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

Research Paper

DYNAMIC AES ENCRYPTION AND BLOCKCHAIN KEY MANAGEMENT: A NOVEL SOLUTION FOR CLOUD DATA SECURITY

PIRANGI HYMAVATHI [1], DARAM LIKHITHA [2], KARNATAPU HARI CHANDANA[3], KATTA SAI SRUJAN REDDY[4], GUNDLAPALLY RAJESH [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— In the rapidly evolving realm of cloud computing security, this paper introduces an innovative solution to address persistent challenges. The proliferation of cloud technology has brought forth heightened concerns regarding data security, necessitating novel approaches to safeguarding sensitive information. The issue centers on the vulnerability of cloud-stored data, usually necessitating enhanced encryption and key management strategies. Traditional methods usually fall short in mitigating risks associated with compromised encryption keys and centralized key storage. To combat these challenges, our proposed solution encompasses a two-phase approach. In the first phase, dynamic Advanced Encryption Standard (AES) keys are generated, ensuring each file's encryption with a unique and ever-changing key. This approach significantly enhances file-level security, curtailing an attacker's ability to decrypt multiple files even if a key is compromised. The second phase introduces blockchain technology, where keys are securely stored with accompanying metadata, bolstering security and data integrity. Elliptic Curve Cryptography (ECC) public key encryption enhances security during transmission and storage, while also facilitating secure file sharing. In conclusion, this comprehensive approach enhances cloud security, providing robust encryption, decentralized key management, and protection against

unauthorized access. Its scalability and adaptability make it a valuable asset in contemporary cloud security paradigms, assuring users of data security in the cloud.

Index Terms – Cloud security, cloud computing, Advanced Encryption Standard (AES), dynamic key generation, blockchain, Elliptic Curve Cryptography (ECC), key management, secure file sharing, data encryption, decentralized storage, data integrity, access control.

I. INTRODUCTION

Given that cloud computing stands as one of the pervasive technologies within the Information Technology (IT) sector, it presents a set of advantages which are: encompassing virtualization, extensive scalability, cost-efficiency, remote data processing, and the provision of on-demand clients centric sharing services. It is useful for different areas in IT, including business applications, educational platforms, and especially, data storage and sharing enabled by cloud services. Cloud storage exhibits several salient characteristics, including immediate availability, affordability, accessibility, ease, reliability, flexibility, and a wide range of leasing choices. Furthermore, cloud computing is underpinned by critical attributes such as security, scalability, economic efficiency, accessibility, data recovery capabilities, and optimized resource utilization. Trust emerges as a pivotal concern when contemplating the transfer of user data to cloud environments, representing a significant challenge in the relationship between users and cloud service providers. Users of cloud storage services necessitate clear visibility and assurance regarding the security and integrity of their data stored in the cloud, given the limited means for monitoring stored data. To address this imperative and foster broad user acceptance, a multitude of data and resource protection strategies have been introduced and integrated within the domain of cloud security, leveraging contemporary cryptographic algorithms. Data protection through encryption in the cloud entails the implementation of robust security measures to safeguard customer data within server centers against external and internal threats, facilitated by encryption algorithms. Two primary categories of encryption methods, supported by cryptographic keys, are symmetric and asymmetric cryptography. The selection between these methods hinges on the number of keys employed: one key for symmetric cryptography and a pair of keys for asymmetric encryption/decryption. The

use of larger and more intricate keys enhances the security of encryption algorithms and renders attacks more formidable. Conversely, cloud users have the opportunity to bolster trust and enhance data protection when engaging in outsourcing and cloud services by harnessing the innovative and emerging technology of Blockchain. Blockchain security offers a more complex and reliable paradigm than centralized database security. Blockchain works by keeping track of documents in a ledger that are safely connected to earlier blocks using cryptographic hash algorithms. A blockchain is a type of distributed ledger that is used to record transactions and prevent tampering. Usually run via a peer-to-peer network, the Blockchain is designed specifically to prevent unwanted manipulation. As a result, Blockchain can furnish security measures on par with those found in central database storage, effectively averting potential attacks and data breaches from a managerial perspective. Furthermore, in scenarios where data transparency is imperative, Blockchain's inherent attribute of openness can facilitate the necessary level of data transparency.

