



E-Healthcare Cloud Solution

Sneha S. Satpute¹, Mahesh Dhangar², Aniket Todkar³, Pratik Jatrare⁴,
Sourabh Kole⁵, Abhishek bhandare⁶

Assistant Professor, Dept. of C.S.E., Dr. J. J. Magdum College of Engineering, Jaysingpur, India¹

B.E. Student, Dept. of C.S.E., Dr. J. J. Magdum College of Engineering, Jaysingpur, India²⁻⁶

Abstract: Previously, patient records were stored in physical form which led to issues such as limited storage space, difficulty in locating records for elderly patients, and vulnerability to damage or destruction. To address these issues, e-health cloud solutions have been introduced as a secure and accessible way of storing patient reports. Data is crucial in making informed decisions and providing optimal patient care. Cloud computing provides a cost-effective means of collecting, storing, and sharing data in real-time among healthcare organizations. However, the security and privacy of patient data are major concerns when using cloud-based healthcare services. Encryption is an essential security measure, which should be easy to implement, provide high protection without compromising network performance, and serve as an additional layer of security to safeguard customers data.

Our focus is on data encryption in the healthcare cloud, which is the primary security concern in cloud computing. Authentication is the first step in data security and traditional authentication methods in cloud computing are insufficient to protect against advanced security threats. A dynamic approach to user authentication, which involves multiple authentication credentials, such as OTP, is necessary to enhance security. We propose a data security architecture that integrates a robust and viable multi-factor authentication scheme to ensure the security and privacy of patient data in the healthcare cloud

Keywords: AES; Cloud; Encryption; Decryption

I. INTRODUCTION

This project offers patient registration and data storage capabilities, allowing for the storage of all patient information on a website. By using a username, users can search for doctors' availability and access patient information. Patients can also access their information through a secure login process using a username and password. The information retrieval process is straightforward, and the system offers an excellent user experience. The data is securely protected for personal use, resulting in faster data processing times. The system is robust, adaptable, and user-friendly, with the primary goal of providing hospitals with the most significant advantages. It is designed specifically for hospital use and will cover various hospital management and administration processes.

An integrated hospital management system that smoothly distributes crucial information throughout the hospital can enable efficient decision-making for patient care, administration, and financial accounting. The primary objective of such a system is to enhance the quality and effectiveness of hospital management in areas such as clinical process analysis and activity-based costing. This system can help improve business growth, productivity, and job quality by effectively managing the essential core processes of the hospital.

This project enables hospitals to utilize cloud services to manage administration and technology needs and upload patient data for real-time access to information. The uploaded data can be accessed remotely through cellular networks and devices, and doctors can access the patient's medical history to aid in accurate treatment. [1] Among the various cloud services available, the e-health system stands out as a primary mode of operation for storing and sharing patient medical data using computer systems and cloud technology. Health information records are stored by a semi-reliable third-party provider (i.e., cloud) using cloud computing, which is an on-demand, self-service Internet infrastructure that enables users to access computing resources from any location at any time. [6]

Continuous and systematic innovation is crucial for healthcare to maintain its cost-effectiveness, efficiency, timeliness, and delivery of high-quality services. Experts and leaders in information technology (IT) anticipate that cloud computing will revolutionize the way IT is used, enhance healthcare services, and advance healthcare research. Several informatics advancements have demonstrated that cloud computing has the potential to solve these problems. However, despite the numerous benefits of cloud computing for the healthcare industry, there are several managerial, technological, security, and non-supervisory challenges that must be addressed.



II. EXISTING SYSTEM

The being system is a homemade system.

The current healthcare system relies on numerous records, resulting in significant time and resource consumption. In comparison to the proposed system, the current system has several drawbacks. One major issue is the risk of unauthorized access to data, which can lead to data tampering or loss. Managing data in the current system requires a substantial amount of hardware and software resources, causing delays in completing other important tasks.

Patients also face challenges accessing their personal data due to security concerns and the possibility of data loss. Moreover, patients are unable to access information regarding their enrolment status, appointments, and other details. The system's large amount of data and records are difficult to manage, leading to system crashes and longer processing times.[7]

III. PROPOSED METHODOLOGY

Data Pre-processing Module:

For the project we are going to use data collected from a hospital.

