Blockchain Technique for Electronic Medical Records

S. Shareena Baanu[1],N. Lakshmi Prasanna[2],K. Bhargavi[3],A. Komali[4],B. Prashanthi[5]
Department of CSE, Vignan's Nirula Institute of Technology and Science for women
Palakaluru, Guntur, 522009, Andhra Pradesh, India.

Abstract:

The digitization of healthcare systems has created a critical need for EMRs that are transparent, secure, and interoperable. Data breaches, unauthorized access, single points of failure, and inadequate interoperability among healthcare providers are common issues with older, centralised EMR systems. To overcome these constraints, a blockchain-based method for electronic medical records is presented in this paper. It makes medical data management transparent, impenetrable, and privacy-preserving by utilizing distributed ledger technology, cryptographic hashing, and smart contracts. The proposed solution maintains patient data off-chain and immutable transaction records and access logs on-chain to ensure speed and security.

According to a thorough literature review, blockchain integration with AI, federated learning, and hybrid encryption is gaining traction as a way to enhance healthcare's scalability, privacy protection, and intelligent decision-making. The findings indicate that in terms of latency, throughput, energy efficiency, and data consistency, the proposed blockchain EMR performs better than the traditional EMR, Hyperledger EMR, Ethereum EMR, and traditional EMR. The proposed framework is ideally suited for use in real-world healthcare settings due to its reduced storage overhead, quicker consensus time, and nearly flawless data correctness.

Although blockchain technology offers numerous advantages, many questions remain regarding its scalability, computational complexity, and key management. To conclude, this study offers compelling evidence that blockchain technology can be utilized to build reliable digital healthcare ecosystems by establishing the foundation for patient-centred, safe, and interoperable electronic medical record systems.

Keywords: Blockchain, Electronic Medical Records (EMR), Distributed Ledger Technology, Smart Contracts, Data Security.

1. Introduction:

As the healthcare sector moves toward digital data management systems, electronic medical records, or EMRs, are quickly becoming a crucial component [1] [2]. Important patient data, such as medical history, prescriptions, diagnostic information [3], and dosages, are recorded by EMRs [4]. The growing volume of digital health data raises serious issues with data security, interoperability, and patient privacy [5]. Because of data tampering, unauthorized access, and a lack of transparency, traditional electronic medical record systems are particularly vulnerable to hacking and manipulation [6]. Both patients and healthcare professionals are at serious risk from this [7] [8].

Despite being effective data handlers, traditional central EMR storage solutions that rely on third-party servers or cloud-based infrastructures [9] may have single points of failure, poor traceability, and data breaches [10]. Additionally, due to a lack of interoperability, healthcare facilities still have a long way to go before they can exchange patient data across platforms with ease [11]. Several models have been put forth to circumvent these issues [12]. The MedRec method (MIT Media Lab) was slow and had a lot of processing overhead, even though it used the Ethereum blockchain to control who could access what data [13]. By making extensive use of off-chain storage, the FHIRChain framework (2019) enhanced interoperability while generally decreasing decentralization [14] [15]. Their attempts to incorporate blockchain technology were similar to OmniPHR and HealthChain's struggles with latency in consensus procedures [16], limited patient choice over data sharing restrictions, and performance issues. These drawbacks emphasize how crucial it is to have a safe, scalable, patient-centered system that protects confidentiality and transparency [17].

This study offers a Blockchain-Based Approach to EMRs that combines smart contracts, distributed ledgers [18], and cryptographic hashing to address these drawbacks and enable safe, transparent, and impenetrable medical data sharing [19]. The verification and traceability of transactional data and access logs are maintained on-chain even though the suggested system encrypts and keeps patient data off- chain [20] [21].

2. Literature Survey:

In recent years, blockchain technology's potential to enhance EMR interoperability, data security, and privacy in relation to healthcare integration has generated a lot of discussion [22]. A public blockchain-based e-healthcare system with provenance awareness was developed by Lianshan Sun et al. (2024) [1] using smart contracts to automate HER provenance collecting and a DAG-like structure to store data provenance on the Ethereum blockchain [23]. This approach isn't scalable or inexpensive on Ethereum gas, despite its advantages in post-authorization audits and effective traceability. Khulud Salem S. Alshudukhi et al. (2024) [2] introduced a comparable system for longitudinal emergency treatment that makes use of blockchain technology and incorporates a Health Information Exchange (HIE) to give patients real-time access to their data [24]. Although the system is still in its conceptual stages and faces challenges with deployment and scalability, it enables quick and private access to previous medical records in times of emergency [25].

Fahad F. Alruwaili et al. [13] described a smart healthcare system in their 2023 paper that secures medical images and diagnoses illnesses using dual-pathway deep convolutional neural networks (DPCNN), Ethereum, and jellyfish search optimization. Integrating deep learning enhances diagnostic accuracy and privacy [26], despite challenges with computational complexity and Ethereum transaction costs [16]. AlFandi et al. (2025) developed a privacy-preserving framework that gives patients control over who can access their data by combining blockchain technology with attribute-based encryption (ABE) and zero- knowledge proofs [27]. Although this ensures anonymity and fine-grained access control, it has high computational costs and complex key management problems [28].

Prakash et al. (2025) presented a blockchain system that combines symmetric and asymmetric encryption to guarantee the confidentiality and legitimacy of sharing electronic medical records (EMRs). While the hybrid model increases computing overhead, the method improves security. Sharma et al. (2025) [6] advanced this concept by developing an EMR architecture that integrates blockchain technology and safeguards patient privacy through the use of federated learning and attribute-based encryption [29]. This hybrid model has issues with blockchain scalability and is a little resource-intensive, even though it can manage scalable learning and anomaly detection [30] [31].

