uniquely the system layer and propose a cutting edge digital security answer for eHealth associations.

Nikunj Joshi and Bintu Kadhiwala [4] introducing the big data in the system. These days, numerous individuals get associated with each other in one virtual world known as "Digital Society" rather than physically associated. The collaboration of individuals with digital society parts, for example, web based life, web crawlers, web journals, sites - with their administrations, causes age of tremendous measure of information named as, "Large Data". With adaption of Big Data in banking, money, retail industry, human services, keen city, social media and IT parts, it has begun picking up significance along with many research difficulties, for example, heterogeneity, information life cycle the board, information handling, adaptability, security and protection, and information representation. Numerous security and protection issues developed with Big Data that are not liable to be illuminated by ordinary security arrangements. Thus, this article is meant to present by and large point of view depiction of security and protection issues of Big Data.

Sudipta Chandra et.al [5] proposed medicinal services information is progressively being digitized today and the information gathered today rolling in from all cutting edge gadgets, has achieved a huge volume everywhere throughout the world. In the US, UK and other European nations, social insurance information needs to be verified and Patient Health Records (PHR) should be ensured so re-ID of patients is impossible from essential data. Protection of medicinal services is an imperative angle administered by Healthcare Acts (for example HIPAA) and subsequently the information should be verified from falling into the wrong hands or from being broken by pernicious insiders. It is vital to secure existing human services enormous information conditions due to expanding dangers of ruptures and breaks from secret information what's more, expanded appropriation of cloud advancements. In this paper the current human services security situation in enormous information conditions has been outlined alongside difficulties confronted and security issues that need consideration. Some current methodologies have been portrayed to show present and standard headings to fathoming the issues. Since human services administration in the US has a solid concentrate on security and protection instead of different nations on this day, the paper centers around Acts and security rehearses in the US setting.

Yinghui Zhang et.al [6] Quality based encryption (ABE) has been generally examined as of late to help fine-grained get to control of shared information. Unknown ABE, which is an important thought to ABE, further shrouds the beneficiaries' characteristic data3 in ciphertexts in light of the fact that numerous traits are delicate and identified with the personality of qualified clients. In any case, in existing unknown ABE work, a client knows regardless of whether the characteristics and the approach coordinate or not just subsequent to rehashing decoding endeavors. What's more, the calculation overhead of every decoding is high as the computational expense develops with the multifaceted nature of the entrance recipe, which for the most part requires numerous pairings in the vast majority of the current ABE plans. Thus, this direct decoding technique in unknown ABE will endure a serious productivity disadvantage. Going for handling the test above, we propose a novel procedure called coordinate then-decode, in which a coordinating stage is furthermore presented before the decoding stage. This method works by registering unique parts in cipher texts, which are utilized to play out the test that if the trait private key matches the shrouded characteristics strategy in cipher texts without unscrambling. In our proposed development, the calculation cost of such a test is substantially less than one unscrambling task. The proposed development is turned out to be secure. What's more, the outcomes in reproduction tests demonstrate that the proposed arrangement is productive and pragmatic, which enormously improves the effectiveness of decoding in unknown ABE.

III. METHODOLOGY USED IN PROPOSED SYSTEM

A. METHODOLOGY

1. **Cipher text - Policy Attribute-Based Encryption:** A CP-ABE scheme consists of four fundamental algorithms:

Setup, Encrypt, Key Generation, and Decrypt, and one optional algorithm, Delegate [1].

• **Setup:** takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK [1].

• **Key Generation (MK, S):** uses the master key MK and a set of attributes S that describe the key and outputs a private key SK [1].

• **Encrypt (PK, M, A):** takes as input the public parameters PK, a message M, and an access structure A over a set of attributes. It will encrypt M and produce a cipher text CT such that only a user who possesses the set of attributes satisfying the access structure will be able to decrypt CT [1].