Because of these unique benefits, Blockchain is used in a variety of industries, such as finance and the Internet of Things (IoT) ecosystem, and its use is expected to grow dramatically. In light of its effectiveness and accessibility, numerous IT environments have embraced cloud computing. Consequently, there has been a heightened focus on exploring critical security facets concerning cloud security and privacy issues. This paper introduces a novel approach aimed at enhancing file storage security within the cloud infrastructure. This approach leverages a hybrid dynamic encryption technique, incorporating elements of Elliptic Curve Cryptography, Advanced Encryption Standard, and Blockchain technology. The primary objective is to establish a highly secure environment conducive to elevating the overall security of cloud-based storage solutions. Dynamic AES File Encryption: The article introduces an innovative approach to file encryption utilizing the Advanced Encryption Standard (AES). This method is characterized by its dynamic and efficient key generation mechanism, which bolsters the security of file storage in the cloud. Blockchain-Powered Key Security: A notable contribution lies in the integration of Blockchain technology to secure cryptographic keys within the cloud environment. This ensures the robust protection of encryption keys and safeguards against potential security breaches. User-

Friendly Key Management: The article streamlines the process of key management for end-users. This simplification empowers users to efficiently manage the substantial volume of dynamic keys required for encryption tasks, thereby enhancing usability and security in cloud-based storage systems.

II. RELATED WORK

A. Blockchain aware proxy re-encryption algorithm based data sharing scheme

The "Blockchain-Aware Proxy Re-Encryption Algorithm-Based Data Sharing Scheme" is a novel approach designed to enhance secure data sharing and privacy in distributed systems. It combines the security features of proxy re-encryption (PRE) with the decentralized trust model of blockchain technology. In this scheme, a proxy server is used to facilitate data sharing between a data owner and a recipient, without the proxy gaining access to the plaintext data. The re-encryption process is controlled through cryptographic keys, ensuring confidentiality. By incorporating blockchain, the system ensures that all access requests, re-encryption processes, and transactions are securely recorded in an immutable ledger, providing transparency, accountability, and tamper-resistance. This hybrid approach helps address key challenges such as unauthorized data access, data integrity, and scalability while enabling efficient and privacy-preserving data sharing across various platforms.

B. Dynamic multimedia encryption using a parallel file system based on multi-core processors

The "Dynamic Multimedia Encryption Using a Parallel File System Based on Multi-Core Processors" project focuses on enhancing the security and efficiency of multimedia data encryption by leveraging the power of parallel computing through multi-core processors. The system dynamically encrypts multimedia files, such as images, videos, and audio, ensuring robust protection against unauthorized access.

By utilizing a parallel file system, the encryption process is distributed across multiple cores, significantly speeding up the encryption and decryption operations, making it ideal for handling large multimedia datasets. This approach optimizes computational resources, improves processing time, and ensures scalability, while maintaining high-level encryption standards. The project addresses the growing need for secure, high-performance solutions for multimedia content, providing a secure environment for sensitive media and

improving the overall user experience in content delivery and storage systems.

C. *Modified advanced encryption standard (MAES) based on non-associative inverse property loop*

The "Modified Advanced Encryption Standard (MAES) Based on Non-Associative Inverse Property Loop" project introduces an innovative enhancement to the widely used AES encryption algorithm by incorporating a non-associative inverse property loop. This modification aims to improve the security and resistance of AES against certain cryptographic attacks, such as brute force and side-channel attacks. By leveraging non-associative properties, the project alters the standard AES transformation steps, creating a more complex and less predictable encryption process.

This added layer of complexity makes it more difficult for attackers to reverse-engineer or break the encryption, while maintaining the efficiency and scalability of AES. The project explores the potential of combining mathematical properties with established cryptographic techniques to offer a more robust and advanced encryption solution, making it suitable for applications that demand heightened security, such as financial services, government communications, and secure data transmission.

