

# Security in E-healthcare System using AES Encryption

Komal Biswal, Sanyam Sharma, Poojan Patel, Prof. Archana Chaugule, Ritika Jain, Prof. Minakshi Retharekar

*Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai, India*  
*Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai, India*  
*Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai, India*  
*Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai, India*  
*Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai, India*

Date of Submission: 20-04-2023

Date of Acceptance: 30-04-2023

**ABSTRACT**—Online healthcare system is a new way of consulting with the in-demand doctors for efficient, frequent, and streamlined checkups and various other concerns. It has become a lot more popular in recent times than expected. Healthcare is with no doubt one of the most important aspects for every individual in the world. It has become a key aspect to make sure that an individual's mental, physical, and social life is smooth-running. The purpose of virtual healthcare systems is to provide medical help from anywhere around the world.

Taking all this deliberation, we planned on designing a completely functional website "Security in E-healthcare System using AES encryption". Here the user can provide details related to their health problems or their family's health problems. The details will be examined by the doctor to understand the medical need an individual requires to overcome the trouble caused to them. The security algorithm which is AES encryption has been incorporated into the system so that integrity is maintained, and privacy of customers are not exploited. Our project promotes online health system and provides awareness and comes up with a sense of relief that the data is safe and not misused.

**Keywords**—healthcare, real-time video processing, AES, security, easy-appointment, shopping, integrity, confidentiality

## I. INTRODUCTION

Today it has become very important to go for regular checkups, tests, examinations for an individual. New variations of viruses, bacteria's

and fungus has taken birth. Taking all these aspects into consideration, E-health, which implies to medical services, its specifics, information, facts, provided via the Internet and associated technologies available, is a developed field at the crossroads of medical informatics, public sanitation, and care, and most importantly business. [1] In a wider sense, the term, E-health not only depicts a high-tech technological evolution but also, an advancement, a growth, a development, a mode of thinking, dedication and a headway to overall analytics in order to use knowledge, facts, figures and intelligence technology to improve health care services locally, regionally, and geographically. Digital world has taken over, almost every country is digitalized in many ways. Online health care system has also become a need due to its quick response, availability and most importantly security, integrity, and accessibility [3]. A user can simply book an appointment and share its medical history and wait for the acceptance with complete security. It is basically delivering medical services, advisement, care, over a simply designed website or an app via internet. This contemporary electronic information and conversation technologies come into picture when patients i.e., the user who registered and respective medical professional are not near one another, and their communication is arbitrated by an advanced technology [2]. The services comprise of various easy-going assistance such as, among others, telepathology, which is transmission of pathology data across remote placements; vital monitoring/tracking; electronic prescription, recommendation, suggestions; teleconsultation, telemedicine, telecare, tele-health and physical and

psychological diagnosis, prognosis and treatment, cure, medicines.

Keeping this into account, we planned to make altogether, a functional website, including features like; set up an appointment as per the availability of the doctor needed by the patient via video chat doing whole payment beforehand to make it a streamline and an easy going process, doctors have authorization to either accept or reschedule the appointment they have received, Once the patient and doctor have discussed the matter, the patient will be directed to the pharma shopping web page which is basically a shopping website for medical equipment's. According to the prescription provided by the doctor, user can add items and modify the cart based on the filters like delivery, medicines, drugs, materials, equipment's. Appointments for the lab tests recommended by the doctor can be scheduled and tests can be done at the patient's house or at the nearest lab as per the requirements needed.

## II. LITERATURE SURVEY

In contrast to the previous research, we uncovered that the users mainly go for the online mode to consult doctors rather than the offline medium due to time saving, no travelling, limited resources requires and many such features. Users of all ages/sex/gender have variety of illness, disorders, infections etc. which needs to be analyzed by the specific doctors who are excellent in that field of job and due to this online mode users get quick and faster service as compared to the offline medium. As an outcome, it has demonstrated a positive trait, and users are happy with the online virtual mode.