• **Decrypt (PK, CT, SK):** takes as input PK, a cipher text CT, which was obtained for an access policy A, and a private key SK for a set S of attributes. If the set S of attributes satisfies the access structure A, then the algorithm will decrypt the cipher text and return a message M [1].

• **Delegate (SK, S_):** takes as input a secret key SK for some set of attributes S and a set S_ ⊆S. It outputs a secret key SK_ for the set of attributes S_. CP-ABE thus supports flexible and fine-grained access control with health-care providers being able to access only relevant EHRs encrypted with access policies that satisfy their keys' attributes. Also, if a secret key is compromised, only EHRs that can be decrypted with that key will be compromised; other EHRs are still protected. The possibility of an adversary pretending to possess unauthorized attributes and the general issue of impersonation resistance of CP-ABE will be discussed in detail in future work [1].

2. AES algorithm

The AES encryption stage can be divided into three stages: the first round, the primary rounds, and the final round. In separate combinations, all stages use the same sub-operations as follows:

Initial Round:

AddRoundKey

- Main Rounds
  SubBytes
  ShiftRows
  MixColumns
  AddRoundKey
- Final Round
  SubBytes
  ShiftRows
  AddRoundKey

The main rounds of AES are repeated a set number of times for each variant of AES. AES-128 uses 9 iterations of the main round, AES-192 uses 11, and AES-256 uses 13[8].

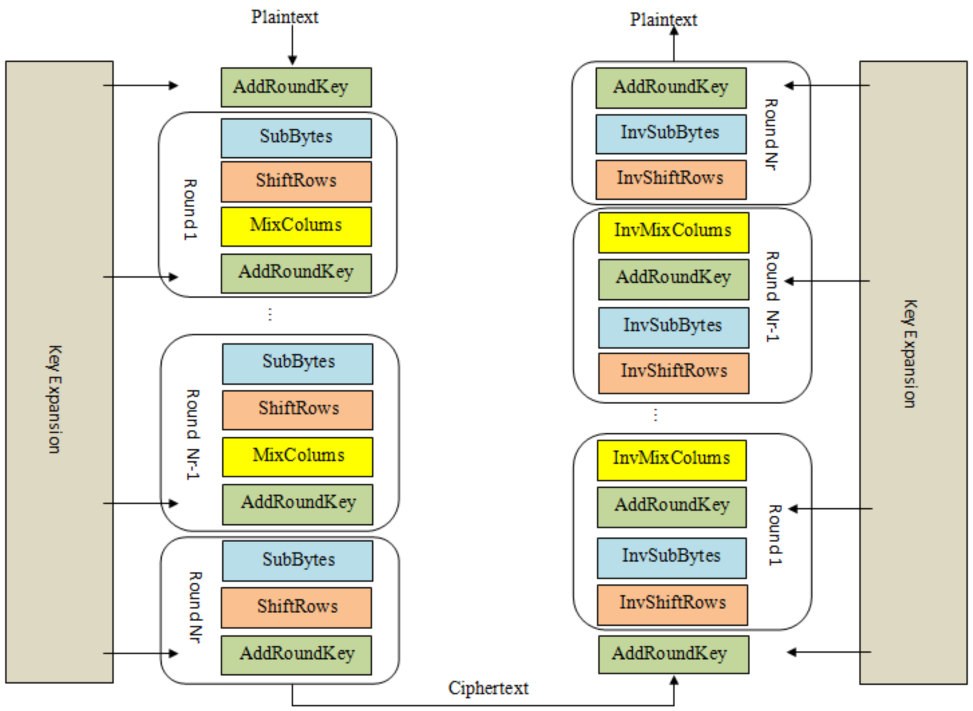


Figure 1: AES Algorithms [8]

B. PROPOSED SYSTEM APPROACH:

In existing system there was different database for different patient and which is manually. So there is take too much time for retrieving data vastly. No schedule for appointment when any patient is in emergency case. This system is time consuming not efficient way to handle patients. Not secure Computerize data about patients and hospital in the proposed system. Provide patient background with security and privacy. It should be able to manage patient test reports performed in the hospital's pathology lab. Patient information should be kept up-to-date and recorded for historical purposes in the system.

