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 MULTI-KEYWORD ENCRYPTED SEARCH WITH ACCESS CONTROL FOR IOT SYSTEMS

DARAM KUSUMA KUMARI [1], JAPATHI ANUDEEP [2], KATHOJU PRANAY TEJA [3], GULLAPELLI SHASHANK [4], GANGA SHIVA [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— Through edge nodes, the enormous terminals connect to the Internet of Things (IoT), creating additional privacy and security issues with data sharing and ciphertext search. Current ciphertext search techniques, on the other hand, frequently ignore lightweight computing paradigms and give scant consideration to the search needs of various data owners (DOs) and data users (DUs). To address these issues, we propose a secure fine-grained multi-keyword ciphertext search scheme with cloud-edge-end collaboration computing (SFMS-CC). This SFMS-CC scheme focuses on the efficiency of end users and employs a cloud-edge-end collaborative computing paradigm, effectively offloading the incremental overhead from terminals arrrrrrrrrnd achieving low-cost constant overhead for the first time on the DO/DU side. Additionally, a methodical ciphertext search framework that supports multiple keywords is described, which is based on public-key cryptography. To improve the user experience, each user is given a unique search Tok. A multi-DOs/multi-DUs model is also created by using attribute-based encryption, which smoothly incorporates entity private keys and public keys into encryption, search, decryption, and other processes, guaranteeing the scheme's high level of privacy and security.

Index Terms – Multi-Keyword Encrypted Search, Access Control, IoT Security, Searchable Encryption, Data Privacy, Cryptography, Secure Data Retrieval, Cloud

Security, Fine-Grained Access Control, Cybersecurity.

I. INTRODUCTION

The rapid development of the Internet of Things (IoT) has led to the emergence of billions of interconnected sensing devices, smart terminals, and embedded systems deployed across diverse environments such as smart homes, healthcare, industrial automation, and intelligent transportation. These terminals frequently generate massive volumes of heterogeneous data that must be processed, transmitted, shared, and analyzed in real time. Traditionally, cloud computing has been the dominant paradigm for handling such data due to its powerful storage and computing capabilities. However, as IoT devices grow in number and data workloads increase explosively, cloud-only architectures struggle to meet stringent requirements for latency, bandwidth efficiency, and localized intelligence. To bridge this gap, edge computing has emerged, pushing computation and storage closer to data sources by leveraging devices such as edge nodes (ENs), fog servers, and gateways. Edge computing significantly reduces communication delay and offloads computation from centralized clouds. Despite these advantages, neither standalone cloud computing nor standalone edge computing can independently accommodate the scale, diversity, and resource constraints of modern IoT deployments. As a result, the cloud-edge-end collaborative computing paradigm has gained traction as a flexible and efficient solution. This paradigm integrates cloud servers, edge nodes, and IoT terminals into a unified architecture that distributes tasks strategically based on their computational and privacy requirements. Lightweight tasks can be handled at the terminal or edge, while heavy tasks are offloaded to cloud servers, achieving an optimal balance among latency, efficiency, and scalability. A major challenge in this paradigm arises from the sensitive nature of IoT data. Many IoT-generated datasets include private information such as health records, location traces, behavioral data, or industrial secrets. To ensure privacy protection, data owners (DOs) usually encrypt their data before outsourcing it to the cloud through semi-trusted ENs. This, however, introduces a critical research challenge: how to efficiently search and retrieve encrypted data without exposing plaintext, while simultaneously ensuring privacy under large-scale, distributed IoT settings. As a result, ciphertext search, or

