E-Healthcare System and Securing EHR using AES Algorithm

Aishwarya S[.1], Nishrithaa M[.2],R. Kalpana[.3],Dr. P. Veeralakshmi[.4].

[1,2.] Students, Prince Shri Venkateshwara Padmavathy Engineering College.

[3,4.] Faculty, Prince Shri Venkateshwara Padmavathy Engineering College.

ABSTRACT:

Cloud computing is the Internet-based on-demand provisioning of computer system resources such as servers, storage, databases, networking, software, and analytics. The process of storing, managing, modifying, and processing data using a network of remote servers hosted on the internet.During pandemics, to make hospital procedures simpler and to prevent immediate communication with the patient and the doctor/hospital, as well as to keep patient records secure.In the proposed framework, the patients receive a prescription from the doctor based on his or her condition through a web application over the internet.Patient records can be held as EHRs (Electronic Health Records) using the AES algorithm to prevent data breaches.An attacker can be used to classify illegal users.It promotes healthcare providers to lower prices, save time, and prevent close contact with patients.

INTRODUCTION:

According to research, the bulk of patients who attend emergency rooms are not in a life-threatening situation, resulting in hospital overcrowding, high treatment rates, delays in clinical service delivery, and poor service quality for patients who actually need emergency services.Telemedicine and e-health are options for delivering health services to patients remotely in order to reduce hospital visits for patients who are not in a life-threatening situation.Telemedicine is intended to improve patient care while also lowering hospital operating costs. It also provides management with a demand-based MIS (Management Information System) report for better decision-making.

Cloud computing refers to the provisioning of computer system services such as servers, storage, databases, networking, applications, and analytics over the Internet on demand. Data is stored, managed, modified, and manipulated over the internet through a network of remote servers.A web application, unlike computer-based software programs that operate locally on the device's operating system (OS), is application software that operates on a web server.The customer accesses online software using a web browser and an active internet connection. These programs are programmed using client-server architecture.Webmail, online retail transactions, online finance, and online auctions are some of the most widely used web technologies.

To obtain a prescription from the concerned Doctor, the patient must first register/login to the website. The patient can choose from a list of available doctors based on the department he or she selects.The patient will upload documents, prescriptions, and medical reports, and will be given a diagnosis based on the condition or symptoms that he or she is suffering.EHR can be used to archive all patient data on a cloud server.A clinical provider is in possession of a patient's medical history. The data is encrypted and decrypted after access is given using the AES algorithm.

AES is used to encrypt confidential data in applications and hardware all over the world.
It is essential for cyber security and the privacy of electronic records.Three block cyphers are used in AES: AES-128, AES-192, and AES-256. To encrypt and decrypt a block of messages, AES-128 uses a 128-bit key length, while AES-192 uses a 192-bit key length and AES-256 uses a 256-bit key length.Symmetric ciphers, also known as hidden key ciphers, encrypt and decrypt with the same key, meaning the sender and receiver must both know the secret key.Information can be categorized as: Confidential, Secret or Top Secret.Safety is essential. As compared to other cyphers, AES has a higher level of attack resistance.The price The candidate algorithms were to be tested on computational and memory efficiency before being published on a globally, nonexclusive, and royalty-free basis.Execution The versatility of the algorithm, its suitability for hardware or software deployment, and its general simplicity were all factors to consider.

RELATED WORKS:

According to Jingti Han [3], uncoordinated and contradictory relationships between doctors and patients are becoming a major issue for the medical profession and community as a whole, adversely affecting people's sense of well-being and health. We use evolutionary game theory and replicating dynamic equations to create the evolutionary game model, which allows doctors and patients to choose a cooperative or confrontation approach based on the various aspects of trust, knowledge asymmetry, and moral hazard. An in-depth analysis of the model and its simulation shows that the doctor-patient relationship will ultimately form a zero-sum game or a win-win scenario. What condition is stable is closely linked to the initial parameters of the evolutionary game model and the evolutionary game's payment matrix. Rising confidence and decreasing intelligence asymmetry and moral hazard will assist doctors and patients in shifting their strategic options from rivalry to collaboration. We also discovered that increasing the degree of confidence, decreasing the degree of knowledge asymmetry, and decreasing the degree of moral hazard in patients could increase the level of cooperation. We also discover that increasing the degree of confidence, decreasing the degree of knowledge asymmetry, and decreasing the degree of moral hazard among patients can all effectively foster cooperation. The study's purpose is to reduce the tension between doctors and patients, overcome the existing doctor-patient quandary, and provide a clear reference for developing a new doctor-patient partnership relationship.