Data cleansing or data cleaning is the process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database and refers to identifying incomplete, incorrect, inaccurate, or irrelevant parts of the data and then replacing, modifying, or deleting the dirty or coarse data. .[4]

Home Page Module: -

Home page module is for access to the website. We give the patient login and Doctor login button. There are some buttons like home, how to register, about us, contact us for give some information to some people who is access our website.

Physician/Patient Registration Module: -

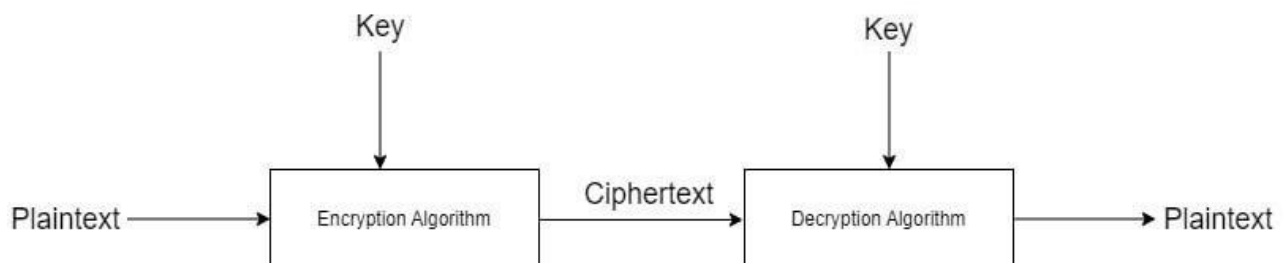
Patient creates their own account in E-health cloud solution website. To login into account for getting username and password. By using this we can store the information of the physician and the patient.

Admin Module:

Admin can add and delete doctor's information. He can create private and public events for both doctor and patient. Admin can also create note for all doctors or one specific doctor. On dashboard of admin top 5 doctors' patient will be displayed and it also displays daily patient count.

Data Encryption/Decryption Module :-

In this module we can store the user data on the cloud database. And retrieving a data in decrypted format.[8]





Physician and patient Login Module :-

Physician and patient can login into system. Using its own id and password given by system. Physician can store data of patient in to cloud. And patient only read the data into the system

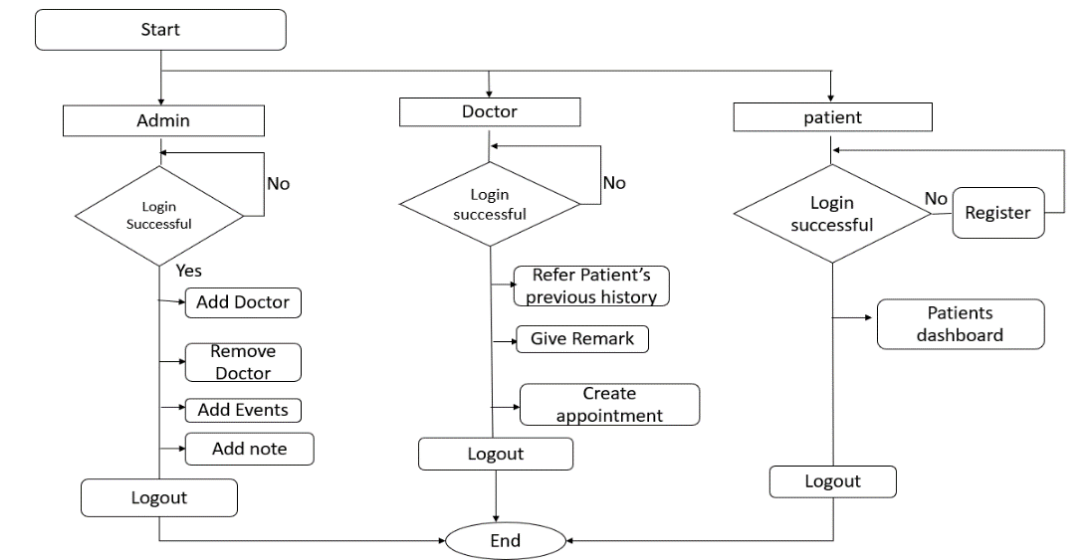


Fig.1 Flow chart of proposed system

Cloud Computing-

Cloud computing in the healthcare industry focuses on using distant servers connected to the internet. It facilitates the management, handling, and processing of medical data. The utilisation of internet servers to keep a sizable volume of data securely on cloud storage is practical for medical institutions and healthcare professionals.

