Alinteri J. of Agr. Sci. (2021) 39(2): 57-61
e-ISSN: 2587-2249
info@alinteridergisi.com

http://dergipark.gov.tr/alinterizbd
http://www.alinteridergisi.com/

# Electronic Health Records Platform: Patient-Centric Healthcare Management

Mr. Madar Bandu[1], Siddharth Thirkateh[1], K. Sai Sandeep Reddy[1], P. Meghana Reddy[1], V. Rishikesh[1]
[1]*Department of Computer Science and Engineering,*
*Anurag University, Hyderabad, India*

***Abstract*— In modern healthcare systems, digitalizing medical records is crucial for optimizing patient care. This paper investigates the creation and execution of a website designed to merge patients' medical records, with the goal of offering a holistic and patient-focused approach to healthcare management. The platform aims to streamline the exchange of information among healthcare providers, enhance treatment decision-making processes, and empower patients to take an active role in their healthcare. By centralizing healthcare data on a digital platform, this initiative aims to revolutionize traditional healthcare practices and ultimately improve patient outcomes.**

***Index Terms* – Healthcare, Encryption, Security, Summary, Centralized**

## I. INTRODUCTION

We can see how the patients' records, to this day, are scattered across many providers, facilities, or even on paper. The lengthy process of filling up a new form with each visit to a new doctor, or filling up a patient's details in the system all over again is a time-consuming and inefficient method to maintain a health record. The hospitals have to conduct the tests again and the patient's communication about the previous results of the tests is generally ignored due to lack of central proof of all the data. This can result in being time-consuming, inefficient, and expensive.

Patient Health Records (PHR) not only encourage the patients to keep track of their health records, store and manage them but also make it easier for them to share the health records whenever necessary.[1] These PHRs make the maintenance of the records easier but, when facing an emergency, the same repeat of tests, checking of medical history, and need to fill up the general details is required. This will again prove to be a time-consuming and expensive affair.

When collecting records from different organizations, the terms start to differ from organization to organization and this might cause a problem in cases of emergencies when one organization tries to interpret the different terms. This is the reason if all the records need to be in the same place then the integration of data will play an important role.[2] Using ontology as suggested may cause issues while displaying the data or compromise the efficiency of the application. The solution to this is by using new technology like NLP so that the model is much more efficient.

As technology advances day by day, cyber threats are increasing exponentially too, Electronic Health Records (EHR) have not been spared either. The security of health records is very important as tampering with these records can result in fatality in some cases. The patient's personal details, health records, and many other aspects of the EHR like storage and access need to be secured from intruders, and unfortunately not much action has been taken in this regard.[3]

To solve these issues, we have developed a web-based Health Record System that can be used by both hospitals and patients to access, manage, and store medical history (e.g. allergies, medical history, past medications, test results, surgeries, ongoing treatments, and more.) We have tried to make our system efficient and cost-friendly; our model lets the hospital access the patient's medical records and even upload the records after the consultation. This helps not only in access to the patient's records in emergencies but also makes it easier for patients to maintain their records.

Section 2 contains the Literature Survey, which will showcase the various research done on Health Records. Section 3 will mention the problem statement, and sections 4, 5, and 6 present the workflow and the functionalities of the proposed system, and finally, section 7 concludes the paper.

## II. LITERATURE SURVEY

Research on Electronic Health Records has been going on for a long time because of how efficient digitalization makes it. Every research conducted in this aspect aims to make the current models even more efficient, faster, and less expensive.

The study reflects on the research on the protection of data while storing and transferring them, the records are stored in a Protected Spreadsheet Container with Data (PROSPECD) which integrates encrypted access control policies with watermarked clinical and administrative data for advanced security measures.[4]

In parallel, a research study highlights the use of blockchain

technology to store the data and the patient's records. In this case, the data which is stored is safe and secure but it is immutable, so no data or records that are entered can be changed at any cost. This might not prove to be cost-efficient.[5]

The study on keeping the data safe, where the data on the client's side is masked using AES-256 and Blowfish encryption highlights the security of the data from any external threats.[6]

