Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 23s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Blockchain and AI based Medical Record Analysis for Bone Fracture on Cloud Environment

S.Balaji[#1], B.Sathya[#3], G.Mugesh[#4], K.Shanmugapriyan[#5]

[#1,2,3,4,5]Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry
Email ID: balajicse@mvit.edu.in

Cite this paper as: S.Balaji, B.Sathya, G.Mugesh, K.Shanmugapriyan, (2025) Blockchain and AI based Medical Record Analysis for Bone Fracture on Cloud Environment. *Journal of Neonatal Surgery*, 14 (23s), 946-958.

ABSTRACT

The widespread adoption of Electronic Medical Records (EMRs) has transformed healthcare by improving the management and sharing of patient information, and thus enhanced patient care. At the same time, this movement toward digital records and sharing of information has resulted in a heightened concern about the privacy and security of this sensitive patient (health) data. The system proposed here addresses these concerns by incorporating Ethereum blockchain technology, which establishes a secure and immutable record of every exchange of patient data. The benefit of blockchain is that it makes it impossible to alter existing patient data; each unit of data exchange is transparent, can be traced, and once established cannot be altered. Using this approach will improve the security and integrity of the healthcare data management process as a whole. In addition, to protect the sensitive patient information in the healthcare records, the project employs the modern encryption protocol XChaCha20 for all exchanges of sensitive patient information. This means that the encrypted records of patients are stored on the InterPlanetary File System (IPFS). Therefore, in the unfortunate event that someone would gain unauthorized access to the relevant data in the system, they will not be able to read the sensitive patient information and privacy will be preserved. The IPFS storage system provides the reliability and security of storing a file in multiple nodes to protect against file loss and file tampering. The IPFS system also implements the ResNet-50 model, a powerful convolutional neural network (CNN) for analyzing medical images. The ResNet-50 deep learning model was trained to predict bone fractures from x-ray images because it could learn how to tie together multiple sophisticated metrics found in the medical data streams. This AI-assisted fracture detection allows for less manual analysis of an image and enables providers to provide faster and better diagnoses. The earlier a bone fracture is identified, the more likely healthcare professionals can intervene and make decisions that can lead to improved care pathways and outcomes for the person. By combining the Ethereum blockchain, XChaCha20 encryption, IPFS storage, and ResNet-50 AI system, the proposed system is a secure, efficient, and automated way to handle healthcare data that is beneficial for providing more secure data. The integration of these systems ultimately promotes a more reliable and efficacious diagnostic approach leading to enhanced patient treatment and care.

Keywords: *Blockchain, Ethereum, XChaCha20 encryption, IPFS, EMRs, ResNet-50, bone fracture detection, AI, smart contracts, healthcare security.*

1. INTRODUCTION

As digital health technologies continue to develop rapidly, the amount of Electronic Medical Records (EMRs) is increasing exponentially every year. This abundance of data presents considerable challenges in the healthcare sector regarding how we continue to store and manage such a vast number of sensitive records. While hospitals may rely on local systems for EMR storage, such systems can be limited by local resources like storage capacity and processing power. Therefore, the demand for scalable systems is increasing, leading some hospitals to consider cloud and cloud computing options for EMR management. Cloud computing enables hospitals to store EMRs for each patient and provide several key strengths in managing a large amount of EMR data, including, scalability, flexibility, and remote access. Hospitals can store their EMRS in the cloud and rely upon remote service to maintain large on-premise data centers, and therefore hospitals can achieve better resource utilization. Once clouds are established, they can also allow collaboration among multiple hospitals, medical institutes, and researchers that facilitate rapid access to medical data which may enhance the collaborative process of data analysis or research. Further, hospitals can more easily scale their storage needs as EMR data continues to grow by leveraging cloud computing without an initial significant upfront capital investment for infrastructure. Yet, the practice of using cloud storage for sensitive medical information is obvious concerning privacy and security. Hospitals and health organizations are slow to share patient information, even for the most benign purposes such as collaboration or mutual improvement of patient outcomes in medical research. The reason these organizations provide cattle-type limitations on sharing is primarily due to patient data breaches or unauthorized access or attacks, which would factor into patient privacy. This could be more easily

construed to be a breach of patient privacy across distinct organizations or collaborators, and across multiple management systems, specifically. Protecting patient privacy in the storage and inter-organizational transfer of sensitive medical information, with total assurances around confidentiality, integrity and security, is crucial to maintaining the integrity of patient privacy generally, and preferable systems that are functioning responsibly as custodians of privacy in their healthcare organization.The usual solution is to encrypt EMRs before they are stored in the cloud to avoid these issues. Because of the use of encryption, if data intercepted by a network intruder or unauthorized users, it could be unreadable if they didn't have permission to access this information in the first place. Specifically, symmetric encryption is used to encrypt EMRs. This type of encryption works on the basis that a sender and recipient must have a copy of the same key to be able to encrypt and decrypt the EMRs. Symmetric encryption is also a good solution for EMR cloud storage as it can encrypt large amounts of data quickly and easily. In summary, symmetric encryption guarantees confidentiality of EMRs, however, it introduces access control and shared data challenges. In conventional symmetric encryption, the same key is utilized during the encryption and decryption phase, making it challenging to implement fine-grained access control. For example, in a hospital setting, a specific access level may be granted by a hospital to various collaborators on a patient. Authenticating an example access level might mean allowing a researcher access to only part of a patient's medical record while ensuring that other portions remain confidential. Such granular access control is difficult to implement efficiently using symmetric encryption since the same key must be used to decrypt the data for access to the underlying text, irrespective of access needed.

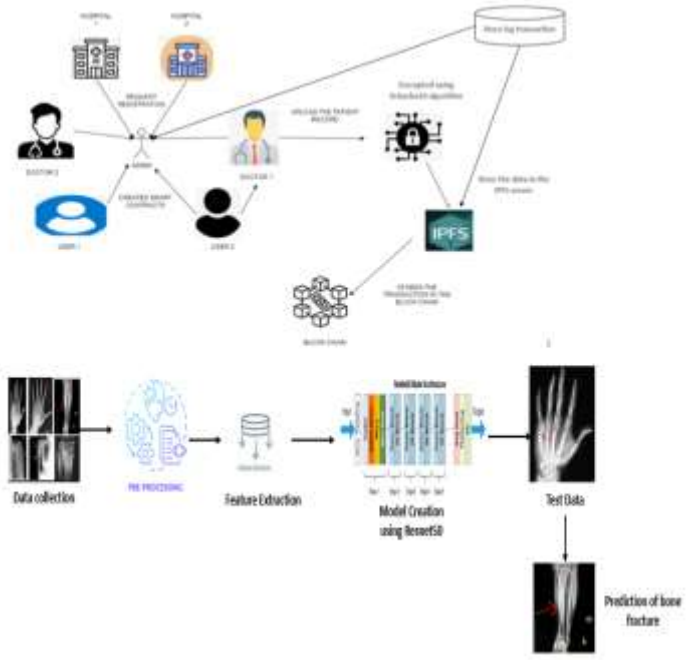
A. BONE FRATURE:

