A SECURE MEDICAL DATA SHARING FRAMEWORK FOR FIGHT AGAINST PANDEMICS LIKE COVID-19 BY USING PUBLIC BLOCKCHAIN

K. VIJAY KUMAR[1], PALLE VARUN[2], TIKKISETTI LALITH ADITYA[3], TEEGALA SREEJA[4], UGGE ANUSHA[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The global impact of the COVID-19 pandemic was huge, and it showed that reporting and collecting accurate healthcare data are crucial operations for governments. Not only the test results but also the vaccination information of people should be shared correctly by trusted systems between countries. Now it is possible with the integration of new practices like blockchain and cryptology with the help of secure, transparent, and privacy-centric methods. There are a lot of recent studies focusing on blockchain usage in healthcare in literature. However, they still have flaws in granting full authorization to individuals, ensuring the security of personal information, speed, and scalability. They mostly use private or consortium blockchains. However, in a public blockchain, a system that everyone can participate in and follow provides more reliable information. At the same time, heavy and slow encryption techniques were used in the models proposed in the literature. Our study focuses on the usage of blockchain in combating pandemics by ensuring privacy and maintaining reliable medical data sharing during pandemics. The proposed system is implemented by leveraging public blockchain on Ethereum with smart contracts, IPFS for decentralized storage, and robust and fast encryption techniques like ChaCha20. In addition to existing techniques, the framework introduces innovative methods, such as storing encrypted keys alongside encrypted data in IPFS, which enhances security and scalability. We also eliminate the usage of doctors' private keys. The framework grants patient's full ownership of their medical data. Patients can grant or revoke access to their

data, enhancing their control over personal information. The use of smart contracts to manage access rights ensures that only authorized parties can access the data, and patients can easily manage these permissions through a decentralized platform. We aim to implement a framework which is fast, easy to use and differs in terms of storing and sharing medical data with different encryption methods and protocols by using a public blockchain. We ensure novel management of COVID-19 medical records that are personal data.

Index Terms – Blockchain, Ethereum, smart contracts, Inter Planetary File System (IPFS), ChaCha20 encryption, COVID-19, electronic health records (EHR), medical data sharing, healthcare blockchain, privacy preservation, decentralized storage, access control, patient-centric healthcare.

I. INTRODUCTION

The COVID-19 pandemic has underscored the importance of secure and efficient sharing of medical data. Historically, hospitals have maintained ownership of medical records for many years. The process of requesting a hospital to transfer these records can be time-consuming, often taking days, and in some cases, proves to be challenging, especially when attempting to transfer records across different countries. Emerging technologies such as blockchain present a transformative opportunity to address this trust deficit, enabling secure and precise sharing of medical information while ensuring robust anonymization for the protection of private data. Blockchain's capabilities in spreading accurate information, ensuring traceability for records, monitoring COVID-19 test results can help to combat pandemics. Blockchain technology offers a decentralized and secure alternative. Block chain's inherent features of decentralization immutability, and transparency can address challenges in healthcare data management, ensuring patient privacy and data integrity. In literature, block chain solutions for healthcare have been proposed more and more in recent years. However, proposed methods use heavy cryptographic algorithms, cloud servers and doctors' signature in procedures which cause the system to slow down. While scalable, cloud solutions can become expensive with increasing data storage needs. They are still subject to the limitations of centralization. Adding more security layer or complexity decreases system performance much. Also, in some publications, the confidentiality of the data is not fully ensured. In addition to this, most

publications use private or consortium blockchains to gain speed and scalability that makes registering the system centralized and difficult to track blockchain activities. Private chains have centralized control and governance, and they are exclusively utilized within a single organization. They are not proper for global usage. On the other hand, using public blockchain provides more trust and ease of usage. Pandemic data like COVID-19 is simpler than other types of medical data since it is small and easy to store as json file. We can use public blockchains for medical data sharing of pandemic data with acceptable latency. This study explores the development of a secure and decentralized framework using public blockchain with strong encryption methods tailored for COVID-19 medical data sharing. There are many enhancements in this study for security and decentralization that are handled by block chain, peer-to-peer storage IPFS and strong cryptography.