These servers are often maintained by IT specialists. We used ‘S3’ which is AWS cloud service to store hospital’s data. Why using AWS for storage is preferable:

1. Many businesses employ this kind of infrastructure.
2. It is incredibly cost-effective due to its free first use and pay-per-use price structure.
3. Availability zone – Their data centres are accessible in more than 50 regions worldwide.

Advantages:

Durability – Amazon offers a wide range of extremely durable services.

Security – When it comes to storage, the safety of our data takes first. By providing automatic data encryption as soon as the uploading process is complete, S3 relieves us.

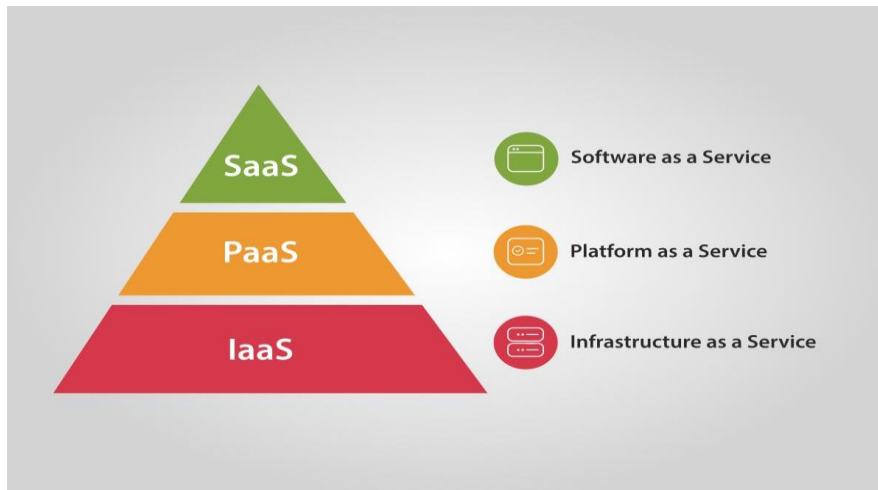


Fig.2 Cloud Service Models



Advanced Encryption Standard (AES) Algorithm:-

Advanced Encryption Standard is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.[2]

Advanced Encryption Standard is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement. .[3]

AES is a block cipher. The key size can be 128/192/256 bits.

Encrypts data in blocks of 128 bits each.

Each round comprises of 4 steps:

Block-diagram

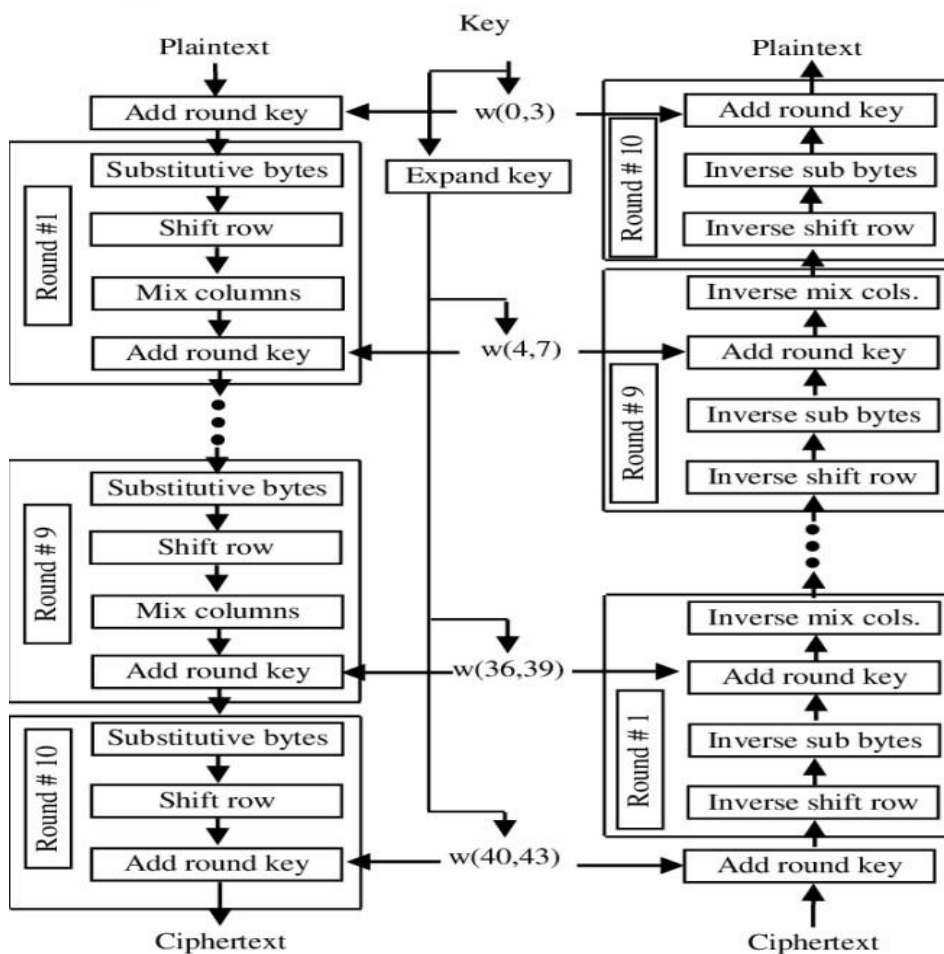


Fig.3 Advanced Encryption Standard (AES) Algorithm

Experimental results :-

In Paper[9], it is argued that RSA is not suitable for use in commercial applications due to several design flaws. If the values of p and q chosen for key generation are too small, the encryption process becomes vulnerable to attacks using random numbers. On the other hand, using larger p and q values leads to slower processing and poorer performance compared to DES. Based on a literature review and research, AES has been identified as the most efficient algorithm in terms of speed, time, throughput, and avalanche effect. Using multiple algorithms can further enhance the security provided by these methods.

The results presented in [10] indicate that the DES algorithm has the lowest CPU time, memory, and battery power requirements, while AES has the lowest memory usage. In contrast, RSA encryption algorithms consume substantial



amounts of CPU, memory, and battery power. The study compared RSA and DES algorithms with both public and secret keys and found that RSA resolves the key agreement and key exchange issues inherent in secret key cryptography, but it does not offer a comprehensive security system. Therefore, DES is still utilized. It should be noted that RSA and DES have differences in their respective features.

By comparing the DES and RSA algorithms with both public and secret keys, it becomes clear that RSA resolves the issues of key agreement and key exchange that arise from using secret key cryptography. However, RSA does not provide a complete security solution, which is why DES is still in use. Furthermore, there are differences in the features of RSA and DES.

As mentioned in [11], AES is a faster and more efficient symmetric encryption method. When data transmission is considered, there is little difference in performance between various symmetric key systems. This provides excellent security over an open network. However, the main disadvantage of symmetric algorithms is key transfer.

Factors	AES	DES	RSA
Developed	1972	2000	1978
Key length	56 bits	128 bits	$n=p*q$
Cipher Type	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Block Size	64 bits	128 bits	Variable
Security	Proven inadequate	Considered secure	Least secure
Rounds	16	10	1
Speed	Fast	Slow	Slowest