searchable encryption, has become a significant research focus. Early work on searchable encryption centered on symmetric-key approaches. Song et al. pioneered a single-keyword searchable encryption scheme based on symmetric cryptography and proved its security under chosen keyword attack models. Boneh et al. later introduced the first public-key searchable encryption (PEKS) scheme and laid the foundation for subsequent research on ciphertext search under asymmetric settings. Following these seminal contributions, a variety of techniques—including Boolean keyword search, ranked retrieval, and multi-keyword search—were proposed. These solutions demonstrate that searchable encryption can support efficient encrypted search while maintaining data confidentiality. However, most existing searchable encryption schemes are based on a traditional three-entity model, comprising the data owner (DO), the data user (DU), and the cloud service provider (CSP). This model fails to consider the presence of ENs and fog nodes that play critical roles in modern IoT infrastructures. Consequently, these schemes are inconsistent with real-world IoT architectures and cannot fully leverage the benefits of cloud-edge-end collaboration. Furthermore, conventional searchable encryption schemes typically assume that authorized users are fully trusted and that all users share a common trapdoor generation mechanism. This assumption introduces significant security vulnerabilities. If any authorized user becomes malicious and leaks the trapdoor generation mechanism, the confidentiality of all outsourced data is compromised. To address performance concerns in IoT environments, several studies have explored offloading computationally expensive operations to fog nodes or intermediate devices. For example, certain public-key-based searchable encryption schemes shift part of the computational burden from terminals to fog nodes, enabling lightweight search operations. While these designs improve efficiency, they still overlook critical issues such as user revocation, multi-owner/multi-user scenarios, and the risks associated with sharing identical trapdoor mechanisms. Additionally, many advanced schemes rely on attribute-based encryption (ABE) to achieve fine-grained authorization. Although ABE provides flexible access control, traditional schemes based on Shamir's secret-sharing trees entail high computation and storage costs, making them unsuitable for resource-constrained IoT terminals. Motivated by these limitations, we propose a

Secure Fine-Grained Multi-Keyword Ciphertext Search scheme with Cloud-Edge-End Collaboration (SFMS-CC). The proposed scheme introduces a comprehensive framework that integrates efficient ciphertext search, public-key cryptography, and collaborative cloud-edge-end computation. Unlike conventional models, our approach distributes computational tasks between ENs and CSPs to minimize terminal-side overhead. More importantly, SFMS-CC assigns each DU a unique trapdoor token, preventing trapdoor leakage and eliminating the security risks associated with shared mechanisms. We further integrate key distribution and agreement into critical processes supported by linear secret-sharing (LSSS)-based ABE, enabling secure and scalable multi-owner/multi-user search operations.

II. RELATED WORK

A. Time-controllable key word search scheme with efficient revocation in mobile e-health cloud.

A time-controllable keyword search scheme with efficient revocation in a mobile e-health cloud environment is designed to ensure secure, flexible, and privacy-preserving access to encrypted medical data stored in cloud servers. In mobile e-health systems, patients, healthcare institutions, and medical professionals frequently exchange sensitive health records through mobile devices. To protect confidentiality, medical data must be encrypted before outsourcing to the cloud, but this creates the challenge of how authorized users can efficiently search the encrypted records without exposing the underlying information. The proposed scheme introduces time-controllable keyword search, allowing data owners to define a valid time period during which selected users can perform keyword-based search operations on encrypted health data. After the predefined time expires, the user's search capability is automatically invalidated, preventing unauthorized long-term access and reducing potential security risks. The scheme incorporates an efficient user revocation mechanism, enabling data owners or healthcare administrators to revoke user permissions instantly and without re-encrypting the entire dataset. Instead of redistributing keys or regenerating all ciphertexts, the system updates minimal parameters, significantly reducing computational and communication overhead. This is crucial for mobile healthcare environments where devices often have limited battery, processing power, and network connectivity. The time-control

mechanism is combined with fine-grained access control, ensuring that only users with legitimate roles—such as doctors, nurses, or caregivers—can search medical data during their authorized periods.