In this study, proposing a stronger and faster alternative medical data sharing framework to fight against pandemics such as COVID-19 is aimed. For this purpose, we used Ethereum as a public block chain. We created user interfaces with React for users. Our react client connects with smart contract via Web3 API. The technologies used shows overall framework design. The proof-ofconcept implementation and test data are given in a GitHub public project as well as installation guide. The proposed framework contributes to the literature in terms of technology and method. Our main contributions are using strong and fast cryptology algorithms and designing a system in which data ownership is totally given to the personal data owner. A comprehensive examination of block chain technology and its application in sharing medical data is presented within the context of strategies to combat pandemics. The literature on block chain-based solutions for healthcare data management and sharing is extensive and diverse. There are many studies which use block chain and IPFS to store medical data. In an early study, in 2018, developed a framework on Ethereum with attribute-based encryption (ABE) methods. They use a secret key generator on a trusted system to use it for access control. They encrypt the file with AES encryption and store it on IPFS. Then the system encrypts the secret key and stores it on the block chain. Requestors who meet the access criteria first decrypt the encrypted secret key then download the encrypted file from the IPFS. In our study, we keep the encrypted key in IPFS next to the encrypted data, not on the block chain. This is important to keep block

size small and for security. Our design makes it more scalable and secure.

II. RELATED WORK

A. *Blockchain technology in a crisis: Advantages, challenges, and lessons learned for enhancing food supply chains during the COVID-19 pandemic*

This study explores the implementation of blockchain technology in the Chinese food supply chain during the COVID-19 pandemic and examines its advantages and challenges. This study uses an interpretive research strategy and theoretical framework to gather positive feedback on blockchain technology from the fresh vegetable food industry, online retailers, state-owned enterprises, the meat industry, the dairy industry, and retail stores. These findings highlight the potential benefits of blockchain, including enhanced efficiency, transparency, reliability, and traceability in the food supply chain. However, difficulties with labor data management, interoperability, data accuracy, financial constraints, and regulatory considerations have been identified. This study collects comprehensive data on labor management, standardized protocols, verification mechanisms, barrier-reduction efforts, and collaboration with stakeholders and regulators to address these challenges. This study aimed to create a more resilient and efficient food supply chain system by providing a roadmap for prioritizing improvements. The practical implications include risk management strategies, targeted support for farmers, and investments in sustainable agricultural practices to ensure food security. Overall, this study provides valuable insights for harnessing the potential of blockchain technology to strengthen the Chinese food supply chain amid crises.

B. *A scalable blockchain based framework for efficient IoT data management using lightweight consensus*

Recent research has focused on applying blockchain technology to solve security-related problems in Internet of Things (IoT) networks. However, the inherent scalability issues of blockchain technology become apparent in the presence of a vast number of IoT devices and the substantial data generated by these networks. Therefore, in this paper, we use a lightweight consensus algorithm to cater to these problems. We propose a scalable blockchain-based framework for managing IoT data, catering to a large number of devices. This framework utilizes the Delegated Proof of Stake (DPoS) consensus algorithm to ensure enhanced performance and efficiency in resource-

constrained IoT networks. DPoS being a lightweight consensus algorithm leverages a selected number of elected delegates to validate and confirm transactions, thus mitigating the performance and efficiency degradation in the blockchain-based IoT networks. In this paper, we implemented an Interplanetary File System (IPFS) for distributed storage, and Docker to evaluate the network's performance in terms of throughput, latency, and resource utilization. We divided our analysis into four parts: Latency, throughput, resource utilization, and file upload time and speed in distributed storage evaluation. Our empirical findings demonstrate that our framework exhibits low latency, measuring less than 0.976 milliseconds. The proposed technique outperforms Proof of Stake (PoS), representing a state-of-the-art consensus technique. We also demonstrate that the proposed approach is useful in IoT applications where low latency or resource efficiency is required.