The term bone fracture in the hand refers to a range of breaks occurring in one or more of the bones of the hand, which include the phalanges (finger bones), the metacarpals (the bones of the palm), and the carpal (bones of the wrist). A fracture of the hand is usually a result of some type of trauma, whether it is a fall, direct impact of an object, or a sporting accident. This type of injury occurs when the force applied is greater than what bones can withstand for absorption, resulting in fracture or breakage of the bone. The severity of a hand fracture can differ from a minor crack in the bone to a full break. With any fracture or break, this will lead to a loss in mobility, strength and functional capability of the hand. Types of fractures include: transverse, oblique, spiral and comminuted fractures, depending on the type of break in the bone. Symptoms associated with fractures of the hand include: pain, swelling, bruising, tenderness, and with a severe fracture there may be deformity, inability to move the fingers or hand, and numbness or tingling in the fingers or hand. An injured individual may lose function, thereby preventing them from performing certain activities of daily living, such as gripping and writing. Diagnosis consists typically of a physical examination and, in many cases, one or more imaging studies like X-rays or advanced imaging to clarify the type, the location, and severity of the fracture. Treatment of a bone fracture in the hand depends specifically on the injury. A minor fracture may be treated with rest, splinting, and pain relief, whereas a more severe fracture may require surgical intervention (pinned, plated, or external fixation). The main goals of treatment are to correct or minimize malalignment, relieve pain, and rehabilitate and optimize function. Rehabilitation and/or physical therapy might be necessary to restore strength, flexibility, and dexterity in the hand after healing. Ultimately, bone fractures require treatment to avoid complications that may lead to suboptimal healing and/or functional impairment.

2. LITRATURE SURVEY:

Álvaro Díaz, Héctor Kaschel [1]The fast development of electronic medical records (EHRs) raises concerns regarding patient privacy, security of patient data, and unauthorized access. Blockchain is being considered to resolve such issues and secure medical data. This study proposes a scalable blockchain-based EHR management system using Hyperledger Fabric, primered, permissioned blockchain. The presented design includes a two-channel, to ensure the privacy and security of patient data while allowing EHRs to be managed effectively. The architecture is structured around entities and user roles and can restrict access to sensitive medical data. We developed a prototype based on Hyperledger Fabric, to demonstrate both the feasibility, and scalability of the proposed solution. We tested our implementation for scalability improvements as we added more assessments to the original configuration. The findings indicate that blockchain technology has the potential to act as an improvement for scalable, secure, and privacy-preserving EHR management. This addresses specific tasks for managing sensitive healthcare data and information.[2] Yujin Han, Yawei Zhang, Sten H Vermund [2]This paper assesses the pros and cons of blockchain technology and electronic health records (EHR). EHR systems offer benefits over paper records in workflow efficiencies, data security, and reductions in redundancy. However, there are some difficult and complicated issues pertaining to EHRs such as their interoperability and shortcomings on privacy. Blockchain as a distributed ledger protocol could help address some of these issues as it would offer secure, transparent, and immutable evidence that can be shared, managed, and accessed. The paper describes some examples of blockchain-based protocols which focus on improving EHRs interoperability and privacy concerns. The paper goes on to introduce current challenges including efficiencies in managing the data itself, the equitable access to that data, and trust in the relationship between the patient and health provider. The authors suggest that more research will be necessary to explore the ethical issues in health care and the implications of data science and informatics on blockchain-based EHRs. If research relating to blockchain and EHRs are pointing in the direction of further issues such as inequities in access to the health, profound consequences due to the environmental effects of the computational load of blockchain and trust around health providing organizations.[3] FILIPPO BOIANI [3]The work presented in this thesis explores a possible implementation of permissioned blockchain technology,

