

Enhanced Medical Data Security Framework

Dr. Madhuri Kovoov¹, Mounika Bandaru², Surya Teja Kancha³, Manvitha Peddapurapu⁴

1. Associate Professor, Dept. of CSE, Anurag University, Hyderabad, India
2. UG Student, Dept. of CSE, Anurag University, Hyderabad, India
3. UG Student, Dept. of CSE, Anurag University, Hyderabad, India
4. UG Student, Dept. of CSE, Anurag University, Hyderabad, India

ABSTRACT: Medical field deals with a lot of physical actions, reactions and responses. Most of the communication between doctor and the patient is not digital. But, it would be easier, if it was. This framework allows the patient and the doctor to have contact over a network. It also follows the security parameters, confidentiality, authentication and integrity, by encryption, access control policy and, key management. Only the authorized doctor will be able to view the patient file. This helps both the parties involved, as the doctor does not need to view every patient file and the patient need not worry about the security.

KEYWORDS: Confidentiality, security, Encryption, Decryption, Key management.

1.INTRODUCTION

Medical data stands out as a highly confidential and crucial subset, encompassing a patient's health records, medical history, diagnosis, and prescriptions. The sensitivity of this data necessitates stringent privacy measures, restricting access solely to the patient and their designated healthcare provider. Data, a versatile information resource, is particularly critical in the context of medical information, encompassing patient health records and other sensitive details. The rising importance of preserving the confidentiality of medical data has led to the development of many strategies. These strategies include secure storage, encryption, access control policies, and regulated data sharing, ensuring that only authorized individuals can access and interact with the information. This approach concentrates on the three security parameters, confidentiality, authentication and integrity. These parameters are the basic units to establish any security framework. Considering them, the framework has been designed. It also encompasses a secure infrastructure of the storage of patient information to ensure everything is only visible to the authorized. It employs encryption protocols to safeguard the information when it is transmitted. Access control policies are implemented to regulate user access.

2. LITERATURE REVIEW

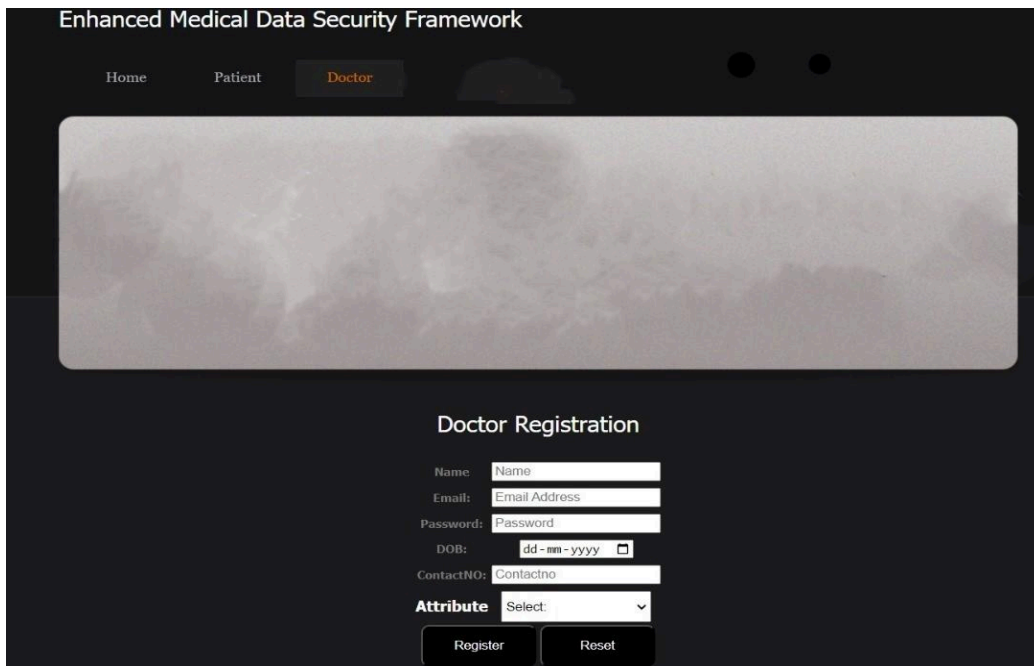
Senthil Murugan Nagarajan's IoMT Security [1] utilizes RES-256 algorithm for ensuring confidentiality and integrity of medical data during transmission. While effective, it may pose computational demands in resource-constrained environments. Proper key management is crucial to avoid vulnerabilities. "Emerging security mechanisms for medical cyber-physical systems"[2] explores security advancements tailored for medical cyber-physical systems, focusing on