The primary objective of this research is to monitor and store the activities of the patient through which we will be able to come to certain conclusions as to how certain medications are working on the respective patients and how to enhance the effect of the medications on the patient.[7]

The methodology of this paper involves the security of data using the proposed multi-source IOH (Internet of Health) data fusion and mining method.[8]

The authors proposed an extensive model with intricate research on how private institutions can share data securely through the cloud and cryptography approach and to make the model even more secure, the integration of blockchain is included in the research.[9]

These literature survey reviews provide the various ways to implement the Electronic Healthcare Records and also give insights on data privacy and security. These insights help enhance the current models to make them much more efficient, faster, and cost-friendly.

## III. Problem Statement

In the context of India's healthcare landscape, the establishment of Patient Records (PR) by some hospitals highlights the challenge of integrating and sharing heterogeneous medical information in an era of globalized internet connectivity. This project aims to address this issue by providing PR to hospitals lacking such systems while harmonizing and consolidating PR data from various sources. By doing so, it facilitates seamless sharing of patient records, offering a comprehensive basis for medical information exchange.

Access to unified PR is increasingly vital for understanding patients' medical histories. Currently, disparate records across hospitals hinder comprehensive insights into patients' health backgrounds. By integrating PR from all hospitals into a single accessible platform, the project streamlines diagnosis and treatment processes, enhancing medical care efficiency. Additionally, centralized PR enables hospitals to exercise greater caution in prescribing medication, minimizing risks and optimizing patient safety. Ultimately, this initiative benefits both hospitals and patients by improving workflow efficiency, empowering patients with better understanding of their medical histories, and reducing unnecessary costs associated with redundant tests.

## IV. Proposed Model

The system interface comprises separate login mechanisms tailored for hospitals and users/patients, ensuring distinct access and functionality. Illustrated through a diagram, the interface delineates a structured navigation pathway across various web pages, each seamlessly integrated with specific application programming interfaces (APIs) to perform defined tasks within the system.

Upon user authentication, facilitated by the "userdata" API, individuals gain entry into their designated dashboard, where they can access pertinent information and functionalities. Subsequent navigation to the personal details page is enabled by the "Udata" API, offering users a platform to manage and update their personal information. The "download" API facilitates the retrieval of reports, empowering users to access and review their medical documentation conveniently. Moreover, the "summary" API provides succinct summaries of reports, aiding users in comprehending and interpreting complex medical information effectively, particularly in urgent situations.

Conversely, hospital login procedures leverage the "hospitaldata" API for authentication, granting authorized personnel access to patient details and administrative functions. Upon login, hospitals utilize the "retrieve" API to access patient information, enabling healthcare providers to view relevant medical records and histories as necessary. Subsequent utilization of the "upload" API allows hospitals to securely submit reports and medical data into the system, ensuring seamless integration and accessibility for authorized users. Furthermore, the "compress_encrypt" API facilitates the secure storage of uploaded reports within the database, employing encryption techniques to safeguard sensitive patient information.

In scenarios necessitating rapid assessment and action, such as emergencies, the "summary" API plays a pivotal role by generating concise summaries of reports, enabling healthcare professionals to swiftly grasp critical information and make informed decisions. Overall, the systematic integration of distinct APIs within the interface ensures efficient and secure management of medical data, optimizing the user experience for both patients and healthcare providers.

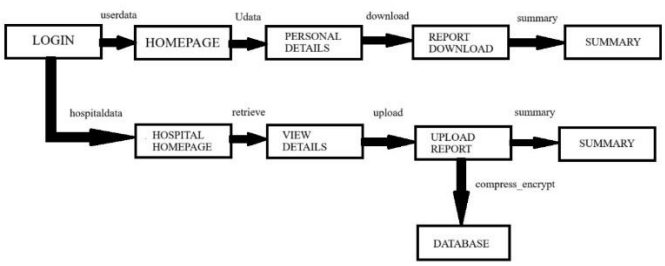


Fig 1. Working of APIs and Navigation through front-end

## V. SECURITY OF DATA

Data privacy and security plays a pivotal role in Electronic Healthcare Record systems since cyber-attacks have been increasing every day. Manipulation, theft, or any threat to medical records o hospital data can prove dangerous. AES and 3DES are the two encryption algorithms used in our model which have proven to be secure and efficient. Decryption is just as essential as encryption so that the receiver has all the right data. With decryption, comes Key management, where the secret key needs to be hidden so that the data is secure throughout both encryption and decryption.

