JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCK CHAIN BASED PATIENT INFORMATION RECORD SYSTEM

Dr.M.Vasumathi Devi[*],Dr.P.Radhika[2*],Balabathini Sai Prasanna[3],Boreddy Sravani[4],Burugupalli Sri Sravya[5], Chinthalacheruvu Shaheena Begam[6]

[1]Associate Professor:Vignan's Nirula Institute of Technology and Science for Women
[2] Professor: Vignan's Nirula Institute of Technology and Science for Women
[3,4,5,6] B.Tech Scholar: Vignan's Nirula Institute of Technology and Science for Women

mvasumathdeviravinuthala@gmail.com,rspaturi@yahoo.com,saiprasannabalabathini@gmail.com, boreddysravani3@gmail.com,22n1a0571sravya@gmail.com,22nn1a0573@gmail.com

Abstract

Every patient's information about medicine prescription and their history of illness in a medical record can be misguided or hacked, causing doctors a problem for proper treatment. Misplacement of medical records may lead to the wrong medication/surgery. Health care systems are less secure to storing secure medical record. Since block chain is a distributed, decentralized ledger, it has an important role in the safety measures of data and transactions. Block chain has been merging into the area of health care systems; it protects the medical record from hackers. These papers provide safety for medical records and allow patients to know about ongoing treatment and transaction procedures of it. Here only patients and doctors can act as information of record. Here, the patient data can not be accessed by any third party or others.

Keywords: Blockchain technology, Medical records, Data security, Healthcare systems, Patient privacy, Decentralized ledger, Health information management, Cybersecurity, Interoperability, Smart contracts, Patient control, Audit trails, Tamper-proof data, Secure sharing, Healthcare transactions.

1.Introduction

Block Chain Technology is a very interesting research area, and now it is going at its boom to revolutionize the way that we had regarding the data of health care; while storing it and finally during its utilization.[1-5] The hand-written mechanism previously, i.e. paper-based system was used for storing the patient's health record.[6-10] This was not an efficient system because it had some problems with it, one of which was that this system took a lot of time since each type was supposed to be stored manually.[11-19] Other issues include: if any patient visited multiple hospitals, then multiple records would have to be maintained for the same patient, which results in data redundancy; this system is not tamper-proof, which means that it is not a secured system; and if any record gets misplaced, then its recovery is a difficult task. [20-25]The motive of this literature is to put forward comprehensive survey of these solutions.

The blockchain-based patient-information record system provides a decentralized and secure approach to storing and managing health-care data[26-30]. In contrast to traditional centralized systems, blockchain provides transparency, immutability, and resiliency to security using cryptographic techniques. Following is how it works:

Once, in 2012, a Howard University Hospital medical technician sold patients' names, addresses, and Medicare numbers on the black market to earn money[31-35]. Another threat to the healthcare sector is phishing attacks, whereby hackers masquerade as authority in order to obtain sensitive information from targeted users. Since some of the data which may be compromised include the details of patients or employees, such as social security numbers, addresses, earnings, and other personal data, these forms of

attacks are very powerful. [36-40]substantial information about employees by providing a fake email from the CEO. In a blockchain-based patient information record system, each patient shall have a cryptographic key that allows one to log in and, thus, take control of health details. This enables patients to be in control of their health information and to share it with doctors easily and safely at any point in time.[41-45] Further, blockchain encryption and its consensus mechanisms address the privacy and confidentiality concerns of patients in relation to strict healthcare data regulations of many countries, like the United States' HIPAA.

Further, blockchain enables interoperability by establishing a standardized framework for the flow of data between the different healthcare systems.[46-47] In essence, this form of interoperability results in an easier way of sharing patient information across various healthcare providers, hence reducing duplication of tests, enhancing care coordination, and ultimately improving patient outcomes.

2. Literature survey

Predicted maximal heart rate. During the whole course of research, the amount of data that has always been produced by the medical institution and the rest of the institutions, like pharmaceutical companies, etc., was from the subject medical health record. It always contributed towards improving medical research. For this reason, the types of applicants for access should be limited to hospitals and pharmaceutical companies. This permit, however, is issued only with participation of medical institutions and pharmaceutical companies, which, thanks to access control based on blockchain, are able to register an application for access[1].

