International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

SECURE AND DECENTRALIZED HEALTH DATA MANAGEMENT USING IOMT AND BLOCK CHAIN

RAMAN KUMAR MANDAL [1], SUNCHU LAHARI [2], SHEELAM GANESH[3],

ABBASANI NANDU [4], YALLAVULA SATHWIK [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 rapid advancement and integration of Internet of Medical Things (IoMT) devices are reshaping modern healthcare by enabling real-time patient monitoring, early diagnosis, and intelligent clinical decision-making. Despite these advancements, a key challenge persists: the fragmentation of sensitive patient data across various healthcare institutions and platforms. This lack of interoperability undermines seamless data exchange, limits the effectiveness of data-driven treatment, and poses risks to both patient privacy and system efficiency. To overcome these limitations, this project proposes a novel block chain-enabled framework for secure, interoperable, and privacy-preserving IoMT data validation and storage. Our solution leverages hyper ledger Fabric, a permissioned block chain architecture, to ensure robust access control, tamper-resistant data storage, and transparent auditability tailored to the needs of healthcare ecosystems. In addition, we integrate edge computing capabilities to perform data processing closer to the data source, significantly reducing latency and network congestion while preserving privacy and security at the device level. This decentralized and scalable architecture ensures secure, real-time sharing of IoMT data among authorized entities while maintaining strict data integrity and confidentiality. The proposed framework supports critical healthcare functions such as remote patient monitoring and preventative care, all while fostering trust among stakeholders. Experimental evaluations

highlight the system's potential to improve healthcare workflow efficiency, support faster clinical decisions, and enable a patient-centric approach through unified and reliable health data management. This work marks a meaningful step toward establishing an interoperable, secure, and efficient digital healthcare infrastructure for the future.

Index Terms – Internet of Medical Things (IoMT), blockchain, Hyperledger Fabric, edge computing, healthcare data security, interoperability, privacy preservation, secure data sharing, patient data management, decentralized healthcare, access control, healthcare blockchain.

I. INTRODUCTION

The Internet of Things (IoT) has emerged due to the growing number of linked devices, which are improving many facets of human existence, including healthcare. The Internet of Medical Things (IoMT), which uses IoT to deliver intelligent and widespread healthcare services, is the result of this evolution. These systems usually consist of a cloud-based data center, an internet gateway, and wearable sensing devices. Wearable devices connected to a wireless body area network (WBAN) create personal health data, which can be analyzed locally on the gateway device or forwarded to the data center for further in-depth analysis. Despite the benefits of real-time data processing, in-depth data analysis is still critical for achieving a better understanding. Digitization of patient records and physiological data, including heart rate, EKG, blood sugar level, etc., for remote monitoring, decision-making, and medical research. The development of information technology and IoT health devices has completely revolutionized the health system. The fragmented storage and management of clinical data hamper large-scale health data research and smooth information interchange. The Internet of Medical Things (IoMT) segment includes smart devices, like wearables and medical/vital surveillance that are only used in the healthcare sector at home, in clinics, hospitals, telemedicine, and other services. IoMT makes it possible to handle data reliably, streamline processes, reduce waste, and lower the possibility of errors. IoMT provides medical treatment in real-time, reducing the need for physicians to be physically present. Among the most critical issues that must be addressed in IoMT data management are data privacy regulations, communication blockages needed due to unusual physical conditions, the increasing likelihood of security breaches, and the usage of block chain

technology in delicate situations. Networks in many medical facilities are not stable enough to support IoMT devices. Doctors may encounter problems retrieving patient information due to the large volume of data being transferred. With block chain technology, patients can establish guidelines for who can access their medical records, giving certain researchers temporary access to specific parts of their records. Block chain technology allows patients to connect to their institutions and automatically collect their medical information. Smart contracts maintain the block chain's security and privacy. Wireless networks and block chain technology enhance data transmission efficiency and security. Wireless networks support real-time communication and the Internet of Things (IoT), while block chain ensures data integrity through decentralization and cryptography. Their integration can transform sectors like finance and healthcare by enabling secure transactions and addressing challenges in data security and privacy, driving innovation in an interconnected world. To protect user privacy, processes must ensure sensitive health data is secure, as cloud services managed by third-party providers may limit users' control over access. Also, for critical health decisions, data should be preserved still and not subject to any change while transmitted or stored. However, most centralized cloud systems cannot provide good data integrity and confidentiality guarantees .As a solution to these problems, permissioned block chain can provide an effective platform for secure storage and scalability due to its characteristics with its data integrity and decentralized peers. A block chain is a distributed ledger where numerous nodes preserve a ledger that records changes to an asset through transactions. A validation process that ensures that there is no discrepancy of data in the database when a transaction is initiated on any of the nodes. The proposed framework utilizes the Internet of Medical Things (IoMT) for the secure recording and storage of health metrics (including body temperature, pulse rate, oxygen saturation, and Photo plethysmography (PPG)). Wearable data is processed in different steps to prepare for secure storage in a distributed ledger. Besides assuring data integrity and security, the system facilitates real-time access and visualization of data for persistent, reliable health status monitoring. It delivers a holistic, multi disciplinary, decentralized tool for continuous, secure, readily available access to vital health information.