IV. RESULT

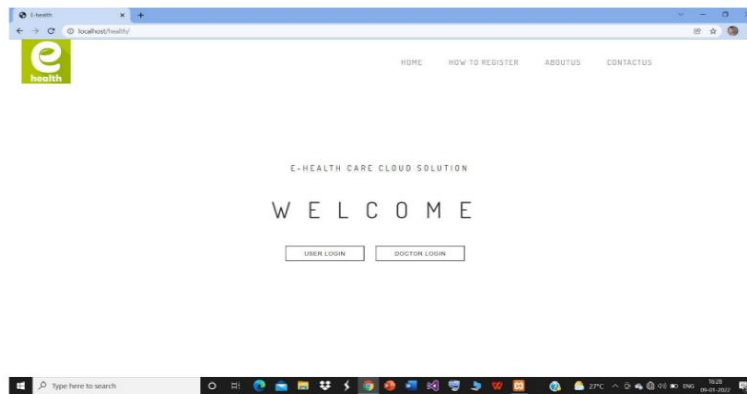


Fig 4 Dashboard

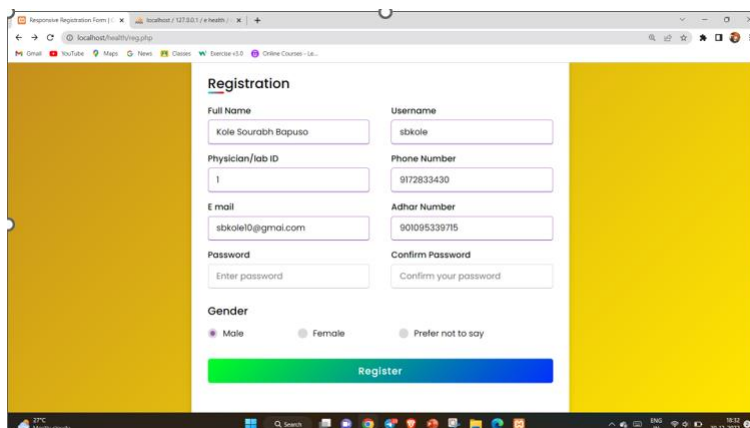


Fig 5 Registration page

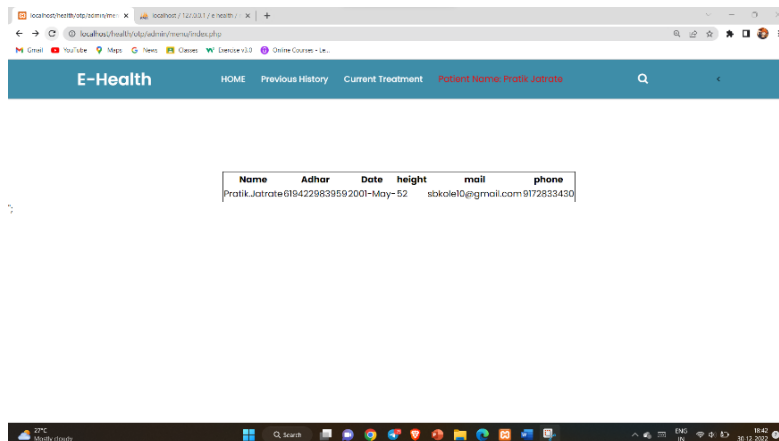


Fig 6. patients' history

V. CONCLUSION AND FUTURE SCOPE

CONCLUSION-

Our research and development project has resulted in a cloud service that provides data management and various capabilities for a health management system. The system utilizes cutting-edge cloud computing technology, and it is both efficient and user-friendly.

FUTURE SCOPE-

Our future plans involve implementing a web application that consolidates information on medication, blood bank (including available blood types), nursing and housekeeping services, financial details such as billing and payments, insurance information, and more. This single platform will provide a comprehensive solution for managing various aspects of healthcare management.

REFERENCES

- [1] Big Health Application System Based on Health IOTs and Big Data. <https://www.ieee.org.com> Y. Ma, Y. Zhang, J. Wan, D. Zhang, and N. Pan, "Robot and cloud-assisted multi-modal healthcare system,"
- [2] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.html
- [3] <https://www.geeksforgeeks.org/advanced-encryption-standard-idea/>
- [4] Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud <http://www.engpaper.in/www.iiitp.org> I. X. Yi, Y. Miao, E. Bertino, and J. Willemsen, "Multiparty privacy protection for electronic health records," in Proc. IEEE Global Commun.
- [5] Development of Smart e-Health System for Covid-19 pandemic. <http://www.iiitp.org/www.iiitp.org>
- [6] <https://www.ijraset.com/research-paper/hospital-management-system-using-cloud-technology>
- [7] <https://www.ijert.org/cloud-based-secure-multi-owner-hospital-management-system>
- [8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symposium on Security and Privacy (SP 2007), 2007, pp. 321–334
- [9] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975–8887) Volume 67–No.19, April 2013
- [10] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011
- [11] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma, "Analysis and Comparison between AES and DES Cryptographic Algorithm", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.