D. *Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey*

The project "Elliptic Curve Cryptography: Applications, Challenges, Recent Advances, and Future Trends – A Comprehensive Survey" provides an in-depth analysis of elliptic curve cryptography (ECC), a powerful cryptographic technique that uses the algebraic structure of elliptic curves over finite fields to secure communications. The project surveys the diverse applications of ECC, ranging from secure key exchange and digital signatures to blockchain and cryptocurrency technologies. It examines the challenges ECC faces, including computational complexity, security vulnerabilities, and its adoption in various industries. The survey also highlights recent advancements in ECC, such as improved algorithms, optimization techniques, and enhancements in performance, along with innovations that strengthen ECC's security. Finally, the project discusses emerging trends and future prospects of ECC, focusing on its potential in next-generation encryption

systems, quantum resistance, and integration with emerging technologies like the Internet of Things (IoT) and cloud computing. The project serves as a comprehensive guide for researchers, engineers, and practitioners looking to understand ECC's evolving role in modern cryptography.

III. PROPOSED METHODOLOGY

In the first phase, dynamic Advanced Encryption Standard (AES) keys are generated, ensuring each file's encryption with a unique and ever-changing key. This approach significantly enhances file-level security, curtailing an attacker's ability to decrypt multiple files even if a key is compromised.

The second phase introduces blockchain technology, where keys are securely stored with accompanying metadata, bolstering security and data integrity. Elliptic Curve Cryptography (ECC) public key encryption enhances security during transmission and storage, while also facilitating secure file sharing. In conclusion, this comprehensive approach enhances cloud security, providing robust encryption, decentralized key management, and protection against unauthorized access. Its scalability and adaptability make it a valuable asset in contemporary cloud security paradigms, assuring users of data security in the cloud.

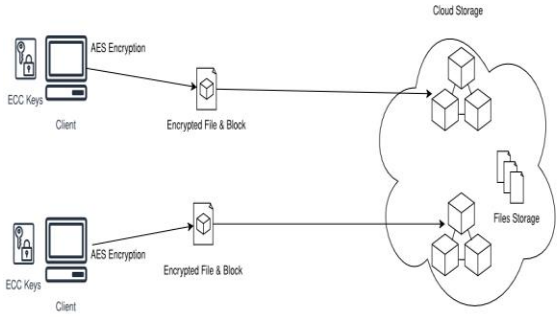
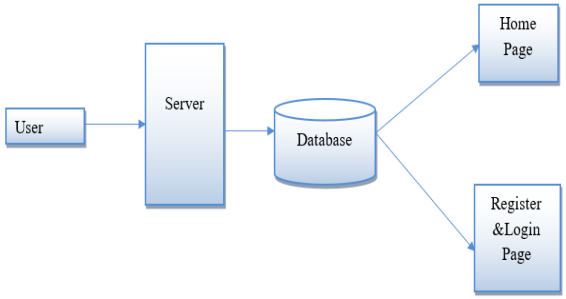


Fig. 1: System Overview

1. User Interface Design

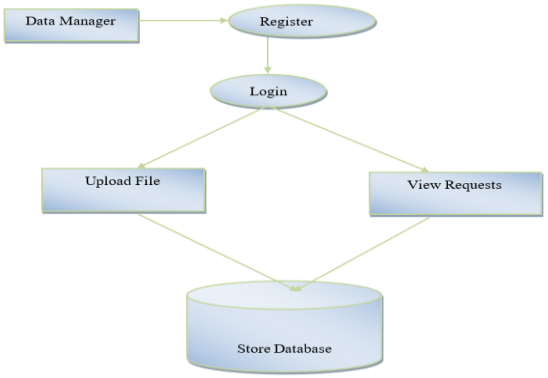
In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server.

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.