II. RELATED WORK

A. 5G and Internet of Things: Next-gen network architecture

The project "5G and Internet of Things: Next-Gen Network Architecture" focuses on developing a high-speed, low-latency, and intelligent communication framework that integrates the power of 5G technology with the Internet of Things (IoT). With billions of interconnected devices emerging across industries, the project aims to design an architecture that ensures seamless connectivity, real-time data processing, and efficient resource utilization. The integration of 5G enhances IoT capabilities by providing ultra-reliable communication, massive device connectivity, and improved bandwidth efficiency. This next-generation network supports applications such as smart cities, autonomous vehicles, industrial automation, and remote healthcare, where speed and reliability are crucial. The project emphasizes network slicing, edge computing, and AI-driven resource management to meet the diverse requirements of IoT devices. It also addresses challenges related to security, scalability, interoperability, and energy efficiency in large-scale IoT deployments. Through this architecture, data can be processed closer to the source, reducing congestion and enhancing responsiveness. The proposed system aims to create a flexible, secure, and intelligent network infrastructure that empowers digital transformation across multiple sectors. Ultimately, this project envisions a future-ready communication ecosystem that bridges the gap between connectivity and intelligence, laying the foundation for a truly smart and interconnected world powered by 5G and IoT integration.

B. Multi-modal secure healthcare data dissemination framework using block chain in IoMT

The project "Multi-Modal Secure Healthcare Data Dissemination Framework Using Block chain in IoMT" aims to develop a secure, transparent, and efficient system for managing and sharing healthcare data collected from diverse Internet of Medical Things (IoMT) devices. In modern healthcare environments, vast amounts of multi-modal data—such as medical images, sensor readings, and patient records—are generated continuously, requiring robust mechanisms for secure storage, validation, and dissemination. This project leverages block chain technology to ensure data integrity, traceability, and tamper-proof management, enabling trusted collaboration among healthcare providers, patients, and researchers. By incorporating smart contracts, it facilitates automated access

control and enforces strict privacy policies during data sharing. The framework also integrates edge computing to enable real-time processing and reduce network latency, ensuring quick medical responses in critical scenarios. It supports interoperability across heterogeneous IoMT devices and healthcare systems, overcoming data silos and fragmentation. The system ensures that sensitive medical data remains confidential, verifiable, and accessible only to authorized users. Furthermore, it enhances scalability and transparency in healthcare data management while complying with privacy regulations. Overall, the project envisions a patient centric, decentralized healthcare ecosystem that combines block chain's security with IoMT's intelligence to achieve secure, efficient, and privacy-preserving healthcare data dissemination across trusted networks.

C. *Metaverse in healthcare integrated with explainable AI and block chain: Enabling immersiveness, ensuring trust, and providing patient data security*

The project "Metaverse in Healthcare Integrated with Explainable AI and Block chain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security" focuses on creating a virtual, intelligent, and secure healthcare ecosystem that combines the immersive power of the Metaverse with the transparency of block chain and the intelligence of explainable AI (XAI). This framework enables virtual medical consultations, remote surgeries, and interactive therapy sessions through immersive 3D environments, enhancing patient engagement and accessibility. Explainable AI is integrated to ensure that medical decisions made by AI systems are transparent, interpretable, and trustworthy for doctors and patients alike. Block chain technology secures the exchange and storage of sensitive medical data, ensuring data integrity, privacy, and traceability across all Metaverse interactions.

The system allows real-time collaboration among healthcare professionals, offering a seamless platform for diagnosis, training, and patient care. Through decentralized data management, it eliminates risks of data breaches and unauthorized access. The integration of IoT and wearable devices enables continuous health monitoring and data visualization in immersive spaces.

The project emphasizes trust, accountability, and user control by combining AI-driven insights with block chain-backed verification. Ultimately, it aims to establish a next-generation virtual healthcare environment that is immersive, secure, and

transparent—redefining how medical services are delivered, experienced, and trusted in the digital era.