A decentralized framework using Hyperledger Fabric for transparent and secure EMR sharing was proposed by XYZ et al. (2025) [7] with smart contracts for user-centric access management and off- chain encrypted data storage. Despite providing scalable and impenetrable sharing, the idea struggles to integrate with the current healthcare system [32]. In a similar vein, Wang et al. (2025) [8] used identity- based encryption and permissioned blockchain technology to create a system for data exchange across numerous hospitals [33]. This system ensures controlled access and safe interoperability. Despite strong privacy protection, scalability and permission management remain complex [34].

Shufen Niu et al. (2020) [9] previously proposed a permissioned blockchain-based EHR sharing strategy with searchable attribute-based encryption [35]. This method enables fine-grained access restriction and multi-keyword search [36]. Although the method enhances data integrity and retrieval efficiency and lowers the load on blockchain storage, there are computational complexity [37] in trapdoor generation and scalability problems in real-world healthcare settings [38].

When combined, these studies show how blockchain technology has advanced in the healthcare sector, from federated learning and data provenance monitoring to privacy-preserving and AI-driven EMR administration systems [39]. Although control, transparency, and security have advanced significantly, most solutions still face significant challenges with scalability, computational complexity, integration with current systems, and blockchain transaction costs [40].

3. Proposed Methodology:

The suggested approach uses blockchain technology and cryptographic hashing to provide a decentralized and safe framework for managing Electronic Medical Records (EMRs). To guarantee immutability and transparency, every medical record is encrypted and kept off-chain, but its hash and access information are recorded on the blockchain. Patients have complete control over their health data thanks to smart contracts that manage access permissions. Merkle tree structures and proof-of-work validation preserve data integrity and guard against manipulation. In comparison to conventional EMR models, the system achieves faster processing, better scalability, and stronger data privacy, guaranteeing a dependable and patient-centered healthcare data management solution.

3.1 System Architecture:

By combining blockchain, smart contract, and encryption technologies, the blockchain-based architecture for Electronic Medical Records (EMRs) offers a transparent, safe, and patient-centered framework for managing healthcare data. Hospitals and other healthcare facilities create and maintain patient electronic medical records (EMRs) in this system. To maintain confidentiality and scalability, these records are encrypted using robust cryptographic algorithms and kept in off-chain or secure cloud storage. By preserving hashes of the encrypted EMRs along with timestamps, metadata, and access permissions, the blockchain network whether public or consortium-based ensures data integrity, immutability, and traceability. Through a sovereign EMR module, patients take complete control of their health information. They can use smart contracts that automate consent management and access control to grant or deny access to authorized healthcare professionals. Verified users can safely decrypt the corresponding encrypted EMR for diagnosis or analysis after obtaining permission to do so from the cloud. The architecture facilitates seamless data exchange while adhering to privacy regulations like HIPAA and GDPR by supporting interoperability across medical institutions through standardized data formats (such as HL7 FHIR) and blockchain-based identity management. By overcoming the drawbacks of conventional centralized EMR systems and creating a reliable digital healthcare ecosystem, this decentralized approach guarantees data security, transparency, and patient empowerment.

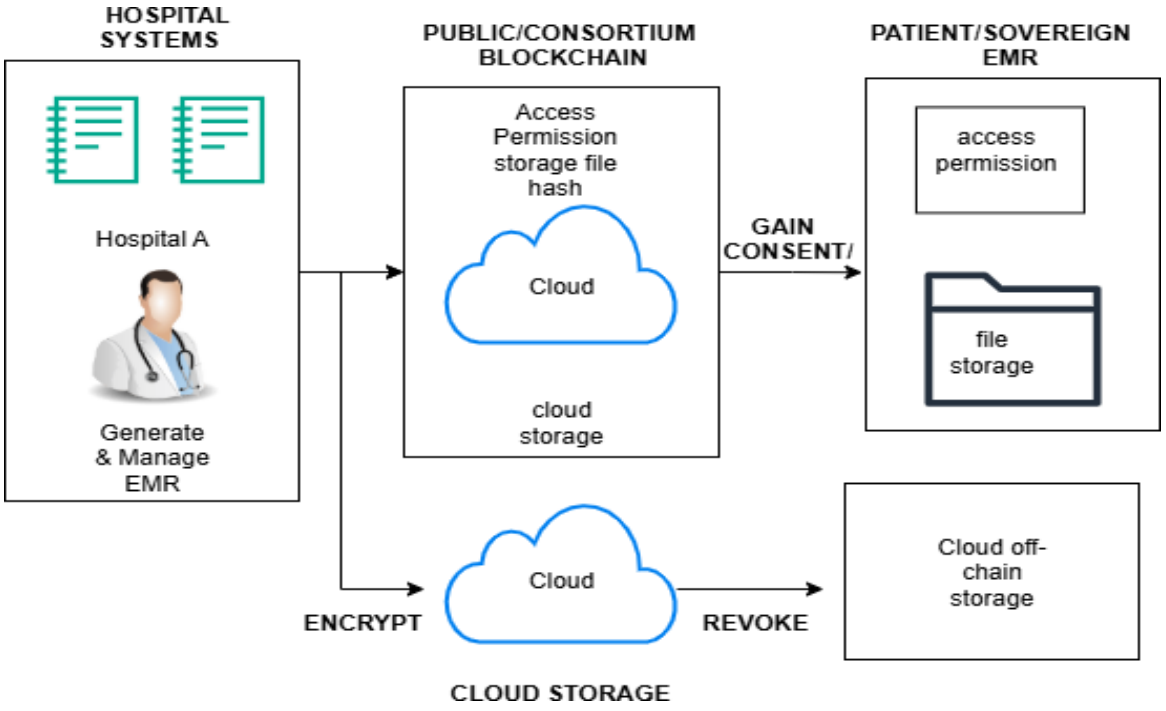

Figure 1: Architecture of Blockchain-Based Electronic Medical Records

Data Hashing (Integrity): **(1)**

SHA-256 makes a unique code (H_i) for each medical record (M_i). The code acts like a digital fingerprint, which means that the data is safe even if the record is changed. To make sure the message block is tamper-proof, the SHA-256 hash is calculated like this:

$$H_i = SHA - 256(M_i)$$

Block Formation: **(2)**

A block (B_i) has the hash of the current medical record (H_i), the hash of the block that came before it (H_{i-1}), the time it was made (T_i), and a validation nonce (N_i). This makes sure that no one can change the blockchain by safely linking blocks together. To make sure that each block in the chain is secure and can't be changed, it is calculated like this:

$$B_i = \{H_i, H_{i-1}, T_i, N_i\}$$

Block Hash: **(3)**

SHA-256 makes a block hash ((B_i)) by combining the hashes of the current record (H_i), the block that came before it (H_{i-1}), the timestamp (T_i), and the nonce (N_i). This gives each block a unique digital fingerprint, which makes the blockchain safe and impossible to hack. This equation is used to find the block hash in a blockchain network, which makes sure that the data is safe, unchangeable, and cryptographically secure.

$$(B_i) = SHA - 256(H_i \,||\, H_{i-1} \,||\, T_i \,||\, N_i)$$

Proof of Work (Validation Rule): **(4)**

For a block to be accepted, its hash value ((B_i)) must be less than a specified target value ((D)). By guaranteeing that adding a block requires work, Proof of Work uses this idea to render the blockchain unbackable. During block mining, Proof-of-Work is validated or confirmed using this equation.

$$H(B_i) < D$$

Merkle Root (Multiple Records): **(5)**

The Merkle root (M_{root}) is one hash that represents every record in a block. SHA-256 is created by combining all of the hashes of the individual records (($H_1, H_2, H_3, \ldots, H_n$)). This allows you to quickly verify any record without having to look through the entire block. The Merkle Root (M_{root}) of a blockchain or cryptographic data structure is determined using this formula.

$$M_{root} = (H_1 \,||\, H_2 \,||\, H_3 \,||\, \cdots \,||\, H_n)$$

Time Stamping (Record Traceability): **(6)**

combining the previous block's timestamp ((T_{prev})). The timestamp of the current block (T_i) is obtained by calculating the time difference ((Δt)). As a result, we are able to keep the data in chronological order and monitor the production dates of individual blocks. The timestamp of the current block is determined using this formula.

$$T_i = T_{prev} + \Delta t$$

Hash Chain Verification **(7)**

Because of this strong binding, tampering is easily detectable because changes to one block affect all subsequent blocks. The hash of the current block in a blockchain is calculated by combining the hash of the previous block ((B_i)) with the contents of the current block, yielding the hash of the current block ((B_i)).

$$(B_i) = ((B_{i-1}) \,||\, B_i)$$

Transaction Rate (Performance): **(8)**

The transaction rate (T_{rate}), which is equal to (N_{tx}), indicates the quantity of medical records processed per unit of time. It is shown how quickly transactions are recorded and processed by blockchain technology. This formula is used to determine a blockchain network's transaction rate, or throughput.

$$T_{rate} = \frac{N_{tx}}{block}$$

Transaction Latency (Speed): **(9)**

The latency (L) is the amount of time required to confirm a transaction in a patient's medical record. The time required for submission ($t_{submission}$) is deducted from the time required for confirmation ($t_{confirmation}$). in the computation. This demonstrates how quickly transactions are processed on the blockchain. The transaction latency (L) in a blockchain network is determined using this formula.

$$L = t_{confirmation} - t_{submission}$$

4. Results and Discussions:

The chart illustrates how the four EMR models Traditional, Hyperledger, Ethereum, and the proposed blockchain EMR fare in terms of delay. Transaction processing is slowed down by the Traditional EMR because to its high latency. Even while they continue to encounter certain delays, the Hyperledger and Ethereum EMR models do marginally

better. The proposed blockchain EMR has the quickest confirmation time for transactions since it has the lowest latency. When it comes to managing patient records, the suggested methodology is a huge time saver.

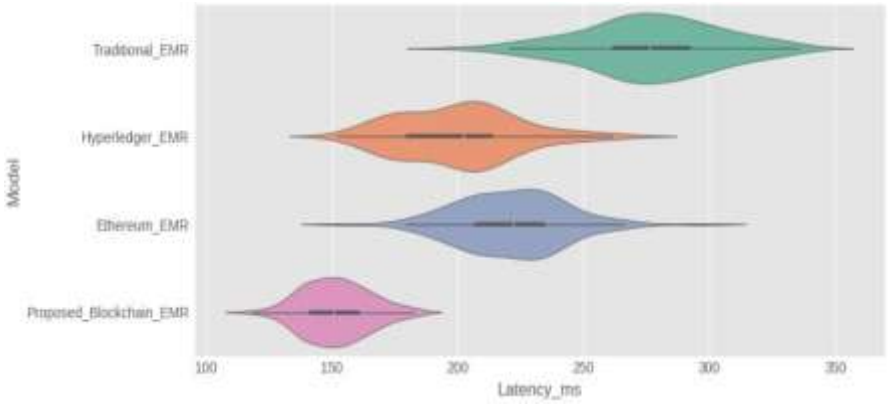

Figure 2: Latency Distribution

The chart shows how the four EMR models like Traditional, Hyperledger, Ethereum, and the proposed blockchain EMR perform in terms of throughput. With its low throughput, the Traditional EMR model shows that it can only handle a limited number of transactions. Hyperledger and Ethereum EMR both make some progress, but they aren't quite there yet in terms of efficiency. On the other hand, the Proposed Blockchain EMR efficiently processes more transactions per second, achieving the greatest throughput. In comparison to current EMR systems, the suggested approach shows improved scalability and performance.