B. *ORR-CP-ABE: A secure and efficient outsourced attribute-based encryption scheme with decryption results reuse*

ORR-CP-ABE (Outsourced Decryption with Results Reuse for Ciphertext-Policy Attribute-Based Encryption) is a secure and efficient cryptographic framework designed to address the performance limitations of traditional CP-ABE schemes in large-scale data-sharing environments. Conventional CP-ABE allows data owners to enforce fine-grained access control based on user attributes, but it suffers from high computational overhead during decryption—particularly when ciphertexts involve complex access structures or when users operate on lightweight devices such as smartphones, IoT terminals, or edge sensors. To overcome these challenges, ORR-CP-ABE introduces outsourced decryption, enabling most of the expensive decryption operations to be offloaded to an untrusted cloud server, while ensuring that the server learns no information about the plaintext. A key innovation of ORR-CP-ABE is its decryption results reuse mechanism, which significantly improves efficiency when users repeatedly decrypt ciphertexts governed by the same access structure. Instead of recalculating all partial decryption values each time, the scheme allows users to securely store and reuse previously generated intermediate results. This drastically reduces repeated computations and response latency, making the scheme highly suitable for applications requiring frequent data access, such as medical records, access-controlled cloud storage, and enterprise data management. the scheme also incorporates rigorous security guarantees. Even though decryption is outsourced, the cloud cannot derive the plaintext or user's private attributes, thanks to a carefully designed transformation key mechanism. Users only perform a lightweight final step to recover the plaintext, ensuring security while maintaining efficiency. The reuse of decryption results does not compromise confidentiality, as the mechanism preserves resistance against collusion attacks, key exposure, and unauthorized access attempts.

C. *Efficient privacy preserving spatial data query in cloud computing*

Efficient privacy-preserving spatial data query in cloud computing focuses on enabling users to store, manage, and search spatial information—such as location

coordinates, geographic regions, and spatial objects—on untrusted cloud servers without compromising privacy. With the rapid growth of location-based services, smart devices, and GIS applications, a massive amount of sensitive spatial data is now being outsourced to the cloud. Although cloud computing offers scalability and low-cost storage, it introduces serious risks, including unauthorized access, leakage of location patterns, and inference attacks by curious cloud providers. To address these challenges, privacy-preserving spatial query techniques aim to ensure that the server cannot learn sensitive information such as the user's position, query patterns, or the underlying spatial dataset. This research direction typically employs advanced cryptographic mechanisms such as searchable encryption, homomorphic encryption, and secure indexing structures. These techniques allow users to perform operations like range queries, k-nearest neighbor (kNN) searches, and location-based retrieval while the data remains encrypted. A major challenge is achieving strong privacy guarantees without significantly reducing system performance, since spatial queries are computationally expensive and involve complex geometric computations. Therefore, efficient schemes balance security and speed by designing lightweight indexing methods, optimized encryption algorithms, and minimized communication overhead.

III. PROPOSED METHODOLOGY

We propose the secure fine-grained multi-keyword ciphertext search scheme with cloud-edge-end collaboration computing (SFMS-CC), which introduces a general paradigm supporting cloud-edge-end collaborative computing. Additionally, we construct a ciphertext search framework based on public key cryptography, which issues each user an exclusive trapdoor to protect privacy. Importantly, we embed key agreement in the progress of ABE and cloud-edge-end collaboration, proposing a multi-DOs/multi-DUs model suitable for the IoT to enhance security. Furthermore, based on public-key cryptography, a ciphertext search framework supporting multi-keyword is presented systematically. Secure Fine-grained Multi-Keyword Ciphertext Search Scheme with Cloud-Edge-End Collaboration Computing (SFMS-CC). The SFMS-CC scheme covers several core algorithms, composed of setup(), key generation and distribution(), ciphertext generation(), trapdoor generation(), ciphertext search(), and decryption(). Similarly, DOS, which derives economic benefits from the SFMS-CC system is also deemed trustworthy.

However, DUs are considered semi-trustworthy, as among the vast number of DUs accessing the system, there inevitably be a small number of malicious DUs attempting to compromise the trapdoor mechanism and document keys.