C. A blockchain-based privacy-preserving healthcare data sharing scheme for incremental updates

With the rapid development of artificial intelligence (AI) in the healthcare industry, the sharing of personal healthcare data plays an essential role in advancing medical AI. Unfortunately, personal healthcare data sharing is plagued by challenges like ambiguous data ownership and privacy leakage. Blockchain, which stores the hash of shared data on-chain and ciphertext off-chain, is treated as a promising approach to address the above issues. However, this approach lacks a flexible and reliable mechanism for incremental updates of the same case data. To avoid the overhead of authentication, access control, and rewards caused by on-chain data changes, we propose a blockchain and trusted execution environment (TEE)-based privacy-preserving sharing scheme for healthcare data that supports incremental updates. Based on chameleon hash and TEE, the scheme achieves reliable incremental updates and verification without changing the on-chain data. In the scheme, for privacy concerns, off-chain data are protected through symmetric encryption, whereas data verification, decryption, and computation are performed within TEE. The experimental results show the feasibility and effectiveness of the proposed scheme.

D. Blockchain technology: Security issues, healthcare applications, challenges and future trends

Blockchain technology provides a data structure with inherent security properties that include cryptography, decentralization, and consensus, which ensure trust in transactions. It covers widely applicable usages, such as in intelligent manufacturing, finance, the Internet of things (IoT), medicine and health, and many different areas, especially in medical health data security and privacy protection areas. Its natural attributes, such as contracts and consensus mechanisms, have leading-edge advantages in protecting data confidentiality, integrity, and availability.

The security issues are gradually revealed with in-depth research and vigorous development. Unlike traditional paper storage methods, modern medical records are stored electronically. Blockchain technology provided a decentralized solution to the trust-less issues between distrusting parties without third-party guarantees, but the "trust-less" security through technology was easily misunderstood and hindered the security differences between public and private blockchains appropriately.

The mentioned advantages and disadvantages motivated us to provide an advancement and comprehensive study regarding the applicability of blockchain technology. This paper focuses on the healthcare security issues in blockchain and sorts out the security risks in six layers of blockchain technology by comparing and analyzing existing security measures.

It also explores and defines the different security attacks and challenges when applying blockchain technology, which promotes theoretical research and robust security protocol development in the current and future distributed work environment.

III. PROPOSED METHODOLOGY

Pandemic data like COVID-19 is simpler than other types of medical data since it is small and easy to store. We can use public blockchains for medical data sharing of pandemic data with acceptable latency. This study explores the development of a secure and decentralized framework using public blockchain with strong encryption methods tailored for COVID-19 medical data sharing. There are many enhancements in this study for security and decentralization that are handled by blockchain, peer-to-peer storage Inter Planetary File System and strong cryptography.

The proposed system is implemented by leveraging public blockchain on Ethereum with smart contracts, IPFS for decentralized storage, and robust and fast encryption

techniques like ChaCha20 or AES encryption.

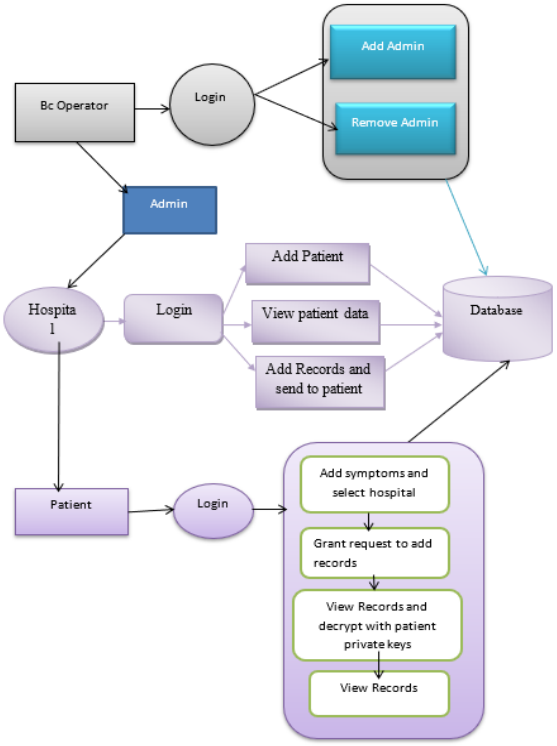
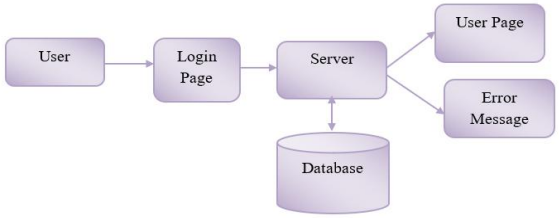