Scheduling an appointment for patient with doctors to make it convenient for both. To find the nearest hospital by patient.

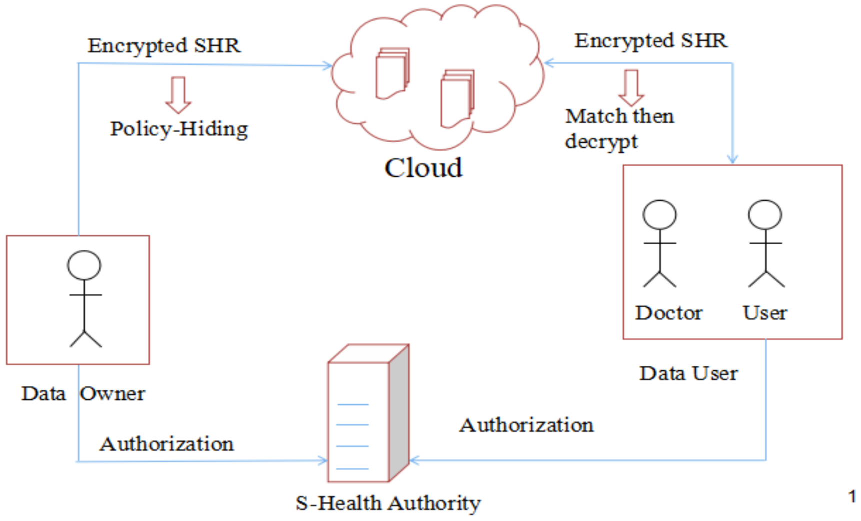


Figure 2: System Architecture

FLOW DIAGRAM:

Here Above diagram shows the actual flow of the system in our system which consists of Patient, doctor, pathologist and admin module. Patient first login to the system and enter the symptoms and book appoint of doctor. Doctor can login to the system and View appointment of patient and view symptoms. Then Pathologist does the test and makes prescription. Patient is request to send secret key to the view report then admin can send secret keys to the patient. After entering the secret key user can view result of test report.