specifically Hyperledger Fabric, for the use of managing an Electronic Health Record (EHR) system for use in a disaster scenario, such as a natural disaster. EHRs store sensitive patient information that need to be stored to a high degree of accuracy, must be kept private, and must have readability policies, especially when in crisis situations such as hurricanes or earthquakes, in which traditional systems can fail or could be tampered with and/or damaged. Based on the features of decentralization, blockchain could provide improved robustness and fault-tolerance compared to existing centralized cloud-based systems. This study focused on the design and implementation of a simple prototype for an EHR management system using Hyperledger Fabric, as well as simulating the 2010 Haiti earthquake to demonstrate the capability of the system. Based on the simulations, even with malicious nodes compromising the system, the study's findings demonstrated that the system maintained acceptable performance levels in terms of throughput, latency, and resources consumed. In addition, the system's performance clearly surpassed permissionless blockchain-based implementations in throughput and latency. This demonstrated that a secure and decentralized model of exchanging EHR is possible without sacrificing performance or the feasibility of decentralized healthcare networks. While enhancements and additional work in the area are still warranted, the model shares promise for facilitating healthcare networks in times of disaster and making sure data sharing continues for continued treatment while maintaining data privacy and confidentially in very extreme circumstances. The work acknowledges a highlight between performance and security, while suggesting the potential for blockchain to positively impact EHR management during emergencies.[4] Alixandra Taylor, Austin Kugler, Praneeth Babu Marella, Gaby G. DagheR [4]The proposed VigilRx system is designed to offer a patient-centric and interoperable solution to the challenges regarding prescription management by utilizing blockchain technology. Current methods of managing prescriptions are often fragmented, leading to a lack of interoperability. Current methods usually have to do with data siloes and duplicity of records, delays of transfer, and less patient control. Patients often need an intermediary to be able to access or transfer their records. Differences in standards, outdated ways of doing things, and separate systems for healthcare records lead to barriers to effective exchange of health records. VigilRx removes the middleman and allows the patient to be directly responsible for the data associated with their prescriptions. The aim is to keep prescriptions from being 'stuck in siloes' at various care providers. The VigilRx system employs smart contracts and blockchain technology to facilitate role-based contracts for patients, prescribers, and pharmacies. It is a patient-centric approach to record ownership and management that puts the ownership of prescription records back into the hands of the patient. By calling upon standardized prescription contracts for patient, prescribers, and pharmacies, the system is interoperable and allows for records to be shared across providers in an efficient manner while ensuring reasonable privacy and security. VigilRx increases transparency by allowing patients to see a list of entities granted access to their prescription information. The system was implemented and tested, showing its scalability and efficiency. VigilRx not only solves the problem of information blocking, but also supports the efficiency of the transfer of records. Further, VigilRx is using the secure and decentralized aspects of blockchai to provide a more reliable, efficient and portable method than the antiquated technologies and fragmented standards that precede it and furthering the notion of the patient's control of their data, while improving interoperability between healthcare stakeholders.[5] Fırat Hardalaç, Ozan Peker, Murat Çiçeklidağ [5]This study aimed to improve the screening for wrist fractures in emergency departments using deep learning. It included various object detection architectures including: SABL, RegNet, RetinaNet, PAA, Libra R-CNN, FSAF, Faster R-CNN, Dynamic R-CNN, and DCN - and various backbones - to analyze wrist X-ray images from patients that presented at the Gazi University Hospital. In total, 20 different fracture detection actions were evaluated, including five ensemble models, which were used to improve the performance of the individual models as a whole. The combinations resulted in a unique fracture detection model referred to as the: 'Wrist Fracture Detection-Combo (WFD-C). Among the 26 models tested, the WFD-C model reached a maximum average precision (AP50) of 0.8639, which represents an increase in fracture detection performance. This study is a collaborative work between Gazi University, Huawei Turkey R&D Centre, and Medskor and showcases how deep learning can assist physicians obtain accurate and efficient diagnosis in an emergencydepartment.[6] B.Hima Vaishnavi, K.Hithaishi , B.Hrishikesh, A.Indhu , G Jagadeesh , Dr.Sujith Das [6] The project details the use of deep learning methods in bone image processing with the aim of developing a capability for bone fracture detection in X-ray images. Thus, it will give consideration to the advantages of deep learning models - employing various from such as artificial neural networks (ANN) and deep learning networks such as convolutional neural networks (CNN) and recurrent neural networks (RNN) in performing more accurate and productive segmentation of medical images. Traditional machine learning algorithms, such as K-means clustering, and decision tree classification such as random forest, will still be used but tend to focus on certain issues compared to deep learning models, particularly in relation to accuracy. Deep learning models are more complex employing layers and barriers to sort data and produce results; but they have proven to be effective in processing X-ray images formatting for detection of bone fractures[10]. The project x-ray objectives classify fractures by removing the association of medical imaging with relying on ”images” of human bone. Building massive deep learning models used to produce supervised learning processes employing labelled datasets of x-ray images of human bone to classify fractures. The processed images of natural bone x-ray can be then categorise fractured or not and immediately underpin support for those working in healthcare professions. Deep learning methods are dictated in traditional machine learning models but have greater successes in all medical imaging segmentation and classification problems.



This architectural diagram illustrates a secure, artificial intelligence-based prediction of bone fractures leveraging blockchain and deep learning. Users (doctors and patients) register with the system using smart contracts that are for the administration of users. Hospitals register for the use of the transparent system and proceed upload the encrypted X-RAY data using the Xchacha20 algorithm, that data is successfully included and stored on the IPFS server and transactional data is verified and logged on the blockchain to ensure transparency. The bottom section represents the AI pipeline. The initial step is to collect X-ray images, then undergoes pre-processing of the data that aids the images quality and delete noise, etc. before the True feature extraction, extracting features are directed to machine learning pipelines, an appropriate deep learning model development was used, ResNet50 is a strong convolution neural network architecture utilized to create the deep learning model. The training used previous images, and validated with the test data (new X-ray images). Finally, the model predicts whether the new x-ray images of the bones are fractured or not. The architecture demonstrates a secure handling of data, a prompt processing, a correct medical diagnosis process, and encourages trust, efficiency, and automate healthcare.

3. PROPOSED SYSTEM:

The proposed system is aimed at strengthening the management of health care data by transforming data management using blockchain, encryption, decentralized storage, and machine learning for security, privacy and diagnosis. The design makes use of an Ethereum blockchain to record all patient data transactions, guaranteeing that any transaction concerning sensitive heath information is visible, non-editable and traceable. In a decentralized ledger system, data corruption is prevented because modifications may only be authorized by a single service provider. Once information is logged, transaction data is not reversible so that data integrity remains intact. This ultimately leads to a higher level of satisfaction for patients and health care providers involved in the therapist-patient relationship, and while both need to be guided in forms of documentation, critical user data can now be delivered in a more secure manner. To further address sensitive health information security, smart contracts were used to automate and enforce health care information security protocols. Smart contracts enforce the rules that have been established for how the information will be accessed, processed, and used. Next, when Medical Officers upload patient data, the data is encrypted using XChaCha20, the new encryption standard, which guarantees no unauthorized person could access or interpret the data. The patient data, once it is uploaded to the blockchain, is uploaded as encrypted file(s), which are then stored on the InterPlanetary File System (IPFS), a decentralized storage method that provides scalability, and protection against tampering or loss of data. The system provides a solid foundation of secure and immutable health data management using a combination of blockchain for transaction logging, XChaCha20 encryption to protect data, and IPFS for storing said data. In conjunction with offering security, the proposed approach includes a novel bone fracture prediction model developed using ResNet-50 deep learning structure, a very competent convolutional neural network (CNN). ResNet-50 can take X-ray images as an input to identify and detect any signs of a bone fracture. When trained previously on a small subset of labeled X-ray images, the model can predict with high confidence that new bone fractures can be predicted automatically in new X-rays. The advantage of integrating the prediction model into the system allows healthcare providers to have

AI supported diagnostics which improves the efficiency and speed of identifying a fracture. This also supports the patient

providing them the ability to control and monitor who had access to their Health data. Thus building trust within the patient and healthcare providers while improving the security and privacy of the medical records.

a. User registration and authentication:

The registration and authentication module provides that only registered hospitals, doctors, and patients can access the system. The registration process requires new users to register through an administrator, who verifies their credentials and issues appropriate access credentials to them. This verification guarantees that unauthorized users do not access sensitive medical data. Once registered, use of smart contracts will authenticate users through cryptographic signatures. A patient can log-in to request for medical visits while allowing a doctor to log-in to access a patient's medical records only if the patient allows it. Using blockchain authentication also guarantees a decentralized system with no centralized credential against which to authenticate, mitigating the risk normally associated with centralized login procedures.

b. Medical record upload and encryption:

Following the consultation, doctors will upload patients' medical records. For security, these medical records are encrypted using the XChaCha20 encryption algorithm before storage. XChaCha20 provides high-speed encryption but also provides good security and therefore unauthorized users cannot access the sensitive data. The encryption process provides a barrier for hackers to access the stored records, therefore if hackers were to access the records they would still be unreadable without a proper decryption key. Once encrypted, the medical data will be prepared to go into decentralized storage while being kept private and secure so no one has access to the records.