Fig. 1: System Overview

1. User Interface Design

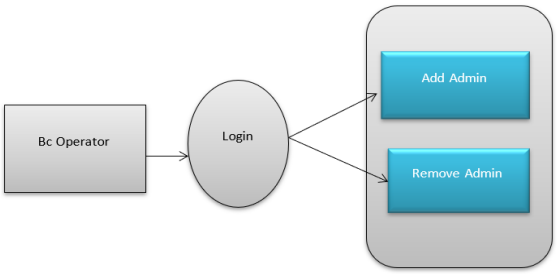
In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server.

If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



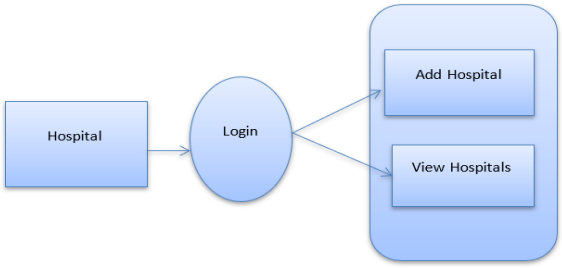
2. BC Operator

BC Operator is the second module in our project, where crucial functional requirements of the project will be carried out. Operator first login with id and password then he will add admin and remove admin.



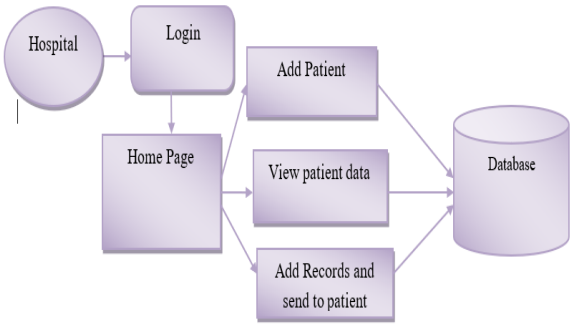
3. Admin

This is the third module in our project is Admin. Here admin will login with his password and Id who has created by the bc operator. After admin login directely will navigate into admin home page. The purpose of admin is to add or create hospital and control hospitals data.



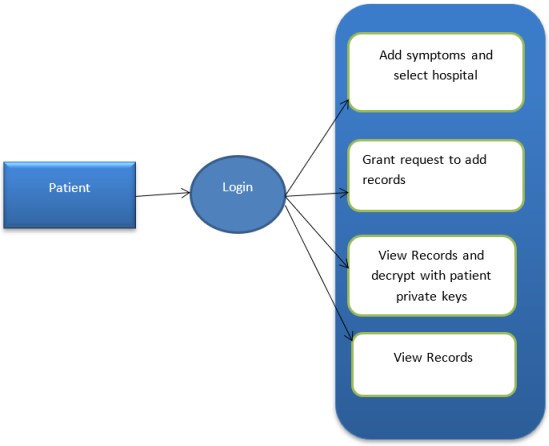
4. Hospital

This is the fourth module in our project is hospital. Here Hospital will login with hospital id and password. After login it will directly navigate home page there we can add patient and create asymmetric key view patients and add records (vaccination and precautions) after taking permission from patient. When hos management will admit the patient automatically the smart contract will be created using block chain.



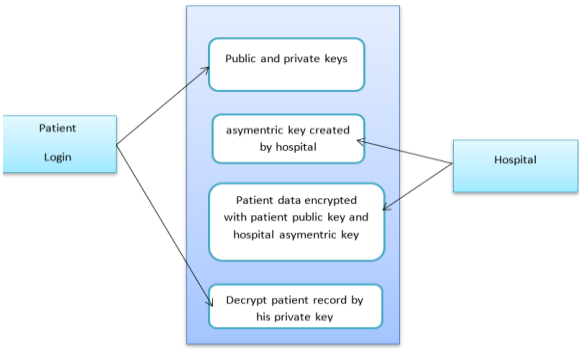
5. Patient

This is the Fifth module in our project is Patient. Here Patient will login with name and mobile number. After login it will directly navigate home page there he have to enter his symptoms and select hospital. The data will be sent to selected hospital, after hospital will add or give vaccination, for that patient have to approve request. Then patient records will be added by hos management. After adding records patient can decrypt the records and view using his private keys.



