International Journal of Engineering Research and Science & Technology

A SECURE BLOCKCHAIN TECHNIQUE FOR INTEGRATION KNOWLEDGE DISCOVERY IN CLOUD

RAVULA ANITHA[1], BOYAPALLY POOJITHA[2], CHANDARAJU RAKESH[3], KOLLU SUNIL[4]

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

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

ABSTRACT— The field of is now being duly recognized as a revolutionary area in industrial automation. With the budding interest of knowledge discovery that on a large scale, researchers are now faced with several major security concerns. Blockchain integration is one of the suggested applications of technology that could help secure data during transmission, storage, and knowledge discovery. Moreover, by integrating smart contracts, a secure architecture could also assimilate accountability during data exchange. Thus, we propose a four-layer security architecture that isolates industrial devices from user-oriented layers and maintains a record of all registered devices within the organization to prevent malicious devices from corrupting the database and the discovery process. Further, by choosing Proof of Authority (PoA), we ensure the fair functioning of the Blockchain nodes. Through PoA consensus for Blockchain nodes and whitelist-based access control for registered devices, we ensure the legitimacy of all participating nodes. We also implement a prototype using a private The network with Proof of Authority consensus and present the time taken for consumed per exchange by the contracts. Additionally, we implemented secure knowledge discovery to understand the significance of the developed scheme. The results show that the exchange can be implemented in an industrial environment and operate with a reasonable amount of resource consumption.

Index Terms – Industrial Internet of Things (IIoT), blockchain, industrial automation, smart contracts, Proof of Authority (PoA), knowledge discovery, data security, access control, private blockchain, whitelist

authentication, secure data exchange, industrial cybersecurity.

I. INTRODUCTION

THE RAPID expansion of IoT technology in the industrial environment (IIoT) has raised several concerns regarding data security and fair practice by servers and clients across the industrial network. Most of the IIoT infrastructure is currently highly vulnerable to malicious attacks and data leaks are easy to exploit even for unskilled malicious actors. Thus, we see that the IIoT environment requires high security and privacy. Also, frequent interactions between nodes which exchange heterogeneous data need to be supported. Integration of Blockchain Technology with IIoT devices solves many of these problems. Some advantages offered by blockchain integration are: The cryptographic techniques employed in blockchain help secure data against man-in-the-middle attacks. The immutable nature of blockchain along with its hash verification allows for data integrity and accountability for every change in the flow of data.

The use of innovative concepts like Cloud Computing, Machine Learning, Big data and Distributed Systems has ushered in a new industrial era. Industry 4.0 involves the use of these technologies to aid in the manufacturing and packaging processes of the industry. To this end, the benefits of blockchain need to be incorporated into the IIoT architecture. One such approach has been proposed in which provides an architecture for blockchain integration while securing important endpoints. In this paper, we build a similar architecture while focusing closely on maintaining trust within the environment. We also argue that a blockchain based architecture is intuitively suited for an IIoT environment if we store the data suitably.

To understand this, consider an IIoT environment where a sensor S produces some periodic data D. Now D has to be accessible to multiple devices/clients within the environment. If we store D as a transaction onto the blockchain, we guarantee availability of the data at a decentralized source, while also providing immutability. Further, if we encrypt D before broadcasting this transaction, we can allow a subset of devices to access the plaintext D using proxy re-encryption.

Thus, an intelligent design of the model can utilize blockchain in IIoT astonishingly well. Further, we discuss threats at different endpoints and the measures that can be taken

to mitigate most attacks. We implement some of the features of this model to demonstrate its working. Our work builds upon previously proposed models like the authors propose a fresh blockchain

structure that narrows down the feasibility of implementation and raises concerns regarding continued support by a largescale community apart from issues regarding performance speed. On the other hand, [3] relies on the assumption that the blockchain network is working impartially and that all updates to the blockchain will be legitimate.