c. Secure file storage in ipfS:

Once encrypted, the medical records are deposited in the InterPlanetary File System (IPFS). IPFS is a decentralized storage network that breaks files into unique content addressed blocks, ensuring that all data cannot be modified or lost. Traditional cloud storage relies on centralized servers that may compromise data security after it is accessed. IPFS is able to enhance external security by making the data distributed across multiple nodes. IPFS would prevent data tampering and unauthorized record modifications by allowing the patients and the doctors to retrieve files with the hash. The benefit of IPFS is that medical records can remain available indefinitely, and not dependent on a single storage provider.

d. Blockchain-based transaction logging:

With the logging feature of the module, all system interactions (including user registrations, appointment requests, file uploads, and access permissions) are logged to the blockchain. Because all blockchain transactions are immutable, there is some validity to having open records available for transparency sake and assuring a user cannot change or rig the data, or change the logic of the process. Every transaction has a timestamp and a cryptographic signature allowing for a verifiable, immutable audit trail. The module has a logging feature allowing every access request and modification attempt pertaining to the system to be logged for ever increasing accountability, which is vital for regulatory compliance, and proof of Data Integrity and Security allowing organizations to meet the ever increasing regulatory demands for Data Protection.

e. File Access and Sharing:

The system relies on smart contracts for permissions, which allows patients to control who accesses their medical data. When a doctor requests access, the patient accepts the request and the records can be encrypted. The system will verify the requestor and their authorisation level, in case of a record or document request. However, all of these assurances prevent the disclosure of sensitive data to unauthorised individuals. Patients are able to share their records with specialists, move their data between hospital systems, and even have their records moved to new hospitals; all while maintaining the portabilty of their medical data while also safeguarding privacy.

f. Smart Contract Execution

Smart contracts are critical elements for automating system functions. They are self-executing contracts that carry out user validation, access control, and transaction verification without relying on intercessors. For example, when a patient grants permission for a doctor to access a file, the smart contract authenticates the permission and registers the transaction on the blockchain. Automating the entire process is important because it ensures that smart contracts cannot be changed because they are immutable. The smart contracts will also ensure that all the rules in the system will execute automatically. Having no manual intervention enhances security, cuts down on operational costs, and eliminates costs to inefficiencies in healthcare data management.

g. Audit and Security Monitoring

This module will constantly monitor transactions and access requests to verify that the system has not been compromised. The use of blockchain logs for the logged transactions provide the ability to audit real-time and identify any unusual or unauthorized access. Suspicious access attempts will immediately prompt an alert, ensuring that security breaches are

promptly identified and mitigated. The audit trail is secure and unalterable enabling any healthcare regulator or organization to verify that compliance with privacy legislation and data protection regulations has taken place. The reduction of the unknown will increase faith in the system as all interactions will be considered transparent, accountable, and protected against cybercriminals.

h. DATA COLLECTION:

As a first step in the system, we need to aggregate a large and diverse dataset of x-ray images from Kaggle, which is a very popular open-source site for locating datasets. These datasets contain labeled images that indicate the presence or absence of bone fractures. The presence of these bone fractures is critical to developing an accurate machine learning model, as an untrained or poorly trained model is likely to generate poor predictions. The availability of open-source data such as Kaggle data means that we are exposed to a wide variety of real-world cases and can move more quickly through the development process with data that is allowed to be used and be structure the way it needs for the methodology. This first step is key to developing an accurate prediction model that is robust and transferrable.

i. PRE-PROCESSING:

Before inserting the data into a model, preprocessing is very important for maintaining the quality and continuum of the data — in this case, X-ray imaging. Preprocessing can be cutting or dimensioning the images into a uniform size, with 224x224 pixels to comply with ResNet-50. One can also convert the image into gray scale in any x-ray data, or normalize the pixel values. Preprocessing may also involve data augmentation techniques (rotation, flip, zoom etc) to enhance size for the original data for the neural networks will be infact better able to generalize based on training examples that have been completely synthetically generated. The purpose for using pre-processing is to ensure the data is uniformly clean, uniform and only then can be ready for the deep neural networks to learn efficiently.

j. FEATURE EXTRACTION:

Feature extraction is the process of isolating relevant features from the raw X-ray images which relate to predicting fractures. In this system, this will be handled by the ResNet-50 model. ResNet-50 is a convolutional neural network (CNN) made up of several deep residual layers, and because it utilizes many layers, ResNet-50 automatically learns to extract hierarchical features from the images (edges, shapes, and textures), and these features are relevant to correctly predicting fractures. These features are more meaningful than the raw pixels in the images, and result in a model that is significantly more accurately predicting fractures.

k. MODEL CREATION USING RESNET-50:

ResNet-50 is the main model for training and classification. It is a 50 layer deep CNN model that solves the vanishing gradient problem using residual connections. Residual connections allow ResNet-50 to gain complex representations of patterns in classification problems even if they are deep. The intended usage for ResNet-50 is to train the model on the X-ray data set by using either one of the two training models above (i.e., training from scratch or transfer learning using the pre-processed X-ray data). The training and image classification should be a learning experience where the model learns to link certain features in X-ray images to the presence (or absence) of bone fractures. It is important to mention ResNet-50 matches up greatly with classes of medical images to classify, based on its stand alone architecture and pre-training layers.

l. Test Data:

After training the model, it is evaluated using the test dataset (commonly a holdout, and thus unknown) to measure the model's generalization ability - or how the model's performance on unseen data compares against the training data. The test dataset will undergo the same pre-processor and the same performance metrics (accuracy, precision, recall, and F1 score) as the training dataset. The assessment of the model during this step provides insight into whether model performance can be reasonably expected to generalize to real world data cases, and also provides some indications of potential overfitting or underfitting during model training.

m. PREDICTION:

In the last stage of the process, a trained ResNet-50 model is put to use to predict on x-ray images never seen before. Once an image has been accepted by the software's model, it is then formatted into a usable image; this image is then passed onto a model to predict if an image has fractures or not based on prior learned patterns. The models' prediction helps clinicians make realtime clinical diagnostic support. This model provides clinicians with an opportunity to make quick decisions regarding treatment. Ultimately, allowing this predictive capability in the healthcare data system backed by blockchain function may come close to ensuring the highest level of efficiency for health-care efficacy.