6. Security

This is the Sixth module in our project is Security. First, Patient need to register to the system. Users interact with the Ethereum network using public and private key pairs. The private key, kept secret by the user, is crucial for authorizing transactions and accessing digital assets. Public keys, derived from private keys, serve as the public address for receiving funds. The encrypted private key is stored locally on the user's device or browser. The encrypted private key can be decrypted later when needed, using the user's password to derive the encryption key.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed Ethereum-based medical data sharing framework enables secure, privacy-preserving, and decentralized management of COVID-19 medical records. The integration of ChaCha20 encryption, IPFS, and smart contracts improves data security, scalability, and sharing efficiency while giving patients full control over access permissions. The elimination of doctors' private keys further simplifies secure data management. Overall, the framework provides a fast, scalable, and reliable solution for secure healthcare data sharing during pandemics.



Fig. 2: Home Page

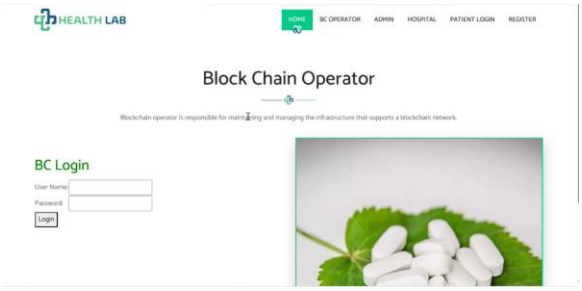


Fig. 3: Login

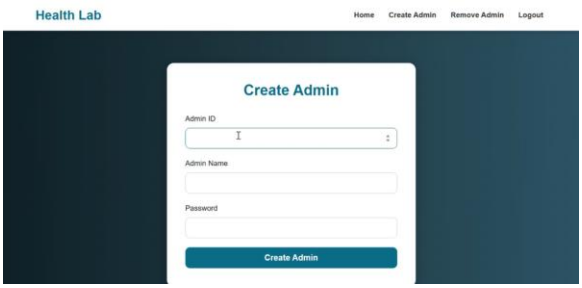


Fig. 4: Create Admin

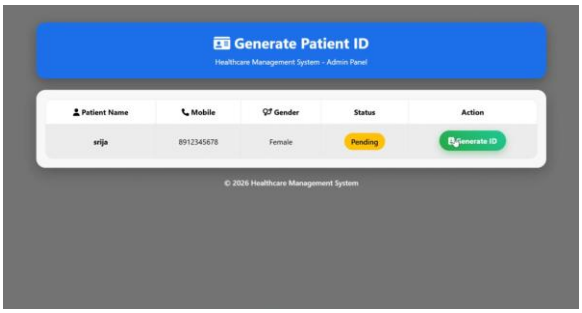


Fig. 5: Generate Patient ID



Fig. 6: Hospital Login

International Journal of Engineering Research and Science & Technology

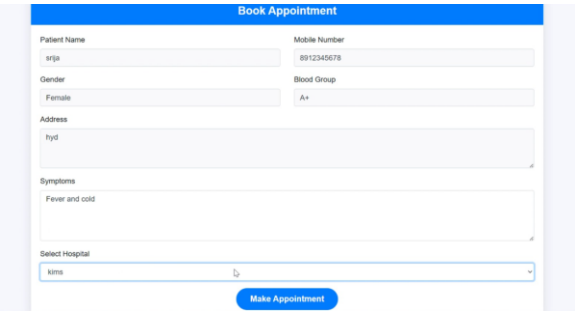


Fig. 6: Book Appointment

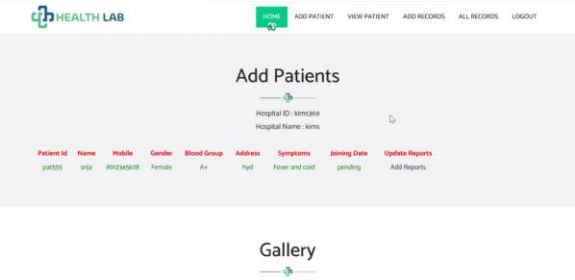


Fig. 7: Add Patient

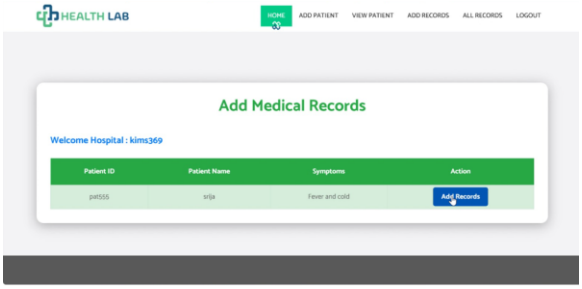


Fig. 8: Add Medical Report



Fig. 8: Patient Record

V. CONCLUSION

The global fight against a deadly pandemic is a collective effort that requires leveraging all available technologies to halt or slow its spread. COVID-19 has exposed a critical issue – the lack of fluidity in health data. Blockchain, an impactful and revolutionary technology with proven applications like Bitcoin and Ethereum as alternative financial systems, can play a pivotal role. It offers distinct advantages such as bypassing third-party verifications, ensuring secure and private data sharing, and outperforming traditional databases in terms of security and efficiency. We used recent technologies and implemented a new framework for medical data sharing, specifically Covid-19 data. We used Ethereum public blockchain for running our smart contract and IPFS for storing medical data. In the literature, they usually use private or consortium blockchains. Using a public blockchain, not only do we ensure transparency and security, but also any user can participate easily. We used an existing encryption method and proposed a new decryption method for the data. In addition to this, usage of ChaCha20 algorithm accelerated the process because it is faster than AES algorithm.