addressing vulnerabilities, ensuring data integrity, confidentiality, and system reliability. It emphasizes adaptability to evolving cyber threats but acknowledges potential complexity and costs in implementation. "A secure IoT-based modern healthcare system with fault-tolerant decision-making process" [3] discusses designing a secure healthcare system leveraging IoT for connectivity and data exchange. It emphasizes fault-tolerant decision-making processes to ensure system resilience without compromising patient care. Challenges may include technical expertise required for implementation. "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0"[4] focuses on designing secure health data sharing mechanisms within medical cyber-physical systems, aligned with the Healthcare 4.0 paradigm. It utilizes user-centric design and evaluates performance on smartphone platforms for efficiency. "Secure Medical Data Sharing For Healthcare System"[5] proposes a mechanism for secure distributed data storing and sharing, using data splitting and encryption approach. It ensures data recovery requires approval from trusted nodes, enhancing robustness and minimizing transmission delays. An iterative algorithm optimizes node selection for data storage.

3. PROPOSED METHOD

3.1 Registration and Login

The proposed method is an interface or a framework that enables an easy communication time between patient and his or her requested doctor. To enter into the interface both the patient and doctor need to either register or login. The login page is the first page that will come up, seeking the email and password of the doctor. If the doctor is not yet registered there is an option for a new user to click and register as shown in Figure 3.1.1.



The screenshot displays a web interface titled "Enhanced Medical Data Security Framework". At the top, there are three navigation tabs: "Home", "Patient", and "Doctor", with "Doctor" being the active tab. Below the tabs is a large, blurred rectangular area. The main section of the page is titled "Doctor Registration" and contains a form with the following fields: "Name" (text input), "Email" (text input with "Email Address" placeholder), "Password" (text input), "DOB" (date picker set to "dd-mm-yyyy"), "ContactNO" (text input with "Contactno" placeholder), and "Attribute" (a dropdown menu with "Select:" as the current selection). At the bottom of the form are two buttons: "Register" and "Reset".

Figure 3.1.1 Doctor Registration page

In this page , the details of the doctor are to be filled in. They include, name, email, a new password, date of birth and contact number. Attribute section of the details is the type of specialist the doctor is referred to as, so it will become easy when taking up cases. As shown in Figure 3.1.2, the doctor fills up all the information and the login page opens up again. The doctor can then put in the password that was previously created and gain access to the interface.

The screenshot shows the 'Enhanced Medical Data Security Framework' interface. At the top, there is a navigation bar with 'Home', 'Patient', and 'Doctor' tabs, with 'Doctor' being the active tab. Below the navigation bar is a large, blurred image placeholder. Underneath the image, the text 'Doctor Login' is centered. Below this, there are two input fields: 'E-Mail:' with a placeholder 'Enter E-Mail' and 'Password:' with a placeholder 'Password'. Below these fields are two buttons: 'Submit' and 'Reset'. At the bottom, there is a link that says 'New User Click Here To Register'.

Figure 3.1.2 Doctor Login page

Similarly, the patient login and registration takes place.

The screenshot shows the 'Enhanced Medical Data Security Framework' interface. At the top, there is a navigation bar with 'Home', 'Patient', and 'Doctor' tabs, with 'Patient' being the active tab. Below the navigation bar is a large, blurred image placeholder. Underneath the image, the text 'Patient Registration' is centered. Below this, there are five input fields: 'Name' with a placeholder 'Name', 'Password:' with a placeholder 'Password', 'Email:' with a placeholder 'Email Address', 'DOB:' with a placeholder 'dd-mm-yyyy' and a calendar icon, and 'ContactNO:' with a placeholder 'Contactno'. Below these fields are two buttons: 'Register' and 'Reset'.