### A. Survey of all the Research Papers studied:

To understand and plan the flow of our project, we read twelve research papers mainly associated with IEEE and Springer. The papers gave us an idea of an actual healthcare system and why is there a need for an e-healthcare system and what approaches are needed, what things are needed to be integrated and many more. Various technologies and techniques were also mentioned which helped us to decide our project technologies, which will benefit our project.

### B. Survey of an existing system:

As we talk about existing system along with our previous research, there are couple of issues which are discussed in references. Some of them are:

#### i. No/very little security for personal documents:

Patients are very serious regarding their personal details. They don't want to share their health history with every doctor, as it could lead to misuse. Healthcare systems store a vast amount of sensitive patient information, including personal details, medical history, health status, medications, and payment information. Patient data is some of the most sensitive information that exists, and it must always be kept secure as tampering with it can cause huge problems. It must be prevented from any unauthorized access, data breaches, theft which are some of the potential harms to patients.

To avoid such issues, various algorithms like AES, triple DES, multiple hashes etc. have been used using cloud systems to protect user's documents.

#### ii. Mismatching of documents of different patients:

Considering there are two patients arriving at the same time at hospital. Since it was a rush hour, the receptionist at the desk by mistakenly switched both the files. This can cause major issue for both doctor and patients. This can also happen in online system if the system is less encrypted and crashes easily but chances are relatively less as compared to the offline version [10].

To avoid this, proper systems with updated software and hardware are used.

#### iii. Cost-effective:

Traveling is one of the major issues of at this time. As many patients are usually students who might have any upcoming exams at that time, employees who might not get sick leaves, patients from one state wanting to consult doctors from different state, senior citizens who find it difficult to go from place to place or patients who live in remote rural areas [5]. All this creates the need for online appointments which can be done through our system. Regular checkups, that is a very common thing can be easily done via online consultation system which is not only cost effective but also relatively a better option considering the Covid.

With the help of Online healthcare system one can easily book appointments and also consult doctors through it [7]. Patients, if features are provided, can also have lab testing done at their homes too. This thereby helps a lot of people who have various issues visiting the clinics, even doctors can manage their time this way.

## III. PROPOSED SYSTEM

The goal we aim at is to design a full-fledged virtual e-health system with advanced security algorithm. Our project "E-healthcare

System using AES encryption” as the name suggest look forward to provide a virtual health management system using an advanced security algorithm which is AES (Advanced EncryptionStandard). It basically uses same key for both encryption and decryption.

We have designed the website acknowledging all the factors one must take into account to ensure ease-going and an effectiveness. Firstly, we added the improved search bar to help the end users to effortlessly search the medical items from the pharma shopping; Secondly, users can easily register and consult with the specific doctors they would like to consult via a real-time video calling feature which we have incorporated in our project. Thirdly, Appointments for the lab tests recommended by the doctor can be scheduled and tests can be done at the patient’s house or at the nearest lab as per the requirements of the patient, this mainly provide help to the individuals who do not have any transportation facility or mainly by senior citizens. Fourthly, displaying of how much stock is left for a particular will also be shown which is mainly called stock inventory. Fifthly, the most important feature which we have incorporated is the security using the AES algorithm which is a security providing algorithm. So basically, whenever a doctor requires any medical information about a patient, he will send a request to the patient and it’s the choice of the patient to either accept it or reject it. This way confidentiality and the integrity of the data is maintained, and no misuse is done as every time a doctor needs to check the medical history, they need to ask for permission from the respective patient [6]. Sixthly, a filtering system is added to the cart where you can basically filter your cart on the basis of; like medicines, controlled drugs, basic needs etc. whatever you want to buy at that moment. You can filter on the basis of the delivery of the items which means how urgently you require a particular item and if its available or not.

