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

CLOUD-NETWORK-END SECURITY INTEGRATION FOR SMART WIRELESS ENVIRONMENTS

PIRANGI HYMAVATHI [1], BOBBALA SNIGDHA REDDY [2], CHITTEDI SNEHITHA REDDY[3], BEECHANI NAVYA[4], TAMMISHETTI SRI SAI LIKHITHA[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 primary objective of network security is to safeguard data sharing's security. The commitment of traditional wireless network security technology is to guarantee the security of data transmission from beginning to end. Communication-computing integration and cloud-network integration, on the other hand, have been significant technical routes as mobile networks, cloud computing, and the Internet of Things have advanced. As a result, the main application requirements of wireless networks have changed from data transmission to cloud-based information services. Traditional data transmission security technology cannot overcome the security requirements of cloud-network-end collaborative services in the new era, and secure semantic communication has become an important model. To address this issue, we propose a cloud-network-end collaborative security architecture. To begin, we define the security mechanisms that are used to protect cloud services, network connections, and end systems, respectively. Next, we elaborate on the meaning of cloud-network-end collaborative security based on the three preceding aspects. We demonstrate the universality of the proposed architecture by providing examples of applications, such as the space-air-ground integrated network security framework, the unmanned system collaborative operations security framework, and heterogeneous network secure convergence framework. Finally, we review the current research on end system security, network connection security, and cloud services security, respectively.

Index Terms – Network security, cloud-network-end collaborative security, cloud computing, Internet of Things (IoT), semantic communication, cloud-network integration, wireless networks, cloud services security, end system security, network connection security, collaborative security architecture.

I. INTRODUCTION

Over the past few decades, wireless communication infrastructure and services have been rapidly increasing to meet the growing demand [1–6]. Wireless networks are now deeply integrated into everyone's daily life, benefiting by technologies such as mobile communications and the Internet of Things (IoT). The core function of wireless networks is data sharing between different entities. However, the openness of wireless networks poses challenges to the security of data sharing. Traditional wireless network security mainly aims to guarantee the authenticity, confidentiality, integrity, and availability of data transmission. The application of cryptographic technologies, including symmetric cryptography, public key cryptography, one-way hash functions, message authentication codes, digital signatures, etc., effectively guarantees the security of end-to-end data transmission. However, with the development of information technologies, data volumes and computing demands are exploding. As a result, the core requirements of information systems are transitioning from data transmission to cloud-based information services, which means that data transmission alone cannot address the application requirements anymore. Cloud computing has made computing resources more widely and economically available to institutions and individuals, while edge computing shifts some data processing works to the edge of the network, reducing network latency and improving system efficiency. These two techniques jointly drive innovation and growth in the information technology industry. Advancements in mobile communications technology have greatly improved the efficiency and reliability of the mobile internet. At the same time, benefiting from the Internet of Things, more and more devices can connect and communicate with each other. Combining these technologies will bring huge opportunities in smart cities, autonomous driving, telemedicine, etc. ML and AI are becoming increasingly important drivers of the information technology industry. Through autonomous learning and analysis of large amounts of data, AI systems can perform complex tasks, changing the way

that traditional industries operate. These technologies are revolutionizing fields such as medical care, finance, transportation, and entertainment. The popularity of cloud computing and AI technology has promoted the popularity of big data applications, and big data has become an important asset for enterprises and institutions. Big data is a valuable asset for enterprises and institutions, offering insights for market analysis, urban services, product innovation, and other fields. These applications provide assistance to institutions and individuals in their decision-making, information services, and daily life. Due to the intelligence, digitization, and automation of information services, the amount of data is becoming increasingly large, and data processing tasks are becoming increasingly complex. The main task of information systems (such as smart city, smart medical, smart industry, e-government, telemedicine, etc.) is transitioning from end-to-end data transmission to cloud-based information services. On one hand, data collection ends are widely distributed and the data access network is heterogeneous (e.g., 4G, 5G, Wi-Fi, satellite networks, aerial networks, etc.), resulting in difficulties in network integration and interconnection. On the other hand, data outsourced to the cloud are accessed to the network through the cloud, but data from different cloud servers are hard to be collaboratively processed securely. Traditional wireless communication networks mainly implement end-to-end data transmission without considering the data collection and processing. Nowadays, wireless communication networks not only are expected to collect and fuse massive data but also process data into information knowledge before distributing and utilizing them. Integration of communication and computing networks can effectively improve the data processing and service capabilities of the information system, thereby enabling intelligent interaction of information flow.