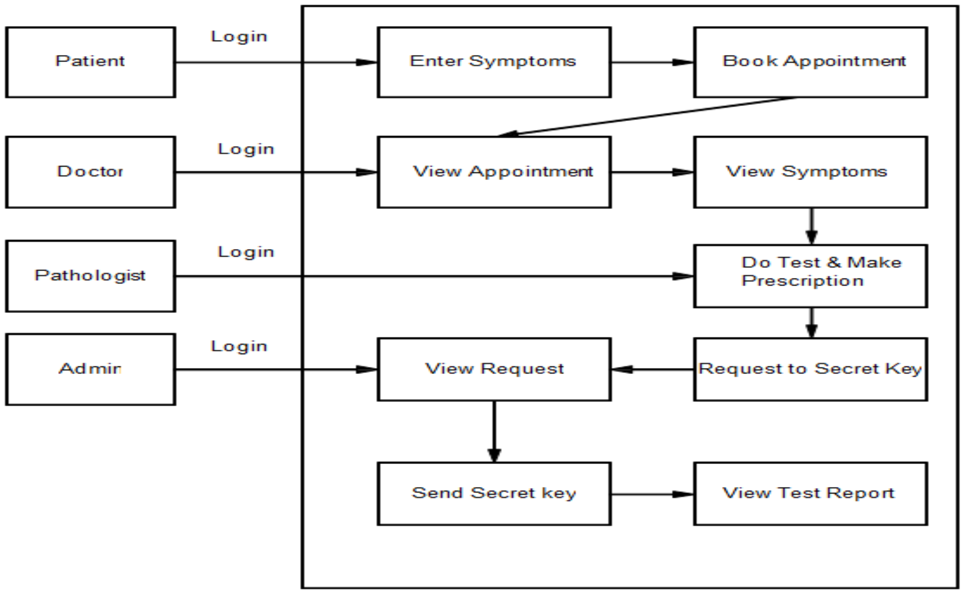
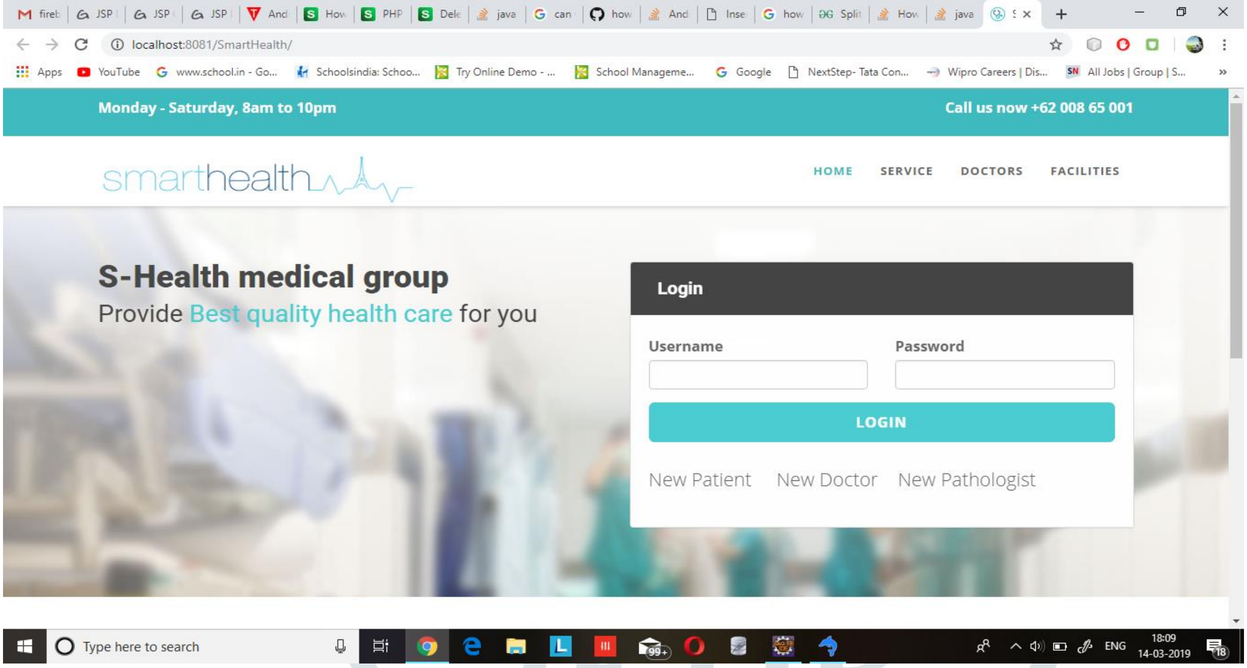