4. RESULT AND DISCUSSION:

The execution of the proposed healthcare data management system presents an important step in supporting privacy, security and efficiency of medical data management. The integration of Ethereum blockchain, XChaCha20 encryption, InterPlanetary File System (IPFS), and a ResNet-50 model for bone fracture predictions enhances upon the shortcomings of traditional

electronic medical record (EMR) systems.

One of the most noteworthy results noted with this prototype implementation, is the increase in transparency and containment of data security due to blockchain integration. Each transaction that occurs with patient data is recorded on the Ethereum blockchain, and tracked in an immutable and traceable fashion. This serves to bolster accountability among healthcare providers as every transaction (accessing or updating records) is tracked, patients can accurately track who accessed their records and when. The integration of smart contracts, in addition to the public and private keys used by each party, further automates access control by ensuring that data access is restricted to certain parties, that meet preconditioned policies, and provide for a level of assurance that data access is limited to authorized individuals. The XChaCha20 encryption algorithm used to further secure patient records before storage significantly lowers exposure risk of a data breach.Even if unauthorized eyes were to take a look, the data would be useless as it is all in encoded format. When this data is stored as an encoded blob on the Inter-Planetary File System (IPFS), they gain the benefits of a distributed and decentralized storage system which greatly reduces the chances of any data being altered, lost, or corrupted. Performance tests show the hybrid architecture scales very well when the volume of data increases, while still maintaining access speed and access reliability.

Furthermore, the ResNet-50 model from deep learning support gives an intelligence layer to the system. After obtaining numerous X-ray images from different online locations e.g. Kaggle, which were all potential fractures, the ResNet-50 deep learning model learnt from the images and returned a high accuracy in regards to fracture identification. During the testing of the model the ResNet-50 exhibited strong generalization properties, meaning that the tests undertaken with the model were on new, unseen X-ray images, and the model was able to define fractures in them. In conclusion, not only does this AI driven component fast track the process of diagnosis, and reduce a reliance on a radiologist to look at the images first, especially in remote or low resource environments, but it gives the patients the power to chart and control their access to their medical data by providing notifications of access and the ability to audit their records. This builds additional trust in the digital healthcare systems for patients.

a. Improved Integrity:

Integrity is an essential component of the management of healthcare data; ensuring patient information is correct, unaltered, secure. The solution proposed in this paperwork improves data integrity as it utilizes the immutable ledger of all transactions in the Ethereum blockchaintechnology. Once patient information has been recorded on the blockchain, it cannot be modified or removed, making it impossible to make illicit alterations. This will eliminate possibilities of fraud, erroneous changes to the records and nefarious tampering, and guarantees that the integrity of all the medical records stays intact. Blockchain provides transparency and a means of verification for any transaction, generating confidence and trust among patients and healthcare providers. In addition to the ledger system that blockchain incorporates, the proposed system includes a means of protecting medical records against unauthorized alterations through the encryption of patient information utilizing the encryption algorithm XChaCha20. Encryption guarantees if the patient data is accessed by malicious actors, or otherwise, they cannot possibly change that data covertly. In addition to encryption of the patient data, the system continuously logs any interaction with patient records, providing the ability to track the patient record and audit it. Therefore, administrators can constantly verify any changes, or attempted access where no changes were made. The functionality of reporting a previous iteration of patient data provides a way of regulating authorized modification of patient data, preventing unauthorized record modifications, and ensuring that healthcare records are valid and reliable.

Integrity = Hash of Data + Blockchain Hash of Block

The InterPlanetary File System (IPFS) also improves data integrity by decentralizing file storage across multiple nodes. In a traditional databases, integrity of data is compromised at a single point of failure. With IPFS, file records are always replicated, and files are stored where no tampering is possible. If any tampering or discrepancies is discovered, the system can return to its original record and maintain its integrity. By decentralizing file storage, IPFS not only improves the integrity of every record, but improves the resiliency of the entire system to retain patient record records consistent over time.

b. Enhanced Security:

Data security is a paramount component of managing health record data, since patient records contain extremely sensitive data. The proposed system provides increased security by using Ethereum blockchain technology, which allows for all transactions that are made regarding patient data will be written to a tamper-proof ledger and remain immutable. Since the blockchain is decentralized by definition, no single entity will be able to alter or delete any transactions that are made regarding patient data. This immutability further guarantees that unauthorized changes are not doable, thereby safeguarding patient data from both outside cyber threats and inside threats. As well, since security policies are performed on smart contracts, the processes of verifying, auditing and controlling access to patient data are machine-driven, sets strict security policies that take human error out of data access or handling.

Encrypted Evidence = Ciphertext(Evidence, Key)

To ensure that patient records are as secure as possible, the system uses XChaCha20 encryption, which is a new and very secure and efficient encryption algorithm. All medical records are encrypted before they are stored, rendering them

unintelligible to unauthorized users. Even if an attacker gains access to the storage system, they will be unable to make sense of that data without having the necessary decryption keys or codes. XChaCha20 is considered to have a much stronger-encrypted design, meaning that it is far more resistant to cryptographic attacks as it ensures that the data is safe when environment credentials could be obtained through coercive or mild risk factors. Lastly, records are controlled by access keys by the eventual users, or patients, giving them complete control over modifications and who is allowed to review their health records. The added benefit of adopting the InterPlanetary file system (IPFS) makes the system more secure since it executes distributed storage models. This dispersed storage model results in a degree of separation from centralized clouds. IPFS allows for encrypted patient records to be stored into many nodes instead of a single. Ultimately, reduced single access points has reduced the ability to launch successful attacks to breach patient records, ransomware attacks and issues with unauthorized access to patient information. Furthermore, the system generates a constant record for all access and modifications in real-time, allowing for both current and retroactive auditability. Using a combination of blockchain-based methods, encryptions and decentralized management, it has resulted in the proposed system being highly secure, threat-resilient and patient privacy-preserving model of records management from a health provider perspective.

c. Automation with Smart Contracts:

The smart contract is the main component of the automatic equivalences of the specified data security and access control functions of the proposed healthcare data management system. The smart contract is a self-executing contract that regulates the many interactions that need to take place with patient records. The smart contract effects these interactions in a manner that eliminates unauthorized use as well as minimizes manual processes. When a patient, physician, or hospital interacts with the system, the smart contract is responsible for validating both their identity and appropriate access rights prior to allowing access to the information. Only authorized (verified) actors (healthcare providers) from the database can view or update patient records, ensuring patient confidentiality.