Scheme of Proxy Re-encryption. A sharing and protection scheme based on blockchain. In this solution, the PMHR data are encrypted and stored with a cloud server by itself, which embeds an access control scheme implemented as a smart contract on a blockchain. It serves as a betterment to the proxy re-encryption scheme meant to secure the data of PMHR while getting rid of computational complexity. All third-party visits had to be verified by the patient themselves, laying extra stress on the patient and dampening the operation efficiency of the medical institutions[2].

Blockchain-based sharing and protection scheme. The users who can apply for access are the hospital and pharmaceutical companies, to ensure the access is efficient and reduce patient workload. An improved proxy re-encryption scheme is introduced to resist the potential MITM attack. The entire system is implemented, and the functioning is verified with 10 nodes using Solidity. The obtained experimental results show that the proposed system works better than the previous one. It analyzes the security of the system under a MITM attack. This access control solution based on blockchain only allows access applications towards medical institutions and pharmaceutical companies. The solution completes data transmission through AES and RSA hybrid encryption[3].

Systematic Literature Review. In this respect, the proposed allocation recommends investigating the existing Blockchain-based approaches with regard to applied improvement of privacy and security for electronic health systems. Further details comprise the main ideas, Blockchain evaluation metrics, types and used tools of each selected paper. Non-use of conference papers. In conference papers, it is also possible to have interesting and highly innovative materials. In this paper, seven of the research questions were stated and outlined[4].

An Architecture for Electronic Health Records Distributed Systems. Existing EHR systems operate with a centralized architecture: utilize traditional and modern methods. These methods are susceptible to weaknesses with respect to security and privacy. This paper gave a systematic review of the existing Blockchain-based approaches that tried to preserve privacy and security in healthcare. The use of only international journals has been done for the paper, with the exclusion of national and domestic journals; non-English papers and book chapters were not used[5].

Decentralized Technology. EHR system privacy and security are ensured by encryption in blockchain technology. Further, being such a decentralized technology, it avoids central failure and central attack points. Open challenges, some issues, and future research directions are discussed. In the search, six valid scientific databases were used with other valid scientific databases to view[6].

Here, the three consensus methods, i.e., PoW, PoS, and PoA have been implemented and used in comparing their performance. The present paper benefits the schema that ensures the storage, access, and interchanging of health data without causing security issues or threats. The scheme is evaluated by analyzing the operating performance by PoW, PoS, and PoA consensus mechanisms[7].

Proof of Authority (PoA), Proof of Work (PoW) Mechanisms. The analytical performance of the proposed scheme is shown to provide about 21% and 9% better results compared to PoA and PoS for non-sensitive data based on block size. Also, this scheme performs better than PoA by approximately 23% as well as PoS by about 32%, for sensitive data, with memory use. All the examinations are being done on the real patient EMRs. The performance results of the proposed scheme suggest that PoW provides the best in block size[8].

Electronic Health Record Frameworks. This paper explores the opportunity to tokenize medical records in efforts to maintain data privacy, data accessibility, and data interoperability for the health care– specific context. A pan level information architecture accessing Smart Contracts, sponsored by EHRs, as info mediators. Although some blockchains assure user anonymity absolutely, some sensitive details need not obviously be shared[9].

Patient driven information sharing technique. Data privacy ensures that data is made available when it is needed and not used, imparted, accessed, altered, or deleted while it is stored, retrieved, or transmitted. It relates to the nature of blockchain technology—decentralized—as well, so this makes EHR more accessible across a larger network. Since it is an application deployed on Distributed Networks, anywhere accessibility becomes possible. However, there are still a few issues that can be resolved in the future[10].

Large scale information infrastructured mechanism. Data privacy refers to affording protection to ensure data is available when needed and not used, imparted, accessed, altered, or deleted while being stored, retrieved, or transmitted. Data accessibility is the ability to access the data regardless of natural or artificial accidents, hardware, or others. It will help the healthcare industry make immutable, authentic and accessible medical records, privacy and faster payments. This electronic record, by the fact that it is on the blockchain, is easily accessed by way of blockchain, as it is accorded to any personnel with authority to access the same[11].

Broader network. Better patient access to health records across the healthcare industry without compromising privacy is seen as an important feature that needs to be provided by any individual or organization. Its advantages range from enabling access to the registry across institutes or hospitals, to issues related to misuse of data once shared, a lack of security, etc. Health records sharing across institutes or hospitals had a big issue regarding misuse of data, so its access should be provided by trusted implementations only, i.e., by a secure process[12].