#### IV. OBJECTIVES AND WORKFLOW

The objective is to provide users with a secure healthcare site using required algorithms. So that users don’t have to go through major or minor risks regarding their personal documents or medical records. Other objectives include the option for booking appointments for lab testing mentioned by doctors to the patients which can be carried out as needed at the patient’s home or immediately at the facility. The course of action of providing medical service has increasingly been used in geographically remote areas where access to medical care is extremely bounded or

nonexistent and when suitably competent medical specialists are only easily available at a single.

The website starts with the homepage, providing the patient, doctor and admin logins. Starting with the patient, if the user has not registered already, he needs to do registration by giving the details like name, email, phone no and address. Next patient will be redirected to the dashboard to fill out the profile details like blood group etc. and can also upload the profile picture. Further various options are provided like uploading reports. The reports which are uploaded are completely encrypted using AES encryption [6]. Next patient can schedule the appointments with the doctor through the appointment page where an advanced search bar is provided to search the doctor as per the name, specialty, or the region. Now the doctor patient requires is filtered and patient can send the request and wait for the doctor to confirm it. Once the doctor confirms it, the patient gets the notification of the confirmation. After that the patient can go to schedule page and check the confirmation and join the meeting as per the slot. The doctor can access the reports and personal details of the patient only if the patient approves it.

For the doctor overview, doctor must put the medical registered number, if not valid the doctor is not allowed to login/register and have any kind of access. If valid, the doctor also needs to fill some basic details required. The doctor will then have to provide the slots they are going to be available. After providing these details, admin will have to approve it. Doctor can view all of his patients, past patients and if doctor wants to view any medical document, he needs to ask for the permission to the respective patient.

For the admin role, he will approve the doctor by making sure the doctor is an authorized person. Any alerts that need to be send to both doctors and patients is done by the admin.

A pharma shopping page has been introduced, if a user is login, all details like name and address will already be there if not, the user has to fil basic details. Here various medical products like medicine, control drugs etc. will be displayed. Users can add the items to the cart and a feature called stock inventory is also introduced.

For lab testing, patients can go to the lab testing page and few mandatory details like type of test needs to be filled in by the patient and when the patient books it, he/she can view nearby lab testing center available as per there locality and can book it. After confirmation, the patient receives the message of confirmation.

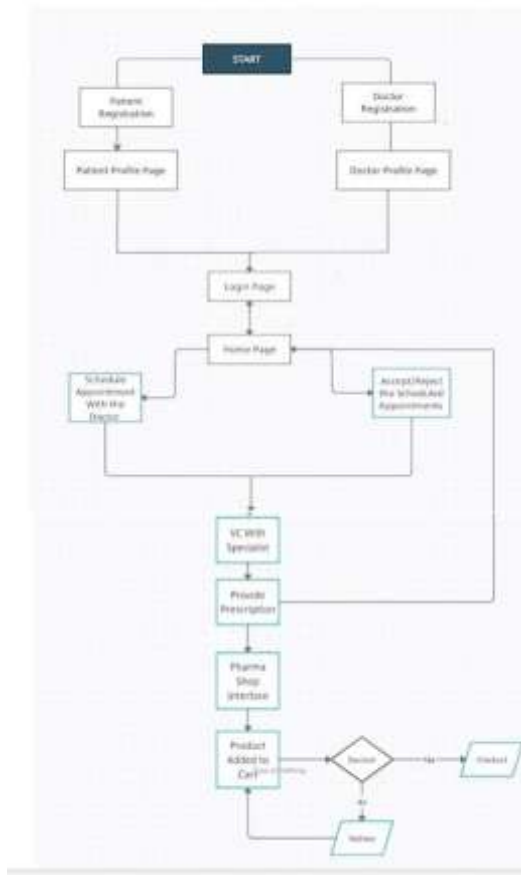


Fig1: Workflow of our system

### V. BENEFITS OF PROPOSED SYSTEM

Security is an essential aspect of any healthcare system. We have majorly focused on this need of the users. We tried to overcome the issues affected by the security to the users for better use of the system [4]. We have worked on “Security in E-Healthcare system using AES encryption”, the system that ensures end users feel safe to use the system while uploading any of their confidential documents. We have designed the website in such a manner that patients will have to grant access to the doctors to view their documents. Every time a doctor needs to view the document, he/she needs to ask the patient to grant access to that respective doctor, this way the integrity and confidentiality of the patient is maintained.