Figure 3.1.3 Patient Registration page

Enhanced Medical Data Security Framework

Home Patient Doctor

Patient Login

E-Mail:

Password:

New User [Click Here To Register](#)

Figure 3.1.4 Patient Login page

3.2 File Upload and Key Generation

After the patient registration and login page the patient will be able to upload a text file in which he or she would address their concerns. As shown in figure 3.2.1, the patient will be able to upload a text file, while also entering his or her id and selecting the type of doctor they want to consult.

Upload Patient Data

Patient ID:

Attribute:

File Upload:

Doctor, I've been experiencing persistent abdominal pain and discomfort for the past few weeks. The pain is localized to the upper right side of my abdomen and often radiates to my back and shoulder. It's a dull, constant ache that sometimes intensifies after eating fatty or greasy foods. Additionally, I've noticed that my appetite has decreased recently, and I've been feeling nauseous, especially in the mornings.

I haven't had any significant changes in my diet or lifestyle that could explain these symptoms. I try to eat healthily and exercise regularly, but the abdominal pain is making it difficult for me to enjoy meals or engage in physical activity. I don't have a history of gastrointestinal issues, but I'm concerned that these symptoms could be indicative of a more serious underlying condition.

I've tried over-the-counter antacids and pain relievers to alleviate the discomfort, but they only provide temporary relief. The pain persists, and it's starting to affect my daily life and productivity. I don't have any allergies or sensitivities to food, and I haven't experienced any recent trauma or injury to the abdomen.

Doctor, what could be causing these symptoms? Could it be related to a digestive disorder or a problem with my gallbladder or liver? Are there any tests you recommend to help diagnose the issue? Also, what steps can I take to manage the abdominal pain and improve my overall digestive health?

Figure 3.2.1 Patient file Upload

After uploading the patient will be able to view data like it is shown in Figure 3.2.2

View Data & Encrypt the Data				
Patient Id	Filename	Data	Attribute	Key Gen
54425	phy2.txt	<p>Doctor, I've been experiencing persistent abdominal pain and discomfort for the past few weeks. The pain is localized to the upper right side of my abdomen and often radiates to my back and shoulder. It's a dull, constant ache that sometimes intensifies after eating fatty or greasy foods. Additionally, I've noticed that my appetite has decreased recently, and I've been feeling nauseous, especially in the mornings.</p> <p>I haven't had any significant changes in my diet or lifestyle that could explain these symptoms. I try to eat healthily and exercise regularly, but the abdominal pain is making it difficult for me to enjoy meals or engage in physical activity. I don't have a history of gastrointestinal issues, but I'm concerned that these symptoms could be indicative of a more serious underlying condition.</p> <p>I've tried over-the-counter antacids and pain relievers to alleviate the discomfort, but they only provide temporary relief. The pain persists, and it's starting to affect my daily life and productivity. I don't have any allergies or sensitivities to food, and I haven't experienced any recent trauma or injury to the abdomen.</p> <p>Doctor, what could be causing these symptoms? Could it be related to a digestive disorder or a problem with my gallbladder or liver? Are there any tests you recommend to help diagnose the issue? Also, what steps can I take to manage the abdominal pain and improve my overall digestive health?</p>	Physician	click

Figure 3.2.2 View Data

Then there is a key generation option that generates a unique key for that specific file. When it is clicked the page immediately shows 'Key generated successfully', as it appears in Figure 3.2.3.



Figure 3.2.3 Successful Key Generation

From the patient's side, keys generated can be viewed along with encryption time of the data as well as the cipher text like shown in figure 3.2.4.