REFERENCES

[1] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Jun. 3, 2024.

[2] S. Wang, Y. Zhang, and Y. Zhang, ‘‘A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems.

[3] Y. Luo, H. Jin, and P. Li, ‘‘A blockchain future for secure clinical data sharing: A position paper,’’ in Proc. ACM Int. Workshop Secur. Softw. Defined Netw. Netw. Function Virtualization, Mar. 2019, pp. 23–27, doi: 10.1145/3309194.3309198.

[4] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, ‘‘Healthchain: A blockchain-based privacy preserving scheme for large-scale health data,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8770–8781, Oct. 2019, doi: 10.1109/JIOT.2019.2923525.

[5] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, ‘‘Blockchain-based solution for COVID-19 digital medical passports and immunity certificates.

[6] K. Christodoulou, P. Christodoulou, Z. Zinonos, E. G. Carayannis, and S. A. Chatzichristofis, ‘‘Health information exchange with blockchain amid COVID-19-like pandemics,’’ in Proc. 16th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2020, pp. 412–417, doi: 10.1109/DCOSS49796.2020.00071.

[7] B. Vardhini, S. N. Dass, R. Sahana, and R. Chinnaiyan, ‘‘A blockchain based electronic medical health records framework using smart contracts,’’ in Proc. Int. Conf. Comput. Commun. Informat. (ICCCI), Jan. 2021, pp. 1–4, doi: 10.1109/ICCCI50826.2021.9402689.

[8] A. Panwar and V. Bhatnagar, ‘‘A cognitive approach for blockchainbased cryptographic curve hash signature (BC-CCHS) technique to secure healthcare data in data lake.

[9] Q. Qin, B. Jin, and Y. Liu, ‘‘A secure storage and sharing scheme of stroke electronic medical records based on consortium blockchain,’’ BioMed Res. Int., vol. 2021, pp. 1–14, Feb. 2021.

AUTHORS Profile



Mr. K. VIJAY KUMAR Received my B.Tech(CSE) in 2017 from Sriindu college of Engineering and Technology (JNTUH).I completed my master of Technology (MTech), computer science in 2021 from Sreenidhi institute of science and Technology (JNTUH) With 3 years of, dificated experience in academia and Research. I currently serves as a Assistant professor in CSE Department at Gurunanak institutions Technical campus ibrahimpatnam, Telangana, india.



Mr. PALLE VARUN pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. TIKKISETTI LALITH ADITYA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. TEEGALA SREEJA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. UGGE ANUSHA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.