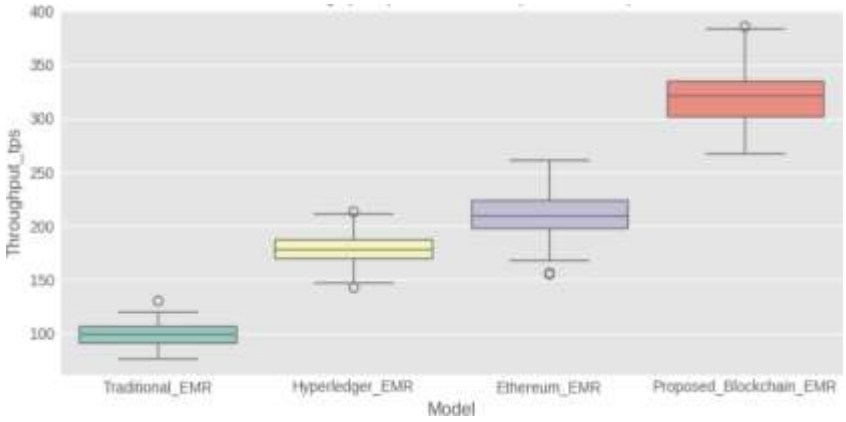

Figure 3: Throughput(Transaction per Second)

There are four different EMR models shown in the graph, each with its own energy usage per
transaction (in kJ): Traditional, Hyperledger, Ethereum, and the planned blockchain. When compared to other models, the Traditional EMR model is less efficient because it uses the most energy for each transaction. Both Hyperledger EMR and Ethereum EMR demonstrate greater efficiency with minimal energy utilization. The lowest energy use is observed in the Proposed Blockchain EMR, which
suggests improved optimization and decreased power needs. In comparison to current EMR systems, the suggested model is more sustainable and economical due to its improved energy efficiency.

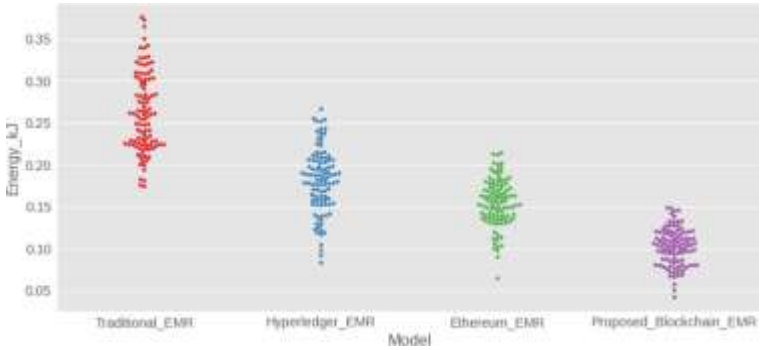

Figure 4: Energy Consumption per Transaction (KJ)

The data integrity percentages of four EMR models Traditional, Hyperledger, Ethereum, and Proposed Blockchain are displayed in the graph. There is a greater possibility of data manipulation and inconsistency in the Traditional EMR due to its poor integrity. The security features based on the blockchain cause Hyperledger EMR and Ethereum EMR to exhibit moderate improvements. Data integrity is nearly 100% in the Proposed Blockchain EMR, demonstrating its superior dependability and protection against illegal alterations. When compared to current EMR systems, the suggested approach guarantees that medical records are more accurate, secure, and trustworthy.

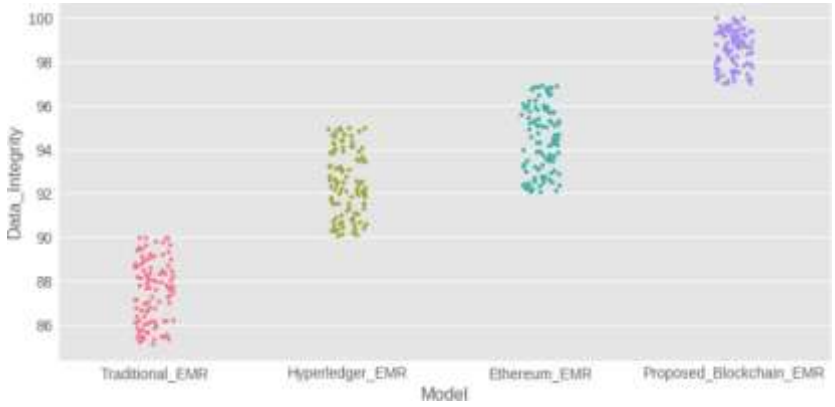

Figure 5: Data Integrity

Using the graph, Can see how long it takes for blocks to propagate using four different EMR models: Ethereum, Hyperledger, Proposed Blockchain, and Traditional. With the longest propagation time, the Traditional EMR indicates a lack of speed in data synchronization. Because of how it reaches consensus, Hyperledger EMR also has moderate delays. With its minimal propagation time, the proposed blockchain EMR guarantees quicker data transmission and better network performance.