Flexi Medi private management system. Flexi Medi is a private, blockchain-based, patient details management system meant to resolve the above problems. The proposed solution is a distributed secure ledger for effective access and retrieval of systems. Flexi Medi enables the use of high principles of data

security, hybrid access control mechanisms, public key cryptography, secure live health condition monitoring mechanisms, and a combination of these. It is worth mentioning that all these mechanisms are attained while considering and conforming to the requirements regarding regularity such as HIPAA and GDPR, so the industry can implement with no worries[13].

Server-Based patient Detail management System, Health condition monitoring system. They are, however, experiencing numerous challenges that range from issues of inter operability, through security and privacy concerns, to cyber-attacks on the centralized storage and maintaining adherence to medical policies. The proposed solution results in the successful deployment of smart contracts as per the roles of the system, real-time maintaining the health of the patient with a more scalable and access-controlled system. With regard to requirement gathering to the results of the research, the later can be changed according to future user requirements. Researchers will be addressing the needed requirements, and will be doing version management accordingly[14].

Hybrid access control mechanism, public key cryptography. It introduces a distributed secure ledger to enable system access and retrieval in a more efficient manner—secure and immutable. The enhanced consensus mechanism, which can realize the data consensus without the drawbacks of massive consumption of high-power and network congestion. In general, the solution aims to achieve the common platform for the whole medical industry through a decentralized approach to store, and share medical details doing away with the maintenance of printed medical details. Fine-tune some of the changes that need to be made in order to make the solution in a state to be of production scale. Key goals and objectives have been met. The following further development can be done to the proposed solution[15].

3.Proposed methodology

In this section, each of the proposed frameworks is formally described, detailing the software platform that will be used for its development and listing the benefits it can provide. The next section details full descriptions of the main components that will drive the implementation of this framework: the first one being Ethereum, and the second, the Interplanetary File System (IPFS).

Designing a blockchain-based patient information record system will ensure that this critical information is managed and stored via a secure, decentralized ledger. A simple algorithm of the blockchain system contains steps such as:

1. Patient registration:

When the new patient gets into the system, he is assigned an identifier.

Information such as the patient's name, date of birth, medical history, is recorded in a block.

2. Block Creation:

Each block maintains a list of transactions, for example, visits by patients, treatments, test results, and so on.

The blocks are self-referential in the form of a chain; every block refers to the previous one through what is called a hash pointer.

3. Mechanism for Consensus:

In such a way, develop a consensus algorithm like Proof of Work or Proof of Stake to validate and add new blocks into the chain.

This ensures that every node in the network agrees on the validity of the data.

4. Security of Data:

Patients must have their data encrypted to protect the privacy of and ensure security over their information.

Fine-grained access controls and permission models of who can view or update the information need to be designed.

5. Decentralization:

Distribute several copies of the blockchain to nodes within the network to avoid a single point of failure. Nodes may have consensus mechanisms that guarantee integrity.

6. Immutability:

Data, once added into blocks and validated, cannot be deleted or changed, hence ensuring integrity of the patient records.

7. Auditability and Transparency:

All the transactions happening in the blockchain are transparent and traceable; hence it provides an easy way of auditing patient records.

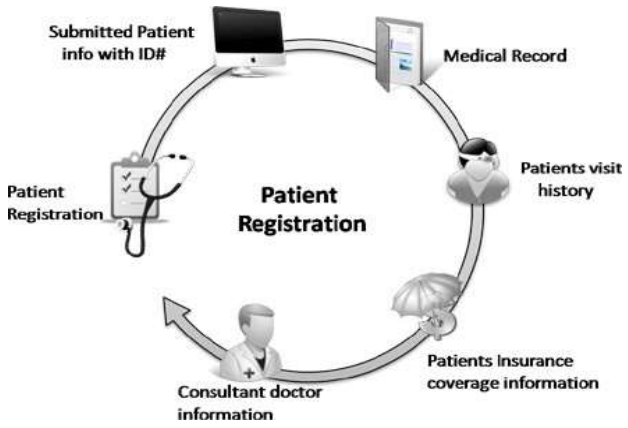


Fig 1:Patient Registration

8. Smart Contracts (Optional):

Run predefined conditions from smart contracts, for instance, insurance claims or appointment scheduling.