II. RELATED WORK

A. A TEE-assisted secured SQLite for embedded systems

A Trusted Execution Environment (TEE)–assisted secure SQLite framework has gained increasing attention as a reliable solution for protecting sensitive data in resource-constrained embedded systems. Recent research highlights the vulnerability of traditional embedded databases to attacks such as memory tampering, unauthorized access, and data leakage due to limited isolation mechanisms. To address these issues, several studies have explored the

integration of TEE technologies, such as ARM TrustZone, with lightweight database engines like SQLite. In these approaches, critical operations such as key management, query execution, and sensitive data storage are isolated within the secure world, while non-sensitive operations remain in the normal operating environment. This separation significantly enhances data confidentiality and integrity without imposing heavy computational overhead. Researchers have demonstrated that TEE-assisted database systems can effectively protect against software-based attacks, including privilege escalation and memory inspection. Additionally, secure key management and access control mechanisms are implemented within the trusted environment to prevent unauthorized data access. Performance evaluations show that such systems introduce minimal overhead while providing strong security guarantees. Recent studies also explore optimizing secure storage and query execution to meet the real-time constraints of embedded and IoT systems. Overall, TEE-assisted secure SQLite frameworks present a practical and efficient solution for safeguarding sensitive data in embedded environments, offering a balanced trade-off between security, performance, and resource utilization.

B. Forward/backward and content private DSSE for spatial keyword queries

Forward and backward private Dynamic Searchable Symmetric Encryption (DSSE) schemes have gained significant attention in recent research for enabling secure and efficient keyword search over encrypted data, particularly in spatial and location-based applications. Traditional searchable encryption schemes often suffer from information leakage during update and query operations, which can expose access patterns and compromise data privacy. To address these challenges, forward and backward privacy mechanisms are introduced to prevent adversaries from learning relationships between newly added or deleted data and previous search queries. In the context of spatial keyword queries, these techniques ensure that both location information and associated keywords remain confidential, even in dynamic environments where data is frequently updated. Researchers have proposed various DSSE frameworks that support secure insertion, deletion, and search operations while preserving query and update privacy. These schemes often combine cryptographic primitives such as pseudorandom functions, hash-based indexing, and encrypted search tokens to protect sensitive spatial

information. Additionally, optimized index structures and secure update mechanisms are designed to reduce communication and computation overhead. Recent studies also emphasize the importance of scalability and efficiency when handling large-scale spatial datasets in cloud environments. By integrating forward and backward privacy with content-aware encryption, these systems effectively prevent inference attacks and unauthorized data disclosure. Overall, forward/backward private DSSE schemes provide a robust foundation for secure spatial keyword search in modern data-driven and location-aware applications.