Our technology offers a communication channel for doctors and patients, enabling patients to consult with them. We have incorporated additional features, Video call, after Video Chat with the doctor, Patient will be redirected to our shopping page where patient can buy prescribed medicines and those medicines will be delivered to them within an hours’ time depending upon the

item they have shopped, resulting in time efficiency and patients can buy medical items with just one click. The doctor's recommended lab tests can also be scheduled with appointments, and depending on the specifics required, the tests can be performed in the patient's home or the closest lab. As a result, patients can make appointments with ease, which is a highly useful feature for senior adults. Displaying of how much stock is left will also be shown on the website, this way end users can know which item is in stock and which is going out of stock and purchase items accordingly.

AES (Advanced Encryption Standard) is a widely used encryption algorithm that can be used to secure sensitive data in a healthcare system. Reasons why we opted for AES encryption is, Firstly, it provides Data integrity by adding an extra layer of shield against unapproved additions, removals, and other forms of tampering, AES-based security can also be used to guarantee the accuracy of healthcare data. Secondly, delivers effective data security, AES encryption is one of the strongest forms of encryption methods currently in use. Without the appropriate permission or decryption key, it is very challenging for unapproved users to access confidential healthcare data because it uses a complex block cypher algorithm. Thirdly, provides effective performance and flexible implementation on significant amounts of data, AES encryption can be completed swiftly and effectively. Because of this, it is a good option for healthcare systems that frequently need to handle and keep large amounts of sensitive patient data. AES encryption can be used at different levels within a healthcare system, giving users the option of choosing the precise data to be secured and the encryption method.

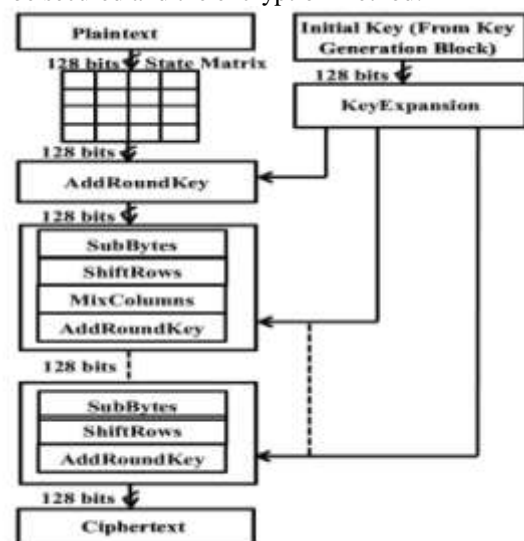


Fig. 2. AES encryption [11]

Sr. No	Parameters	AES	DES	RSA
i.	Computation Time	Faster	Moderate	Slower
ii.	Memory Utilization	Requires moderate memory space	Requires least memory space	Requires more memory space
iii.	Security Level	Excellent security	Adequate security	Least security

Table no 1: Comparison between AES and other encryption algorithms [12]

Overall, AES-based security can help healthcare systems ensure the confidentiality and integrity of sensitive patient data, while also meeting regulatory and compliance requirements. By providing a strong and efficient encryption solution, AES can help healthcare providers build trust with their patients and maintain the confidentiality of their health-related information.

This leads to fewer medical errors; Patient's pertinent information is easily accessible; The medical staff spends less time on administrative, managerial, and supervisory activities; patients spend less time in the hospital; and all the patient's data is mustered in a substantial way. Improved control of human resources; improved communication amongst hospital staff members, especially between physicians, nurses, and administrative personnel.