D. A survey on block chain technology and its security

The project "A Survey on Block chain Technology and Its Security" aims to provide a comprehensive study and analysis of block chain technology, focusing on its architecture, mechanisms, applications, and security challenges. Block chain, as a decentralized and distributed ledger system, offers transparency, immutability, and trust less data exchange, making it a revolutionary technology across domains such as finance, healthcare, supply chain, and IoT. This survey explores the core components of block chain, including consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), and their role in maintaining network reliability and security. It examines the cryptographic foundations—such as hashing, digital signatures, and public-key infrastructure—that ensure data integrity and authentication. The study also investigates major security threats, including 51% attacks, double spending, Sybil attacks, and smart contract vulnerabilities. Additionally, it discusses privacy preserving techniques and improvements through zero-knowledge proofs and sidechains. The project highlights comparative analyses of public, private, and consortium block chains to evaluate their suitability for different applications. It also reviews emerging trends, including block chain interoperability, scalability solutions, and integration with AI and IoT. Ultimately, this survey provides a detailed understanding of block chain's strengths, limitations, and evolving security landscape, offering insights for researchers and developers to build more secure, efficient, and trustworthy decentralized systems in the future.

III. PROPOSED METHODOLOGY

The proposed system introduces a secure, decentralized, and efficient healthcare data management framework that integrates Internet of Medical Things (IoMT) devices with block chain technology and edge computing to overcome the limitations of traditional centralized systems. This architecture uses hyper ledger Fabric, a permissioned block chain network, to securely store and manage sensitive health data, ensuring data privacy, and immutability. The use of edge computing enhances real-time data processing and enables timely clinical responses, while block chain ensures that all health records are tamper-proof and transparently auditable.

The framework supports real-time data visualization for healthcare professionals, improves scalability to accommodate growing IoMT networks, and facilitates patient-centric care by empowering patients with control over their medical data. Block chain and edge computing work together to create a secure, efficient, and scalable healthcare data management system using Internet of Medical Things (IoMT). This ensures data integrity, transparency, and privacy, allowing only authorized parties to access medical records. On the other hand, edge computing brings data processing closer to the data source, meaning the health data from IoMT devices is analyzed locally at or near the gateway device before being sent to the block chain. This reduces latency, minimizes network congestion, and allows real-time monitoring and decision-making without relying entirely on cloud resources. Together, these technologies enable secure, real-time healthcare monitoring, improve response times, and support critical health decisions, especially in remote or resource-constrained environments.

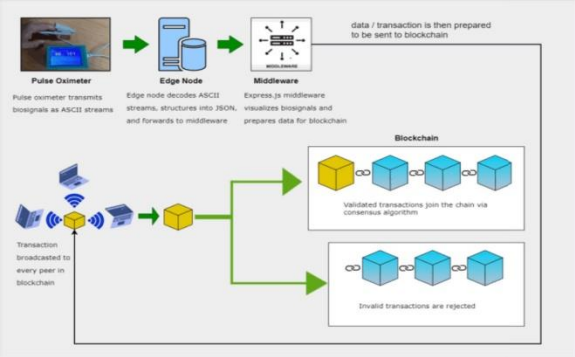
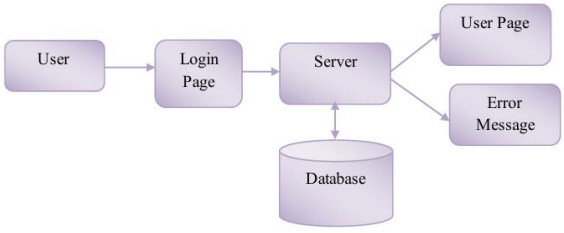


Fig. 1: System Overview

1. User Interface

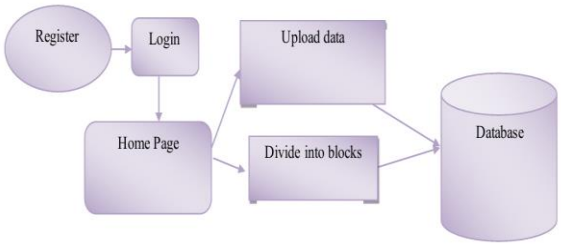
Design To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will 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. It will search the query and display the query.



