VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Title: SECURE E - PERSON HEALTH CARE SYSTEM USING AES ALGORITHM

Submitted By

Sethumadhavan V (19MIS0010)

ABSTRACT:

We live in a world where information is available in our fingertips. This has made life easy not only for the everyday consumer but also for healthcare industry as it means that they are able to get the crucial information that they need within a few seconds rather than waste time manually going through a paper trail. The successful storage, manipulation and retrieval of electronic medical records are some of the important functions of Electronic Health Care Systems. So, the confidentiality and integrity of health information is of paramount importance to healthcare management organizations. Unfortunately, the occurrence of information security breaches with regards to Electronic health records, which include loss of valuable data as a result of theft by unauthorized users, is increasingly becoming worrisome situations. We believe that there is a need for a system that provides timely information while at the same time protecting the confidentiality of the patient. Thus, the aim of our project is to design a healthcare database management system that ensures that unauthorized personnel can't access it. It will also enable quick and swift access for the authorized entities.

KEYWORDS:

Electronic Medical Records, E- Health Care Systems, Information hiding, Security, Symmetric encryption, AES.

Motivation: In recent time, the lose of data has been increased in medical system. To overcome this, we have taken this project . the motivation of this project is to secure the data of the patient using AES algorithm. The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.

PROBLEM STATEMENT:

Clinical and administrative data collection has been increasingly popular in recent years. To handle and regulate the collected data, medical centres such as hospitals, clinics, and other organisations use electronic healthcare systems. When it comes to data collecting, storage, and management, each industry faces its own set of regulatory and governance problems. However, the challenges faced by the healthcare industry are distinct. The data generated in healthcare is frequently complicated and subject to severe regulations. Most health care practitioners collect info on patients employing a kind of forms, together with patient intake forms, consent forms, treatment analysis forms, and health assessment forms, among others. This manual method, on the other hand, leaves a lot of possibility for errors like typos, incorrect entries, or filing the wrong documents in a patient's records. Furthermore, most paper forms do not enable for patient information to be available to all caregivers within 24 hours, particularly information gathered from outside sources. This may result in a patient's care being disconnected. In addition to that, patient health data may be exposed during the process.

SOLUTION:

It is recommended that there is a need for a system that provides timely information while at the same time protecting the confidentiality of the patient’s health records. If any attackers/intruders gain access to the data, it must be encrypted. The attacker should be unable to reveal the data. To do so employing symmetric encryption systems is one of the benefits of ensuring SAFETY in medical records. The AES encryption technique is used by model to encrypt the data. By using this, information on healthcare data can be saved. We are using fernet symmetric key encryption as it combines encryption along with message authentication and a time stamp to ensure that the data is protected, and

it has not been modified. Fernet uses 128-bit AES in CBC mode, with HMAC using SHA256 for authentication.

LITERATURE SURVEY TABLE:

Paper Title Authors & Year published	Proposed Methodology	Merits	Limitations/ Challenges
Assessment of Encryption and Decryption Schemes for Secure Data Transmission in Healthcare Systems. Authors: Kazeem B. Adedeji. Nnamdi I Nwulu, Clinton Aigboa and Saheed L. Gbadamosi. Year: 2019.	➢ Elliptic Curve ➢ Cryptography (ECC), ➢ Rivest Cipher 4 (RC4). ➢ Data Encryption Standard (DES), ➢ Advanced Encryption Standard (AES).	➢ Robust security protocols. ➢ It's hard to hack AES algorithm.	AES uses too simple algebraic structure and every block is always encrypted in the same way.
An Efficient Data Security in Medical Report using Block Chain Technology. Authors: Mary Subaja Christo, Anigo Merjora A, Partha Sarathy G. Priyanka C and Raj Kumari M. Year: 2019	Quantum Cryptography, for Encryption. 1.Authentication 2. Encryption and 3. Data Retrieval using Block Chain technology. AES(Advanced Encryption Standard).	➢ AES is fast algorithm with high security. ➢ Trustworthiness, ➢ Secure Authentication, ➢ Data Retrieval (only Doctors)	Patient can't modify the patient's medical History
Complexity of Cyber Security Architecture for IoT Healthcare Industry: A Comparative Study. Authors: Aysha, K. Alharam, and Wael Elmadany.	Complexity for cyber security architecture and its application in IoT healthcare industry	➢ AES Encryption algorithm is a symmetric block cipher algorithm. ➢ AES was known for its	Unable to sync the health and wellness information to our personal devices due to cyber security architecture.

Year: 2017		efficiency and its fast and strong algorithm. ➢ S-Box Implementation is used along with AES encryption.	
Cloud-Based E- Health Systems: Security and Privacy Challenges and Solution Authors: Mohanad, Dawoud, D.Turgay, Altılar. Year: 2017	→Integration of the e-health systems with the cloud computing systems. →Using Wireless Body Area Network (WBAN)	Home server is used to communicate between sensor and other devices. Very good in security and privacy protection.	Very hard to implement as it requires lot of resources and cost.o Maintenance cost is very high.
An Efficient Lightweight Cryptographic Technique For IoT based E-health care System. Authors: Ravi Raushan Kumar Chaudhary, Kakali Chatterjee. Year: 2020.	→Lightweight Block ciphers Technique (AES, DES AND SIMON)	Secure transmission of data of patients from these, IoT devices.Remote Health monitoring will save lot of time.	Wearable Devices may not show accurate data because of various factors like not wearing the smart watch Properly and so on.
Towards Secure and Smart Healthcare in Smart Cities Using Blockchain. Authors: Jinglin Qiu, Xueping Liang, Sachin Shetty.	Block Chain	Patient privacy. Patient confidentiality maintained.	User evaluations should be made both in laboratory and real hospital environments to study the usability of

Year: 2018.			access control solutions and how they impact on clinical work processes
A Privacy Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. Authors: Mingwu Zhang, Yu Chen, and Willy Susilo, Senior Member. Year:2020	→Clinical pathway development process using patient data. →Cloud Servers (CS) is used to outsource the medical data.	Better medical treatment. Privacy protection.	Privacy is still be Compromised, because no Encryption is used.
A Hybrid Data Access Control Using Aes And Rsa For Ensuring Privacy In Electronic Healthcare Records. Authors: S. Kanaga Suba Raja, A. Sathya, Year:2020	→The challenge of credential leakage in cloud storage system. →They have used RSA Algorithm.	Data owners encrypt their data under the relevant access policies prior to outsourcing the (encrypted) data to a Industrial cloud.	RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer. Data availability will be Compromised
[Ensuring Privacy and Security in Health. Authors: Jayneel Vora, Prit Italiya, Sudeep Tanwar, Year: 2018	Implemented the AT&T scheme to manage the access control mechanism of patient's data. →For security reasons, they have used applicable communication protocols.	The involvement of access control mechanism of patient's data brings a low cost alternative in Healthcare sector.	Drawback is that communication protocol includes weakness against the known network attacks.