An online appointment reservation system has become a common trend, according to Luona Yin, Aiqing Zhang, Xinrong Ye, and XiaojuanXie [2] in a modern hospital information system. It provides patients with ease and lowers waiting time in the hospital. However, it also exposes patients' confidential information and creates security vulnerabilities. To resolve these questions, we suggest a novel secure-aware online appointment registry system that can accomplish department matching and doctor searching while preserving privacy. Next, a patient may explain his or her symptoms using searchable cryptography, and the ciphertext is sent to the cloud server. The cloud server of the electronic health record (EHR) then pairs details from the department with related symptoms and transfers the department to the patient in ciphertext. Furthermore, the patient sends his/her specifications to the doctors' profile system (DPS) server, which will scan for the relevant doctors corresponding to the encrypted requirement without decrypting it. The profiles of the doctors are submitted to the searcher in ciphertext. Finally, the patient will schedule an appointment with the anticipated doctor electronically. According to the security review, the device will achieve data confidentiality and honesty, shared verification, protected discovery, anonymity, and trapdoor unlinkability.

As mentioned by BaharHoutan and AbdelhakimSenhajiHafid [6], the incorporation of different individual documents, such as patient data, into a unified repository remains a significant obstacle. In the one hand, gathering critical data will support physicians, experts, and healthcare service providers in delivering better services to patients. In the other hand, since patients do not specifically manage their data, their self-sovereign status and the ability to access personal data are called into question. DLT (Distributed Ledger Technology) is a novel approach for safely recording time-stamped data and allowing patient-driven health and identification information. We study the state-of-the-art of Blockchain (BC)-based self-sovereignty and patient data information in healthcare in this article. Our inspiration is to look at the use of BC technologies in patient data and identity management. BC can be very useful as a distributed autonomous technology, allowing patients power of their own data and self-sovereign status. To the best of our

understanding, there is no literature on the topic. More precisely, the focus is on strategies that seek to achieve holistic results. Electronic Health Reports (EHR) and Patient Health Records (PHR) in British Columbia (PHR). As a result, the growth of pure decentralised. In terms of architectural and technological structure, Healthcare Information Systems (HIS) face a major challenge. Designing stable and dependable EHR and PHR, which serve as the basis for many other healthcare systems, necessitates a cautious balancing of many considerations, such as degree of decentralisation, anonymity, scalability, and data throughput. We study the state-of-the-art and include an overview of design trade-offs in this article.

Rajeev Kumar [14] states that, continuous data breaches directed at sensitive patient records have been a nightmare for healthcare organisations. A stable and efficient information management model in healthcare web apps will help healthcare organisations benefit and raise sales. A multi-criteria judgement approach may be a significant step toward achieving this aim. The writers employed a hybrid applied Fuzzy Analytical method. Fuzzy AHP-TOPSIS (Hierarchy Process-Technique for Order of Choice by Similarity to Ideal Solution) approach for assessing different information security variables of a web application in order to provide developers and researchers with effective and usable performance. The study's conclusions and philosophy would certainly assist professionals in creating stable and effective information management within a web application. Furthermore, the analytical study performed in our research sought to carve a structured direction for developers to pursue in order to concentrate on the most critical considerations for guaranteed and meaningful information security within a web application.

ShekhaChenthara, Khandakar Ahmed, and Hua Wang [8] have created a rigorous security model for EHR; this paper highlights the research concerns and future directions in cyber security. We performed a comprehensive review of the IEEE, Science Direct, Google Scholar, PubMed, and ACM databases for papers on EHR methods published between 2000 and 2018, and summarised them in terms of architecture types and evaluation strategies. Several publications were surveyed, analysed, and evaluated, and the tasks listed below were identified: 1) EHR protection and privacy; 2) e-health data security and privacy specifications in the cloud; 3) EHR cloud architecture; and 4) various EHR cryptographic and non-cryptographic methods. Abuse of privilege happens when a user takes an activity that he or she may not be able to do in compliance with corporate policies or the statute. To deter data leaks, authentication algorithms such as encryption and decryption are used to protect patients' privacy.

PROBLEM DESCRIPTION:

Cloud computing is the on-demand provisioning of computer device services such as servers, storage, databases, networking, applications, and analytics via the Internet. The process of storing, maintaining, updating, and processing data through an internet-hosted network of remote servers. During pandemics, hospital protocols are streamlined to eliminate direct contact between the patient and the doctor/hospital [11], and patient records are kept safe. According to studies, the majority of people who visit emergency rooms are not in a life-threatening condition [1], resulting in hospital overcrowding, high treatment costs, gaps in healthcare care delivery, and inadequate service quality for patients who do need emergency services. Telemedicine and e-health are options for digitally providing health care to patients in order to minimise hospital costs for patients who are not in a life-threatening condition.Medicines are prescribed over the internet to reduce the waiting period [7] for patients in non-urgent cases. Telemedicine seeks to boost patient safety thereby lowering hospital operating costs. It also gives managers a demand-based MIS (Management Information System) study to help them make smarter decisions. In the suggested system, patients request a prescription from the doctor depending on their diagnosis from an internet-based online application. Using the AES algorithm, medical information can be maintained as EHRs (Electronic Health Records) [10]. To deter data breaches, patient information should be stored as EHRs (Electronic Health Records) using the AES algorithm.The data uploaded by the user is encrypted and saved using the AES algorithm [5]. If the doctor needs to login and use, he should request the administrator for the hidden key. Once the request is approved, the doctor may decrypt the file by entering the secret key produced which is done by AES algorithm, and after the file has been decrypted, he may view or download the medical documents. The admin should be used to distinguish between legitimate and unauthorised users. It encourages healthcare providers to increase their costs, save time, and avoid direct contact with customers.