*Key Management*: Ensuring the protection of encryption keys, as they are vital for decrypting sensitive data. Employing secure methods for storing keys and exploring the use of Hardware Security Modules (HSMs) to prevent unauthorized access to keys.

*AES:* The Advanced Encryption Standard (AES) is like the guardian angel of our digital world, ensuring the safety of our sensitive information. Picture it as a master lock that operates on blocks of data, each chunk being 128 bits in size. What's impressive about AES is its adaptability, offering different key sizes of 128, 192, and 256 bits, depending on the level of security needed.

AES follows a nifty structure called the Substitution-Permutation Network (SPN). It's like a puzzle-solving algorithm that expands the original key into a unique set of round keys. Each round involves a series of transformations—think of them as secret moves—like swapping bytes, shifting rows, mixing columns, and adding special round keys swapping bytes, shifting rows, mixing columns, and adding special round keys

But here's where AES truly shines: its commitment to security. It's designed to be like a maze where every twist and turn makes it impossible for anyone without the key to navigate through. Even the tiniest change in the starting point—the plaintext—leads to a completely different path—the ciphertext. This complexity makes AES a formidable fortress against cyber threats.

AES remains the go-to choose for encryption, ensuring our online conversations stay private and our personal data stays safe. So, just like we upgrade our home security systems, it's crucial to stay informed about the latest in encryption technology to keep our digital lives secure. But here's where AES truly shines: its commitment to security. It's designed to be like a maze where every twist and turn makes it impossible for anyone without the key to navigate through. Even the tiniest change in the starting point—the plaintext—leads to a completely different path—the ciphertext. This complexity makes AES a formidable fortress against cyber threats

3DES, also known as Triple Data Encryption Algorithm (TDEA), acts like the upgraded version of the original Data Encryption Standard (DES), aiming to enhance security measures. It's like having a lock with three layers of protection instead of just one. Here's how it works: the DES algorithm is run three times in a row in a sequence called Encrypt, Decrypt, Encrypt (EDE). Each run operates on blocks of data that are 64 bits long

With 3DES, there are two key options: 2TDEA (Double DES), where two different keys are used for the three steps, and 3TDEA (Triple DES), which brings in three unique keys for each pass. These keys can be either 56, 112, or 168 bits long, achieved by using three 56-bit DES keys.

Even though 3DES might not be the quickest option out there, it continues to stand firm as a top pick for numerous applications, especially those that value rock-solid security over lightning-speed encryption. In essence, it's like choosing a sturdy lock over a flashy but flimsy one – sometimes, durability and reliability are worth the extra time it takes to secure your valuables. So, while other encryption methods may boast faster processing speeds, 3DES remains the trusted go-to for safeguarding sensitive data in environments where security reigns supreme.

We can see that both AES and 3DES bring a lot of value to data privacy and security. AES brings the encryption speed and 3DES makes sure that no one gets past the encrypted data. Using both algorithms enhances security and maintains data privacy.

## VI. SUMMARIZATION

The summary of the patient records when either the hospital or the patient accesses the records is displayed which is an upgrade in our model. This summary was intended especially for emergencies when the procedures are needed to be performed immediately. These summaries display the essential details from the records (e.g. allergies, medications, medical history, surgeries, and more) so that the consulting doctors will not have to check the whole records before operating in emergencies. These even save money as the test results are also displayed in the summary and there is no need to repeat the tests. This feature saves time, money and can be very helpful in emergencies.

### *A. Working:*

We used the innovative methodology for text summarization by integrating the cutting-edge Pegasus model into our application. Our methodology is meticulously crafted to give

both the patients and the doctors a concise summary of the records whenever they want to access them.