Smart Contract Execution = f(Conditions, Actions, Parties)

Smart contracts also enact the chain of custody for medical records by enforcing that all transactions be publicly logged on the Ethereum blockchain. When doctor enters a new patient record the smart contract logs its transaction automatically and this binds the particular user. Any time someone enters a physician or healthcare institution as the recipient of that data, our contract captures this ephemeral event writing to an immutable audit log. This ensures prevention of data manipulation and modify access only in the right way with traceability, accountability for medical data sharing. Smart contracts can be also used in combination with automated rule enforcement for data protection as well. E.g. they can dynamically set access permissions based on patient consent for temporary exposure of patients to consultative specialists but can still enforce the long term security system. When the condition of emergency is activated, medical records for critical patients can be retrieved immediately (for the authorized personnel only) bypassing patient privacy. Smart contracts not only solve the betterment of manual errors through proper enforcement of strict security policies and real-time logging in this process to make healthcare records management significantly more safer and secure in decentralized model but they also eliminate.

d. Increased Transparency:

Medical System for Suggestion Block chain medicine to bring transparency in managing and accessing patient data from all sides. Whereas the data in ordinary electronic medical record (EMR) systems is centralized, with one authority over existing records [3] the concept builds its theoretical base on the immutability of transactions which are written to the ledger of all nodes. Nothing is changeable by unauthorized party as each patient record, file or database access is recorded on an unalterable blockchain ledger. Medical data is tracked and trace in terms of patients, doctors and other authorized stakeholders which facilitates accountability and transparency for healthcare processes. Additionally, smart contracts ensure that access to information only goes to the parties who should have access and make sure they are only able to read/write patients records through pre-defined rules. Each access request is time stamped, so that a patient can know who has seen his/her health information and when. Thus, the systems would be less prone to data misuse and also medical records are handled in right manner. The system will provide an indisputable record of the incident that helps ensure compliance with regulations and thwart the frauds of unwarranted data sharing.

Transparency = Public Ledger(Transaction History)

Also, the system incorporates InterPlanetary File System (IPFS) for a more open storage system medicamentous files accessible and safer in incident of single points of failure. As all transactions (i.e. patient data uploads & modifications + sharing) happen on the blockchain itself, the stakeholders can cross-check medical history without any single administrator. This transparency promotes data integrity, increases trust of patients in health system and maintains data availability, security and immutability for the better medical decision.

e. Enhanced Traceability:

Improve traceability The proposed medical system leverages blockchain's immutability of the blockchain ledger to track every patient data transaction. They are timestamped and logged decentralized-wise, so all actions related a data steps; from creation of medical records, its updates and access requests are traceable. In contrast with changes in traditional systems,

blockchain keeps a tamper-proof audit trail meaning not even the owner of the data can delete records from the history. The benefit of that, is to detect illegitimate tries at access and guarantee to some extent, access accountability within health care providers.

Traceability = Evidence Log(Timestamps, Actions)

Also, smart contract are essential to automate and facilitate access controls. When a medical officer/ doctor or insurance provider requests about the patient health records that time forward a smart contract logs that event with timestamp, identity who requested and reason of access. This prevents only allowed users to get hold of those secrets, and any other modification from the standard protocols can be sniffed out and audited in realtime. This automation reduces the probability of data leak, fraudulent claims where patient records get compromised and can be traced completely during their life cycle.

Also the implementation of InterPlanetary File System (IPFS) for decentralized storage meant that the medical file were to be spread over multiple nodes, and not a single-point system. This structure underpins traceability as it enables verification of data authenticity in real time. Even slight discrepancies like loss of record or unauthorized changes are easily catchable and can be corrected at once. The system forms a blockchain-powered, verifiable & auditable (on public ledger and all decentralized through IPFS) framework for patient data management with the growth of security, compliance and trustworthiness in healthcare by IPFS.

f. Accuracy:

Accuracy is one of the prime performance indicators for classification models (eg ResNet-50 for fracture prediction of bone fracture). Accuracy in Machine Learning is, the percentage of data that a model correctly predicts (pos& neg both). It serves to indicate to what extent the model can be confident in the detection of actual fractures against noise (not fracturing cases).

$$\text{Accuracy} = \frac{\mathbf{TP+TN}}{\mathbf{TP+\ TN+\ FP+\ FN}}$$

Where:

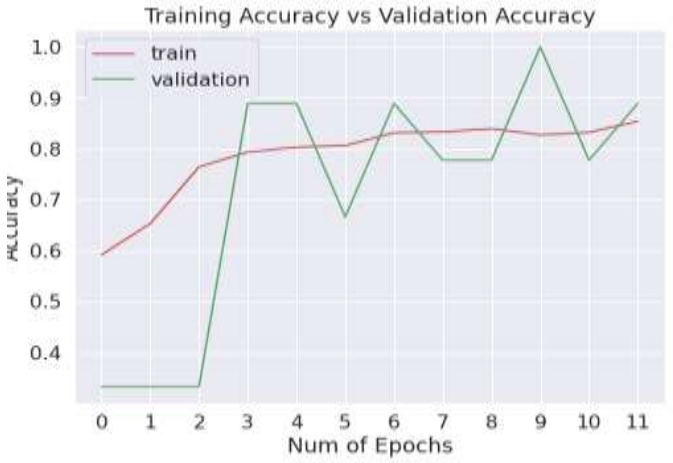
TP (True Positive): Fractures correctly predicted as fractures

TN (True Negative): Normal cases correctly predicted as normal

FP (False Positive): Normal cases incorrectly predicted as fractures

FN (False Negative): Fractures incorrectly predicted as normal

The above formula basically gives the total correctness of model predictions for final output aggregating over both kind of true classifications —pos and neg. For instance, if a model accurately labels 90 out of 100 cases (fractured and non-fractured together) For accuracy, we need to use that but along with other metrics; like precision, recall and F1-score particularly for imbalanced datasets (i.e., normal bones could overwhelm any other class). In cases like this, accuracy has the potential to be misleading as high accuracy does not necessarily mean good at recognizing rare outcomes (eg actual fractures). This means accuracy gives the high level overview, but a much more thorough examination is usually necessary for critical uses like medical decision making.



The training vs validation accuracy over 11 epochs of the graph of the proposed system"s graph where we are predicting bone fracture using ResNet-50 in validation, as well as training with accuracy. As the red line indicating training acc grows across epochs, it seems that the model is converging to learn from the training dataset (fitting/pattern recognition). In same time, green line which is representatingval accuracy fluctuates at beginning but go up and reach near 100% around epoch 9.