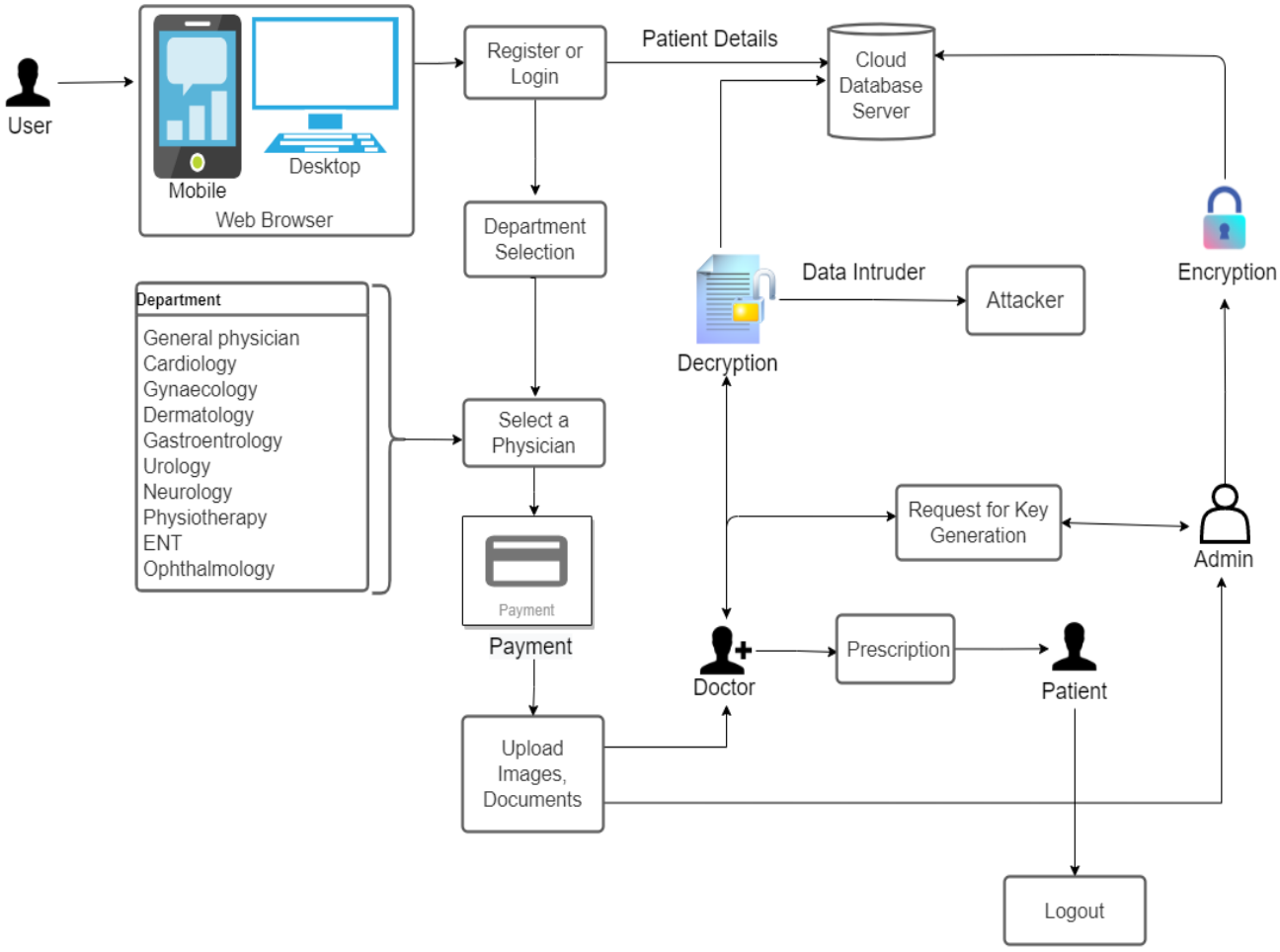

Fig. 1 System Architecture

IMPLEMENTATION:

As seen in (Fig 1), when a person is suffering from a major illness, he or she can visit our web application [4]. If he/she is a first time user, then they will go through a registration process. The registration process includes name, aadhar card number, mobile number, mail id etc. Once the registration process is completed the user will be directed to the login page. For every login, an OTP (One Time Password) will be generated to the registered mail id. The patient can select the available Doctor according to the department the patient chooses without appointment [12] and has to make a payment (consultation fee). As shown in (Fig. 3), the patient must upload documents and health records. The Doctor will administer medications for the patient's disease after uploading and entering the signs [9], as seen in (Fig 2).Once the consultation is completed the user can logout from the web page. The patient's medical records (EHR) will be stored in the cloud server [15]. The data uploaded by the user is encrypted and stored using the AES algorithm as given in fig. 4. If the doctor needs to login and use, he should request the admin for the hidden key as shown in the (Fig. 5). Once the request is accepted, the doctor may decrypt the file by entering the secret key produced by the AES algorithm, as shown in (Fig. 6) and after the file has been decrypted, he may view or download the medical

documents.Using attacker, you can track down the intruder and the file will not be accessed with a warning stating you are an attacker.

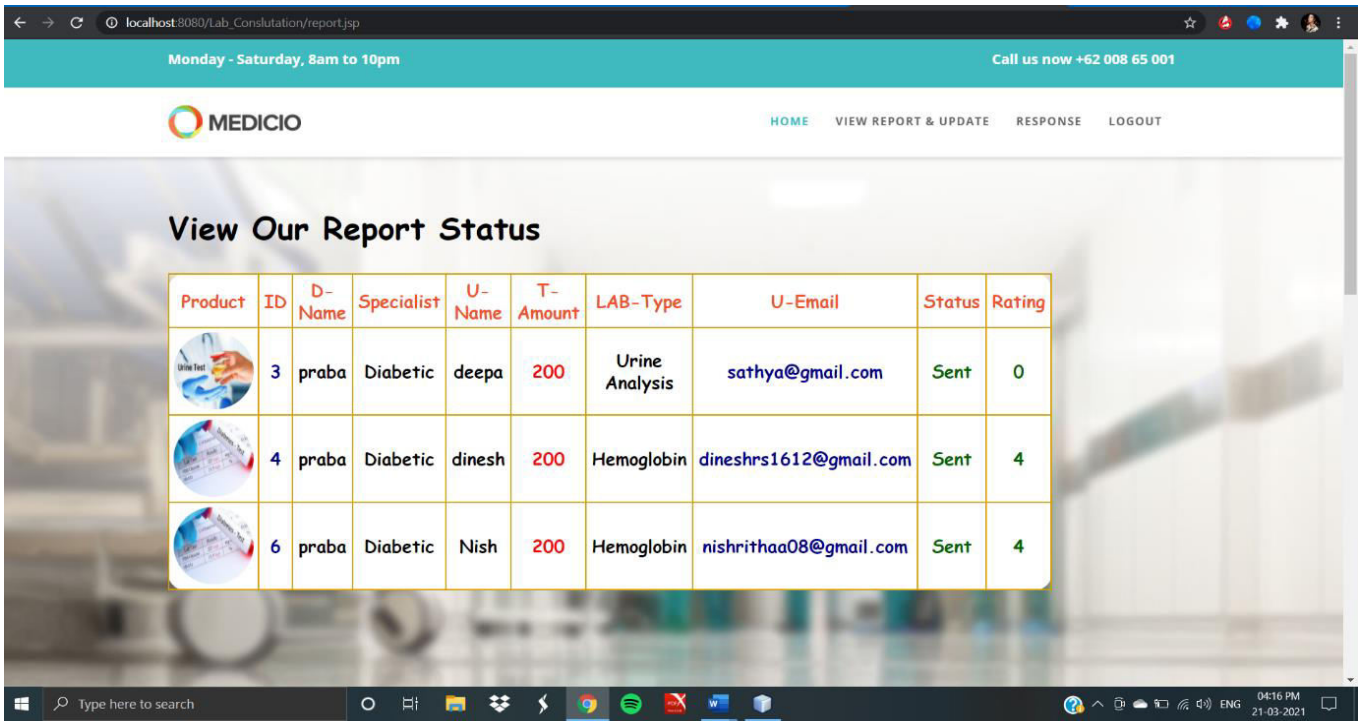

Fig. 2

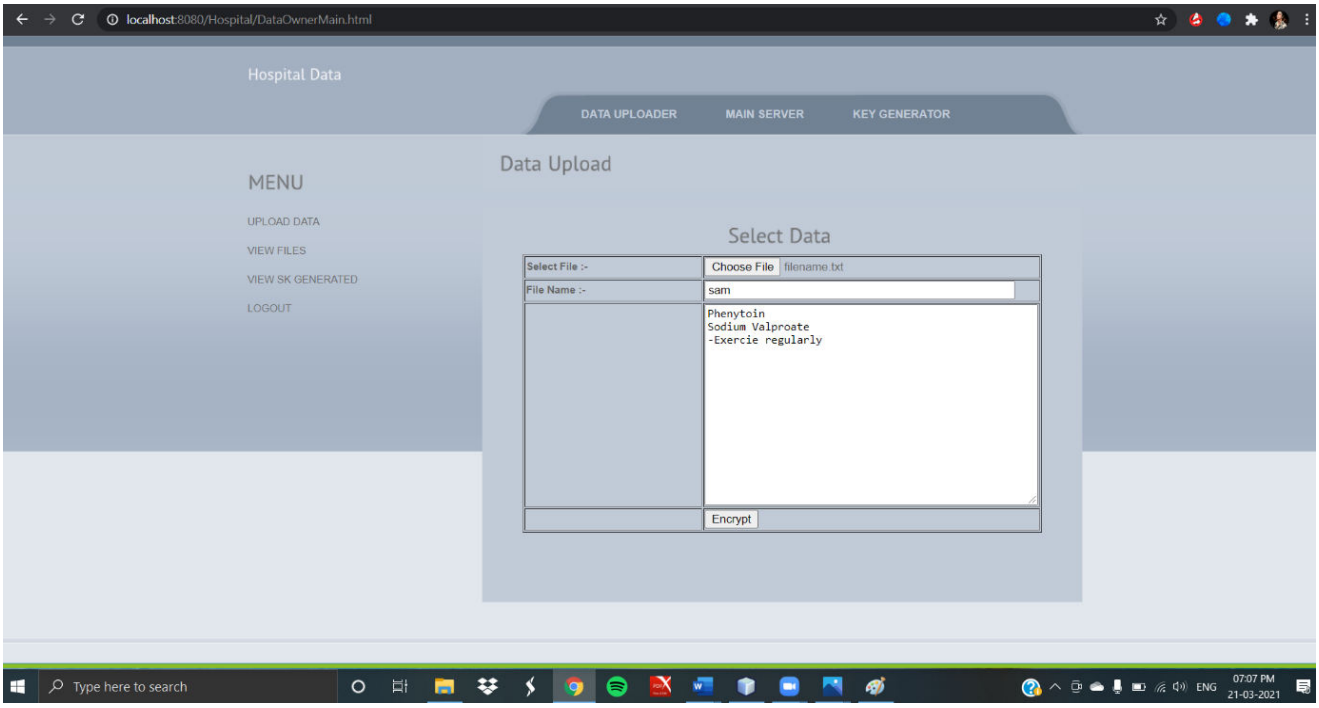
localhost:8080/Hospital/DataOwnerMain.html
Hospital Data
DATA UPLOADER
MAIN SERVER
KEY GENERATOR
MENU
UPLOAD DATA
VIEW FILES
VIEW SK GENERATED
LOGOUT
Data Upload
Select Data
Select File :-
Choose File
filename.txt
File Name :-
sam
Phenytoin
Sodium Valproate
-Exercie regularly
Encrypt
Type here to search
ENG
07:07 PM
21-03-2021