C. *MU-TEIR: Traceable encrypted image retrieval in the multi-user setting*

MU-TEIR (Multi-User Traceable Encrypted Image Retrieval) has emerged as an important research direction for securing image data in cloud-based and distributed environments. Traditional encrypted image retrieval schemes often face challenges in supporting multiple users while maintaining strong privacy and traceability guarantees. MU-TEIR addresses these limitations by enabling authorized users to search and retrieve encrypted images without revealing image content, query information, or user identity to the cloud server. In this approach, images are encrypted using advanced cryptographic techniques, and searchable indexes are constructed to allow efficient retrieval based on image features or keywords. A key contribution of MU-TEIR is its ability to support traceability, allowing the system to identify malicious users who misuse search privileges or leak secret keys. The framework incorporates secure key management, access control, and user accountability mechanisms to prevent unauthorized data access. In addition, privacy-preserving search techniques ensure that both image content and query patterns remain hidden from untrusted servers. Recent studies demonstrate that MU-TEIR systems achieve a good balance between security, retrieval accuracy, and computational efficiency. Experimental evaluations show that the scheme scales well with large image datasets and multiple users, making it suitable for real-world applications such as medical imaging, surveillance systems, and cloud-based multimedia services.

D. *VRFMS: Verifiable ranked fuzzy multi-keyword search over encrypted data*

VRFMS (Verifiable Ranked Fuzzy Multi-keyword Search) is an advanced searchable encryption approach designed to support secure, efficient, and accurate information retrieval over encrypted cloud data. Traditional searchable encryption schemes

often suffer from limited query expressiveness, inability to handle fuzzy keyword matching, and lack of verification mechanisms for returned results. VRFMS addresses these limitations by enabling users to perform ranked multi-keyword searches while tolerating minor spelling errors or variations in query terms.

The scheme incorporates verifiable mechanisms that allow users to confirm the correctness and completeness of search results returned by an untrusted cloud server. By using cryptographic primitives such as secure index structures, hash-based verification, and ranking algorithms, VRFMS ensures both data confidentiality and query privacy. The system supports relevance-based ranking, allowing users to obtain the most relevant encrypted documents without revealing keyword information.

Additionally, VRFMS enhances search accuracy through fuzzy matching techniques, which are particularly useful in real-world applications where user input may be imprecise. Security analysis shows that the scheme resists keyword guessing and inference attacks while maintaining efficient search performance.

Experimental evaluations demonstrate that VRFMS achieves low computation and communication overhead, making it suitable for large-scale cloud environments. Overall, VRFMS provides a practical and secure solution for searchable encrypted data, balancing privacy protection, usability, and system efficiency.

III. PROPOSED METHODOLOGY

The cloud-based information services system enables intelligent services through network-based multi-party data sharing and collaboration processing between cloud servers and ends. To ensure data security, it is necessary to resist security threats not only from a single party but also from collaborative data services. Therefore, information services security is collaborative and systematic, covering the entire lifecycle of data sharing and collaboration processing. To ensure data security in cloud-network-end collaborative services, the key issue is to achieve secure communication (for network) and secure computing (for end system and cloud).

In the local network, the network center collects and fuses the local-domain data securely, and outsources data on the local-domain cloud to prepare for cross-cloud data sharing. Each cloud server corresponding to

the local network securely shares data with other servers. This allows data from different networks to be securely integrated through cross-cloud computing and enables cross-network collaboration.

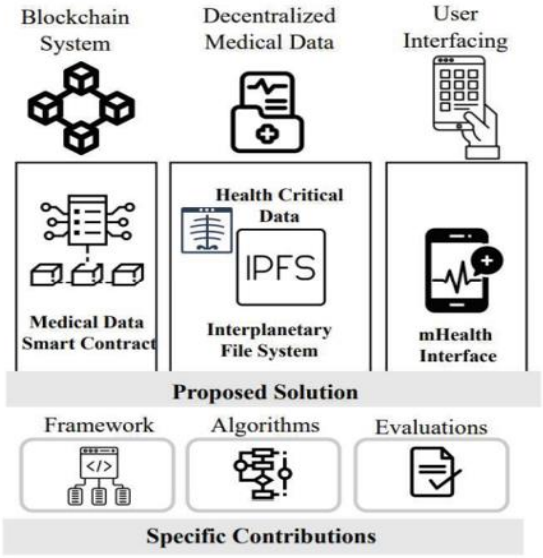
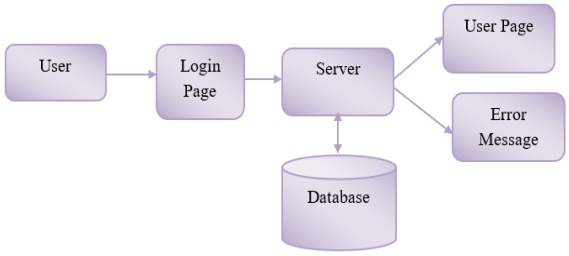