Figure 3: Flow Diagram

Output Screen

Home Screen



Monday - Saturday, 8am to 10pm

Call us now +62 008 65 001

S-Health medical group

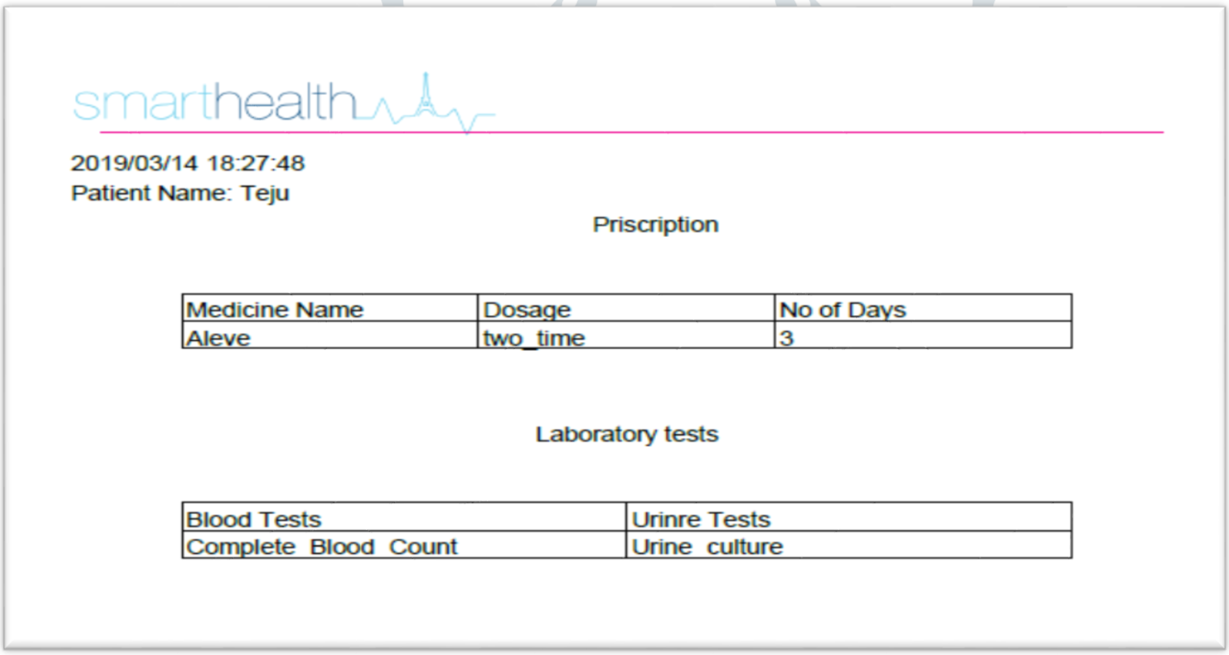
Provide Best quality health care for you