Fig. 3

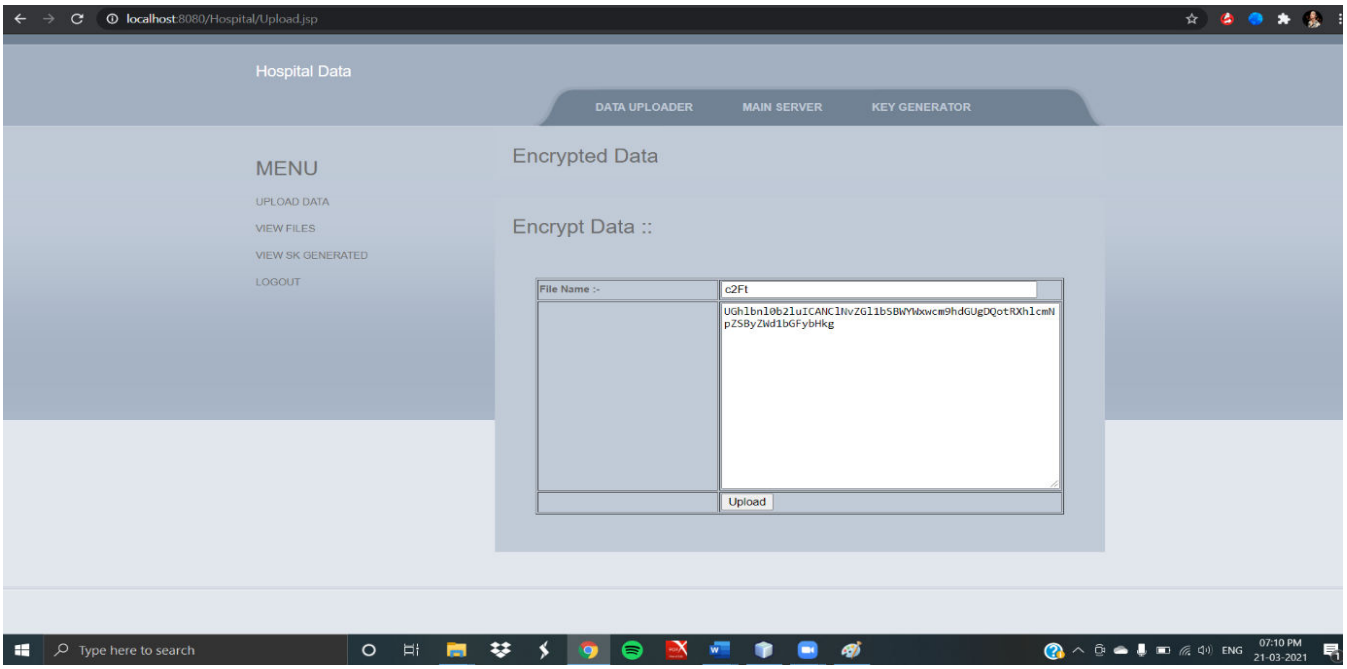
localhost:8080/Hospital/Upload.jsp
Hospital Data
DATA UPLOADER
MAIN SERVER
KEY GENERATOR
MENU
UPLOAD DATA
VIEW FILES
VIEW SK GENERATED
LOGOUT
Encrypted Data
Encrypt Data ::
File Name :-
c2Ft
UGhlbnl0b2luICANClNvZGl1bSBWYWxwcm9hdGUgDQotRXhlcmNpZSByZWd1bGFybHkg
Upload
Type here to search
ENG
07:10 PM
21-03-2021

Fig. 4

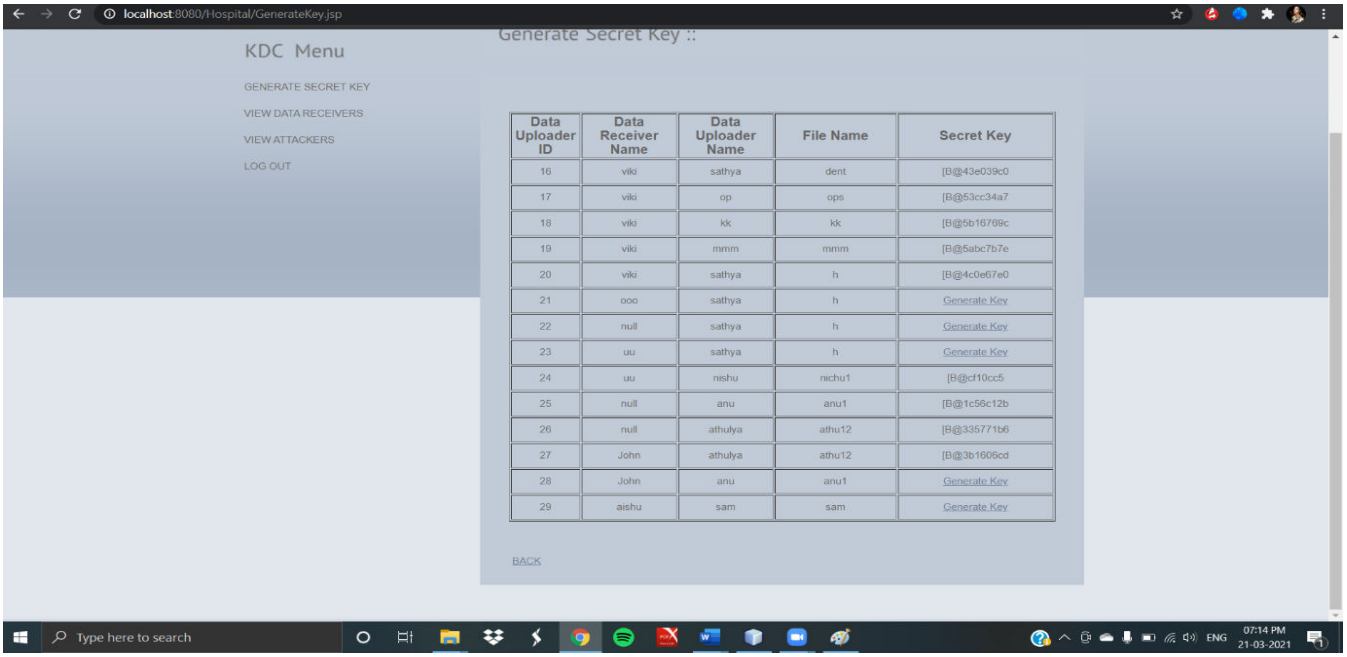
localhost:8080/Hospital/GenerateKey.jsp
KDC Menu
GENERATE SECRET KEY
VIEW DATA RECEIVERS
VIEW ATTACKERS
LOG OUT
Generate Secret Key ::
Data Uploader ID | Data Receiver Name | Data Uploader Name | File Name | Secret Key
16 | viki | sathya | dent | [B@43e039c0
17 | viki | op | ops | [B@53cc34a7
18 | viki | kk | kk | [B@5b16769c
19 | viki | mmm | mmm | [B@5abc7b7e
20 | viki | sathya | h | [B@4c0e67e0
21 | ooo | sathya | h | Generate Key
22 | null | sathya | h | Generate Key
23 | uu | sathya | h | Generate Key
24 | uu | nishu | nichu1 | [B@cf10cc5
25 | null | anu | anu1 | [B@1c56c12b
26 | null | athulya | athu12 | [B@335771b6
27 | John | athulya | athu12 | [B@3b1606cd
28 | John | anu | anu1 | Generate Key
29 | aishu | sam | sam | Generate Key
BACK
Type here to search
ENG
07:14 PM
21-03-2021