Fig. 1: System Overview

1. User Interface Design

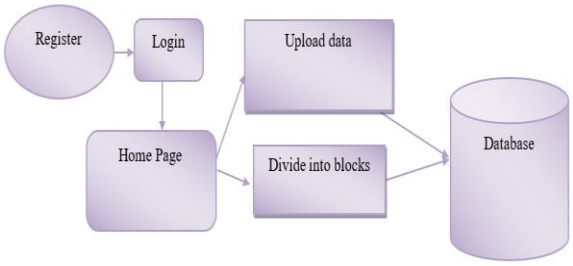
To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create 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. Cloud–Network–End Collaborative Security Architecture

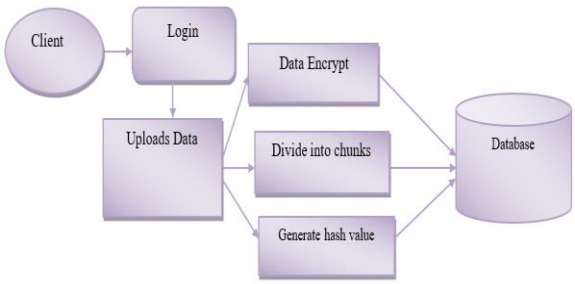
Cloud–Network–End Collaborative Security Architecture is an integrated security framework designed to protect data, communication, and services across cloud platforms, network infrastructures, and end-user devices. As modern applications increasingly rely on distributed computing environments, this architecture ensures seamless coordination between cloud resources, network communication layers, and edge or end devices. It enables secure data collection, transmission, processing, and storage by combining advanced cryptographic techniques, intelligent network management, and trusted computing mechanisms. By addressing security challenges such as data leakage, unauthorized access, and integrity threats across heterogeneous environments, the cloud–network–end collaborative model enhances overall system reliability and resilience. This architecture supports emerging applications such as smart cities,

intelligent transportation, IoT, and cloud-based services by ensuring secure, efficient, and scalable interaction among all participating components.



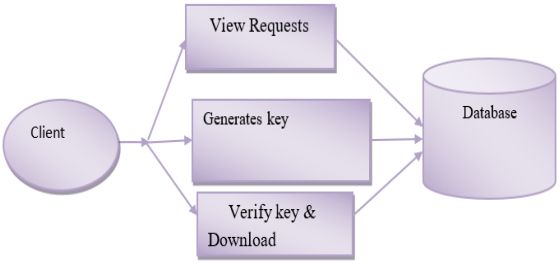
3. SHA-256

The SHA-256 (Secure Hash Algorithm-256) module is responsible for maintaining the integrity and authenticity of healthcare data across all transactions. Whenever a doctor, patient, or file is created or uploaded, a unique hash value is generated using SHA-256. This hash acts as a digital fingerprint that verifies whether the data has been modified. Even a minor change in data alters the hash, immediately alerting the system to possible tampering. In this project, SHA-256 is used to generate hash values for doctor and patient IDs, as well as for each file and its divided blocks. This ensures end-to-end verification, secure identity management, and immutability of all stored medical information within the block chain network.