2. Block Chain

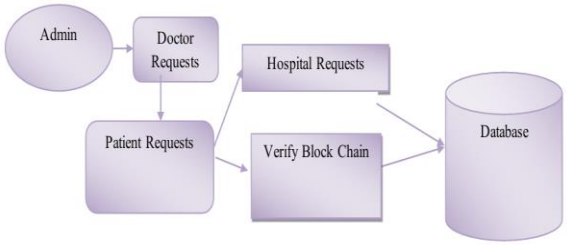
The Block chain module forms the core security layer of the proposed healthcare

system. It provides a decentralized, immutable, and transparent ledger for storing encrypted patient data and system transactions. Each patient file is divided into blocks and securely stored across the block chain network, ensuring that data cannot be deleted or modified without consensus. Smart contracts regulate data sharing among patients, hospitals, and doctors, ensuring that only authorized users with valid keys can access specific information. This module enhances trust, accountability, and traceability in the IoMT-based healthcare network by eliminating single points of failure and preventing unauthorized manipulation of health records.



3. Edge Computing

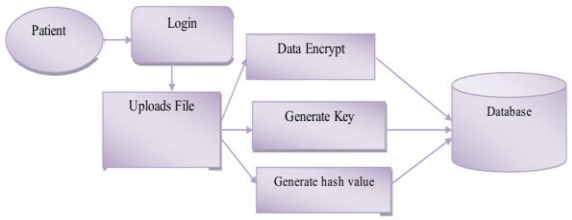
The Edge Computing module is integrated to ensure low latency, fast data processing, and efficient resource utilization in healthcare environments. Instead of sending all medical data to centralized cloud servers, computations are performed at the network's edge — closer to IoMT devices such as sensors, wearables, and hospital monitoring systems. This reduces bandwidth usage and response time, which is critical for real-time patient monitoring and diagnosis. In the proposed system, edge computing complements block chain by providing scalable, fast, and secure data transmission, ensuring that time-sensitive healthcare decisions are supported by immediate data access and processing at the edge nodes.



4. AES

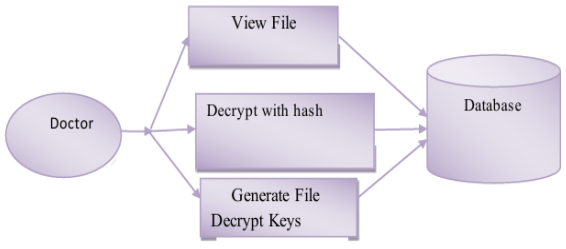
The AES module is implemented to achieve strong data encryption of medical files uploaded by patients. AES, a symmetric key encryption algorithm, ensures that patient records are converted into secure cipher text before being stored or transmitted. Only authorized users possessing the secret key can decrypt and access the data. This module guarantees confidentiality and protects medical information against unauthorized access or interception during transmission between patients, hospitals, and doctors. The use of AES in this healthcare framework enhances security efficiency, speed, and reliability, ensuring that sensitive data

remains protected throughout its lifecycle in the IoMT ecosystem.



5. SHA-256

The SHA-256 (Secure Hash Algorithm 256-bit) module is responsible for generating a unique hash value for each uploaded medical file. This hash acts as a digital fingerprint, ensuring data integrity by verifying that the file has not been altered or tampered with. Even a minor modification in the file changes the hash value entirely, making unauthorized changes immediately detectable. In the proposed healthcare system, SHA-256 works alongside block chain to maintain tamper proof medical records and support secure key generation processes. It establishes trust and verification mechanisms that are crucial in maintaining the credibility of medical data shared across multiple entities.



6. JSP

Dashboard Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

7. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed IoMT and Hyperledger Fabric-based framework enables secure, interoperable, and privacy-preserving health data management. The integration of edge computing reduces latency and network

congestion while supporting real-time data processing. Blockchain ensures tamper-resistant storage, secure access control, and transparent auditing of patient records. Overall, the framework improves healthcare workflow efficiency, supports faster clinical decision-making, and enables reliable sharing of medical data across healthcare providers.