View Keys				
Patient Id	Filename	Data	Cipher Data	Encryption Time
54425	phy2.txt	<p>Doctor, I've been experiencing persistent abdominal pain and discomfort for the past few weeks. The pain is localized to the upper right side of my abdomen and often radiates to my back and shoulder. It's a dull, constant ache that sometimes intensifies after eating fatty or greasy foods. Additionally, I've noticed that my appetite has decreased recently, and I've</p>	<p>YJAaH6//3Xplil4GpXEkS445BPr1rftz6w6uXZ6YH4j9KbPU05 jB2sQ78tocvjwCO+ESKo/dq3hLS aDL0szvkYUu8fL6NTEAkyOeVksnmfPxCPIiISy+G0PB6K7UJ 7IVgXlJch7FqosVQJgwbRKRd47 LoOu7PwmczNYG0B30V9MAwJjlni+rnrrnlsui8N523PxhWQ5et qP6sYMRnbZTKswXSozQyqC8Rsem udPusQmC0158UZDq1aRhwQualEIsvu/gQ9N1rvCW0HCct9rD/ nrcJEJg149hR6KHZ6VCg+ACVfV rRXjaLX38kehBEaEPA0CCF4bgFv6tQ7m3mjQetkH++6p58eby</p>	39

Figure 3.2.4 View Keys

3.3 Key Requests and Receiving Files

In the doctor's side of the interface, he or she will be able to see a series of files in encrypted form. If the doctor wants to view and treat a certain patient, they can send for a key request. Then the key request will be sent successfully as shown in the Figure 3.3.1

View Data & Send request				
Patient Id	Patient Name	Filename	Data	Send request
5441	sowp8029@gmail.com	phy1.txt	YY6bJI4LPT0C+3QRpomb qEu/t15nRFokFoLrM1J5	click
5419	20eg105419@anurag.edu.in	skin1.txt	HrFdp6c7xNKTEqdL8qnE gUZMwtp3DLewzsI19HjD	click
5404	bhanu@gmail.com	heart1.txt	50sRG7jP0i+Eqb/KoKHx TwHwiIdwIevv52UjttWE	click
5160	kiran@gmail.com	heart2.txt	pUUsfVa6aakgNx/iGXj9 K1tp22axwTHnFkVBOhnF	click
5472	shivam@gmail.com	skin2.txt	A2WLbQRKUaz6I7ZkvEeu /QXMwgdhJpH0n2uhhkYp	click
54410	bhavya@gmail.com	skin1.txt	NreApSuJvv1B5JacYZXE 0PW4LgKPWUFQTHDeGfp9	click
54425	20eg105425@gmail.com	phy2.txt	Y3AaH6//3Xp1i14GpXEk S44SBPr1rMz6w6uXZ6YH	click

Figure 3.3.1 Send Request

The patient will immediately receive a request along with the doctor's attribute. If the request is sent by the specialist the patient wants to consult, he or she will be able to verify and send the key(Figure 3.3.2) The key will be sent to the doctor's mail from which he or she can copy the key for further process as shown in Figure 3.3.3

View Doctor's Request & Send Skey				
Doctor	Patient Id	Filename	Doctor Attribute	Verify Attribute & Send Key
svnikutti@gmail.com	54425	phy2.txt	Physician	click

Figure 3.3.2 Send Key

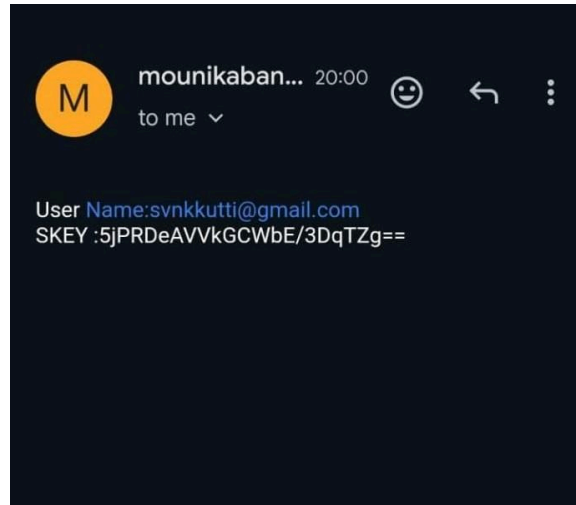


Figure 3.3.3 Mail

The file can be downloaded by the doctor after the correct key is given and if the wrong key is provided it denies the access (figure 3.3.3 and 3.3.4).