Fig. 5

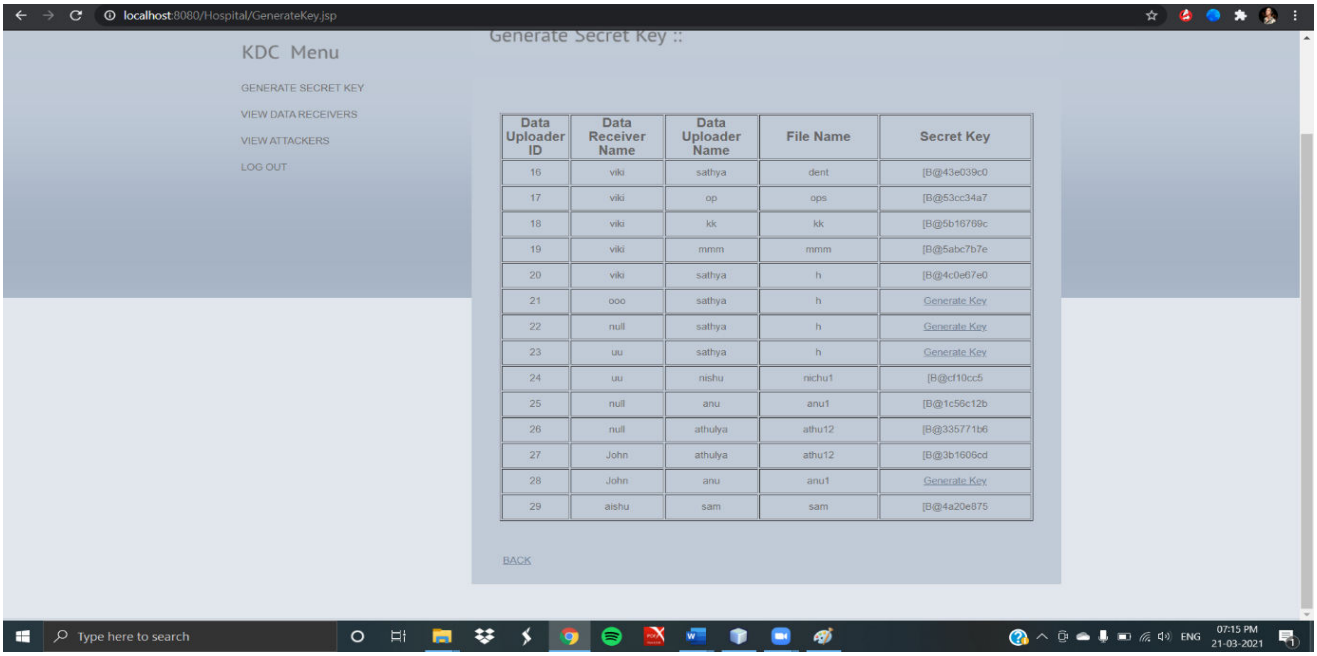
localhost:8080/Hospital/GenerateKey.jsp
KDC Menu
GENERATE SECRET KEY
VIEW DATA RECEIVERS
VIEW ATTACKERS
LOG OUT
Generate Secret Key ::
Data Uploader ID | Data Receiver Name | Data Uploader Name | File Name | Secret Key
16 | viki | sathya | dent | [B@43e039c0
17 | viki | op | ops | [B@53cc34a7
18 | viki | kk | kk | [B@5b16769c
19 | viki | mmm | mmm | [B@5abc7b7e
20 | viki | sathya | h | [B@4c0e67e0
21 | ooo | sathya | h | Generate Key
22 | null | sathya | h | Generate Key
23 | uu | sathya | h | Generate Key
24 | uu | nishu | nichu1 | [B@cf10cc5
25 | null | anu | anu1 | [B@1c56c12b
26 | null | athulya | athu12 | [B@335771b6
27 | John | athulya | athu12 | [B@3b1606cd
28 | John | anu | anu1 | Generate Key
29 | aishu | sam | sam | [B@4a20e875
BACK
Type here to search
ENG
07:15 PM
21-03-2021