Username

Password

New Patient New Doctor New Pathologist

Generated Prescription



2019/03/14 18:27:48

Patient Name: Teju

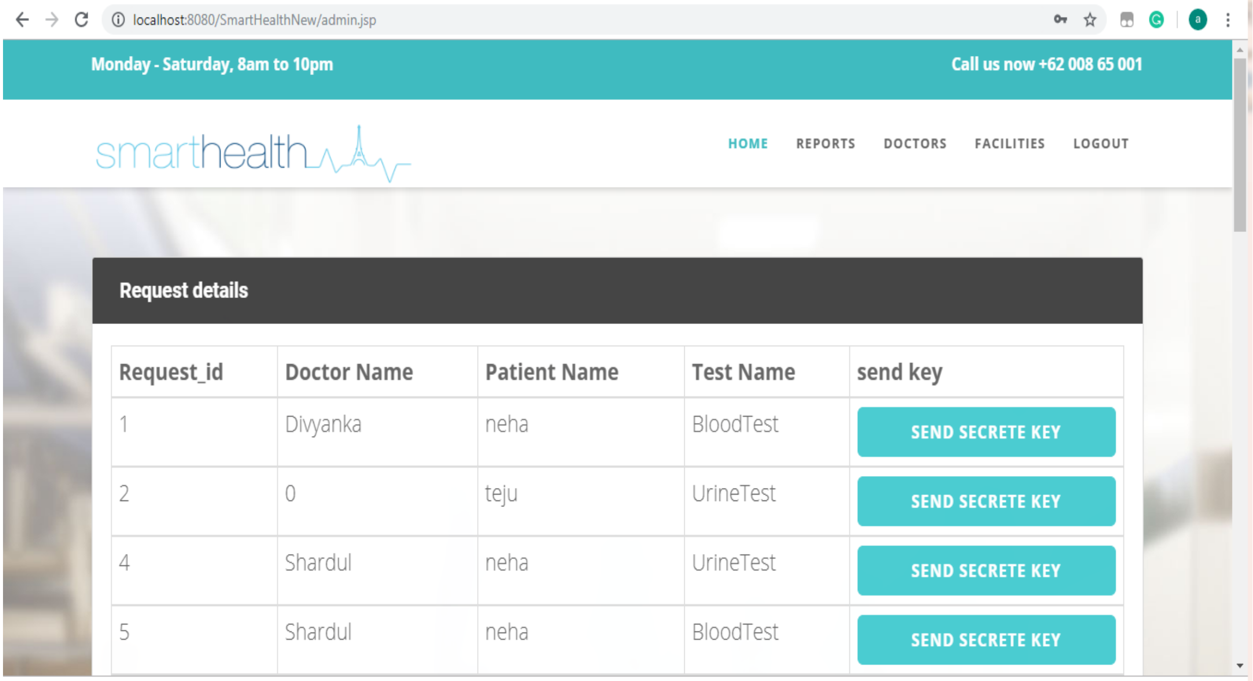
Priscription

Medicine Name	Dosage	No of Days
Aleve	two_time	3

Laboratory tests

Blood Tests	Urinre Tests
Complete Blood Count	Urine culture

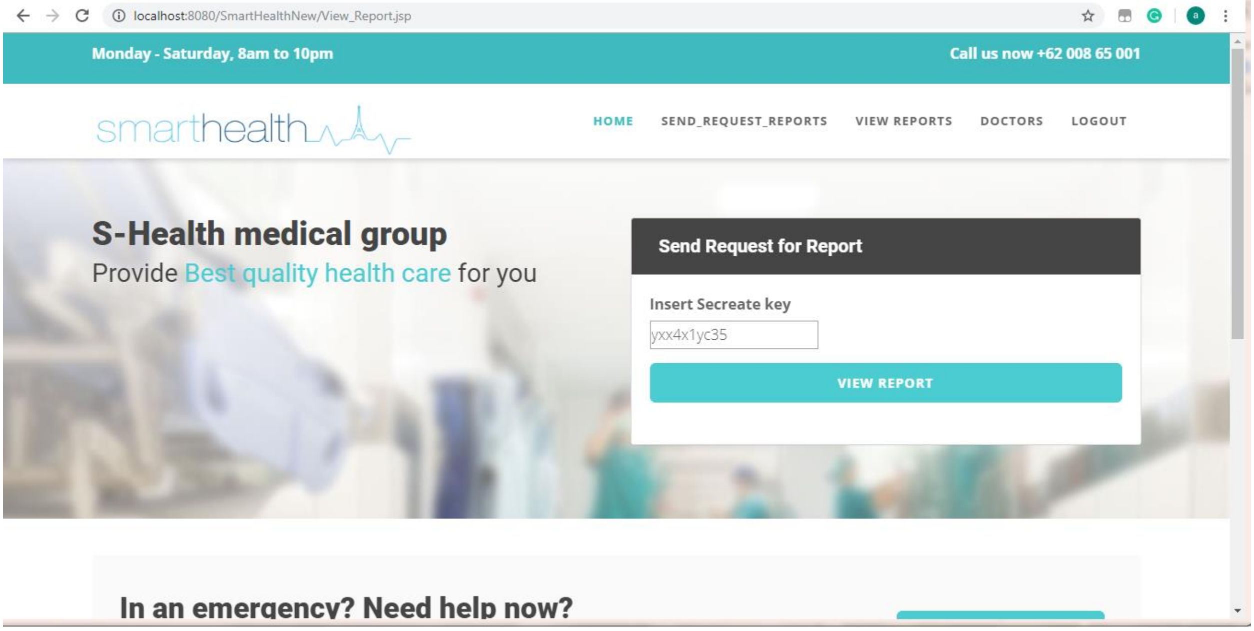
Admin Login


localhost:8080/SmartHealthNew/admin.jsp
Monday - Saturday, 8am to 10pm
Call us now +62 008 65 001
smarthealth
HOME
REPORTS
DOCTORS
FACILITIES
LOGOUT

