AN OPENSOURCE WEB APPLICATION DATA MANAGEMENT

E. MOUNIKA REDDY [1], GOLCONDA SHASHANK REDDY [2], PANJALA SAI ABHISHEK [3], CHALLA MANIDEEP [4], CHITHALURI SATHWIK [5]

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

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Managing posthumous data is becoming increasingly difficult in the digital age, and existing technological solutions frequently fall short in terms of usefulness. Most of the tools that are currently available are closed-source, opaque, do not support multiple platforms, and have restricted access control. In order to safely handle and distribute digital assets after death, this paper presents "Beyond Life," a cross-platform digital will management solution. A customized Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme known as PD-CP-ABE, which provides effective, fine-grained control over access to will content at scale, is the foundation of this solution. Beyond Life gives users more control and transparency over the creation, storage, and execution of their wills than current systems because it functions independently of service providers. Additionally, the system is portable, enabling users to switch service providers at any time. The suggested system has been thoroughly developed and tested to guarantee functionality and viability in the real world. The public is given access to the system implementation.

Index Terms – Digital will management, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), PD-CP-ABE, attribute-based encryption, digital inheritance, access control, cloud security, cross-platform system, secure data sharing, privacy preservation, digital assets, cryptography.

I. INTRODUCTION

We deal with a wide range of online services in the Internet era daily. From using email to connect with colleagues to sharing family photos on social media platforms, our digital

presence is vast and varied [4], [10]– [12]. However, have you ever wondered what happens to your data during your lifetime after you pass away? You may wish to permanently erase your digital footprints, making your digital identity vanish from the Internet, exercising the 'right to be forgotten' [13], [17], [18]. You may consider applying access controls on various accounts posthumously to prevent identity ghosting [15], [19]. You may also want to pass on your online accounts to your next of kin or friends for them to manage [14], [16]. However, most users do not have a clear digital legacy plan, and much data may be permanently lost or misused [2], [6]. Postmortem data management is often overlooked, and one of the main challenges is at the technological level and the adequacy of existing solutions [3], [14]. Our focus in this paper is the technological aspect of this emerging problem. Digital will management systems can be categorized into three main types: password management tools, native platform-provided solutions, and third-party services. However, each of these approaches has notable limitations. While helpful in organizing credentials, password management tools are not designed specifically for digital estate management and typically require users to store sensitive information in a secure vault, which may not cover all digital assets. Native platform provided tools, such as Google's Inactive Account Manager (IAM), are limited by their lack of cross-platform compatibility. This makes it difficult for users to manage digital assets spread across multiple platforms, as these tools are not customizable to individual needs and can vary in functionality depending on the provider. Moreover, they often require users to rely on the platform's continued existence, with the risk of data loss if the service is discontinued or the provider shuts down. While offering the potential to address some of these challenges, third-party solutions often struggle with trust issues, as users may be reluctant to rely on lesser known providers due to privacy concerns. These services are also frequently criticized for lacking essential features, making them impractical for widespread adoption. As a result, many third-party providers have failed to gain a significant user base and have discontinued their services [3]. This paper proposes "Beyond Life", an open-source Privacy Enhancing Technology (PET) solution for posthumous data management. The proposed solution automatically manages and distributes digital assets according to preset policies after the user's death. Using a newly designed encryption

scheme, data access rights can be flexibly and efficiently controlled on the content level. The system combines blockchain technology and multi cloud storage mechanisms to ensure transparency in the digital will system and reduce trust assumptions between entities. The proposed solution allows users to move their digital will between different service providers and generate their will content (i.e., retrieving information from various providers) locally or remotely Our key contributions are as follows:

Cross-platform Support: We design a cross platform digital will system that supports the secure management and distribution of digital assets across multiple service providers and currently supports integration with X (Social media platform), Gmail (Email) and Google Drive (Cloud storage).

Content-level Granular Access Control for Digital Wills: We develop a customized and novel Rieti of the Ciphertext-Policy Attribute-based Encryption (CP-ABE) known as PD-CP-ABE. This scheme allows for efficient and content-level fine grained access control at scale. We have evaluated the proposed solution to ensure efficacy and scalability for real-world deployment.

Decentralized and Portable Architecture: To eliminate the reliance on centralized third-party services and ensure full transparency of any action on a digital will, our system leverages blockchain as an immutable ledger for managing digital wills. The proposed system is designed to allow portability between third-party digital will service providers for a user with ease.