Workflow:

- *Hospital Input Acquisition:* The summarization starts only when the hospital or the consulting doctor uploads the patient records through the application.
- *Preprocessing for Summarization:* The acquired reports undergo preprocessing steps tailored to facilitate effective summarization by the Pegasus model. This preprocessing step serves as a directive to the Pegasus model, indicating the intention to generate a summary of the input content.
- *Tokenization for Model Input:* Subsequently, the preprocessed patient report is subjected to tokenization using the Pegasus tokenizer. This process involves breaking down the textual input into discrete tokens, which are numerical representations of the constituent words and subwords within the text. This tokenized format enables seamless integration with the Pegasus model for summarization.
- *Leveraging Pegasus for summarization:* The tokenized input text is then fed into the Pegasus model for summarization. Leveraging the advanced transformer architecture of Pegasus, the model engages in an abstractive summarization process, wherein it synthesizes the salient information and key insights from the input text to generate a coherent and concise summary.
- *Decoding and Presentation:* Following the summarization process, the generated summary undergoes decoding from its numerical token representations to human-readable text. This decoding operation translates the token IDs into their corresponding linguistic elements, effectively transforming the summary into a comprehensible format. The summarized content is then presented to users via the web application interface for their review and utilization.
- *User Interaction and Utilization:* The presented summary lets both doctors and patients grasp the essence of the reports. This can be utilized very well in cases of emergencies and the patients can be treated quicker.

*Pegasus:* The Pegasus model, referenced in the context above, is a state-of-the-art neural network architecture developed by Google Research for text summarization tasks. Unlike extractive summarization methods that select and assemble existing text segments, Pegasus employs an abstractive approach, meaning it generates summaries by paraphrasing and synthesizing information from the input text.

One of the notable features of Pegasus is its capability to produce coherent and concise summaries that capture the key points and main ideas of the input text. It achieves this by understanding the context and semantic relationships within the text, allowing it to generate human-like summaries.

Pegasus is based on the transformer architecture, which has demonstrated remarkable performance in various natural language processing tasks. It is pre-trained using a large corpus of text data and fine-tuned for specific summarization objectives.

Overall, Pegasus understands the context and semantic relationship between texts, which allows it to produce human-like summaries, making it the best open-source model to use for this application. It makes the summaries concise but captures the key points very well making it easy and faster for the doctors to understand the records and act accordingly.

## VII. Results and Evaluation

We dedicated considerable effort to optimize our project for maximum efficiency, recognizing the critical importance of securing hospital data and patient records. Given the potential risks associated with data tampering, particularly in healthcare settings, we prioritized implementing robust security measures. After thorough exploration of encryption algorithms such as DES and 3DES, we found that the Advanced Encryption Standard (AES) offered the best balance of speed, key management, and flexibility in key size, making it the optimal choice for ensuring the security and privacy of our data.

Additionally, we introduced a feature for summarizing patient records to streamline the treatment process, reduce costs, and improve responsiveness in emergency situations. While experimenting with various Python packages and natural language processing (NLP) techniques, we encountered challenges with generating concise and relevant summaries. However, our search led us to discover Pegasus, a Google tool specifically designed for text summarization. Leveraging transformer neural networks, Pegasus proved highly effective in producing succinct, accurate summaries, empowering healthcare professionals to expedite treatment decisions and enhance patient care efficiently.

## VIII. Conclusion

In wrapping up the strategies we've implemented to ensure patient medical records remain confidential and intact, we've achieved some significant milestones. We've beefed up security by deploying strong encryption methods like AES

and 3DES both for safeguarding data in storage and during transmission. This not only bolsters overall security but also puts us in line with important healthcare data protection regulations such as HIPAA and GDPR. We're also staying proactive by regularly assessing risks and classifying data meticulously. Strict access controls and a robust key management system are in place to keep data secure.

We've also paid close attention to addressing potential security incidents and human-related risks through effective incident response, real-time monitoring, and comprehensive user training. To stay ahead of the curve, we conduct regular security audits and keep stakeholders informed about any evolving cybersecurity challenges.