Request details

Request_id	Doctor Name	Patient Name	Test Name	send key
1	Divyanka	neha	BloodTest	SEND SECRETE KEY
2	0	teju	UrineTest	SEND SECRETE KEY
4	Shardul	neha	UrineTest	SEND SECRETE KEY
5	Shardul	neha	BloodTest	SEND SECRETE KEY

Patient View Report


localhost:8080/SmartHealthNew/View_Report.jsp
Monday - Saturday, 8am to 10pm
Call us now +62 008 65 001
smarthealth
HOME
SEND_REQUEST_REPORTS
VIEW REPORTS
DOCTORS
LOGOUT
VIEW REPORT

S-Health medical group

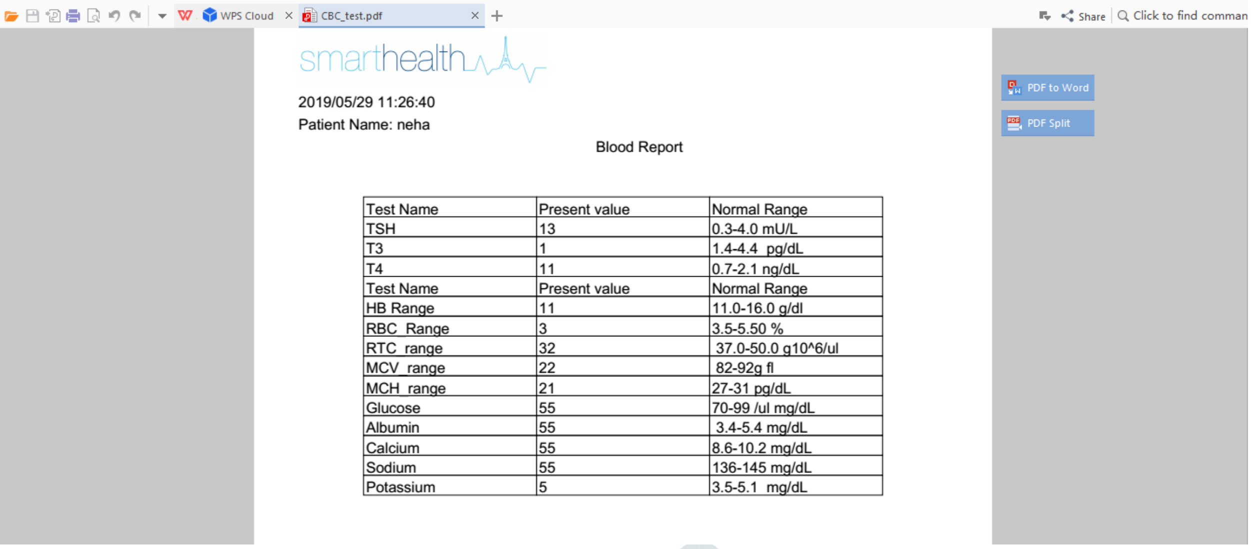
Provide Best quality health care for you

Send Request for Report

Insert Secreate key: yxx4x1yc35

In an emergency? Need help now?

Lab Report



2019/05/29 11:26:40

Patient Name: neha

Blood Report

Test Name	Present value	Normal Range
TSH	13	0.3-4.0 mU/L
T3	1	1.4-4.4 pg/dL
T4	11	0.7-2.1 ng/dL
Test Name	Present value	Normal Range
HB Range	11	11.0-16.0 g/dl
RBC Range	3	3.5-5.50 %
RTC range	32	37.0-50.0 g10^6/ul
MCV range	22	82-92g fl
MCH range	21	27-31 pg/dL
Glucose	55	70-99 /ul mg/dL
Albumin	55	3.4-5.4 mg/dL
Calcium	55	8.6-10.2 mg/dL
Sodium	55	136-145 mg/dL
Potassium	5	3.5-5.1 mg/dL