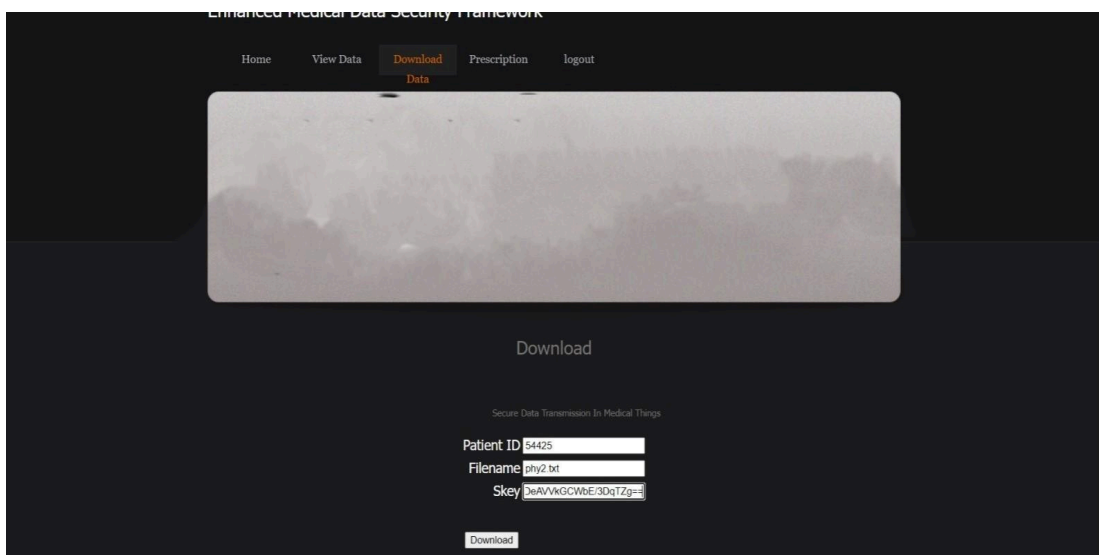


Figure 3.3.3 Download



Figure 3.3.4 Key Not Matched

The doctor is now able to view and diagnose the patient's concern. The communication between both the parties is established successfully and securely. One way communication is not sufficient when it comes to medical issues. The doctor should also be able to send his or her answer as a prescription to the patient. To achieve that, there is an option called share prescription that allows the doctor to write medication and tell the patient what to do further with the condition as mentioned in Figure 3.3.5

Share Prescription

Secure Data Transmission In Medical Things

Patient ID

Patient Name

Prescription

For abdominal pain and discomfort associated with digestive issues such as gallbladder inflammation (cholecystitis) or gallstones, healthcare providers may prescribe pain relievers, antacids, proton pump inhibitors (PPIs), or antibiotics, depending on the underlying cause.

One specific medication commonly used for gallstone-related symptoms is ursodeoxycholic acid (UDCA). UDCA is a medication that can help dissolve small cholesterol gallstones and reduce the severity of symptoms. It's often prescribed in cases where surgery to remove the gallbladder (cholecystectomy) is not immediately necessary or desired.

Figure 3.3.5 Prescription

The screen will show that the prescription is sent successfully. On the other side, the patient receives the prescription and will be able to view it directly like it is shown in Figure 3.3.6.

View Doctor's Prescription

Doctor Name	Patient Id	Patient Name	Doctor's Prescription
svnkkutti@gmail.com	54425	20eg105425@gmail.com	For abdominal pain and discomfort associated with digestive issues such as gallbladder inflammation (cholecystitis) or gallstones, healthcare providers may prescribe pain relievers, antacids, proton pump inhibitors (PPIs), or antibiotics, depending on the underlying cause.
			One specific medication commonly used for gallstone-related symptoms is ursodeoxycholic acid (UDCA). UDCA is a medication that can help dissolve small cholesterol gallstones and reduce the severity of symptoms. It's often prescribed in cases where surgery to remove the gallbladder (cholecystectomy) is not immediately necessary or desired.

Figure 3.3.6 Prescription View

4. RESULTS

The encryption algorithms such as AES encrypting data of different types and sizes. Parameters like key lengths and modes of operation will be varied to analyze their impact on encryption strength and speed. Encryption time for existing methods and proposed methods is compared

based on the values of Table 4.1 and Figure 4.1 shows the graph of encryption times.