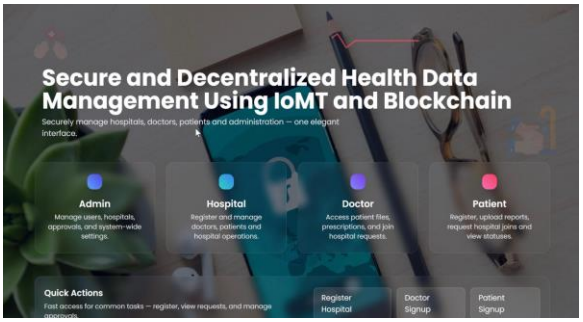


Fig. 2: Home Page

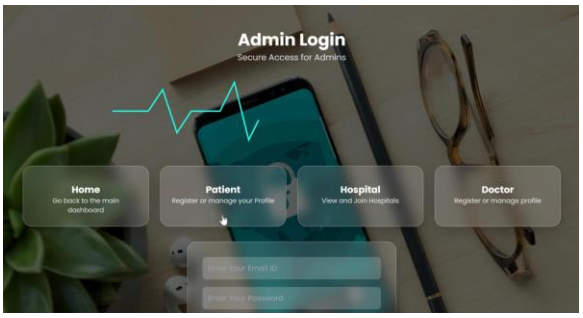


Fig. 3: Admin Login



Fig. 4: Registration

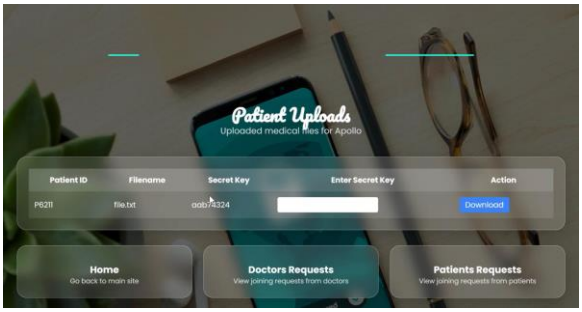


Fig. 5: Patient Uploads

V. CONCLUSION

In conclusion, the proposed Block chain-enabled IoMT healthcare system successfully establishes a secure, transparent, and decentralized platform for managing sensitive medical data among patients, doctors, and hospitals. By integrating AES encryption for data confidentiality and SHA-256 hashing for integrity verification, the system ensures that patient records remain protected from unauthorized access and tampering. The use of Block chain technology provides immutability and traceability, making every medical transaction verifiable and trustworthy. Through the Admin-controlled approval mechanism, only authenticated users gain access, enhancing overall data governance. The Hospital module streamlines patient–doctor interactions, while the Doctor module allows secure viewing and updating of medical details using secret keys. The Patient

module empowers individuals to control their medical data and securely share it with healthcare professionals. With edge computing integration, the system achieves low-latency processing and real-time data handling from IoMT devices. Overall, this architecture enhances security, privacy, scalability, and reliability in healthcare data sharing, contributing toward a more intelligent and trustworthy digital healthcare environment.

REFERENCES

[1] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015.

[2] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," J. Infection Public Health, vol. 13, no. 10, pp. 1567 1575, Oct. 2020.

[3] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, vol. 5, pp. 26521–26544, 2017.

[4] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," Sensors, vol. 20, no. 8, p. 2195, Apr. 2020.

[5] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda, "Survival study on blockchain based 6G-enabled mobile edge computation for IoT automation," IEEE Access, vol. 8, pp. 143453–143463, 2020.

[6] M. A. Habib, C. M. N. Faisal, S. Sarwar, M. A. Latif, F. Aadil, M. Ahmad, R. Ashraf, and M. Maqsood, "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," Int. J. Distrib. Sensor Netw., vol. 15, no. 9, Sep. 2019, Art. no. 155014771987565.

[7] K. P. Satamraju, "Proof of concept of scalable integration of Internet of Things and blockchain in healthcare," Sensors, vol. 20, no. 5, p. 1389, Mar. 2020.

[8] G. Manogaran, N. Chilamkurti, and C.-H. Hsu, "Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks," Pers. Ubiquitous Comput., vol. 22, nos. 5–6, pp. 879–882, Oct. 2018.

[9] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219

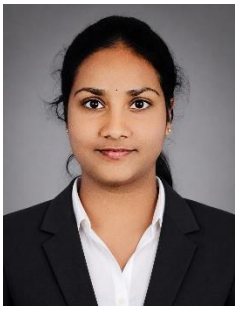
[10] Susarla, R. S., Boyapati, P. K., & Kandula, S. T. R. (2025, July). Cloud-Based Secure Data Storage in Smart Cities Using Central-Smoothing Hypergraph Neural Networks. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 279-284). IEEE.

[11] Akinapalli, S. (2026). AN AI-POWERED DATA TRUST AND QUALITY SCORING FRAMEWORK FOR ENTERPRISE DECISION INTELLIGENCE SYSTEMS. International Journal of Data Science and IoT Management System, 5(1), 946-950.

AUTHORS Profile



Mr. RAMAN KUMAR MANDAL received a B.Tech degree in Computer Science and Engineering from Ranchi University in 2010 and an M.Tech degree in Computer Science and Engineering from Bhagwant University in 2020. He has 8 years of teaching experience and is currently pursuing a Ph.D. degree in Computer Science and Engineering from Atal Bihari Vajpayee Indian Institute of Information Technology and Management, Gwalior. At present, he is working at Guru Nanak Institutions Technical Campus, Telangana. His research areas include Machine Learning and Artificial Intelligence.



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



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



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



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