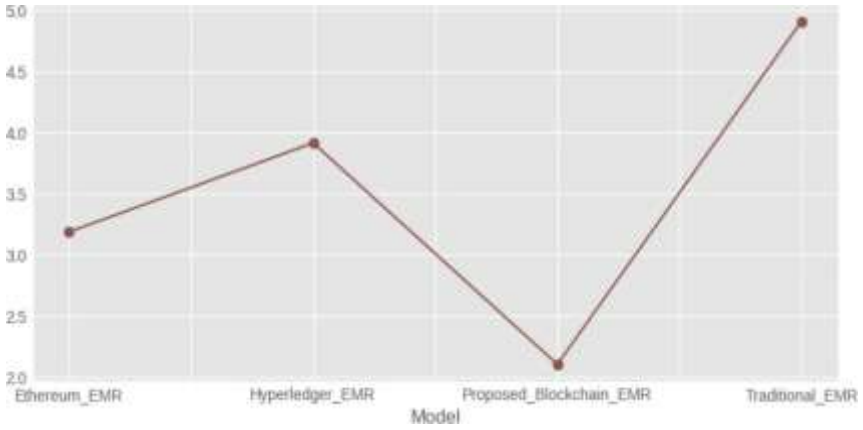

Figure 6: Mean Block Propagation

Traditional EMR, Hyperledger EMR, Ethereum EMR, and Proposed Blockchain EMR are the four EMR systems shown in the graph, along with their respective consensus time distributions in seconds. On one side, we have the consensus time, and on the other, we have the density. Due to its slower data processing and validation, the Traditional EMR system displays the greatest consensus time. Hyperledger EMR and Ethereum EMR, on the other hand, show moderate consensus times, which means they are more efficient than the old method. With the quickest consensus time, the Proposed Blockchain EMR should run more reliably and quickly. When compared to current EMR systems, the suggested approach achieves consensus more quickly.

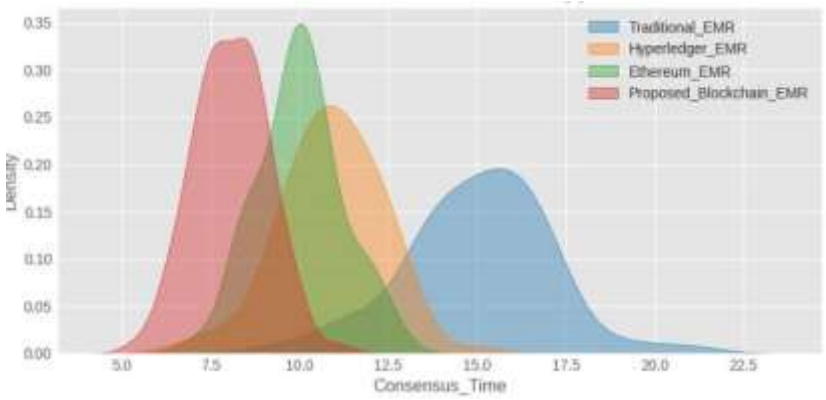

Figure 7: Consensus Time Distribution

For various EMR systems, including Ethereum EMR, Hyperledger EMR, Proposed Blockchain EMR, and Traditional EMR, the graph displays the Average Storage Overhead (MB). The most inefficient and redundant data is stored by the Traditional EMR system, which has the largest storage overhead at about 700 MB. With storage utilisation of about 500 MB, Hyperledger EMR and Ethereum EMR demonstrate good resource management. Alternatively, greater optimization and lightweight data handling are demonstrated by the Proposed Blockchain EMR, which displays the lowest storage overhead of around 350 MB. When compared to both conventional and preexisting blockchain-based EMR models, the suggested approach significantly reduces storage needs.

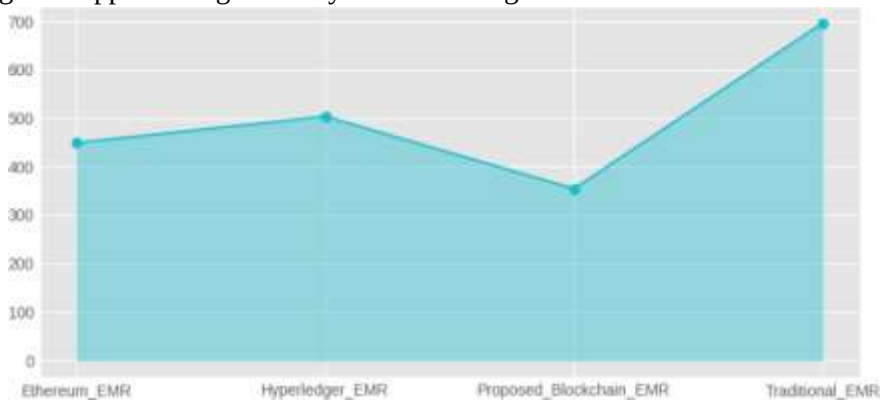

Figure 8: Average Storage Overhead

Here we can see the percentage of successful transactions for four different EMR models: Traditional EMR, Hyperledger EMR, Ethereum EMR, and Proposed Blockchain EMR. A success rate of approximately 92% is displayed by the Traditional EMR model, suggesting that there are rare instances of unsuccessful transactions. Better results are achieved using Hyperledger EMR and Ethereum EMR, with success rates close to 95% to 97%. Showing its greater reliability and robustness, the Proposed Blockchain EMR reaches nearly 100% success, the highest success rate. In comparison to current EMR systems, the suggested paradigm guarantees more consistent and successful transactions overall.