This makes the architecture highly dependent on third parties and limits the flexibility of blockchain parameters like mining difficulty which can be an important trade-off parameter between security and speed of operations. Also [3] does not provide any authentication scheme to ensure that all connected IIoT devices are non-malicious. This can lead to a new form of attacks on the fog nodes when connected devices send bogus data to the fog node and adversely affect its workload, creating unreasonable overheads in the processing of legitimate data. To enhance the security of these existing models, our work proposes the following contributions:

The establishment of a private blockchain network with permissioned access. This allows for security enhancement while ensuring large-scale community support for the development platform. Our prototype uses an Ethereum-based blockchain network for this purpose. This work provides a secure solution for IoT-driven industries, enabling a protected knowledge discovery framework that helps organizations grow faster while ensuring the security of their data.

The use of an optimized and energy-efficient consensus algorithm on the blockchain. We recommend the Proof of Authority (PoA) consensus mechanism which ensures the legitimacy of the nodes involved in block validation.

In this mechanism, each validator stakes its reputation on the line when broadcasting a block. Malicious nodes would soon end up with a bad reputation and will no longer be able to broadcast blocks. Validation of connected IIoT devices by assigning a unique identifier to each device and resetting the device whitelist based on complaints from the Client. A prototype implementation tested for time taken and gas used by the exchange. Experimental results provided and their comparison with provided.

II. RELATED WORK

A. *Blockchain-Based Secure Cross-Domain Data Sharing for Edge-Assisted Industrial Internet of Things*

In the Industrial Internet of Things (IIoT), blockchain-based data-sharing frameworks can effectively build cross-domain trust and facilitate data sharing. However, secure data-sharing schemes are lacking for the IIoT scenario, in which smart devices cannot communicate across domains and can only access data through edge servers. In this study, we propose a lightweight and secure data-sharing scheme for the blockchain-enabled cross-domain IIoT, in which authorized smart devices can access cross-domain data anonymously. First, smart devices can dynamically generate pseudonyms by themselves and without the online participation of domain authorization centres, effectively reducing the storage overhead of smart devices and the workload of domain authorization centres. Second, the scheme combines broadcast encryption and proxy re-encryption techniques, which realize flexible data sharing across domains while protecting the privacy of smart devices. Detailed security proofs and analyses demonstrate that the proposed scheme is secure and resistant to various attacks. The performance analysis shows that our proposed scheme is efficient and performs better than related schemes.

B. *A blockchain based scalable domain access control framework for industrial Internet of Things*

Industrial Internet of Things (IIoT) applications consist of resource constrained interconnected devices that make them vulnerable to data leak and integrity violation challenges. The mobility, dynamism, and complex structure of the network further make this issue more challenging. To control the information flow in such environments, access control is critical to make collaboration and communication safe. To deal with these challenges, recent studies employ attribute-based access control on top of blockchain technology. However, the attribute-based access control frameworks suffer due to high computational overhead. In this paper, we propose an improved role-based access control framework using Hyperledger blockchain to deal with IIoT requirements with less computational overhead making the information control process more efficient and real-time. The proposed framework leverages a layered architecture of chain codes to implement the improved access control framework that handles the permission delegation and

conflict management to deal with the dynamism of the IIoT network. The system uses a Policy Contract, Device Contract, and Access Contract to manage the workflow of the whole access control process. Each chain code in the proposed framework is isolated in terms of its responsibilities to make the design low coupled. The integration of improved access control with blockchain enables the proposed framework to provide a highly scalable solution, tamper-proof, and flexible to manage conflicting scenarios. The proposed system outperforms the recent studies significantly in computational overhead in extensive simulation results. To verify the scalability and efficiency, the proposed is evaluated against a large number of concurrent virtual clients in simulation and statistical analysis proves that the proposed system is promising for further research in this domain.