Proposed Model

Advanced Encryption Standards – (AES ALGORITHM):

The initial round, the main rounds, and the final round are the three phases of the AES encryption phase.

The same sub-operations are used in different combinations in each step, as follows:

1. Initial Round

- Add Round Key

2. Main Rounds

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

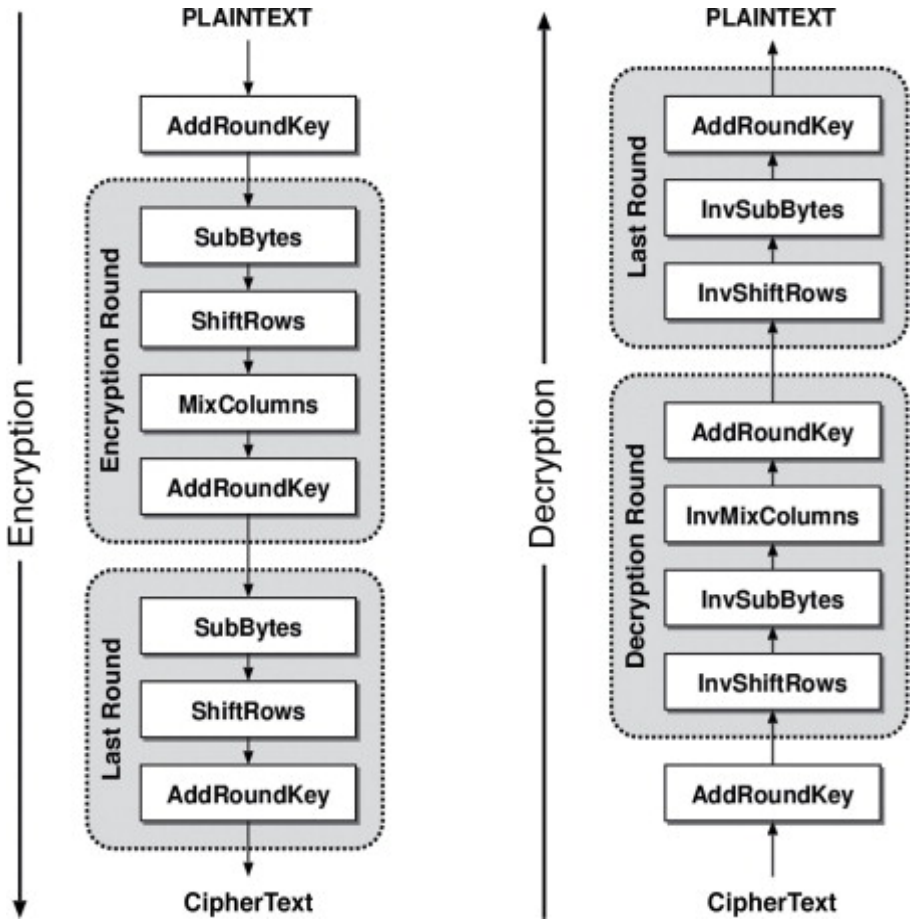
3. Final Round

- Sub Bytes,
- Shift Rows,
- Add Round Key.

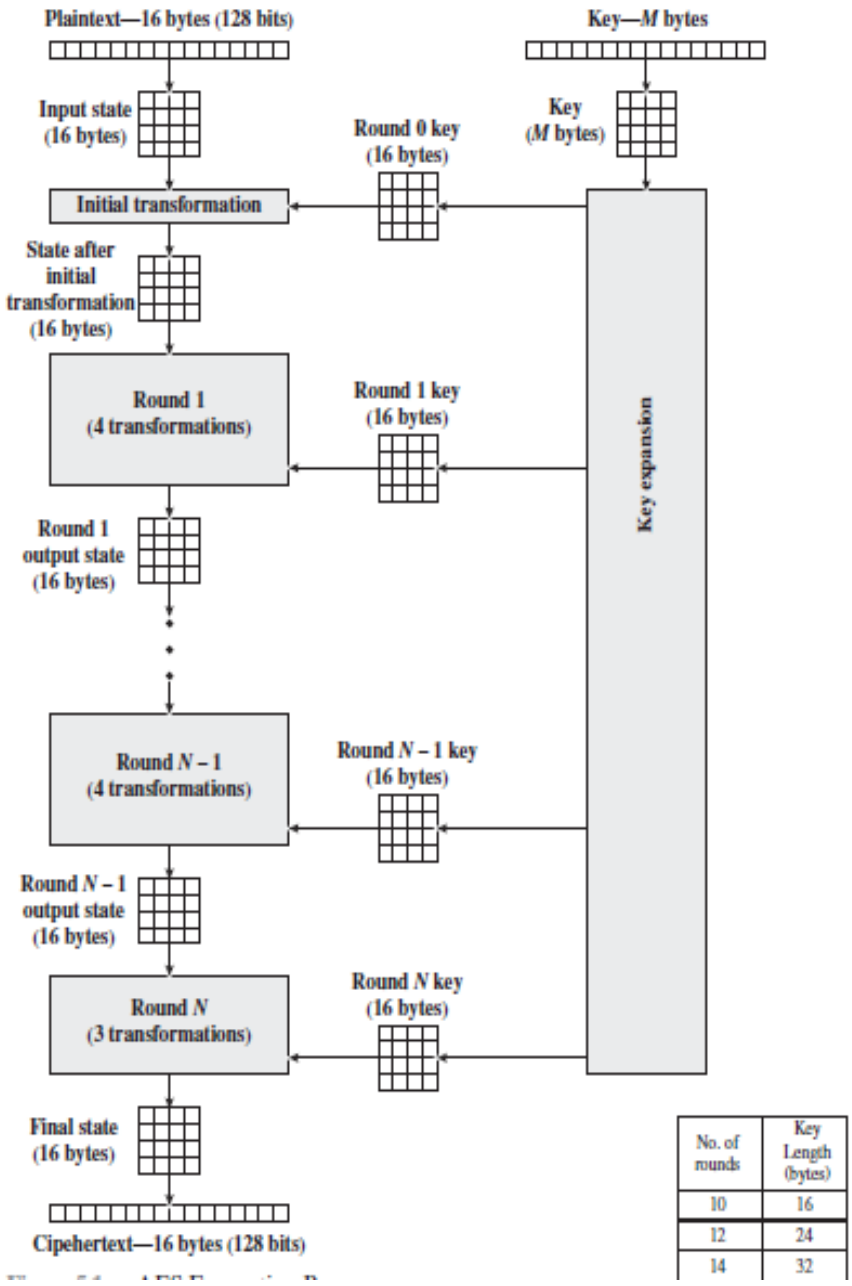
- Instead than using the Feistel cypher, AES uses an iterative approach. It is built on the substitution and permutation networks, which are two common approaches for encrypting and decrypting data (SPN). SPN refers to a set of mathematical operations used in block cypher techniques.