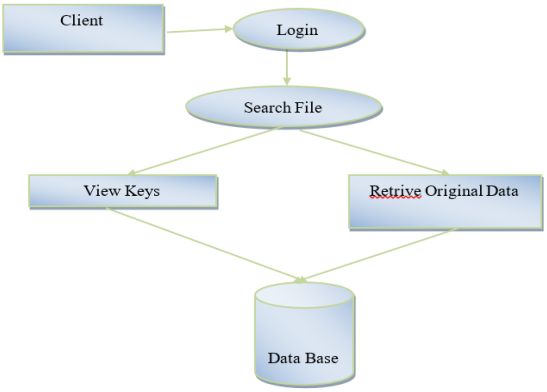
2. Data Manager

In this context, the data manager plays a crucial role in managing and securing the sensitive data stored in the Cloud Data Warehouse (CDW). The data manager will also monitor the storage and sharing of data, ensuring that only authorized individuals have access to sensitive files, and that security measures remain intact throughout the lifecycle of the data. The data manager will upload the text file and he will view the requests sent by the users and provide the private keys.



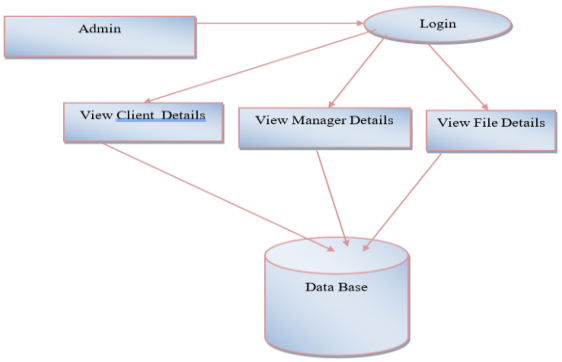
3. Client

The user is an authorized individual who interacts with the Cloud Data Warehouse (CDW) to perform searches over the encrypted data cubes. Users are granted access based on the access control policies defined by the data owner, and they are provided with the necessary decryption keys to retrieve the query results. When a user submits a search query, they provide the relevant private key to search through the encrypted data cubes stored in the cloud.



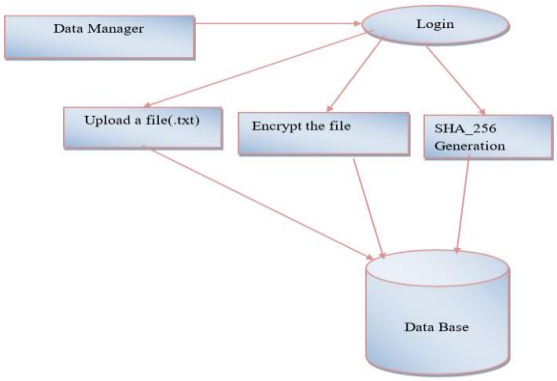
4. Admin

The admin acts as the administration in this project where he will have all the client details, all the manager details and all the file details and he can retrieve all the information present in client and manager database. He has the right to check whatever the files uploaded by the manager also. He can retrieve all the file details uploaded by data manager also. Therefore, here admin will have the all the information about clients and mangers and files uploaded by managers also.



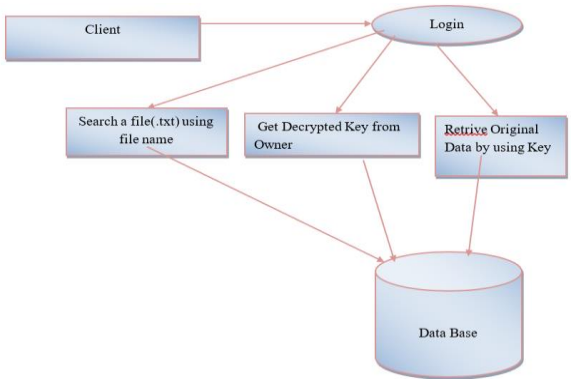
5. Upload

When a user uploads a file, the system first generates a dynamic AES key specifically for that file, ensuring that each file is encrypted with a unique and constantly changing encryption key. This dynamic key management mechanism strengthens file-level security by reducing the risk of decryption even if one key is compromised. Additionally, the encryption process is further enhanced by utilizing Elliptic Curve Cryptography (ECC) during the transmission of the file, ensuring that the file is securely encrypted during the upload process, protecting it from unauthorized interception.