Input File Type (KB)	Existing Method	Proposed Method
1	50	45
2	120	105
3	207	190
4	250	230
5	303	275

Table 4.1

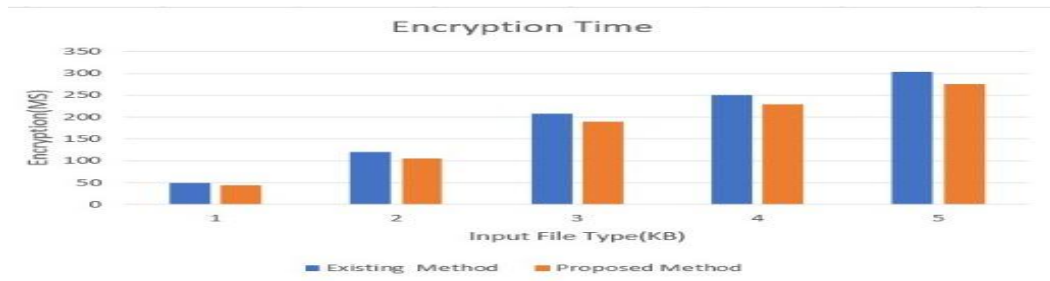


Figure 4.1

Just like encryption. We use AES algorithms to decrypt the encrypted data, evaluating the speed and accuracy of the decryption process. The comparison is based on Table 4.2 and the graph is shown accordingly in Figure 4.2.

Input File Type (KB)	Existing Method	Proposed Method
1	90	85
2	160	147
3	210	190
4	285	250
5	315	275

Table 4.2

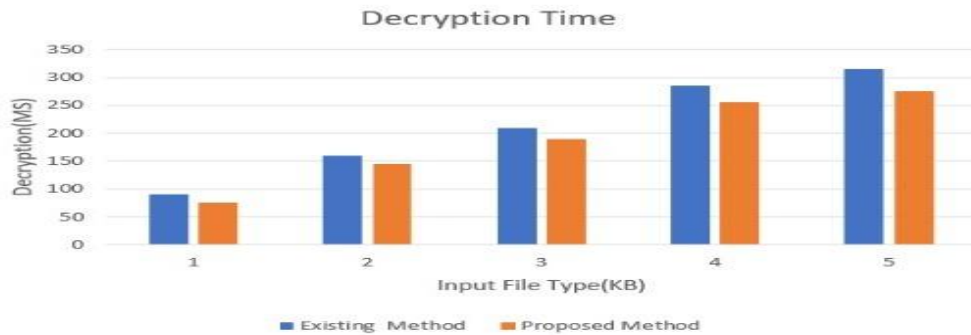


Figure 4.2

5. CONCLUSION

The results of this study indicate that the proposed security and privacy mechanisms effectively prevent unauthorized access to patient data, thereby bolstering confidentiality and protecting healthcare services from potential vulnerabilities and attacks. The utilization of public and private keys, along with strong password protection, ensures controlled remote access while maintaining data confidentiality. By enhancing security measures and protecting patient data, the ultimate goal is to improve patient care, elevate medical standards, and ensure the integrity of healthcare services in the digital age.

6. REFERENCES

- [1] S. M. Nagarajan, G. G. Deverajan, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri and S. Alkhalaf, "Secure Data Transmission in Internet of Medical Things Using RES-256 Algorithm," in IEEE Transactions on Industrial Informatics
- [2] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging security mechanisms for medical cyber-physical systems," IEEE/ACM Trans. Comput. Biol. Bioinf., vol. 13, no. 3, pp. 401–416, May/Jun. 2016
- [3] P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, "A secure IoT-based modern healthcare system with fault-tolerant decision-making process," IEEE J. Biomed. Health Informat., vol. 25, no. 3, pp. 862–873, Mar. 2021.
- [4] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," IEEE J. Biomed. Health Informat., vol. 24, no. 9, pp. 2499–2505, Sep. 2020
- [5] Z. Chkirbene, R. Hamila and A. Erbad, "Secure Medical Data Sharing For Healthcare System," 2022 IEEE 33rd Annual International Symposium Communications (PIMRC), Kyoto, Japan, 2022.