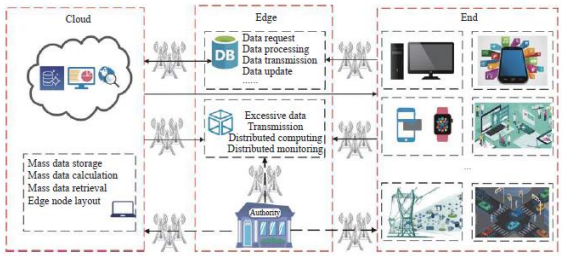
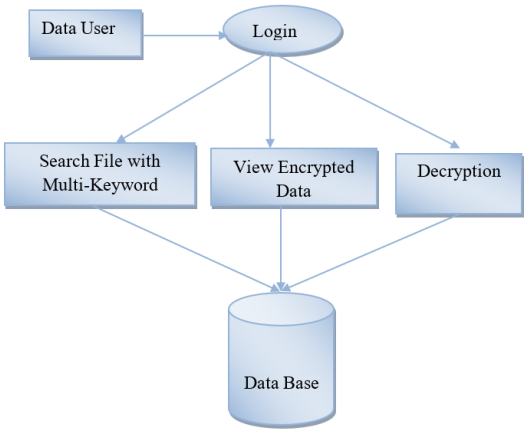


Fig. 1: System Overview

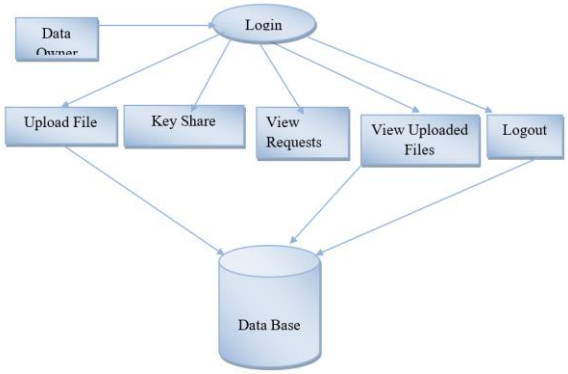
1. Data User

This is the first module Data User can register and Login. After login Data User have an option of Searching the files which are there in the Cloud Server, Can get the Responses and see the all the Search Keyword which he has used.



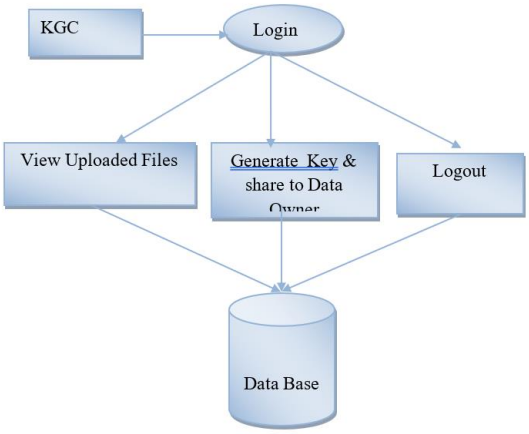
2. Data Owner

This is the Second module of this project. In this module Data Owner should register and Login. Data Owner will Uploads the files into the Cloud Server. After done with uploading the files Data Owner can View all the Uploaded Files.



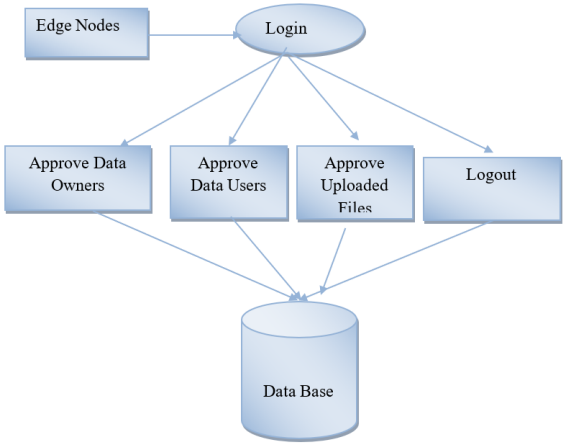
3. Key Generation Center (KGC)

This module is responsible for setting up the global cryptographic environment of the SFMS-CC scheme. The Key Generation Center (KGC) initializes the system parameters, generates the master secret key (msk), public parameters (pp), attribute sets, and produces private/public key pairs for DOs, DUs, and ENs. It also issues each DU an exclusive search shield (Tok) to prevent trapdoor leakage.