Following these steps and having implemented blockchain technology, you will have a secure, efficient patient information record system that assures integrity, security, and transparency of data stored.

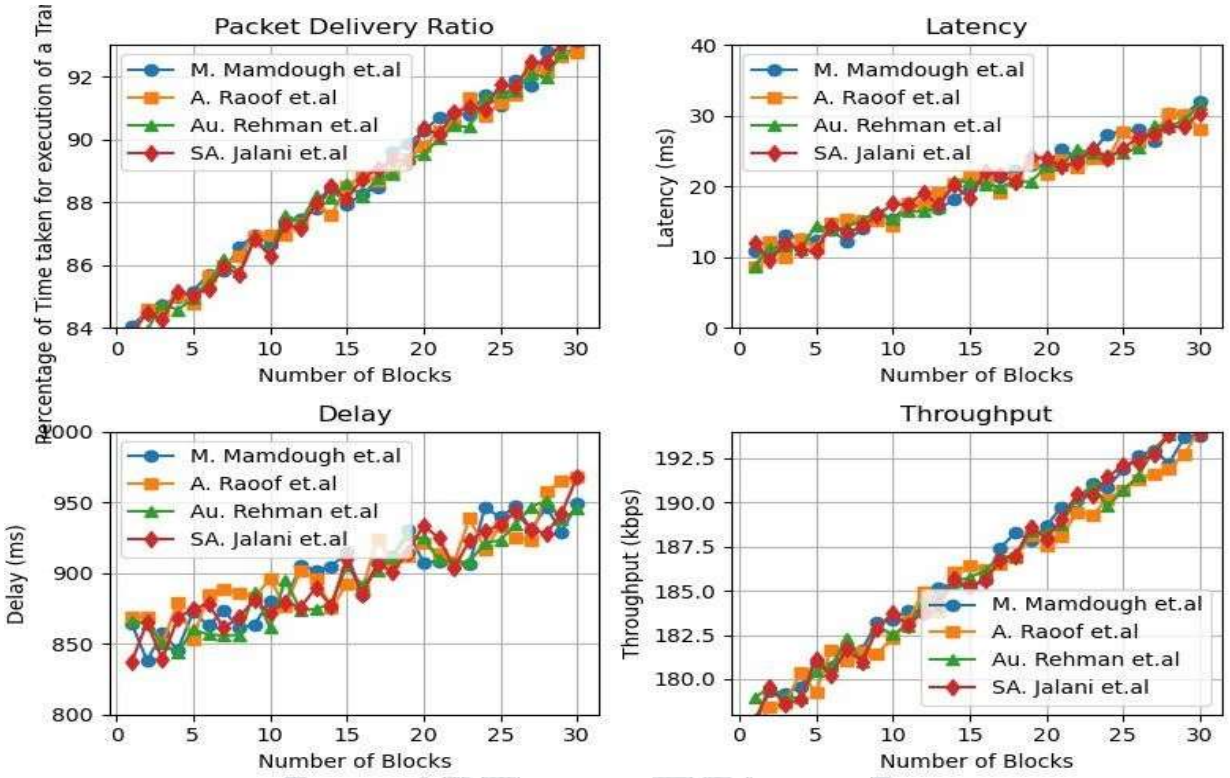
Implementation

This is what identifies the patient's data. The step ensures that all information belonging to a patient is traceable and unique, an aspect that becomes relevant when managing records as events occur in a health environment. The blockchain refers to a series of blocks holding a record of multiple transactions. This ensures chronological ordering of the records because each block is linked to the previous through hash pointers. A permanent, tamper-evident history of transactions is thus formed. The consensus mechanism is key to the integrity of blockchain. It involves making sure that all participants on the network agree on the state of the blockchain so as to eliminate fraud and ensure that only relevant data is added. Security related to data is a critical issue in healthcare since the information contains patients' history, which is sensitive. Encryption protects the data from access by unauthorized parties; access controls prevent interaction with patients' records by unauthorized entities. Decentralization removes a single point of failure and distributes data across a network of nodes. This enhances resilience and reliability in that even if one node goes down or is compromised, it does not affect the whole system. The immutability ensures that information, once recorded on the blockchain, is immutable. This feature is important in ensuring that accurate and reliable patient records are maintained over time. Some of the large advantages associated with blockchain technology are transparency and auditability, which allow healthcare providers and different auditors to trace and verify transactions in an attempt to ensure accuracy and integrity of patient records. Smart contracts are an additional layer of blockchain technology in that they automate some of the complicated processes and agreements. While they are not required, they can really simplify operations, reduce the administrative load, and enforce contractual terms with ease.