These could be possible cases for overfitting or having a lop-sided validation set that is typical in the medical image analysis. However, the high validation accuracy implies that our model is good at generalizing. It is a very clear proof of the efficacy and dependability in fracture detection as well demonstrates to a degree that can be improved more, and the system's performance can be more stablished by tuning (balanced data, regularization methods/schemas or more training samples) with this supervision algorithm. This seems to validate the ability of the proposed system to help clinicians in making precise diagnostics through artificial intelligence.

g. LOSS:

Loss is such a value in machine learning that tells about how model predication aligned with respect to actual target values good or bad. It captures the error during training and how much to move in optimization direction. The loss function which is most often used to solve classification task such as bone fracture prediction, is the categorical cross-entropy. This function takes the difference between the predicted probability distribution and the true distribution (labels) as inputs, giving feedback which is then used to tune model's weights. Training loss usually goes down during the training as the model learns to classify. However, keeping an eye on validation loss as well to see how well our model is performing on unseen data. So Remember used decreasing training and validation loss as indicator of overfitting if training loss is reducing but validation loss is increasing. Observing the loss decrease steadily, which shows that the model is learning effectively in the proposed system. The behaviour of training and validation losses over epochs is something we should monitor to fine-tune, detect overfitting and stop training at right time.

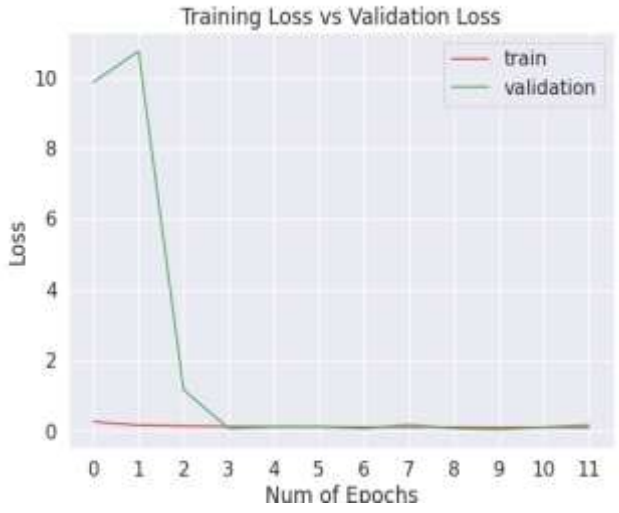
$\text{Loss} = -\sum_i^n y_i \log(\hat{y}_i)$

Where:

y_i is the actual label (1 for the correct class, 0 for others)

$\hat{y}_i$ is the predicted probability for class i

n is the number of classes



ResNet-50(Graph) bone fracture prediction model, trend of training and validation loss over 11 epoch in graph bone fracture loss. Training loss decreases monotonously meaning that the model learns to fit training patterns successfully. Validation loss is expected to have minor wanders as well, a side effect from smaller or unbalanced validation. But if we observe validation loss increasing, on the hand, training loss continues to drop that is overfitting as model works great on training data but not for out-of-distribution examples. Both loss curves coming down at a healthy pace signifying that the model is generic and will perform well in real world scenarios with minor changes. The discrepancy between two curves should imply that use of methods such as early stopping, regularization and / or dataset augmentation etc. need to be applied when observing such behavior while monitoring these losses is very important since it tells us about efficiency of the learning process and also helps us on making decisions during training. This analysis of the loss behavior guarantees that accuracy and reliablity of bone fracture prediction model be reproducible over different datasets.

h. Precision:

Precision is an important evaluation criterion of classification models, especially in medical use cases (e.g bone fracture prediction).Precision — number of correctly predicted positives over all predicted positives It translates to, the precision here just means how many of fracture calls we made were true fractures. In healthcare this can be catastrophic as the false positive

(fracture predicted when none exists) would create false cause for tests or procedures.

$$\textbf{Precision} = \frac{\textbf{True Positives (TP)}}{\textbf{True Positives (TP)} + \textbf{False Positives (FP)}}$$

In this setting, True Positives (TP) are fracture cases that are predicted correctly and False Positive (FP) is a normal case predicted as fracture. Precision score is higher, keep the false positive rate of your model so low it actually becomes zero in the clinical setting where correct diagnosis matters. In bone fracture detection for example high precision means no non-fractures should be classified as fracture, nothing gets done.

Precision is especially useful when false positives are very costly. Precision in scenario healthcare entails the chances that a physician can rely on for legitimate cases that are actually worth looking at. If it balances well with recall, where the model is asking for how many actual positives were found. But, also recall is needed as in many medical systems a high precision model is somehow integrated with other measures to make sure they are both accurate and complete. Implementation in medicine can significantly improve diagnosis and patient care by providing a well-tuned bone fracture prediction model with high precision and decrease diagnostic errors.

i. RECALL:

Recall is a crucial metric for classificaitonmodels performance especially recall in healthcare classification tasks, hereupon bone fracture prediction. It quantifies the model's capacity to correctly mark all actual positive instances. In other words, recall quantifies how many fractures of the actual were correctly identified by the model. Which contributes to the situation especially in medical diagnosis, in case fracture is missed (i.e. false negative) it may be a serious concern such as late therapy or wrong diagnosis.

$$\textbf{Recall} = \frac{\textbf{True Positives (TP)}}{\textbf{True Positives (TP)} + \textbf{False Negatives (FN)}}$$

TP: True Positives (the fracture cases that are correctly predicted as cases and False Negatives (FN): fracture cases predicted as non-fracture) A model with higher recall would imply that the model is flagging most of the real fracture cases, absolutely necessary in minimizing missed diagnosis, it saved time and spare trouble of doctor etc. High recall in bone fracture detect system means ensures that there are no leakage of fractures to the downstream for possible clinical interventions.

Recall is especially useful in situations where missing a positive case will incur much greater cost than issuing some false positives. On a dataset of bone fractures — failing to recognize a fracture can land your patient in major trouble, so it is better if we can detect as many fractures as possible —even if some of them are false alarms. That said, you want to be careful that you dont over-look recall and precision in order not treat too many false positives. A model that has high recall and high precision is perfect healthy as it means the vast majority of fractures are identified correctly, and thereby reducing the chance of misses as well as no need treatments.

j. F1 SCORE:

The **F1 Score** is a performance metric that combines both precision and recall into a single number, making it particularly useful when evaluating models where there is an imbalance between the positive and negative classes. It is the harmonic mean of precision and recall, providing a balanced view of the model's performance. While precision and recall each measure different aspects of the model, the F1 score gives equal weight to both, making it ideal for situations where a balance between the two is required.

$$\textbf{F1 Score} = 2\ \textbf{X}\ \frac{\textbf{Precision X Recall}}{\textbf{Precision} + \textbf{Recall}}$$

Where Precision Recall it already defined as metrics. F1 score is from 0 to 1, where 1 is the best possible score (equal precision and recall) An F1 score of 0 would mean that either precision (P) or recall(R) => 0^1 — The model is unable to make any correct forecasts In healthcare especially for bone fracture prediction the F1 score helps one whether a model has the capacity to possibly find an equilibrium on correctly detecting fractures (high recall + low false positive rate i.e high precision).