- AES can cope with plain text blocks of 128 bits (16 bytes) as a constant size. AES operates on a matrix of bytes, and these 16 bytes are represented in a 4x4 matrix. Another important element of AES is the number of rounds.

- The length of the key determines the number of rounds. The AES method uses three different key sizes to encrypt and decrypt data, including (128, 192 or 256 bits). The number of rounds is determined by the key size; for example, AES utilises ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys.



AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128- bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and in addition the round key. The order in which these four steps are executed is different for encryption and decryption. Unlike DES, the decryption algorithm differs substantially from the encryption algorithm. Although, the overall, same steps are used in encryption and decryption, the order in which the steps are carried out is different, as mentioned previously. Figure show, the overall structure of the AES encryption process.

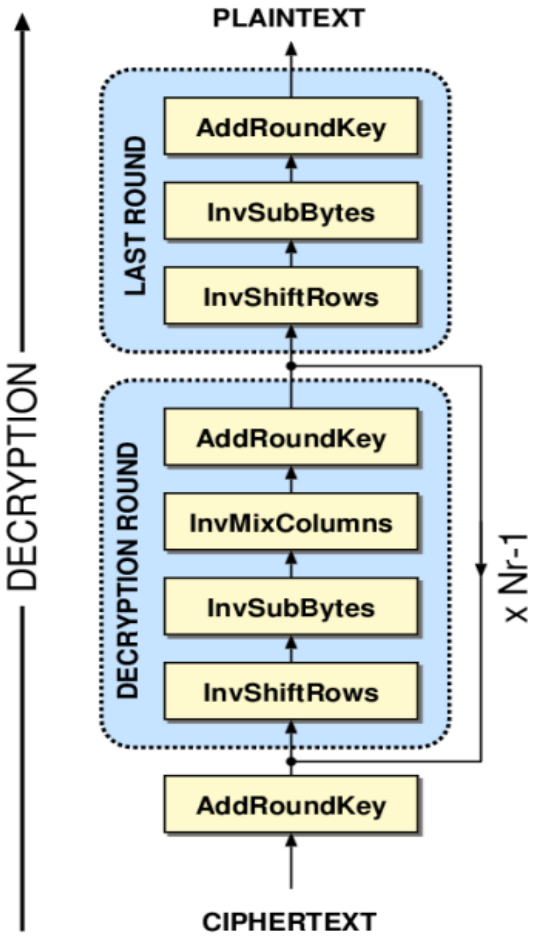


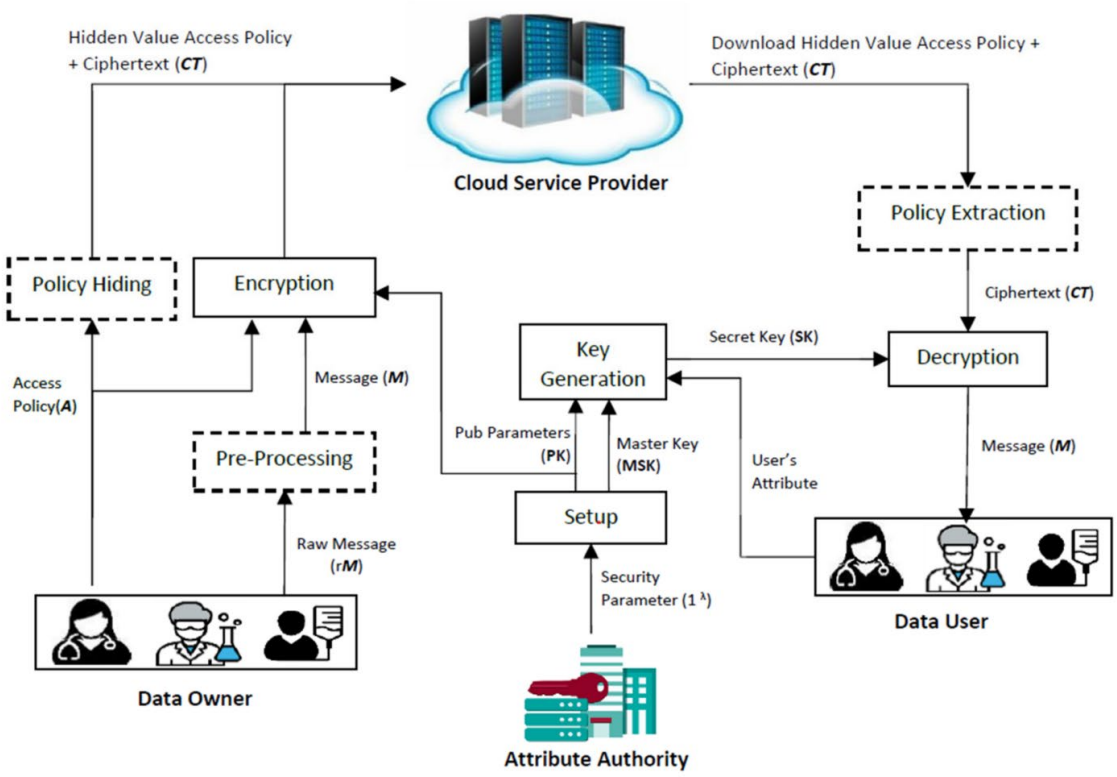
No. of rounds	Key Length (bytes)
10	16
12	24
14	32

The AES decryption method is similar to the encryption process in reverse order, and both the sender and the receiver use the same key to encrypt and decrypt data.

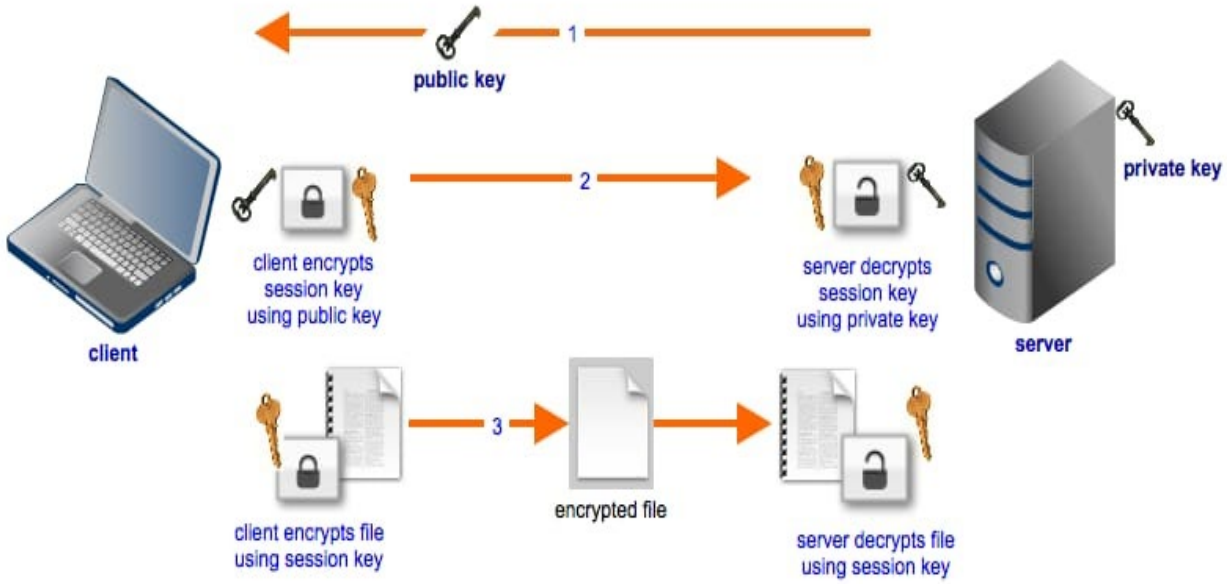
Three stages make up the final round of a decryption stage:

- Inv Shift Rows,
- Inv Sub Bytes,
- Add Round Key.