4.Results and discussion

It begins with a structured patient profile, well documented, all of them. All transactions related to patients are maintained in chronological order and, in an immutable way, using the same system of validation that every data added to the blockchain are validated in it and agreed upon previously by multiple network users. The system ensures that no failure or attack can be successful against it and maintains the integrity with multiple nodes having the same data for redundancy. The system ensures that with the passage of time, the records of the patients remain as original and authentic as when these were first made.

Graph-1: This following graph represents the relation between the throughput and number of nodes.



The system maintains a clear and understandable record concerning all transactions—all of which inadvertently led to increased trust and accountability due to the system. The system can provide automation and streamlining of a number of processes and can make things efficient so that the administrative overhead is decreased.

5.Conclusion

Implementing a blockchain-based patient information record system offers a transformative approach to managing healthcare data. This system utilizes blockchain technology to address key challenges in the healthcare sector, including data security, integrity, and transparency. Below is a detailed conclusion summarizing the effectiveness, benefits, potential challenges, and future directions for such a system. Design according to this algorithm, and develop a blockchain-based patient information record system that provides a secure, transparent, and efficient platform for the management of patient records. This arrangement rides on the strengths of blockchain technology to meet some critical requirements in healthcare data management, hence offering a solution that ensures improved security and integrity while supporting efficient operations and regulatory compliance.

6.References

1. Yuan, W. X., Yan, B., Li, W. (2023). Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control.

2. Amir Masoud Rahmani, A.M., 2023. Blockchain-based privacy and security preserving in electronic health: a systematic review.

3. Bodur, H., I. F. T. (2024). An Improved blockchain-based secure medical record sharing scheme.

4. Patibandla, R. S. M. L., & Narayana, V. L. (2021). Computational intelligence approach for prediction of COVID-19 using particle swarm optimization. In *Advances in Computational Intelligence and Data Analytics* (Vol. 923, pp. 175–189). Springer. https://doi.org/10.1007/978-981-15-8534-0_9

5. Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., & Khadherbhi, R. (2021). Traffic analysis using IoT for improving secured communication. In *Advances in Intelligent Systems and Computing* (Vol. 213, pp. 499–507). Springer. https://doi.org/10.1007/978-981-33-4443-3_48