6. Search

When a user initiates a search for a particular file, the system ensures that only authorized users can access the file by verifying their credentials and ensuring that the encryption keys necessary for decryption are securely retrieved. As the files are stored with unique dynamic AES keys, the search process includes a mechanism that checks the file's associated metadata and verifies the correct key for decryption. The search process is, therefore, designed to be both secure and efficient, ensuring that users can retrieve their files while maintaining confidentiality and integrity.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed dynamic AES encryption with blockchain-based key management significantly improves cloud data security. The use of unique AES keys for each file

reduces the risk of data exposure, while blockchain provides secure and tamper-resistant key storage. The integration of Elliptic Curve Cryptography (ECC) further enhances secure key exchange and file sharing. Overall, the framework offers a scalable, efficient, and secure solution for protecting cloud-stored data against unauthorized access.

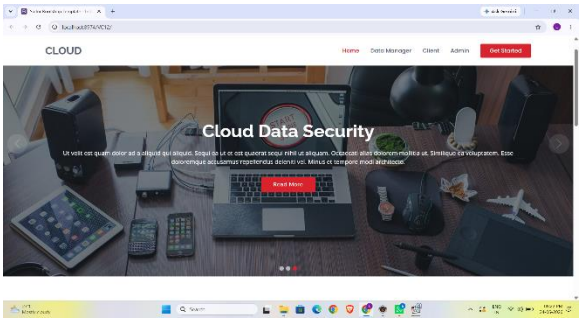


Fig. 2: Home Page

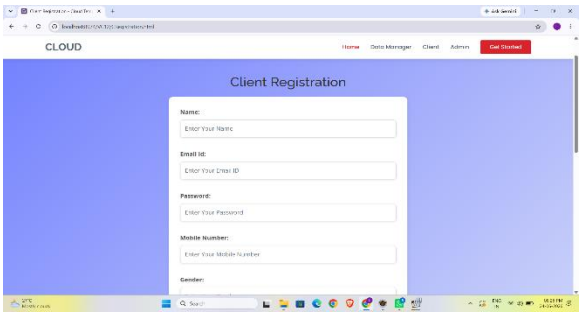


Fig. 3: Registration

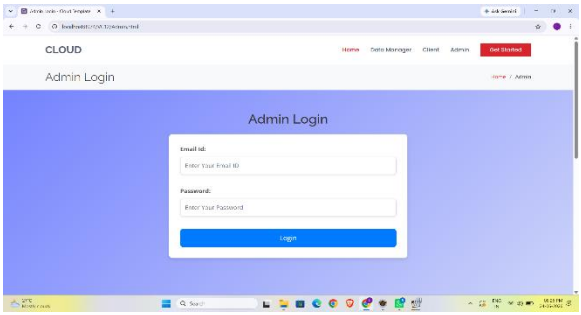


Fig. 4: Login

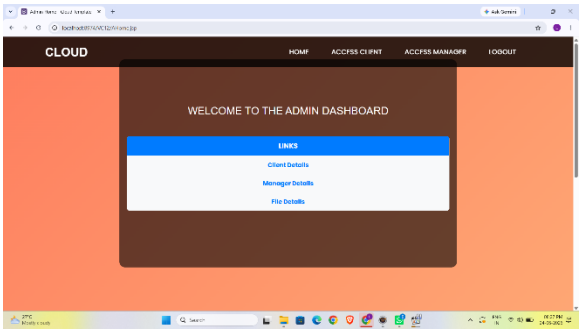


Fig. 5: Admin Dashboard

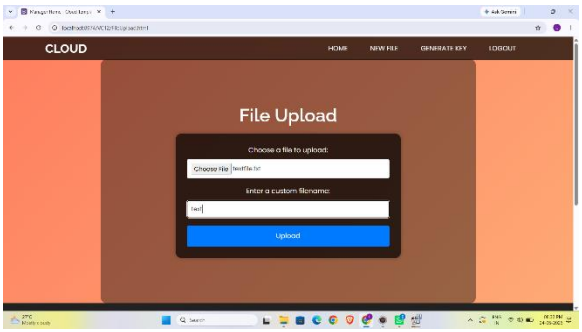


Fig. 6: Upload File

V. CONCLUSION

In this paper, a comprehensive and innovative solution to address critical security concerns in cloud computing environments has been introduced. The suggested approach utilizes an ECC, AES, and Blockchain hybrid dynamic encryption method, which being a multi-layered defense mechanism ensures high degree of security for sensitive data. In the process, widely regarded security issues in cloud computing have been explained, specifically, the deficiency of centralized key management and the necessity of privacy reinforcement.

The proposed answer, acting in two stages, is quite solid to the problems that have been discovered. At first, dynamic AES keys are created to make sure each file is encrypted differently and changes often. This dynamic key generation greatly enhances file-level security, mitigating the risk of compromise. The second phase introduces the use of blockchain technology, providing an immutable and decentralized ledger to securely store encryption keys. By encrypting these blocks with ECC public keys, we ensure that unauthorized access is effectively prevented during both transmission and storage. The combined strength of