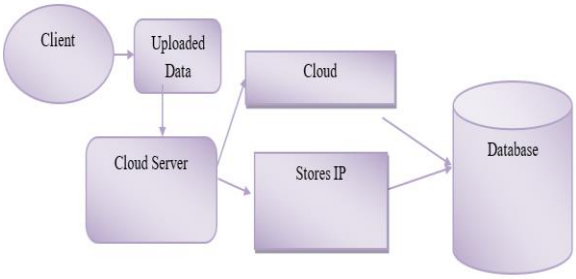
4. AES

The AES (Advanced Encryption Standard) module is implemented to ensure the confidentiality of patient medical data during transmission and storage. When a patient uploads a file, AES encryption is applied to convert the original data into unreadable cipher text using a unique secret key. This key is securely stored and later verified when a doctor requests to download the file. Only if the correct secret key is provided can the file be decrypted and accessed. AES provides high-speed, strong symmetric encryption, making it ideal for protecting sensitive health records against unauthorized access. Its integration ensures that even if data is stored in a distributed block chain environment, privacy and data secrecy remain uncompromised.



5. Cloud Server

The server acts as the central processing and control unit within the cloud–network–end collaborative security architecture. It is responsible for managing data storage, computation, authentication, and access control across the system. The server securely receives encrypted data from end devices, processes requests from users or applications, and coordinates communication between network components and cloud services. By implementing robust security mechanisms such as encryption, authentication, and access control policies, the server ensures data confidentiality, integrity, and availability. Additionally, it supports scalability and high availability, enabling efficient handling of large volumes of data and multiple concurrent users in smart and distributed environments.



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.

6. 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 analysis shows that the proposed cloud-network-end collaborative security architecture provides comprehensive protection for cloud services, network connections, and end devices in smart wireless environments. The framework effectively supports secure semantic communication and demonstrates its applicability across scenarios such as space-

air-ground networks, unmanned systems, and heterogeneous network integration. The results indicate improved security, scalability, and interoperability compared to traditional transmission-based security models. Overall, the proposed architecture offers a robust solution for next-generation wireless network security.