6. Narayana, V. L., & Bharathi, C. R. (2019). Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs. In *Advances in Intelligent Systems and Computing* (Vol. 104, pp. 649–658). Springer. https://doi.org/10.1007/978-981-13-1921-1_63
7. Narayana, V. L., & Bharathi, C. R. (2018). Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS. *Mathematical Modeling of Computer Systems*, 91(2), 73–76. https://doi.org/10.18280/mmc_a.910207
8. Lakshman Narayana, V., Lakshmi Patibandla, R. S. M., Pavani, V., & Radhika, P. (2023). Optimized nature-inspired computing algorithms for lung disorder detection. In *Advances in Intelligent Systems and Computing* (Vol. 1066, pp. 103–118). Springer. https://doi.org/10.1007/978-981-19-6379-7_6
9. Narayana, V. L., Sudheer, B. N., Maddumala, V. R., & Anusha, P. (2020). Fuzzy base artificial neural network model for text extraction from images. *Journal of Critical Reviews*, 7(6), 350–354. https://doi.org/10.31838/jcr.07.06.61
10. Narayana, V. L., Bhargavi, S., Srilakshmi, D., Annapurna, V. S., & Akhila, D. M. (2024). Enhancing remote sensing object detection with a hybrid Densenet-LSTM model. In *Proceedings of the International Conference on Computer Science and Advanced Technology* (pp. 264–269). IEEE. https://doi.org/10.1109/IC2PCT60090.2024.10486394
11. Narayana, V. L., Syamalatha, P., Vatsalya, P., Sricharitha, V., & Akhila, V. (2023). Multi-level node authorization using recurrent neural networks for secure health monitoring system. Proceedings of the IEEE International Conference on Smart Computing and Networking Applications (ICSNA), 1697–1705. https://doi.org/10.1109/ICSCNA58489.2023.10370543
12. Gopi, A. P., Swathi, V., Harshitha, G. S., Swetha, B., & Alekhya, N. (2023). Prediction of paddy yield based on IoT data using GRU model in lowland coastal regions. In Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023) (pp. 1747-1752). https://doi.org/10.1109/ICSSIT55814.2023.10060935
13. Arepalli, P. G., Naik, K. J., & Amgoth, J. (2024). An IoT-based water quality classification framework for aqua-ponds through water and environmental variables using CGTFN model. International Journal of Environmental Research, 18(4), Article 73. https://doi.org/10.1007/s41742-024-00625-2
14. Gopi, A. P., Babu, E. S., Raju, C. N., & Kumar, S. A. (2015). Designing an adversarial model against reactive and proactive routing protocols in MANETs: A comparative performance study. International Journal of Electrical and Computer Engineering, 5(5), 1111-1118. DOI: 10.11591/ijece.v5i5.pp1111-1118
15. Sravanthi, G. L., Devi, M. V., Sandeep, K. S., Naresh, A., & Gopi, A. P. (2020). An efficient classifier using machine learning technique for individual action identification. International Journal of Advanced Computer Science and Applications, 11(6), 513-520. DOI: 10.14569/IJACSA.2020.0110664
16. Gopi, A. P., Durga Mani, P., Chandana, V. B., Sulthana, S. R., & Parameswari, P. P. K. (2024). Classification of fake news using enhanced capsule neural network. In 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation, IATMSI 2024. DOI: 10.1109/IATMSI60426.2024.10502837
17. Arepalli, P. G., & Khetavath, J. N. (2023). An IoT framework for quality analysis of aquatic water data using time-series convolutional neural network. Environmental Science and Pollution Research, 30(60), 125275-125294. https://doi.org/10.1007/s11356-023-27922-1
18. Gopi, A. P., & Jairam Naik, K. (2021). A model for analysis of IoT based aquarium water quality data using CNN model. In 2021 International Conference on Decision Aid Sciences and Application, DASA 2021 (pp. 976-980). https://doi.org/10.1109/DASA53625.2021.9682251
19. Roshini, P., Khajavali, S., Snigdha, M. L. S., Harsha, B. D., Srilakshmi, B., & Gopi, A. (2024). CNN design with AlexNet algorithm for diagnosis of diseases in cassava leaves. In Proceedings - 2024 International Conference on Expert Clouds and Applications, ICOECA 2024 (pp. 711-718). https://doi.org/10.1109/ICOECA62351.2024.00129
20. Narayana, V. L., Gopi, A. P., Khadherbhi, S. R., & Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodology. Journal of Critical Reviews, 7(6), 381-384. https://doi.org/10.31838/jcr.07.06.67
21. Rao, B. T., Patibandla, R. S. M. L., Narayana, V. L., & Gopi, A. P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems (pp. 249-267). https://doi.org/10.1002/9781119764175.ch11
22. Patibandla, R. S. M. L., Gopi, A. P., Narayana, V. L., & Rao, B. T. (2023). Decentralized smart healthcare systems using blockchain and AI. In Blockchain applications in healthcare: Innovations and practices (Vol. 1, pp. 139-154). DOI: 10.1002/9781394229512.ch8
23. Lakshman Narayana, V., & Gopi, A. P. (2020). Enterotoxigenic Escherichia coli detection using the design of a biosensor. Journal of New Materials for Electrochemical Systems, 23(3), 164-166. DOI: 10.14447/jnmes.v23i3.a02
24. Narayana, V. L., & Gopi, A. P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34, 197-208. DOI: 10.3166/ts.34.197-208
25. Arepalli, P. G., Narayana, V. L., Venkatesh, R., & Kumar, N. A. (2019). Certified node frequency in social network using parallel diffusion methods. Ingenierie des Systemes d'Information, 24(1), 113-117. https://doi.org/10.18280/isi.240117