PLAINTEXT
AddRoundKey
InvSubBytes
InvShiftRows
LAST ROUND
AddRoundKey
InvMixColumns
InvSubBytes
InvShiftRows
DECRYPTION ROUND
x Nr-1
DECRYPTION
AddRoundKey
CIPHERTEXT


Hidden Value Access Policy + Ciphertext (CT)
Cloud Service Provider
Download Hidden Value Access Policy + Ciphertext (CT)
Policy Extraction
Policy Hiding
Encryption
Ciphertext (CT)
Key Generation
Secret Key (SK)
Decryption
Access Policy(A)
Message (M)
Pub Parameters (PK)
Master Key (MSK)
User's Attribute
Message (M)
Pre-Processing
Setup
Raw Message (rM)
Security Parameter (1 λ)
Data User
Data Owner
Attribute Authority

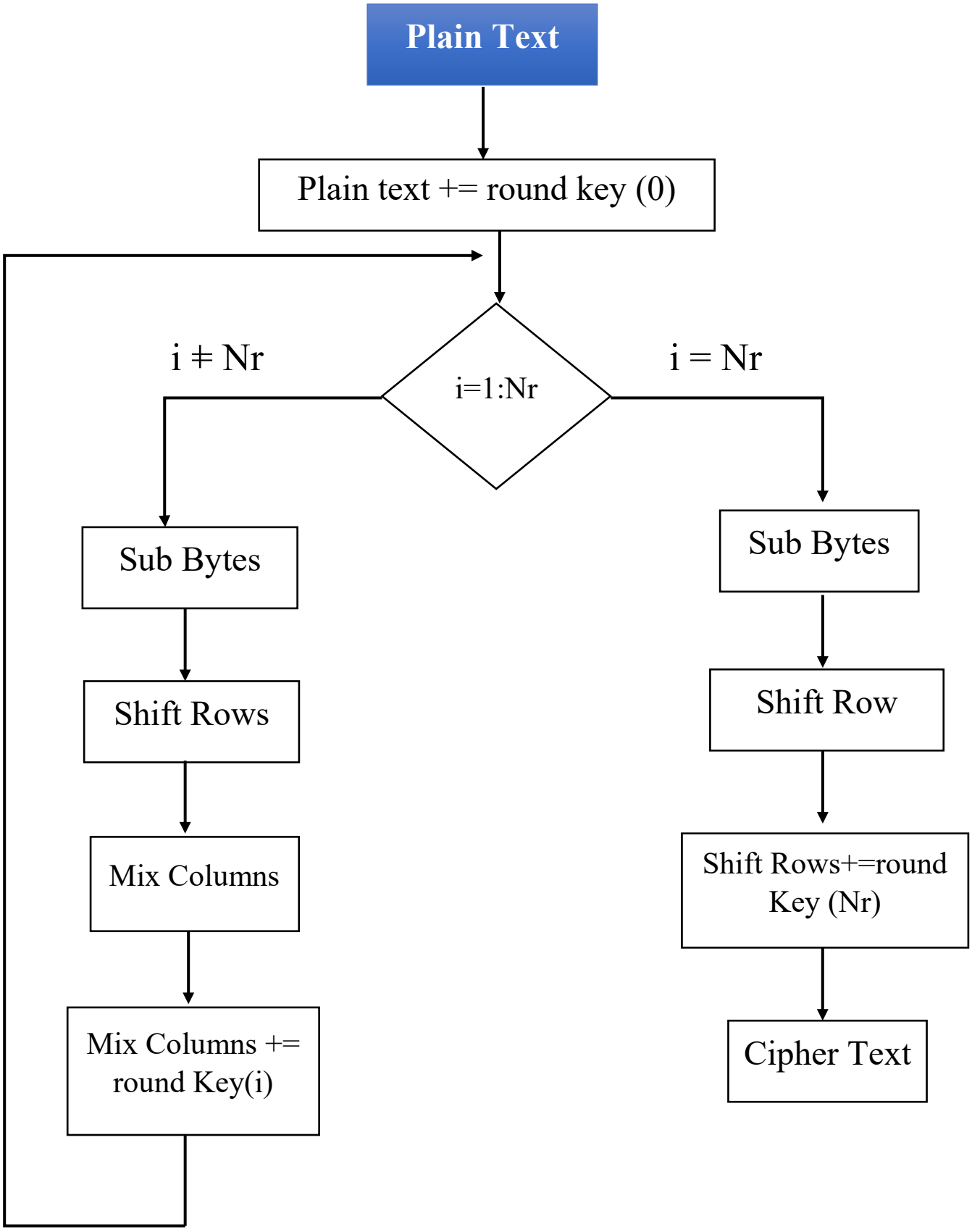
Functional architecture:



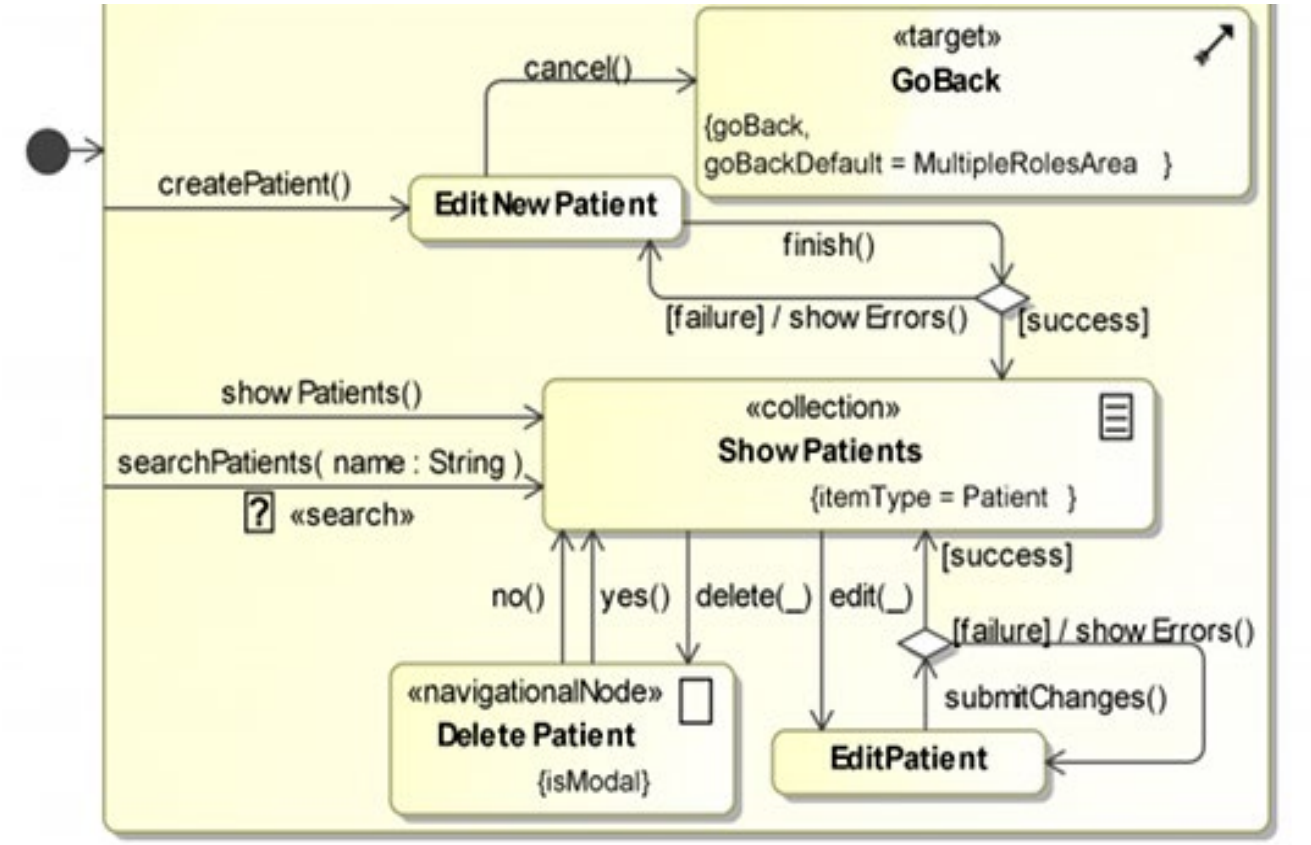
The criteria for being chosen as the next AES algorithm included the following:

- **Security:** Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition.
- **Cost:** Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- **Implementation:** Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.
- **Key Expansion:** It takes a single key up during the first stage, which is later expanded to multiple keys used in individual rounds.
- **Byte Data**: The AES encryption algorithm does operations on byte data instead of bit data. So it treats the 128-bit block size as 16 bytes during the encryption procedure.
- **Key Length:** The number of rounds to be carried out depends on the length of the key being used to encrypt data. The 128-bit key size has ten rounds, the 192-bit key size has 12 rounds, and the 256-bit key size has 14 rounds.

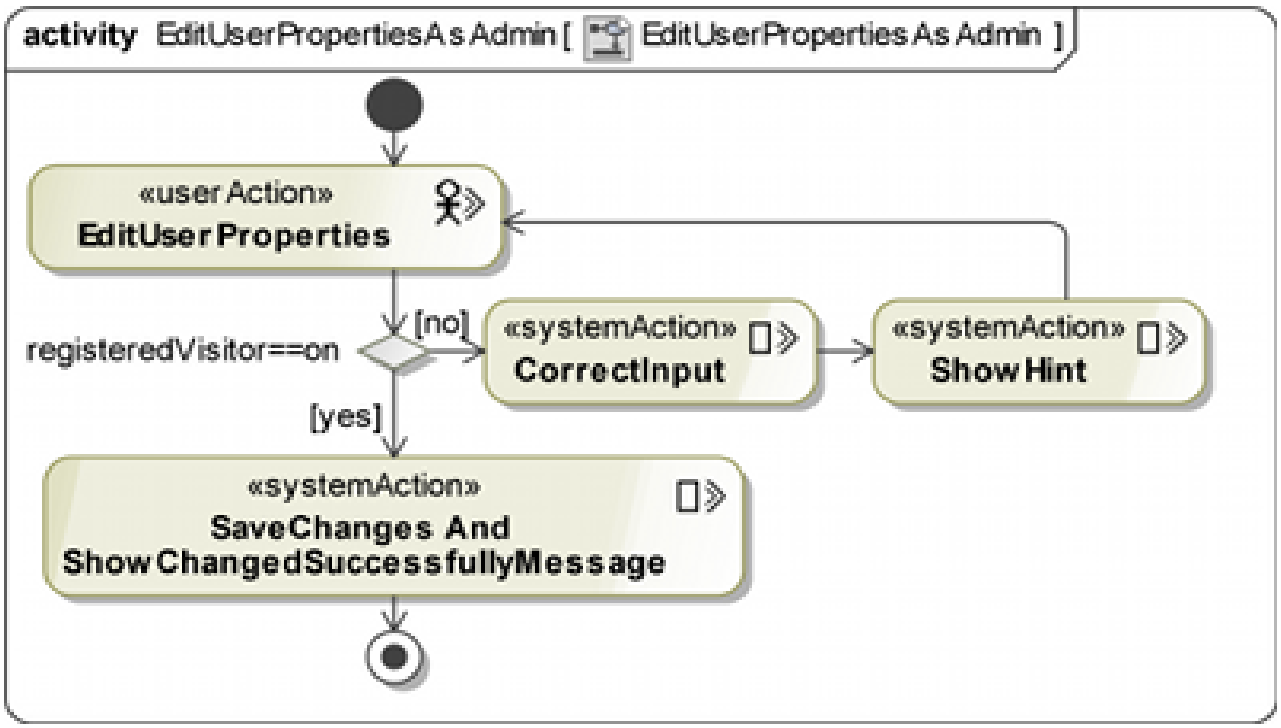
Modular design Flow diagram of AES Algorithm:



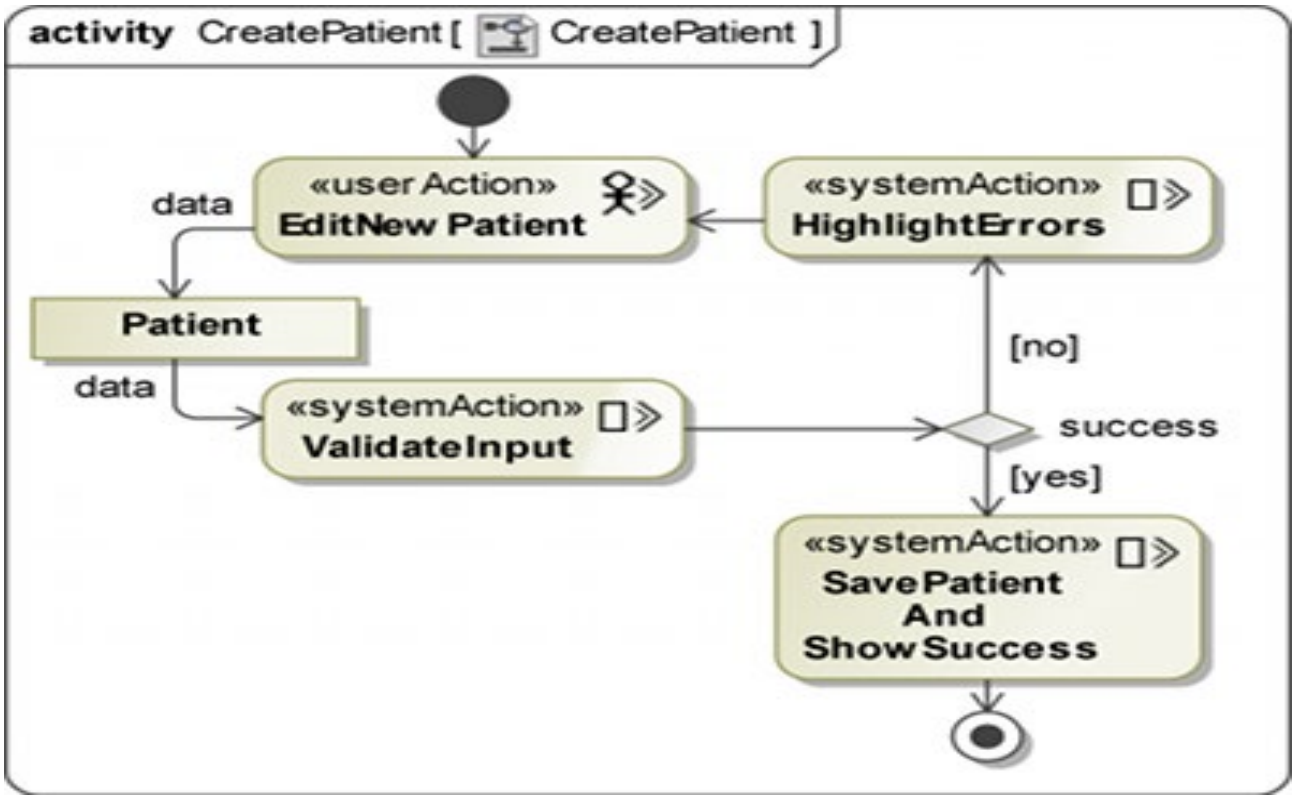
Doctor module:



Dean module:



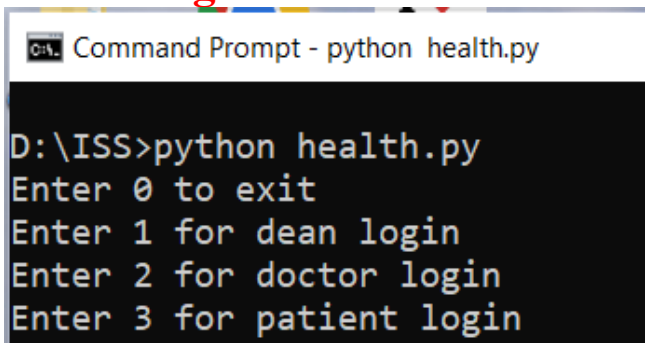
Patient module:



Platform / Tools:

Language: - Python
Platform: - IDLE Python

Home Page:



Dean Login:

Command Prompt

```
C:\Users\SETHU>D:

D:\>cd D:\ISS

D:\ISS>python health.py
Enter 0 to exit
Enter 1 for dean login
Enter 2 for doctor login
Enter 3 for patient login
Enter choice: 1
Enter password: PASSWORD
Verified
Enter 0 to exit
Enter 1 to add new doctor credentials
Enter 2 to access patient record
Enter 3 to access log book
Enter choice1
Enter doctor ID: 2002
Enter new password: 10.05.2002
Enter 0 to exit
Enter 1 to add new doctor credentials
Enter 2 to access patient record
Enter 3 to access log book
Enter choice2
Enter 0 to exit
Enter 1 to add patient record
Enter 2 to display patient record
Enter choice: 1
Enter patient ID: 005
Enter patient name: Sanjay
Enter patient blood type: B+
Enter patient gender: M
Enter patient age: 22
Enter patient's DoB: 12.09.2001
Enter patient's height: 198
Enter patient's weight: 98
Enter no: of allergies: Skin
        - tonic
 Patient medical conditions:
        - Cancer
        - TB
 Pathological test report:  0
 Patient phone no.:  9150636210
 Patient emergency no.:  9150636210
 Remarks:
        - Neck
        - hand
 Patient since :  Tue Nov  8 13:35:58 2022


 Enter 0 to exit
 Enter 1 to add patient record
 Enter 2 to display patient record
 Enter choice:
```

Doctor Login:

C:\Windows\System32\cmd.exe - python health.py

```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

D:\ISA>python health.py
Enter 0 to exit
Enter 1 for dean login
Enter 2 for doctor login
Enter 3 for patient login
Enter choice: 2
Enter doctor ID: 2002
Enter password :10.05.2002
Verified
Enter 0 to exit
Enter 1 to add patient record
Enter 2 to display patient record
Enter choice: 1
Enter patient ID: 0064
Enter patient name: Sai dhanush
Enter patient blood type: B+
Enter patient gender: Male
Enter patient age: 22
Enter patient's DoB: 20.11.2000
Enter patient's height: 187
Enter patient's weight: 87
Enter no: of allergies: 1
Enter allergy: Skin
Enter no: of medications: 1
Enter medication: oin.Fourdearm
Enter no: of medical conditions: 0
Enter pathological test report: 0
Enter phone no.: 9159299878
Emter emergency no.: 108
Enter no: of remarks: 0
Enter 0 to exit
Enter 1 to add patient record
Enter 2 to display patient record
Enter choice: 2
Enter patient ID: 0064

Patient ID:  0064
Patient name:  Sai dhanush
Patient blood type:  B+
Patient gender:  Male
Patient age:  22
Patient's DoB:  20.11.2000
Patient height:  187
Patient weight 87
Patient allergies:
        - Skin
Patient medications:
        - oin.Fourdearm
Patient medical conditions:
Pathological test report:  0
Patient phone no.:  9159299878
Patient emergency no.:  108
Remarks:
Patient since :  Wed Nov 16 17:21:05 2022


Enter 0 to exit
Enter 1 to add patient record
Enter 2 to display patient record
Enter choice:
```