Fig. 6

CONCLUSION:

As a result, the vast majority of people who enter emergency departments are not in a life-threatening situation which leads to hospital overcrowding, high treatment rates, delays in clinical service delivery, and poor service quality for patients who actually need emergency services.This online application was designed to provide medical assistance to those in distress without the need for an appointment.Available round the clock.To prevent close contact with the doctor or the hospital (during pandemic). Multiple users can login at the same time.The patient will be monitored for their condition without needing to see the hospital in the safest manner possible by using online therapy.

FUTURE ENCHANCEMENT:

1. Patients who are going to the same physician with the same sickness will benefit from a follow-up consultation.
2. Patients may also use a speech recorder to capture their voice when describing their symptoms.
3. When registering for the first time, more identity evidence can be used to clear fake accounts.
4. With the assistance of admin, the patient will access their medical record/reports that they uploaded to the doctor.
5. By training them with various data sets, we will use machine learning to provide prescriptions to patients.

REFERENCES:

[1] E. Bruballa, A. Wong, F. Epelde, D. Rexachs, and E. Luque, ``A model to predict length of stay in a hospital emergency department and enable planning for non-critical patients admission,'' Int. J. Integr. Care, vol. 16, no. 6, p. 24, Dec. 2016.
[2] W. Cao *et al.*, ``A Web-based appointment system to reduce waiting for outpatients: A retrospective study,'' *BMC Health Services Res.*, vol. 11, no. 1, p. 318, Dec. 2011.
[3] J. Cao and J. Wei, ``Evolution of the perception of the doctor's role in China,'' Lancet, vol. 384, no. 9945, p. 742, Aug. 2014.
[4] Y.-W. Chang, P.-Y. Hsu, Y. Wang, and P.-Y. Chang, ``Integration of online and offline health services: The role of doctor-patient online interaction,'' Patient Edu. Counseling, vol. 102, no. 10, pp. 19051910, Oct. 2019.
[5]Chiuchisan, I., Balan, D.-G., Geman, O., Chiuchisan, I., &Gordin, I. A security approach for health care information systems. *2017 E-Health and Bioengineering Conference (EHB),* 2017
[6] D. V. Dimitrov, ``Blockchain applications for healthcare data management,'' Healthcare Informat. Res., vol. 25, no. 1, p. 51, 2019.
[7] N. C. Eze and C. J. Uneke, ``Assessment of out-patients' perception on timing hospital appointment to reduce waiting time at primary health care centreAbakaliki, South East Nigeria: A cross-sectional study,'' Int. Med.
Res. J., vol. 5, no. 2, pp. 1924, May 2017.
[8] L. Griebel, H.-U. Prokosch, and F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel, and M. Sedlmayr, ``A scoping review of cloud computing in healthcare,'' BMC Med. Inform. Decis. Making, vol. 15, no. 1, p. 17, Mar. 2015.
[9] W. Jing, H. Otten, L. Sullivan, L. Lovellsimons, M. Granekcatarivas, and K. Fritzsche, ``Improving the doctor-patient relationship in China: The role of balint groups,'' Int. J. Psychiatry Med., vol. 46, no. 4, pp. 417427, 2013.
[10] C. S. Kruse, M. Mileski, A. G. Vijaykumar, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram, ``Impact of electronic health records on long-term care facilities: Systematic review,'' JMIR Med. Inform., vol. 5, no. 3, p. e35, 2017.
[11] P. Liu, G. Li, S. Jiang, Y. Liu, M. Leng, J. Zhao, S. Wang, X. Meng, B. Shang, L. Chen, and S. H. Huang, ``The effect of smart homes on older adults with chronic conditions: A systematic review and meta-analysis,'' Geriatric Nursing, vol. 40, no. 5, pp. 522530, Sep. 2019.

[12]M. Samadbeik, M. SamadbeikSaremian, and A. Garavand, ``Assessing the online outpatient booking system,'' Shiraz E-Med. J., vol. 19, no. 4, p. e60249, Mar. 2018.
[13] E. Shojaei, D. Rexachs, A.Wong, F. Epelde, and E. Luque, ``A method for projections of the emergency department behaviour by non-communicable diseases from 2019 to 2039,'' IEEE J. Biomed. Health Informat., vol. 24, no. 9, pp. 24902498, Sep. 2020.
[14] Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., &Tzovaras, D. On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, 2018.
[15] C. Zhang, L. Zhu, C. Xu, and R. Lu, ``PPDP: An efcient and privacypreserving disease prediction scheme in cloud-based e-healthcare system,''