26. Peda Gopi, A., & Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4), 175-181. https://doi.org/10.3166/TS.34.175-181
27. Narayana, V. L., Gopi, A. P., Anveshini, D., & Lakshmi, G. V. V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4), 391-397. https://doi.org/10.1504/IJWMC.2020.108539
28. Challa, R., YAMPARALA, R., KANUMALLI, S. S., & KUMAR, K. S. (2020, November). Advanced patient's medication monitoring system with ardunio UNO and NODEMCU. In *2020 4th International conference on electronics, communication and aerospace technology (ICECA)* (pp. 942-945). IEEE.
29. Kanumalli, S. S., Chinta, A., & Chandra Murty, P. S. R. (2019). Isolation of Wormhole Attackers in IOV Using WPWP Packet. *Revue d'Intelligence Artificielle*, *33*(1)
30. Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2018). Advances in Modelling and Analysis B. *Journal homepage: http://iieta. org/Journals/AMA/AMA_B*, *61*(1), 5-8.
31. Kosaraju, Chaitanya, et al. "A model for analysis of diseases based on nutrition deficiency using random forest." 2022 7th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2022.
32. Chaitanya, Kosaraju, and Gnanasekaran Dhanabalan. "Secure Route Detection with Multi Level Trust Evaluation Model Using Replicated Auditor Node for Extended Packet Delivery Rate in WSN." Revue d'Intelligence Artificielle 37.4 (2023).
33. Chaitanya, Kosaraju, et al. "Risk Stratification for Stroke Using Attention Transformer Model." 2024 2nd International Conference on Disruptive Technologies (ICDT). IEEE, 2024.

34. Sujatha, V., Prasanna, K.L., Niharika, K., Charishma, V., Sai, K.B.,K(23),"Network Intrusion Detection using Deep Reinforcement Learning,*Proceedings - 7th International Conference on Computing Methodologies and Communication", ICCMC 2023*, 2023, pp. 1146–1150
35. Sujatha, V., Anitha, B.S., Rama, G.T., Niharika, N., Sahithi, A.,K(23),"Convolutional Neural Network (CNN) based Blood Vessel Segmentation from Ocular Images*Proceedings - 7th International Conference on Computing Methodologies and Communication",ICCMC 2023*, 2023, pp. 518–523

36. Majety, V. D., & Murali, G. (2018). Remote health watchdog framework for seizure patient using electronic sensors. *International Journal of Engineering and Technology(UAE, 7*, 783–785. https://doi.org/10.14419/ijet.v7i3.12132
37. Alapati, N., Anusha, N., Joharika, P., Jerusha, N.J., Tanuja, P.(2023)Prediction of Parkinson's Disease using Machine Learning in 2023 2 nd *International Conference on Electronics and Renewable Systems(ICEARS)(pp.1357–1361).IEEE*
38. *Naresh, A., Reddy, B.A., Reddy, G.P., Kumari, K.R., Vaishnavi, M.S.(2023)Melanocytic Pigmented Skin Lesion Detection and Classification using Hybrid Deep Features based on Fully Convolutional Network* in 2023 2 nd *International Conference on Electronics and Renewable Systems(ICEARS)(pp.1011–1018).IEEE*
39. Pavani, Vellalacheruvu, and I. Ramesh Babu. "Three level cloud storage scheme for providing privacy preserving using edge computing." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1929-1940.
40. Vellalachervu, Pavani and Babu, I. Ramesh, A Novel Method to Optimize the Computation Overhead in Cloud Computing by Using Linear Programming (May 10, 2019). INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS(IJRAR), May 2019, Volume 6, Issue 2, Available at SSRN: https://ssrn.com/abstract=3452191

41. Rama Krishna, Komanduri Venkata Sesha Sai, and Battula Bhanu Prakash. "Intrusion Detection System Employing Multi-level Feed Forward Neural Network along with Firefly Optimization (FMLF2N2)." *Ingénierie des Systèmes d'Information* 24.2 (2019).

42. Krishna, K. VSS Rama, et al. "Identification of Fraud Transactions using Lightgbm Technique." *2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. IEEE, 2022.

43. S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 1260-1268, doi: 10.1109/ICEARS53579.2022.9752280.
44. Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1916-1928.

45. Qi, Zhang, P. SilpaChaitanya, and T. Sudhir. "Spoofing attack detection wireless networks using advanced KNN." *International Journal of Smart Device and Appliance* 4.1 (2016): 1-8.

46. S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 1260-1268, doi:10.1109/ICEARS53579.2022.9752280.
47. Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1916-1928.