these components not only bolsters the security of cloud-stored data but also enhances user trust. Users can confidently manage an array of files with distinct encryption keys using a single key stored on their device, while service providers benefit from decentralized key management. In simple words, the suggested way makes a strong and flexible security system that matches with the changing needs of cloud computing. It works well to solve security problems in cloud environments. It makes sure that the data is safe and private, while meeting the different wants of people using it or service providers.

REFERENCES

[1] R. Anandkumar, K. Dinesh, A. J. Obaid, P. Malik, R. Sharma, A. Dumka, R. Singh, and S. Khatak, ‘‘Securing e-health application of cloud computing using hyperchaotic image encryption framework,’’ Comput.Electr. Eng., vol. 100, May 2022, Art. no. 107860.

[2] Z. Bashir, T. Rashid, and S. Zafar, ‘‘Hyperchaotic dynamical system based image encryption scheme with time-varying delays,’’ Pacific Sci. Rev. A,Natural Sci. Eng., vol. 18, no. 3, pp. 254–260, Nov. 2016.

[3] W. Y. Chang, H. Abu-Amara, and J. F. Sanford, Transforming Enterprise Cloud Services. Berlin, Germany: Springer, 2010.

[4] Bhagwat, V. B. (2025). Simplifying Payroll Balance Conversions in Payroll Systems Implementation through the Use of Generative AI.

[5] N. M. Sultana and K. Srinivas, ‘‘Survey on centric data protection method for cloud storage application,’’ in Proc. Int. Conf. Comput. Intell. Comput.Appl. (ICCICA), Nov. 2021, pp. 1–8.

[6] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, ‘‘A novel effective

lightweight homomorphic cryptographic algorithm for data security in cloud computing,'' Int. J. Intell. Netw., vol. 3, pp. 16–30, 2022.

[7] Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708.

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

[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

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. DARAM LIKHITHA pursuing B.Tech degree in computer science and engineering at guru nanak institutions technical campus affiliated to JNTUH in 2022-2026.



Ms. KARNATAPU HARI CHANDANA pursuing B.Tech degree in computer science and engineering at guru nanak institutions technical campus affiliated to JNTUH in 2022-2026.



Mr. KATTA SAI SRUJAN REDDY pursuing B.Tech degree in computer science and engineering at guru nanak institutions technical campus affiliated to JNTUH in 2022-2026.



Mr. GUNDLAPALLY RAJESH pursuing B.Tech degree in computer science and engineering at guru nanak institutions technical campus affiliated to JNTUH in 2022-2026.