C. End-to-end security mechanism using blockchain for industrial Internet of Things

The urgent penetration of the Industrial Internet of Things (IIoT) in industrial sectors has fostered unmatched benefits in terms of efficiency, productivity, and overall performance. Although current security frameworks already offer a sound level of protection, they do not adequately scale to the growing diversity and number of devices integrated into the Industrial Internet of Things. They rely on static, centralized network organization and management, which cannot ensure data integrity across a huge number of highly distributed devices. The proposed research provides insight into an innovative end-to-end security solution model, which caters to the needs of IIoT via the introduction of the blockchain. The current security solutions seem to fail in terms of security, scalability, data efficiency, integrity, and the actual needs of IIoT. As a result, the top chance of a cyberattack or similar threat remains high. The proposed work demonstrates that IIoTs may benefit from blockchain frameworks because blockchains reuse existing security mechanisms, enable transaction validation without central trust, and implement appropriate authorization. Additionally, the IIoT environment can benefit from implementing security frameworks that reflect their characteristics. In this paper, an overall solution that employed the decentralized setup of blockchain was proposed for authentication, authorization, and data integrity for all devices. Our approach is free from the need for any central authority. That mechanism is based on smart contracts that enforce security policies. Our

framework allows for the switching of any access rule at any time, as well as it can immediately react to some suspicious behavior. In our paper, we proposed some lightweight cryptographic schemes, and Data management overhead which could fit any device. Moreover, our algorithm for the blockchain implementation is hybrid because this approach incorporates all the best features of the private and public implementation due to the individual blocks containing feasible information rather than the entire history.

D. Blockchain based identity authentication and data interaction scheme for industrial Internet of Things

The easy, convenient and remote access to internet is definitely changing the way we live. It has also become a major factor in the financial lives of millions. Using the Internet to carry out online banking simplifies our financial affairs when compared to the traditional banking method. The inclusion of Online Banking by different sectors like health, financial, educational institutions etc. which accounts for most of the population has not only increased its importance but at the same time has attracted the cyber criminals to take the advantage of the loopholes in the process of online transaction. The cybercriminals can make use of these loopholes and carry out transaction which might not come in the knowledge of user and the bank. Recent studies have shown that the OTP which was developed as a part of two factor authentication is vulnerable to attacks. In this paper, we present a new framework for enhancing authentication during online transaction which secures our There are numerous identities in the Industrial Internet of Things (IIoT), and the security of the industrial data generated by these identity devices is crucial. However, problems such as single point of failure caused by centralization and inefficiencies of participant identity authentication are still persistent in the current IIoT. To address these problems, we propose a blockchain-based identity authentication and data interaction scheme for IIoT. In our scheme, we first design a decentralized and staged key generation authentication method based on the Sign Identity Composite (SIC), which uses key generation in stages to realize efficient identity authentication based on Schnorr's non-interactive zero-knowledge proof. Then, we propose asynchronous data interaction based on the Diffie–Hellman (DH) key negotiation algorithm and SIC. Finally, we prove the security of our scheme through security analysis, and the performance is evaluated and analysed by

simulation experiments. The results show that our scheme can perform identity authentication and asynchronous data interaction while maintaining security, outperforms the comparison scheme.

III. PROPOSED METHODOLOGY

Thus, we propose a four-layer security architecture that isolates industrial devices from user-oriented layers and maintains a record of all registered devices within the organization to prevent malicious devices from corrupting the database and the discovery process. Further, by choosing Proof of Authority (PoA), we ensure the fair functioning of the Blockchain nodes. The cryptographic techniques employed in blockchain help secure data against attacks.

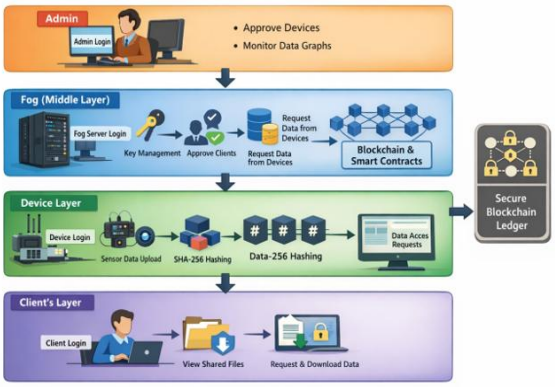
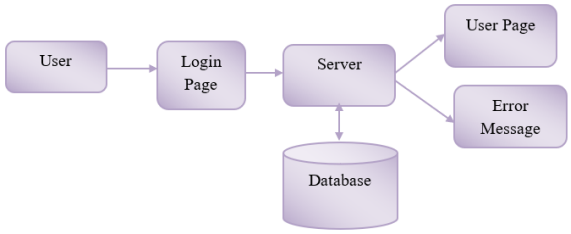


Fig. 1: System Overview

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.