In general, F1 score is most useful in imbalanced datasets going to near zero for any class that occurs less frequently (e.g. no fracture cases may be way more common than fracture). When optimization is based only on accuracy, this just might not be a true representation of the model performance as it could be potentially predicting all classes as majority and it still look accurate.

This is not due to a lack of F1 score which corrects for overly-precision or recall (or both) models to be well-rounded, striving to maximize true positives while penalizing false positives equally with false negatives.

5. CONCLUSION

All in all, the suggested system is very appreciable step towards health data management from privacy security point of view and diagnostic impact [21] [22]. The system chains the transaction logging of medical records with immutable and visible transaction records on an Ethereum blockchain technology, thus belonging your electronic medical record (EMRs). Smart contracts enhance data security by automatically applying access control rules and also enforcing them, keeping out unauthorized users from modification and anonymity. Additional the patient records are encrypted with XChaCha20 cipher algorithm too so even though the adversary have access to system sensitive data is protected. Integration of ResNet-50 a deep learning convolutional neural network improves the diagnostic performance in this system, especially bone fractures recognition from X-ray images. A model trained on a bone fractures dataset with ResNet-50 finetuned allows to identify fractures even those extremely subtle which humans might miss. Not only helps to increase the speed of diagnosing and reducing human glitches but also promotes efficient treatment for the patients undergoing the treatment. Additionally, the decentralized storage powered by InterPlanetary File System (IPFS) from the system provides an extra layer of security to not only have patient data and X-ray images be stored securely but tamper-proof too. These technologies combined provide a strong, scalable solution for managing healthcare data; their secure and fast platform can record the patients-data as well do medical diagnosis. Using blockchain, encryption and AI the system met a higher level of trust, security, performance, and accuracy for diagnostics which resulted in better patient care impacting outcomes. The next steps for the proposed system could be the implementation of wearable health devices to actively enforce real-time monitoring and predictive analytics in addition to improving the AI model by exploring other deep learning architectures on augmenting dataset from bone fracture detection. The system could also be developed into medical diagnosis for other ailments, providing increased diagnostic accuracy.

REFERENCES

[1] O. Abuzaghleh, B. D. Barkana, and M. Faezipour, ``SKINcure: A real time image analysis system to aid in the malignant melanoma preven-tion and early detection," in Proc. IEEE Southwest Symp. Image Anal. Interpretation (SSIAI), Apr. 2014, pp. 8588.

[2] R. P. Braun, H. Rabinovitz, J. E. Tzu, and A. A. Marghoob, ``DermoscopyresearchAnupdate, "Seminars Cutaneous Med. Surgery, vol. 28, no. 3, pp. 165171, 2009.

[3] C. Doukas, P. Stagkopoulos, C. T. Kiranoudis, and I. Maglogiannis, ``Automated skin lesion assessment using mobile technologies and cloud platforms," inProc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), Aug./Sep. 2012, pp. 24442447.

[4] A. Karargyris, O. Karargyris, and A. Pantelopoulos, ``DERMA/Care: An advanced image-processing mobile application for monitoring skin cancer," in Proc. IEEE 24th Int. Conf. Tools Artif. Intell. (ICTAI), Nov. 2012, pp. 17.

[5] C. Massone, A. M. Brunasso, T. M. Campbell, and H. P. Soyer, ``Mobile teledermoscopy Melanoma diagnosis by one click?" Seminars Cutaneous Med. Surgery, vol. 28, no. 3, pp. 203205, 2009.

[6] PragatiRajendra Mahajan Prof.Mrs.A.J.Vyavahare "Artefact Removal and Contrast Enhancement for Dermoscopic Images Using Image Processing Techniques", 2013.

[7] M. Rademaker and A. Oakley, ``Digital monitoring by whole body pho-tography and sequential digitaldermoscopy detects thinner melanomas,'' J. Primary Health Care, vol. 2, no. 4, pp. 268272, 2010.

[8] S. Suer, S. Kockara, and M. Mete, ``An improved border detection in dermoscopy images for density basedclustering,"BMCBioinformat., vol. 12, no. 10, p. S12.

[9] Gaofan Lin, Haijiang Wang ∗ , Jian Wan ∗ , Lei Zhang, Jie Huang A blockchain-based fine-grained data sharing scheme for e-healthcare system 2023 https://www.sciencedirect.com/science/article/pii/S1383762122002168.

[10] N. Palanivel, D. S, L. P. G, S. B and S. M. M, "The Art of YOLOv8 Algorithm in Cancer Diagnosis using Medical Imaging," 2023 International Conference on System, Computation, Automation and Networking (ICSCAN), PUDUCHERRY, India, 2023, pp. 1-6, doi: 10.1109/IC

[11] HAZILAH MAD KAIDI , (Senior Member, IEEE), MOHD AZRI MOHD IZHAR , (Member, IEEE), RUDZIDATUL AKMAM DZIYAUDDIN A Comprehensive Review on Wireless Healthcare Monitoring: System Components 2023 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10439065

[12] ABDULLAH AL MAMUN 1 , SAMI AZAM 2 , (Member, IEEE), AND CLEMENTINE GRITTI 3 Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9673752

[13] Samad Rashid&Arash NematiHuman-centered IoT-based health monitoring in the Healthcare 5.0 era: literature descriptive analysis and future research guidelines

https://link.springer.com/article/10.1007/s43926-024-00082-5

[14] Vonteru Srikanth Reddy, Kumar Debasis Statistical Review of Health Monitoring Models for Real- Time Hospital Scenarios https://ijritcc.org/index.php/ijritcc/article/view/7025

[15] KegomoditsweBoikanyo, Adamu Murtala Zungeru Remote patient monitoring systems: Applications, architecture, and challenges 2023 https://www.sciencedirect.com /science/ article/ pii/S2468227623000959

[16] Basem Assiri A Modified and Effective Blockchain Model for E-Healthcare Systems 2023 https://www.mdpi.com/2076-3417/13/23/12630.

[17] Yazeed Yasin Ghadi, Tehseen Mazhar, Tariq Shahzad, Muhammad Amir khanTherole of blockchain to secure internet of medical things https://www.nature.com/articles/s41598-024-68529-x.

[18] Dhaneshwar Shah, Sunanda Rani, Khadija Shoukat Blockchain Factors in the Design of Smart-Media for E-Healthcare Management https://www.mdpi.com/1424-8220/24/21/6835