II. RELATED WORK

A. Data after death: Australian user preferences and future solutions to protect posthumous user data

The digital footprints of today's internet-active individuals are a testament to their lives, and have the potential to become digital legacies once they pass on. Future descendants of those alive today will greatly appreciate the unprecedented insight into the lives of their long since deceased ancestors, but this can only occur if today we have a process for data preservation and handover after death. Many prominent online platforms offer nebulous or altogether absent policies regarding posthumous data handling, and despite recent advances it is currently unclear who the average Australian would like their data to be managed after their death (i.e., social media platforms, a trusted individual, or another digital executor). While at present the management of deceased accounts is largely performed by the platform (e.g.,

Facebook), it is conceivable that many Australians may not trust such platforms to do so with integrity. This study aims to further the academic conversation around posthumous data by delving deeper into the preferences of the Australian Public regarding the management of their data after death, ultimately to inform future development of research programs and industry solutions. A survey of 1020 Australians revealed that most desired a level of control over how their data is managed after death. Australians currently prefer to entrust the management of their data to a trusted close individual or thirdparty software that they can administrate themselves. As expected, social media companies ranked low regarding both trust and convenience to manage data after death. Future research focus should be to conceptualise and develop a third-party solution that enables these preferences to be realised. Such a solution could interface with the major online vendors (social media, cloud hosting etc.) to action the deceased's will.

B. Digital legacy: A systematic literature review

To more effectively support the dying and bereaved in end-of-life contexts, over the past two decades HCI and social computing scholars have sought to understand digital legacy. In this paper, we argue that it is time to take stock of digital legacy scholarship, examining what we know, what gaps remain, and what areas are imperative for future work. Through a Grounded Theory Literature Review, we identify four foci in digital legacy research to date: how identity is navigated in the passing of digital legacy, how digital legacies are engaged with, how digital legacies are put to rest, and how technology interfaces with offline legacy technologies. Based on our analysis, we present a model depicting how digital legacy research examines a lifecycle of data as it is passed down. This model identifies that digital legacy data moves through three stages: encoding, accessing, and dispossessing. The model illustrates gaps in current research and charts possible inflection points for future social computing research. Specifically, we highlight the importance of multi-user and multi-generational networks of people in end-of-life scenarios. Additionally, the model exhibits emerging theoretical findings and major concepts in the nascent field of digital legacy research.

C. The right to be forgotten in the digital age

This article explores the challenges of the extraterritorial application of the right to be forgotten and, more broadly, of EU data protection law in light of the recent case law of the ECJ. The paper explains that there are good arguments for the EU to apply its high data protection standards outside its borders, but that such an extraterritorial application faces challenges, as it may clash with duties of international comity, legal diversity, or contrasting rulings delivered by courts in other jurisdictions. As the article points out from a comparative perspective, the protection of privacy in the digital age increasingly exposes a tension between efforts by legal systems to impose their high standards of data protection outside their borders – a dynamic which could be regarded as 'imperialist' – and claims by other legal systems to assert their own power over data – a dynamic which one could name 'sovereigntist'. As the article suggests, navigating between the Scylla of imperialism and the Charybdis of sovereigntist will not be an easy task. In this context, greater convergence in the data protection framework of liberal democratic systems worldwide appears as the preferable path to secure privacy in the digital age.

D. Ciphertext-policy attribute-based encryption

In several distributed systems a user should only be able to access data if a user possess a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

III. PROPOSED METHODOLOGY

This paper proposes ”Beyond Life”, an open-source Privacy Enhancing Technology (PET) solution for posthumous data management. The proposed solution automatically manages and distributes digital assets according to preset policies after the user’s. Using a newly designed encryption scheme, data access rights can be flexibly and efficiently controlled on the content level. The system combines blockchain technology and multi load storage mechanisms to ensure transparency in the digital will system and reduce trust assumptions between entities. The proposed solution allows users to move their digital will between different service providers and generate their will content.

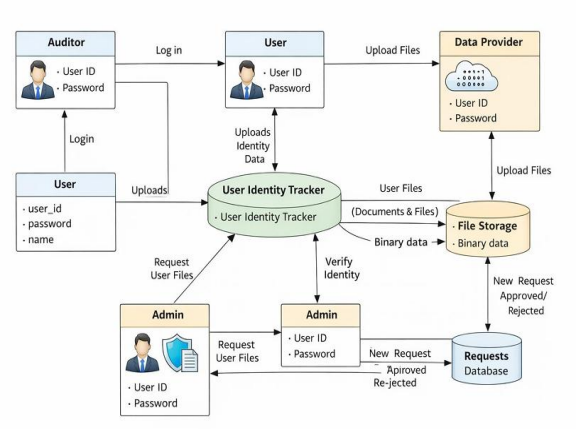
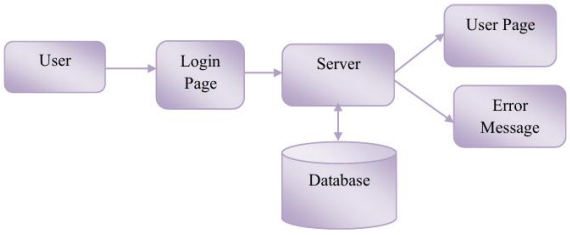


Fig. 1: System Overview

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.