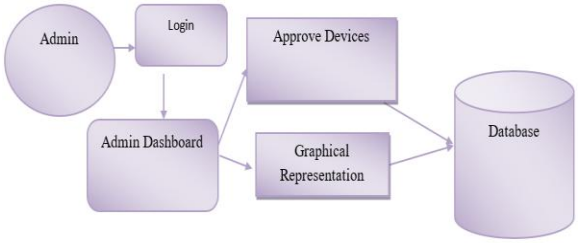
If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used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



2. Admin

The administrator plays a crucial role in managing and securing the system. The administrator can log in to the platform using a valid user ID and password, ensuring that only authorized personnel can access administrative functions. After successful authentication, the administrator is responsible for approving devices in the device layer before they are allowed to participate in the system. This approval process helps prevent unauthorized or malicious devices from entering the network and corrupting data or disrupting operations.

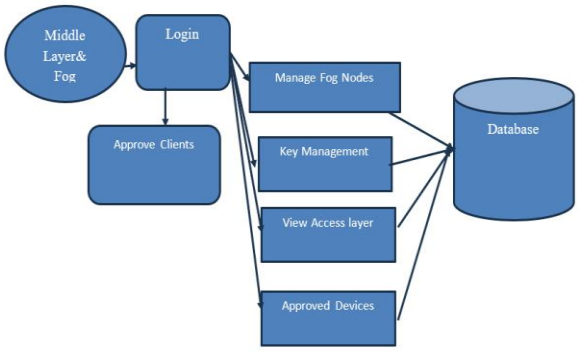
Additionally, the administrator has access to a graphical representation of system data, which provides a clear and intuitive overview of device activities, data exchanges, and system performance. These visual dashboards assist the administrator in monitoring real-time data flow, identifying anomalies, and making informed decisions. By combining secure login, controlled device approval, and graphical data visualization, the administrator ensures system reliability, transparency, and effective management within the industrial automation environment.



3. Middle Layer

The fog server operates in the middle layer and acts as an intermediary between the device layer and the user layer. Access to the fog server requires a valid user ID and password, ensuring that only authorized entities can control and manage data operations. The fog layer plays a critical role in regulating data flow by approving clients before allowing them to participate in the system. Only clients that have been verified and authorized by the fog are granted permission to access resources.

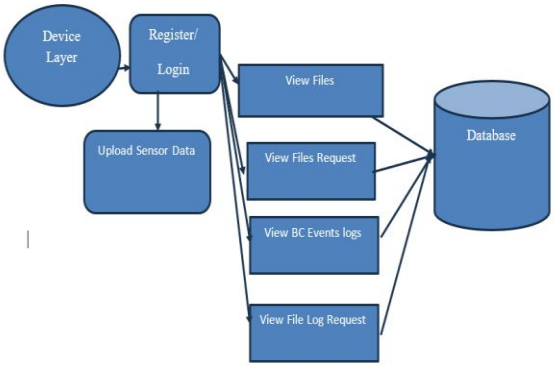
The fog server is responsible for managing nodes within the network and maintaining secure communication among them. It securely shares private keys with approved clients and performs key validation to ensure data confidentiality and integrity. Additionally, the fog server can examine data from the access layer, submit data requests to devices, and wait for device approval. Once the devices authorize the request, the fog server retrieves the required data. This controlled process ensures secure, authenticated, and efficient data exchange across the system.