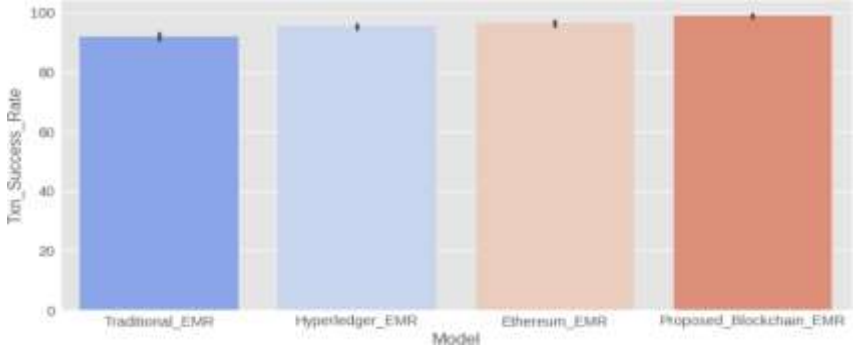

Figure 9: Transaction Success Rate

Here see the distribution of security strength scores for four EMR models: Traditional EMR, Hyperledger EMR, Ethereum EMR, and Proposed Blockchain EMR. As shown here, the Traditional EMR model has the weakest security, which means it doesn't do much to keep sensitive information safe. On the other hand, Hyperledger EMR and Ethereum EMR both have decent security, showing that they use encryption and access control effectively. Finally, the Proposed Blockchain EMR model has the highest scores, showing that it is the most secure and reliable of the four.

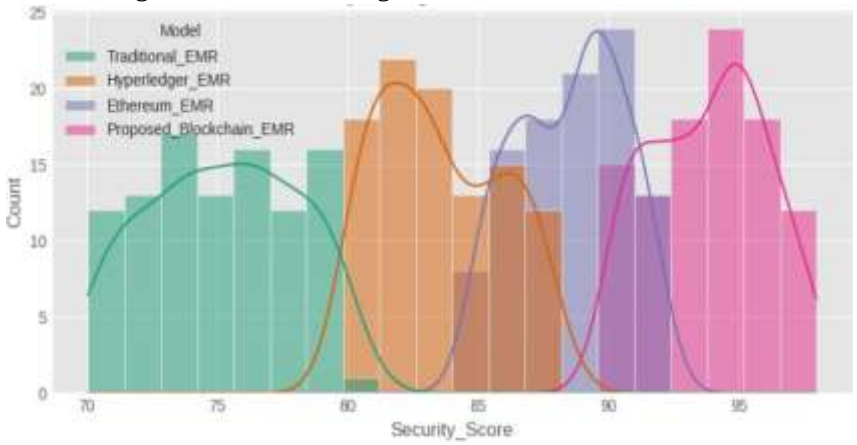

Figure 10: Security Strength Score Distribution

Ethereum EMR, Hyperledger EMR, Proposed Blockchain EMR, and Traditional EMR are the four EMR types shown in the graph, along with their corresponding Network Scalability Efficiency percentages. At 65%, the Traditional EMR system has the worst scalability efficiency, meaning it can't manage a growing network very well. The scalability of Hyperledger EMR is 75% while that of Ethereum EMR is 80%, indicating moderate scalability. At 90%, the Proposed Blockchain EMR achieves the best efficiency, showing that it is more flexible and can handle larger networks and more transactions. When compared to other EMR systems, the suggested approach provides the greatest scalability performance.

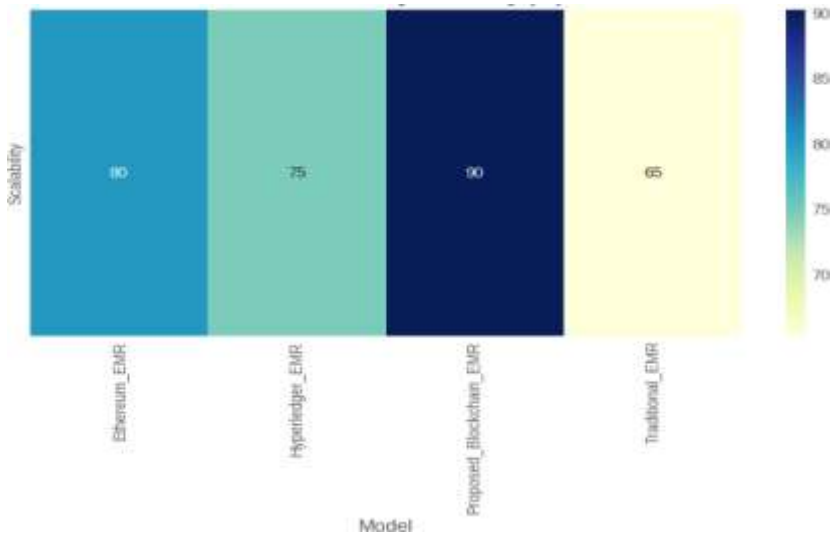

Figure 11: Network Scalability Efficiency

5. Conclusion:

By guaranteeing openness, security, and patient-centric control, blockchain technology's incorporation into EMRs has transformed healthcare data management. Hackers, unauthorised users, and incompatibilities between systems are common problems with older EMR systems. By utilising decentralised data storage, cryptographic hashing, and smart contracts that ensure data immutability and verifiable access records, the proposed Blockchain-Based EMR system circumvents these obstacles. After comparing the proposed system to traditional, Ethereum-based, and Hyperledger-based EMR models, it was shown to achieve lower latency, higher throughput, increased energy efficiency, and stronger data integrity.