## VI. CONCLUSION AND FUTURESCOPE

In this era of 'Online System', the most dangerous or most concerned part is security. Having a properly secured system enhances the patient's trust in our system and allows them to freely use this. Health-care providers must make sure that health information/facts/figures are not only up to date and highly accurate, but also simple for patients of all backgrounds to comprehend [8][9]. This obviously necessitates the personalization and/or alteration of the information's presentation and substance. Patients and the community of medical professionals (health service providers) both comprise of people with a variety of backgrounds, specialties, and demographic, psychological, and cognitive traits.

The variety of e-Health system users and presentation techniques highlight the need for user interface customization (UIA). For optimal use and better services, it is important to figure out and manage health care system effectively including all managerial, organizational, administration functions.

The intent of our project is to come out with a system for end user/patients who find it difficult to trust web sites for uploading their personal documents, doubting the security system. The project's major aim is to build trust among the end users where they can without any second doubts upload their confidential documents and trust the process. The focus of our project is to serve and help both the end users i.e. the patients and the doctors in convenient and appropriate ways.

For future scope, we are thinking of opting for more advanced secure system, adding highly classified security algorithms like AES encryption which we couldn't develop due to the limited technology and algorithm's knowledge. A security system is something which gets on changing with new developments of different algorithms, technologies, networks and even systems too.

## REFERENCES

- [1]. Hemant B Mahajan, Ameer Sardar Rashid, Aparna A Junnarkar, Nilesh Uke, Sarita Deshpande, Ahmed Alkhayyat, Bilal Alhayani - Integration of Healthcare 4.0 and blockchain into secure cloud based electronic health records systems, IEEE 2022.
- [2]. Pushkar Kishore; Swadhin Kumar Barisal; Kulamala Vinod Kumar; Durga Prasad Mohapatra – Security Improvement and Privacy Preservation in E-Health, IEEE 2021.
- [3]. Aqeel Sahi , David Lai, and Yan Li - A Review of the State of the Art in Privacy and Security in the eHealth Cloud, IEEE 2021.
- [4]. Priyanka, Amit Kumar Singh - E-health Web Application Framework and Platform Based on The Cloud Technology, Springer 2021.
- [5]. Mohammad Jabirullah; Rakesh Ranjan; Mirza Nemath Ali Baig; Anish Kumar Vishwakarma - Development of e-Health Monitoring System for Remote Rural Community of India, IEEE 2020.
- [6]. Abhishek Kumar Pandey, Asif Irshad Khan, Yoosef B. Abushark, Md. Mottahir Alam, Alka Agrawal, Rajeev

- Kumar, Raees Ahmad Khan - Key Issues in Healthcare Data Integrity: Analysis and Recommendations, IEEE 2020.
- [7]. Yung-Tien Huang; Ching-Wen Chen - A Study on the Mobile Personal Health Management System, IEEE 2019.
- [8]. Abid Mehmood, IynkaranNatgunanathan , Yong Xiang, Howard Poston, and Yushu Zhang - Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications, IEEE 2018
- [9]. Jun Lu Song Zhang - E-health Web Application Framework and Platform Based on The Cloud Technology, IEEE 2013.
- [10]. S.Mfurnel, NJSalmon, P. Wsander, C. T.Stockez, MJWarren - Approaches to security in healthcare multimedia systems, Springer.
- [11]. [https://www.researchgate.net/figure/Block-Diagram-of-AES-Algorithm\\_fig1\\_326596710](https://www.researchgate.net/figure/Block-Diagram-of-AES-Algorithm_fig1_326596710)
- [12]. [https://www.researchgate.net/figure/Comparison-table-between-AES-DES-and-RSA\\_tbl3\\_333755102](https://www.researchgate.net/figure/Comparison-table-between-AES-DES-and-RSA_tbl3_333755102)