4. Device Layer

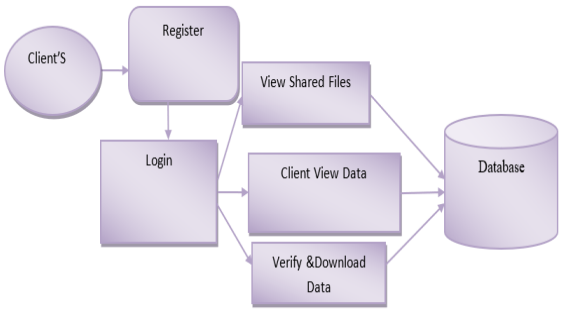
The device layer is responsible for data generation, registration, and secure interaction with higher layers of the system. Initially, each device must be registered by providing its relevant details in the device layer. Only after the administrator approves

the registered device is it allowed to participate in the network. Once approved, the device can log in using a unique user ID and password, ensuring authenticated access. After successful login, the device uploads sensor data to the system. For enhanced security and integrity, the uploaded data is divided into three separate blocks. A SHA-256 hash is generated for each data block, allowing the system to verify data integrity and detect any unauthorized modification. These hash values are stored and later used for validation during data exchange and retrieval. The device layer also provides a file-view interface, enabling devices to view previously uploaded data files. Additionally, devices can view file requests submitted by clients through the fog layer and decide whether to approve or reject those requests. Blockchain event records related to data uploads, access requests, and approvals are visible at the device layer, ensuring transparency and traceability.



5. Clients

The client layer enables authorized users to securely access and request data from the system. Initially, the client must register by providing the required personal or organizational details. After successful registration, the client can log in using a valid user ID and password, ensuring secure and authenticated access to the platform. Once logged in, the client can view shared files that are stored securely in the database and made available through approved data-sharing mechanisms. The client is allowed to examine available data resources and submit requests for specific files or sensor data as needed. Each request is carefully validated by the fog layer and the respective device owner to ensure authorization and data integrity. Only after the request is approved are the requested files made available for download. This controlled approval-based mechanism ensures secure data access, prevents unauthorized usage, and maintains accountability within the system.



6. ID Generation & Data Retrieval Module

Every database uploaded by an operator is assigned a unique blockchain-linked ID for tracking and retrieval. The system generates this ID using SHA-256 hashing of the data and metadata, making it tamper-proof and unique across the blockchain network. Users can later retrieve data by simply entering this ID into the system. The retrieval process verifies the ID against the blockchain ledger to confirm integrity before fetching the corresponding encrypted data blocks. This guarantees that users always access the original and untampered version of the data.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed blockchain-based security architecture enables secure data exchange and knowledge discovery with reasonable resource consumption in industrial cloud environments. The use of Proof of Authority (PoA) consensus and whitelist-based access control ensures the legitimacy of participating devices and blockchain nodes. Smart contracts provide secure and accountable data exchange with acceptable execution time. Overall, the framework demonstrates an efficient, scalable, and secure solution for blockchain-integrated knowledge discovery in cloud-based industrial systems.