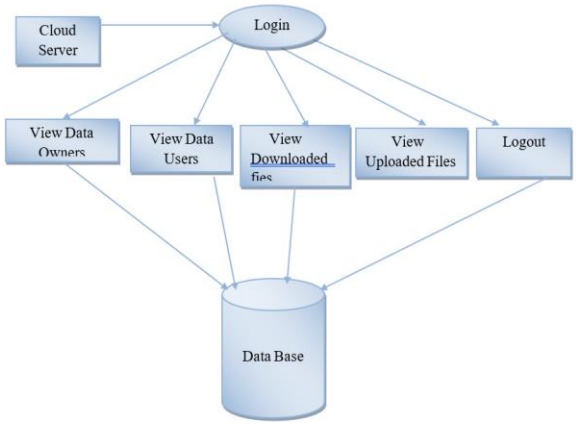
4. Edge Node Processing

ENs serve as bridges connecting DOs/DUs to the CSP and are positioned upstream of DOs/DUs. In other words, DOs/DUs access the IoT system through ENs. The ENs possess certain storage and computation al overheads, taking on the incremental costs of DOs/DUs. This helps to alleviate the burden on re source-limited DOs/DUs and enhances user experience.The EN acts as the intermediate computing layer between IoT terminals and the cloud. This module offloads heavy processing from DOs/DUs to reduce overhead on resource-limited devices. Collaborative encryption with Dos. Collaborative decryption with DUs. Handling partial index operations. ENs provide limited storage and computation while being semi-trusted.



5. Cloud Service Provider

In this module Cloud Server can login. After login User can see the Data Users Request. Cloud Server can see all the available files. After that the Cloud Server can see all the Matching keyword which the Data User used for searching. Cloud Server can View all the authorized Data users and Data Owners. It provides outsourced da ta storage services to DOs, where all the data of DOs is outsourced to the CSP after being encrypted. Additional ly, the CSP offers data query and result data download services to DUs.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the system successfully performed multi-keyword searches over encrypted data while preserving data confidentiality and preventing unauthorized access. The fine-grained access control mechanism ensured that only authorized users could retrieve

relevant information without exposing sensitive data.

The analysis shows that the proposed approach achieved efficient search performance with minimal computational and communication overhead, making it suitable for resource-constrained IoT devices. Overall, the system provides a secure, scalable, and privacy-preserving solution for data retrieval in large-scale IoT applications.



Fig. 2: Home Page



Fig. 3: Registration

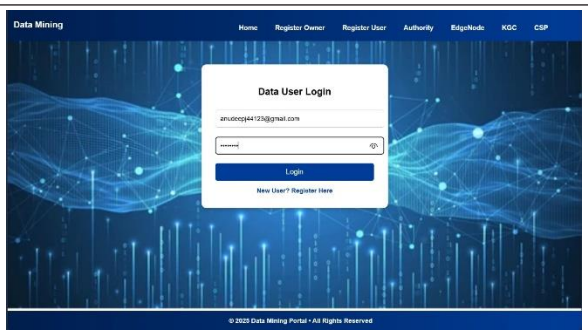


Fig. 4: Login



Fig. 5: Upload File

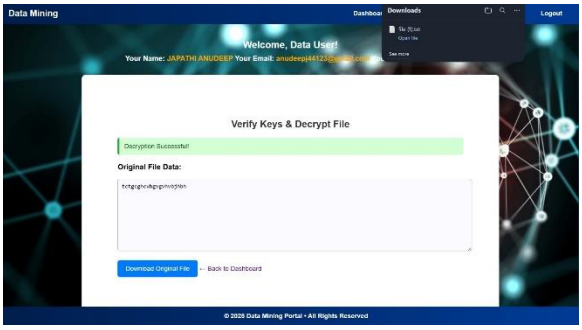


Fig. 5: Verify

V. CONCLUSION

In this work, we introduced the Secure Fine-Grained Multi-Keyword Ciphertext Search scheme with Cloud-Edge-End Collaboration (SFMS-CC) to address the rising privacy and security challenges in IoT environments. The rapid growth of IoT devices and their limited