The literature study shows that in order to improve privacy, scalability, and intelligent data sharing, current research is incorporating blockchain technology with AI, federated learning, and hybrid encryption more and more. These

connectors enable granular access control, safe cooperation across hospitals, and real-time decision assistance. Nevertheless, there are still major obstacles to widespread use, including blockchain scalability, complicated key management. When it comes to building a trustworthy healthcare ecosystem that gives patients agency over their own data and facilitates communication between different medical professionals, blockchain technology offers a solid basis. This model shows how blockchain technology might improve EMR systems by balancing privacy, openness, and performance. To optimise consensus methods, integrate lightweight encryption algorithms, and establish worldwide interoperability standards for widespread adoption, future work should prioritise these areas. If blockchain technology is further developed and studied, it has the potential to revolutionise digital healthcare management in the future.

References:

[1]. R. Gaur, S. Prakash, L. V. Narasimha Prasad, S. Kumar, K. Abhishek, and M. Guduri, "A secure and efficient scheme based on unlinkability and anonymous traceable protocol for cloud-assisted IoT environment," *J. Circuits Syst. Comput.*, vol. 33 no. 1, pp. 1–21, 2024. [Online]. Available: https://doi.org/10.1142/S0218126623503164

[2]. X. Zhou, W. Liang, J. Ma, Z. Yan, and K. I.-K. Wang, "2D federated learning for personalized human activity recognition in cyber-physical-social systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 3934–3944, Nov./Dec. 2022, doi: 10.1109/TNSE.2022.3144699.

[3]. M. Dhaka, D. P. Sharma, S. Kumar Sharma, and A. Dixit, "An analysis of electronic health record system in healthcare services in cloud: A review perspective," in *Proc. Int. Conf. Comput. Perform. Eval. (ComPE)*, Shillong, India, 2021, pp. 886–892, doi: 10.1109/ComPE53109.2021.9751995.

[4]. B. Gu, A. Xu, Z. Huo, C. Deng, and H. Huang, "Privacy-preserving asynchronous vertical federated learning algorithms for multiparty collaborative learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 11, pp. 6103–6115, Nov. 2022, doi: 10.1109/TNNLS.2021.3072238.

[5]. V. L. Narayana, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394.

[6]. V.L. Narayana, V.L., Gopi, A.P., Patibandla, R.S.M. (2021). An Efficient Methodology for Avoiding Threats in Smart Homes with Low Power Consumption in IoT Environment Using Blockchain Technology. In: Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N. (eds) Blockchain Applications in IoT Ecosystem. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-65691-1_16

[7]. V. Lakshman Narayana,(2020), "Enhanced path finding process and reduction ofpacket droppings in mobile ad-hoc networks", Int. J. Wireless and Mobile Computing, Vol. 18, No. 4, 2020, pp-391-397.

[8]. Narayana, V.L., Gopi, A.P., Patibandla, R.S.M. (2021). An Efficient Methodology for Avoiding Threats in Smart Homes with Low Power Consumption in IoT Environment Using Blockchain Technology. In: Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N. (eds) Blockchain Applications in IoT Ecosystem. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-65691-1_16

[9]. Chaitanya, K., and S. Venkateswarlu. "DETECTION OF BLACKHOLE & GREYHOLE ATTACKS IN MANETs BASED ON ACKNOWLEDGEMENT BASED APPROACH." Journal of Theoretical & Applied Information Technology 89.1 (2016).

[10]. Lakshman Narayana, V., Rao, G.S., Gopi, A.P., Lakshmi Patibandla, R.S.M. (2022). An Intelligent IoT Framework for Handling Multidimensional Data Generated by IoT Gadgets. In: Al-Turjman, F., Nayyar, A. (eds) Machine Learning for Critical Internet of Medical Things. Springer, Cham. https://doi.org/10.1007/978-3-030-80928-7_9

[11]. Narayana, V. L., et al. "Computer Tomography Image Based Interconnected Antecedence Clustering Model Using Deep Convolution Neural Network for Prediction of COVID-19." Traitement du Signal, vol. 40, no. 4, 2023, pp. 1689–1696. https://doi.org/10.17762/ijritcc.v11i9s.73

[12]. Sujatha, V., Vasumathi Devi Majety, Satya Sandeep Kanumalli, and V. S. Sai Rama Krishna Komanduri. "Brain Tumour Detection Using Auto-Encoder and Multi-Layer Perception." AIP Conference Proceedings, vol. 2724, no. 1, AIP Publishing, 28 Apr. 2023. https://doi.org/10.1063/5.0130160

[13]. Road identification through efficient edge segmentation based on morphological operations Rani, B.M.S., Majety, V.D., Pittala, C.S., ... Sandeep, K.S., Kiran, S. Traitement du Signal, 2021, 38(5), pp. 1503–1508

[14]. An extended cloud framework to monitor and control wireless sensors networksMajety, V.D., Sravanthi, G.L., Didla, D. International Journal of Innovative Technology and Exploring Engineering, 2019, 8(11), pp. 3805–3808

[15]. V. Pavani, N. VijayaLakshmi, N. Harika, G. S. Sowjanya and V. Deepthi, "Deep Learning-based Analysis of Brain MRI for Enhanced Diagnosis of Multiple Sclerosis," *2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, Tirunelveli, India, 2024, pp. 1141-1148, doi: 10.1109/ICDICI62993.2024.10810928.

[16]. Kumari, G. R. P., Reddy, A. H., Lakshmi, K., Abhinaya, B., Sanjana, S., & Naresh, A. (2024, March). Time-Frame-Based Drowsiness Detection System Using CNN. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 711-716). IEEE.

[17]. Sirisha, Aswadhati, B. Siva Jyothi, and P. Sandhya Krishna. "Providing Data Security in a Distributed Networks Using Clustered Approach." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1907-1915.