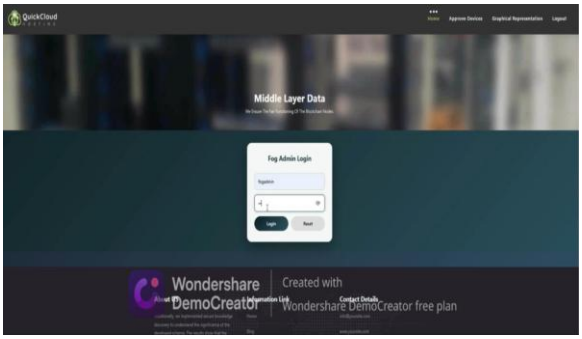


Fig. 2: Admin Login

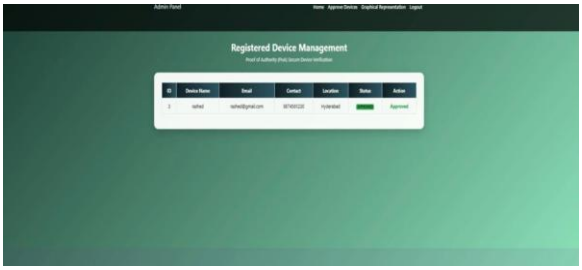


Fig. 3: Registered Devices

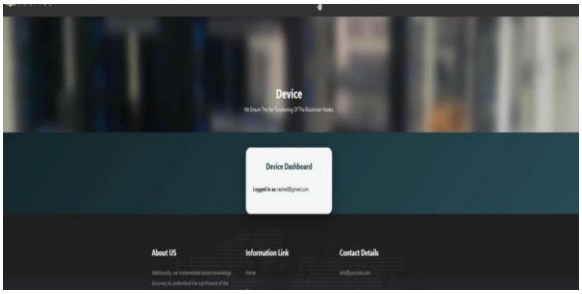


Fig. 4: Device Dashboard

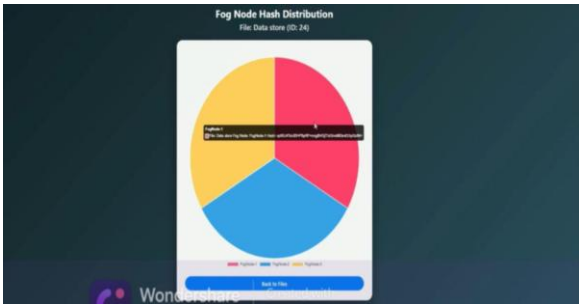


Fig. 5: Hash Distribution

V. CONCLUSION

This paper provides an overview of recent work carried out in securing IIoT infrastructure and operations using Blockchain Technology and other innovative concepts. This is followed by a summary of the works, their key contributions, and shortcomings which provide research gaps. Further, based on past work, we provide a four-layer architecture for secure data sharing in an industrial environment while implementing security at various critical endpoints. We present a hybrid scheme of request management and demonstrate that our model theoretically satisfies the key security requirements for industry operations. Our implementation of this model utilizes the Ethereum blockchain platform and runs the Cloud, Client, and Fog Nodes on Ubuntu-based machines. We have used the SHA-256 hash algorithm commonly used with Ethereum and the AES algorithm for message encryption. The scalability of the model is dependent on aspects like the performance of the controller contract and the initialization and encryption procedures. The overall performance is also important as TCP message relays also take non-negligible time. Thus, we measured the time taken for these operations and the overall time separately. The results indicate that our additional security measures at the fog node (whitelisting) and the validation of IIoT Devices before addition to the whitelist all occur within a very reasonable amount of time.

REFERENCES

[1] M. Wollschlaeger, T. Sauter, and J. Jasperneite, “The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0,” IEEE Ind. Electron. Mag., vol. 11, no. 1, pp. 17–27, Mar. 2017.

[2] J. Wan, J. Li, M. Imran, D. Li, and F. E. Amin, “A blockchain-based solution for enhancing security and privacy in smart factory,” IEEE Trans. Ind. Informat., vol. 15, no. 6, pp. 3652–3660, Jun. 2019.

[3] J. Sengupta, S. Ruj, and S. Das Bit, “FairShare: Blockchain enabled fair, accountable and secure data sharing for industrial IoT,” IEEE Trans. Netw. Service Manag., vol. 20, no. 3, pp. 2929–2941, Sep. 2023.

[4] P. Gupta, S. S. Kanhere, and R. Jurdak, “A decentralized IoT data marketplace,” 2019, arXiv:1906.01799.

[5] M. Benedetti et al., "A PoW-less Bitcoin with certified Byzantine consensus," 2023, arXiv:2207.06870.

[6] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in Proc. 11th Int. Workshop Pract. Theory Public Key Cryptogr. (PKC), 2008, pp. 360–379.

[7] M. Soori, F. K. G. Jough, R. Dastres, and B. Arezoo, "Blockchains for industrial Internet of Things in sustainable supply chain management of industry 4.0, a review," Sustain. Manuf. Service Econ., vol. 3, Jul. 2024, Art. no. 100026.

AUTHORS Profile



Mrs. RAVULA ANITHA has received her B.Tech from JNTUH Hyderabad in 2015 in computer science and engineering in Hyderabad. And M.Tech from JNTUH University, Hyderabad in 2019, in Computer science and Engineering. She has been dedicated to teaching for the last 5.5 years. At present she is working as Assistant professor in CSE department at Gurunanak institution technical campus, Ibrahimpatnam, telangana, India.



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



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



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