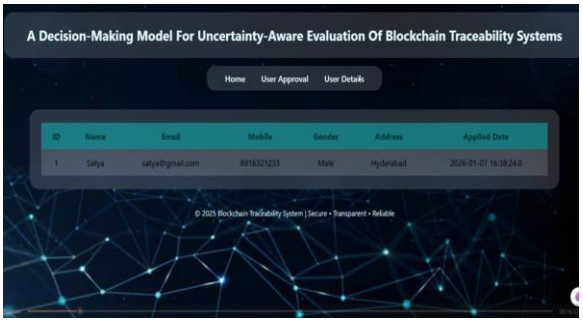


Fig. 2: Home Page



Fig. 3: Private Key Access

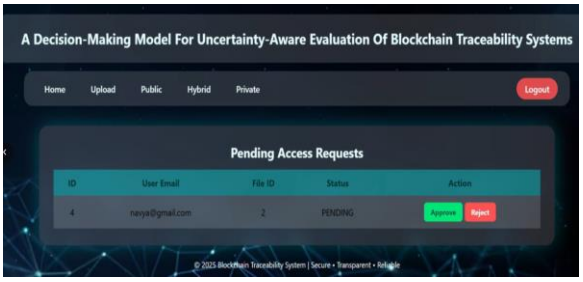


Fig. 4: Pending Access Request

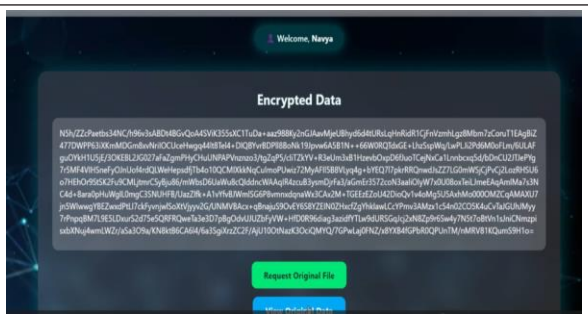


Fig. 5: Encrypted Data

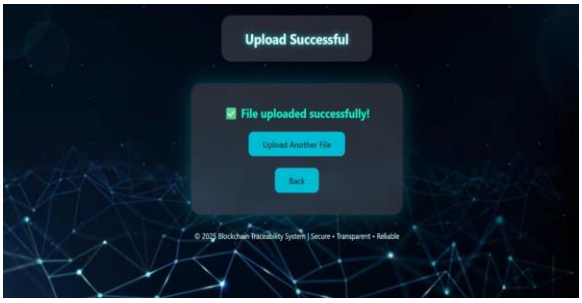


Fig. 6: Upload File

V. CONCLUSION

The proposed Cloud–Network–End Security Integration framework provides a comprehensive and forward-looking solution to address the growing security challenges in modern wireless communication environments. As data generation, transmission, and processing continue to expand rapidly, traditional end-to-end security mechanisms are no longer sufficient to protect sensitive information across heterogeneous and distributed networks. By integrating cloud computing, network intelligence, and end-device security, the proposed approach establishes a unified and robust security architecture capable of

supporting large-scale, data-driven applications. The framework enhances confidentiality, integrity, and availability through coordinated security mechanisms operating across all layers of the system. It effectively bridges the gap between data generation, transmission, and processing by enabling secure collaboration among cloud services, network infrastructures, and edge devices. Furthermore, the incorporation of intelligent processing and adaptive security strategies allows the system to respond dynamically to evolving threats and changing network conditions. The proposed architecture also supports scalability and flexibility, making it suitable for diverse application domains such as smart cities, healthcare systems, intelligent transportation, and industrial automation. By enabling secure data sharing, efficient resource utilization, and reliable communication, the framework enhances overall system trustworthiness and operational efficiency. Ultimately, the Cloud–Network–End Security Integration model lays a strong foundation for future smart environments, offering a secure, scalable, and intelligent solution capable of meeting the demands of next-generation wireless communication systems.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless sensor networks: A survey, Comput. Netw., vol. 38, no. 4, pp. 393–422, 2002.

[2] I. F. Akyildiz and X. Wang, A survey on wireless mesh networks, IEEE Commun. Mag., vol. 43, no. 9, pp. S23–S30, 2005.

[3] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, Wireless body area networks: A survey, IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1658–1686, 2014.

[4] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, Space-air- ground integrated network: A survey, IEEE Commun. Surv. Tutorials, vol. 20, no. 4, pp. 2714–2741, 2018.

[5] C. Zhang, P. Patras, and H. Haddadi, Deep learning in mobile and wireless networking: A survey, IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2224–2287, 2019.

[6] Z. Shen, J. Jin, C. Tan, A. Tagami, S. Wang, Q. Li, Q. Zheng, and J. Yuan, A survey of next-generation computing technologies in space-air-ground

integrated networks, ACM Comput. Surv., vol. 56, no. 1, p. 23, 2023.

[7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends, Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.

[8] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[9] R. Perez, R. Sailer, and L. Doorn, vTPM: Virtualizing the trusted platform module, in Proc. 15th Conf. USENIX Security Symposium, Vancouver, Canada, 2006, pp. 305–320.

[10] B. Kauer, OSLO: Improving the security of trusted computing, in Proc. 16th Conf. USENIX Security Symposium, Boston, MA, USA, 2007, pp. 1–9.

[11] Shashank, A. (2025). AI-Enhanced ETL Processes: Leveraging Artificial Intelligence for Optimized Data Integration Systems. Journal Of Multidisciplinary, 5(8), 219-225.

AUTHORS Profile



Mrs. PIRANGI HYMAVATHI has received her B.Tech from JNTUH, Hyderabad in 2016, M.Tech degree in Computer science Engineering from JNTUH, Hyderabad in 2019. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



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



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



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



Ms. TAMMISHETTI SRI SAI LIKHITHA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.