C. RESULTS AND DISCUSSION

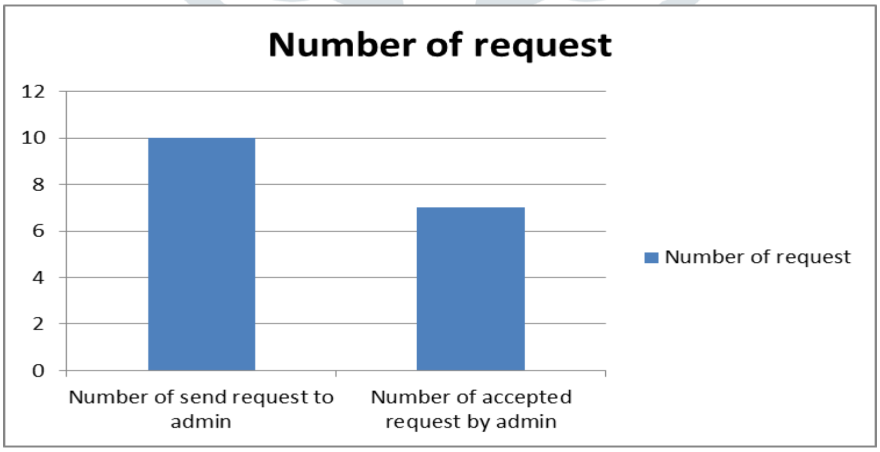
In proposed system experimental setup, we identified that in number of valid test report request send to the admin if all attributes are valid like doctor name and test name etc. then also send proper request to the admin. If request is not valid means the test attribute are not match, then request is not send to the admin. In following table 1 shows that 10 test report request to the admin.

After accepting request, admin sends secret key to authorized patient for downloading the report using the secret key. In our system 7 requests are accepted by the admin.

According to below table 1 following graph shows number of request to the admin the graph; we see 10 users send request to the admin and 7 requests are accepted by the admin.

Sr. No	Number of request send to the admin	Number of request accepted by the admin
1	10	7

Table 1: Number of request to the admin



Graph 1: Number of request

IV. CONCLUSION:

As a kind of basic & fundamental technologies in smart cities, the Internet has been widely used to interconnect all available medical resources and also provide reliable & effective s-health services to the elderly and respective patients. Cloud-based s-health is expected to provide desirable health care in the nearest future. We aim to computerize all details regarding patient details & hospital data. To provide Security and privacy to patient history, the test reports of patients conducted in the pathology lab of the hospital, scheduling an appointment for patient and doctors to make it convenient for both. Patient will be able to find the nearest Hospital.

REFERENCES:

[1] Yinghui Zhang, Member, IEEE,Dong Zheng, Robert H. Deng,“Security and Privacy in Smart Health: Efficient Policy- Hiding Attribute-Based Access control”, IEEE Transactions on Cloud Computing, VOL.3,NO.1 ,APRIL2018.

[2] Prachi Garg Research Scholar Computer Department M. M. Engineering College, Maharishi Markandeshwar University Mullana, India,“Security Techniques for Cloud Computing Environment” (ICCCA2017).

[3] Hossam Ahmed, et.al. “Next Generation Cyber Security Solution for an eHealth Organization” University Study Centre, Sydney, Australia Multimedia University, Malaysia Walden University, USA.

[4] Nikunj Joshi “Big Data Security and Privacy Issues – A Survey”, PG Student Computer Engineering Department Sarvajanik College of Engineering and Technology Surat, Gujarat, India.

[5] Sudipta Chandra, Soumya Ray, R.T.Goswami “Big Data Security in Healthcare” Birla Institute of Technology, Mesra Kolkata Campus, Kolkata

[6] Yinghui Zhang et.al. “Anonymous Attribute-Based Encryption Supporting Efficient Decryption Test”, P.R. China Jin Li School of Computer Science and Educational Software, Guangzhou University, Guangzhou.

[7] Shengpeng Lu et.al., “Implementation of the KNN algorithm based on Hadoop”, International Conference on Smart and Sustainable City and Big Data (ICSSC),2015.

[8] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.