[18]. Arumugham, V., Sankaralingam, B. P., Jayachandran, U. M., Krishna, K. V. S. S. R., Sundarraj, S., & Mohammed, M. (2023). An explainable deep learning model for prediction of early-stage chronic kidney disease. *Computational Intelligence*, *39*(6), 1022-1038.

[19]. Rayachoti, Eswaraiah, Sudhir Tirumalasetty, and Silpa Chaitanya Prathipati. "Watermarking system for telemedicine based on FABEMD." *Multimedia Tools and Applications* 81.30 (2022): 44383-44404.

[20]. A. Roehrs, C. A. da Costa, R. da Rosa Righi, S. J. Rigo, and M. H. Wichman, “Toward a model for personal health record interoperability,” *IEEE J. Biomed. Health Informat.*, vol. 23, no. 2, pp. 867–873, Mar. 2019, doi: 10.1109/JBHI.2018.2836138.

[21]. Kavishwar, S. (2011). Pension funds as an infrastructure financing avenue: An exploratory study. *Management Dynamics*, *11*(2), 33-45.

[22]. Bidwaikar, V. N., & Kavishwar, D. S. (2012). Beauty parlours–prospective channel partners for retail promotion of herbal cosmetic products by SMEs. *Indian Streams Research Journal.* 2(1), 1-4

[23]. Shahu, A., Tiwari, H., Joshi, M., & Kavishwar, S. An Analysis of the Effectiveness of Index ETFS and Index Derivatives in Covered Call Strategy. *Journal of Informatics Education and Research.* 4(3), 42-48.

[24]. Kavishwar, S., & Uppal, S. K. (2020). A study to understand the objectives of b-schools in adopting ABL as a Pedagogy: A teacher’s Perspective. *Sambodhi.* 43(04), 180-185.

[25]. Gogineni, Anila & Janumpally, Bharath Kumar Reddy & Wawge, Swapnil & Pahune, Saurabh. (2025). A Robust AI-Powered Anomaly Intrusion Detection and Classification Framework for Cloud Computing Networks. 1-6. 10.1109/INDISCON66021.2025.11253743.

[26]. A. Joon, B. K. R. Janumpally, A. Gogineni and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-8, doi: 10.1109/CONIT65521.2025.11167760.

[27]. S. S. R. Tummuri, "Machine Learning-Driven Data Quality Monitoring for Fault-Tolerant Data Pipelines," 2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Singapore, Singapore, 2025, pp. 154-159, doi: 10.1109/ICCMSO67468.2025.00036.

[28]. S. S. R. Tummuri, "Generative AI for Data-Centric Healthcare with Integrated Anomaly Detection and Monitoring," 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET), Vasai, India, 2026, pp. 520-526, doi: 10.1109/IC3ET64989.2026.11467187.

[29]. "Ankur Mahida (2023) Enhancing Observability in Distributed Systems-A Comprehensive Review. Journal of Mathematical & Computer Applications. SRC/JMCA-166. DOI: doi.org/10.47363/JMCA/2023(2)135"

[30]. Mahida, A. 2024. Integrating Observability With Devops Practices in Financial Services Technologies: A Study on Enhancing Software Development and Operational Resilience. International Journal of Advanced Computer Science & Applications, 15.
[31]. Jonnalagadda, P.K. (2026). Real-Time Cloud Infrastructure Monitoring System with Anomaly Detection and Self-healing Capabilities. In: Kumar, V.N., Senkerik, R., Prasad, V.K., Kumar, T.K. (eds) Intelligent Computing and Communication. ICICC 2025. Lecture Notes in Networks and Systems, vol 1839. Springer, Cham. https://doi.org/10.1007/978-3-032-18349-1_43
[32]. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.
[33]. Veginati, Navya. "Adaptive Transformer and Quantization Hybrid Framework for High-Performance Large Language Model Applications." United International Journal of Engineering and Sciences, vol. 5, no. 4, Dec. 2025, pp. 46–56
[34]. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.
[35]. Racha, Ganesh. "Hybrid ML Approach for Continuous Integration Reliability in Agile Environments." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 3, 2025, pp. 9–21.
[36]. Racha, Ganesh. "Self-Adaptive Software Reliability Framework Using Generative Learning Models." International Journal for Modern Trends in Science and Technology, vol. 12, no. 1, 2026, pp. 30–37.
[37]. Eswarawaka, R., Subash Chandra, C., Srinivas, V., Viswas, K. (2020). Adaptive Way of Particle Swarm Algorithm Employing the Fuzzy Logic. In: Das, K., Bansal, J., Deep, K., Nagar, A., Pathipooranam, P., Naidu, R. (eds) Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing, vol 1057. Springer, Singapore. https://doi.org/10.1007/978-981-15-0184-5_56
[38]. Kanumuri, V., Srinisha, T., Bhaskar Reddy, P.V. (2019). Color-Texture Image Segmentation in View of Graph Utilizing Student Dispersion . In: Kumar, A., Mozar, S. (eds) ICCCE 2018. ICCCE 2018. Lecture Notes in Electrical Engineering, vol 500. Springer, Singapore. https://doi.org/10.1007/978-981-13-0212-1_70
[39]. Jingar, N. K. (2022). Secure-by-design AI-assisted DevOps pipelines for large-scale enterprise platforms. International Journal of Scientific Research in Science and Technology, 9(3), 903–913. https://doi.org/10.32628/IJSRST2291348
[40]. Jingar, N. K. (2022). Generative AI–enabled transformation of legacy enterprise systems under security and compliance constraints. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 760–770. https://doi.org/10.32628/CSEIT23906219