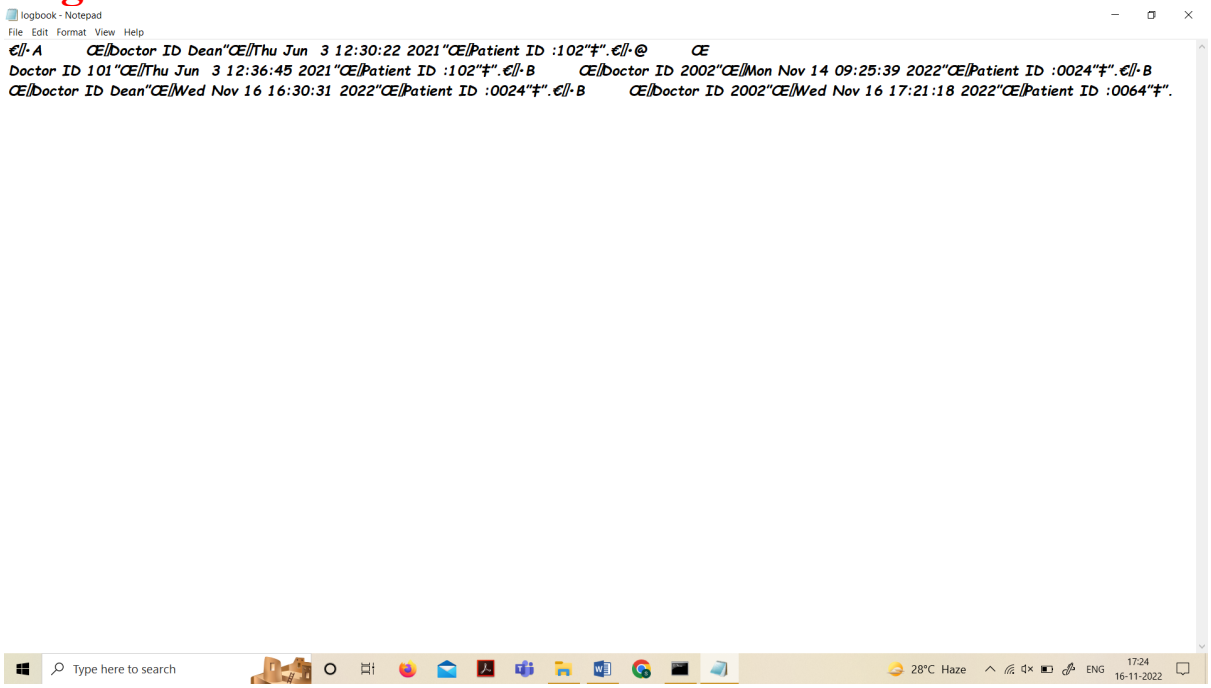
Patient Login:

C:\Windows\System32\cmd.exe - python health.py

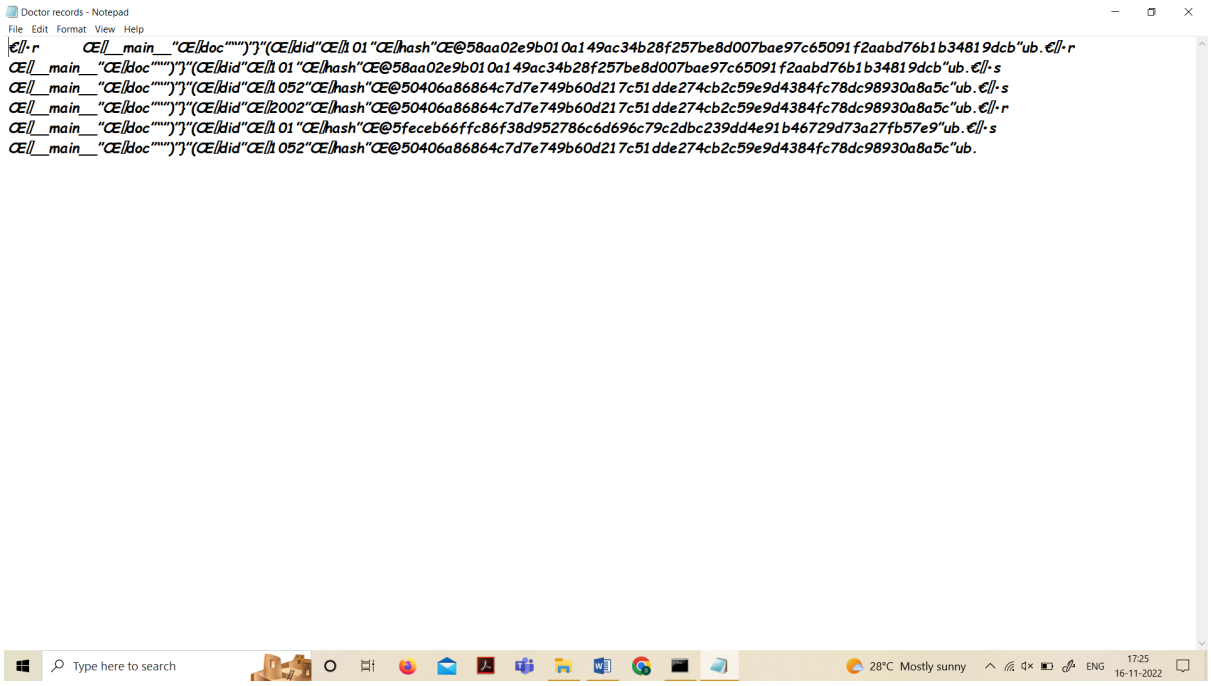
```
Enter date of birth : 20.11.2000


Patient ID:  0064
Patient name:  Sai dhanush
Patient blood type:  B+
Patient gender:  Male
Patient age:  22
Patient's DoB:  20.11.2000
Patient height:  187
Patient weight 87
Patient allergies:
        - Skin
Patient medications:
        - oin.Fourdearm
Patient medical conditions:
Pathological test report:  0
Patient phone no.:  9159299878
Patient emergency no.:  108
Remarks:
Patient since :  Wed Nov 16 17:21:05 2022
```