By successfully implementing these measures, we've instilled trust in the secure management of medical records. The summarization of patient records, powered by the Pegasus model, plays a vital role here. It ensures that the summaries are not just robotic but human-like, making them easily understandable for both doctors and patients. This not only saves time but also cuts costs, as doctors won't need to repeat tests already conducted in the past—the results are conveniently summarized.

In essence, our focus on encryption and data compression keeps patient information secure, while efficient summarization aids doctors in working faster, more affordably, and with greater efficiency.

## REFERENCES

[1] V. Ved, V. Tyagi, A. Agarwal and A. S. Pandya, "Personal Health Record System and Integration Techniques with Various Electronic Medical Record Systems," 2011 IEEE 13th International Symposium on High-Assurance Systems Engineering, Boca Raton, FL, USA, 2011, pp. 91-94, doi: 10.1109/HASE.2011.63. keywords: {Medical services;Servers;DICOM;Insurance;Information systems;Computer architecture;Personal Health Record System;EHR (Electronic health records);EMR (Electronic medical records);CDO (care delivery organizations)}

[2] Cai Xiufen and Xu Yabin, "Computer-based patient record data integration method based on ontology," 2011 IEEE International Symposium on IT in Medicine and Education, Guangzhou, China, 2011, pp. 551-554, doi: 10.1109/ITiME.2011.6132170. keywords: {Ontology;CPR;Data Integration}

[3] S.T.Argaw, N-E Bempong, B.E.Chauvin, A.Flahault, The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review, BMC medical informatics and decision making, 19:10, 2019, 1-11, DOI:10.1186/s12911-018-0724-5

[4] D. Ulybyshev et al., "Protecting Electronic Health Records in Transit and at Rest," 2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS), Rochester, MN, USA, 2020, pp. 449-452, doi: 10.1109/CBMS49503.2020.00091. keywords: {Cryptography;Access control;Servers;Containers;Electronic medical records;Metadata;Watermarking;Electronic Health Records, data privacy, data leakage prevention, HIPAA, access control}

[5] H. Wang and R. Zhou, "The Application of Blockchain to Electronic Health Record Systems:A Review," 2021 International Conference on Information Technology and Biomedical Engineering (ICITBE), Nanchang, China, 2021, pp. 397-401, doi: 10.1109/ICITBE54178.2021.00092. keywords: {Electric potential;Precision medicine;Medical services;Blockchains;Safety;Electronic medical records;Information technology;Blockchain;Internet of Things;Electronic health record}

[6] A. Shibu, A. M, A. T. Anilkumar, A. Radhakrishnan and S. Izudheen, "Secure Storage and Retrieval of Electronic Health Records," 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), Kochi, India, 2022, pp. 1-5, doi: 10.1109/IC3SIS54991.2022.9885484. keywords: {Data privacy;Privacy;Hospitals;Medical services;Encryption;Blockchains;Electronic medical records;Encryption;Electronic Health Records;AES;Blowfish;EHR;Secure storage}

[7] V. Shukla, A. Mishra and A. Yadav, "An Authenticated and Secure Electronic Health Record System," 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 2019, pp. 1-5, doi: 10.1109/CICT48419.2019.9066168. keywords: {Electronic medical records;Password;Radio transmitters;Encryption;Authentication;Authentication; Electronic Health Record (EHR);Encryption;Security}

[8] Q. Zhang, B. Lian, P. Cao, Y. Sang, W. Huang and L. Qi, "Multi-Source Medical Data Integration and Mining for Healthcare Services," in IEEE Access, vol. 8, pp. 165010-165017, 2020, doi: 10.1109/ACCESS.2020.3023332. keywords: {Data privacy;Data integration;Medical diagnostic imaging;Medical services;Distributed databases;Encryption;Service recommendation;Internet of Health;locality-sensitive hashing;user privacy;data integration}

[9] H. Jin, Y. Luo, P. Li and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," in IEEE Access, vol. 7, pp. 61656-61669, 2019, doi: 10.1109/ACCESS.2019.2916503. keywords: {Medical services;Cloud computing;Blockchain;Biomedical imaging;Data privacy;Cryptography;Access control;blockchain;encryption;medical data;privacy;security}