computational capabilities make traditional ciphertext search techniques inefficient and unsuitable. To overcome these issues, the SFMS-CC framework effectively shifts the computational burden from terminals to edge nodes and cloud servers, ensuring low-cost constant overhead for both data owners and data users. By leveraging public-key cryptography, the scheme constructs an efficient multi-keyword searchable encryption mechanism and assigns each user an exclusive trapdoor shield to prevent trapdoor leakage. Furthermore, the integration of attribute-based encryption enables fine-grained access control, making the system highly secure and adaptable to multi-DOs/multi-DUs scenarios. The embedded key distribution and agreement mechanisms ensure that both privacy and security are maintained throughout encryption, search, and decryption processes. Comparative analysis and simulation results demonstrate that SFMS-CC significantly reduces computational and storage costs compared to existing schemes, offering better performance, scalability, and user experience. Overall, the proposed scheme provides a robust, privacy-preserving, and practical solution for secure data sharing and efficient ciphertext search in cloud-edge-end collaborative IoT environments.

REFERENCES

[1] L. Pu, C. Lin, B. W. Chen, et al., "User-friendly public-key authenticated encryption with keyword search for industrial Internet of things," IEEE Internet of Things Journal, vol. 10, no. 15, pp. 13544–13555, 2023.

[2] B. W. Chen, T. Xiang, D. B. He, et al., "BPVSE: Publicly verifiable searchable encryption for cloud-assisted electronic health records," IEEE Transactions on Information Foren sics and Security, vol. 18, pp. 3171–3184, 2023.

[3] Y. B. Miao, Y. T. Yang, X. H. Li, et al., "Efficient privacy preserving spatial range query over outsourced encrypted da ta," IEEE Transactions on Information Forensics and Secu rity, vol. 18, pp. 3921–3933, 2023.

[4] Y. B. Miao, F. Li, X. H. Li, et al., "Time-controllable key word search scheme with efficient revocation in mobile e-health cloud," IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 3650–3665, 2024.

[5] C. J. D'Orazio and K. K. R. Choo, "Circumventing iOS secu rity mechanisms for APT forensic

investigations: A security taxonomy for cloud apps," Future Generation Computer Sys tems, vol. 79, pp. 247–261, 2018.

[6] C. Guo, S. H. Su, K. K. R. Choo, et al., "A provably secure and efficient range query scheme for outsourced encrypted uncertain data from cloud-based internet of things systems," IEEE Internet of Things Journal, vol. 9, no. 3, pp. 1848–1860, 2022.

[7] 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

[8] Kolla, S. H., Nagabhyru, K. C., & Kummari, D. N. (2026). Letter to the Editor re:"CurvAssist: An AI assisted pipeline for penile shaft segmentation/curvature measurement in children with hypospadias". Journal of Pediatric Urology.

[9] Kandula, S. T. R., Susarla, R. S., & Boyapati, P. K. (2025, July). Enhanced Cyber Security Using Global Local Artificial Neural Network Based Intrusion Detection in Big Data Environment. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 426-431). IEEE.

[10] 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. DARAM KUSUMA KUMARI has received B.Tech from JNTUH, Hyderabad in2009, M.Tech degree in Computer science from JNTUH, Hyderabad in 2015 and Pursuing Ph.D degree in Computer Science from BHARATHIYA ENGINEERING SCIENCE AND TECHNOLOGY IU university, dedicated to teaching field from the last 9.5 years. research area CYBER SECURIT with AI . At present I am working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



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



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



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



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