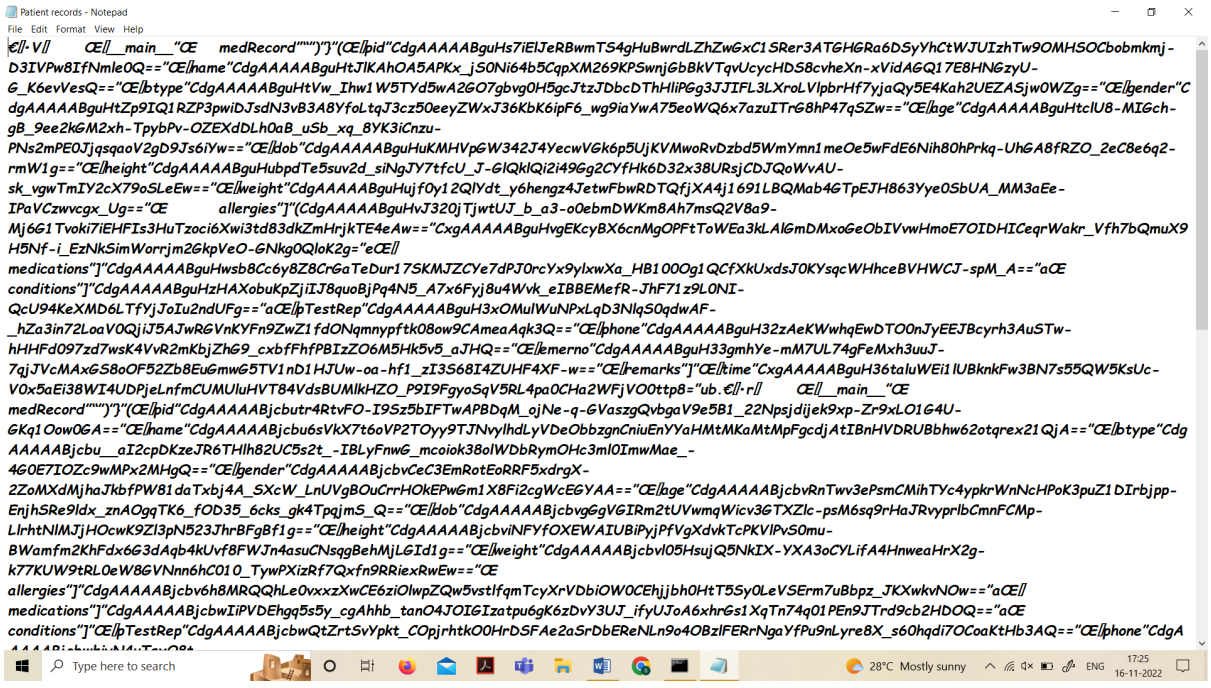
Log Book Record:



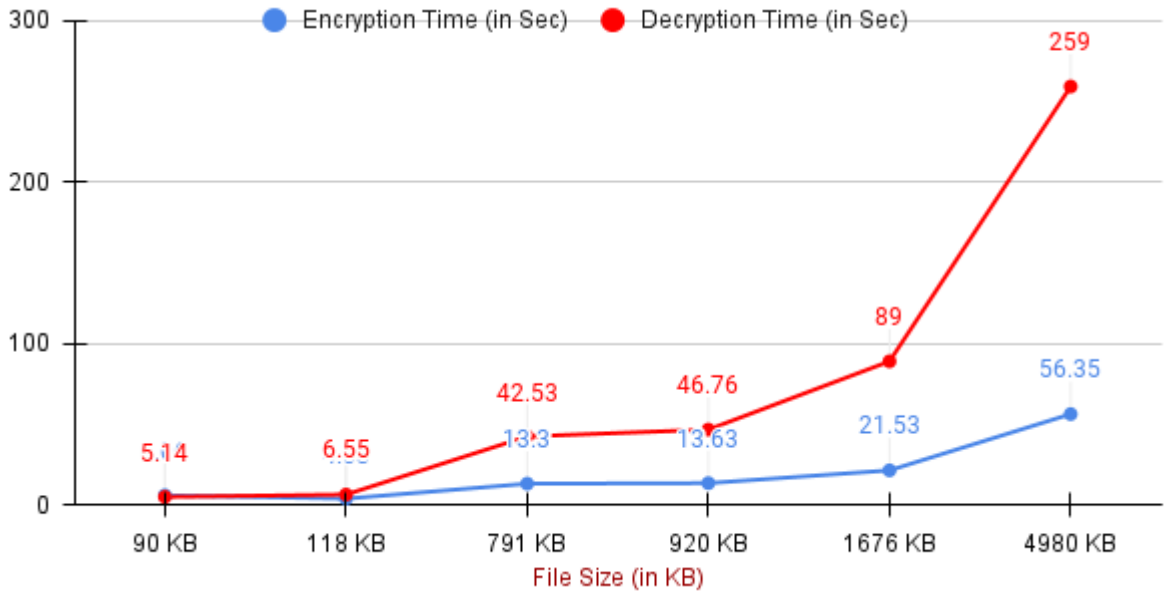
Doctor Record:



Patient Record:



Encryption and decryption time in terms of graph:



Real Time Application: -

Health care today is more digitally enabled than ever before, and the transformation has demonstrated major benefits for patients and providers alike. With patient information stored digitally, physicians can quickly access and update accurate records. The added speed of care this enables can save lives, and organizations around the world are doing all they can to ensure their digital capabilities evolve on pace with the sector. As with any high-speed digital evolution, however, there are complexities and risks. Namely, new capabilities come with their own security issues. Hospitals and other facilities must invest heavily in **SECURE E - PERSON HEALTH CARE SYSTEM,** with well-trained staff members taking responsibility for putting these processes in place.

Conclusion:

The system which hospital managements are using currently is extremely liable to data breach and is not available handy all the time. There's always the likelihood that data are often stolen, modified, or tampered. The information is maintained in an exceedingly record file or book manually and also the book is kept with the hospital staff. It's a awfully tedious job to look the mandatory records from the book and to take care of the book for a protracted time. Hence there is a need for a system that maintains data properly and also keeps it secure and easy to use. We have successfully designed a healthcare database management system using, AES and SHA-256 algorithms to secure the sensitive data and passwords. We were able to create a program that could protect a patient's privacy while at the same time ensuring the information is available to the required personnel when required.

Improvements in future:

- Cloud based server development.
- Mechanism to provide data for research without revealing patient's personal data.
- Giving dean the power to re-assign a patient to a new doctor.

References

[1]. Kazeem B. Adedeji, Nnamdi I. Nwulu, Clinton Aigboa and Saheed L."Assessment of Encryption and Decryption Schemes for Secure Data Transmission in Healthcare Systems.Authors: Gbadamosi".2019.

[2]. Nikhil Nair R, Kiran K A. "Smart Secure System for Human Health Monitoring". 2017.

[3]. Mary Subaja Christo, Anigo Merjora A, Partha Sarathy G, Priyanka C and Raj Kumari M. "An Efficient Data Security in Medical Report using Block Chain Technology". 2019.

[4]. Aysha, K. Alharam, and Wael Elmadany. "Complexity of Cyber Security Architecture for IoT Healthcare Industry: A Comparative Study". 2017.

[5]. Mohanad, Dawoud, D.Turgay, Altilar. "Cloud-Based E-Health Systems: Security andPrivacy Challenges and Solution". 2017.

[6]. Jayneel Vora, Prit Italiya, Sudeep Tanwar, Sudhanshu Tyagi."Ensuring Privacy and Security in Health". 2018

[7]. Ravi Raushan Kumar Chaudhary, Kakali Chatterjee. "An Efficient Lightweight Cryptographic Technique For IoT based E-health care System".2020.

[8]. Mingwu Zhang , Yu Chen, and Willy Susilo , Senior Member."A Privacy Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems". 2020.