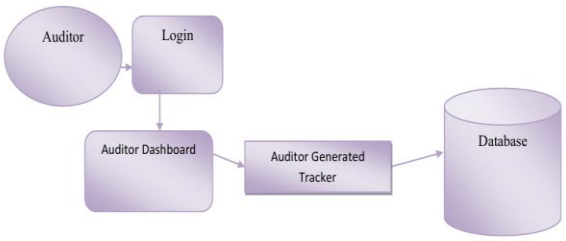
If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used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



2. Auditor

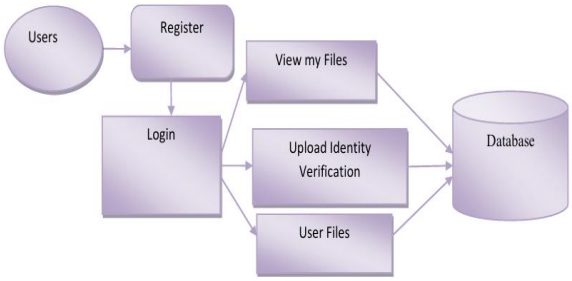
The auditor module is a key component for ensuring security and accountability in the system. The auditor logs in using a secure user ID and password, which verifies their identity before granting access to sensitive auditing functions. This authentication prevents unauthorized access and ensures that only authorized auditors can oversee system operations. To manage user identities, the auditor maintains a tracker that generates unique identifiers for each registered user. These identities are used for access control, encryption, and auditing, ensuring that each user is distinct, verifiable, and tamper-

resistant. The tracker supports fine-grained access policies by linking user attributes to their identities, enabling secure, attribute-based encryption mechanisms. Moreover, the tracker provides traceability for all system activities. Every access request, key usage, and data operation is logged against a specific identity, supporting accountability, non repudiation, and forensic analysis. This mechanism ensures transparency, prevents identity misuse, and strengthens overall system security.



3. Users

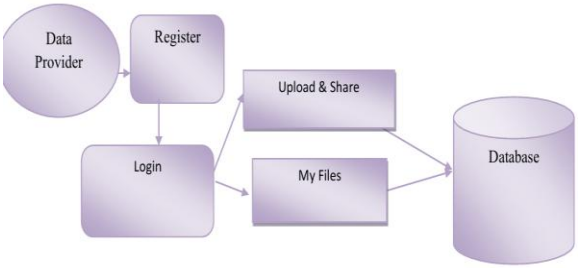
In this system, a user can log in using a unique user ID and a secure password, ensuring that only authorized individuals gain access. Once logged in, the user can view their files stored within the system. For verification purposes, if the user needs to obtain the original version of any data, they are required to upload proof of identity. This step ensures that sensitive or confidential files are accessed only by verified users, adding a layer of security. The system distinguishes between general file access and full access: while basic viewing allows users to see their files, accessing all files including original and sensitive data requires the user to authenticate their identity through the upload process. This design maintains data confidentiality, prevents unauthorized access, and ensures that users can verify and manage their information securely within a controlled environment.



4. Data Provider

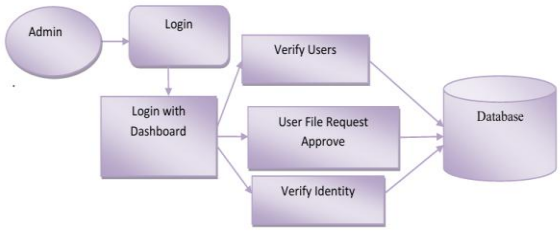
In this system, the data supplier maintains a registry containing important information, ensuring that records are organized and accessible. To access the system, the data provider must log in using a unique user ID and a secure password, which guarantees that only authorized personnel can upload or manage data. The data provider can upload various types of files, including documents, images, or PDF files. Once uploaded, these files are processed by an algorithm that converts them into binary form, enabling secure storage and efficient handling within

the system. This transformation ensures that the files are standardized and can be used for further processing or verification. After uploading, the data supplier has the ability to view the files, allowing them to monitor, manage, and validate the uploaded content. This approach maintains data integrity, ensures secure access, and provides a reliable method for managing files in digital form.



5. Admin

In this system, the administrator has secure access through a user ID and password, ensuring that only authorized personnel can manage user activities. One of the administrator's key responsibilities is user verification. When a user requests access to files or submits identification, the administrator examines the provided credentials to confirm authenticity. User file requests are carefully reviewed and can be approved by the administrator based on verification results. If the user's identification matches the records, the administrator can verify the user's identity and retrieve the necessary data for processing or validation. This ensures that sensitive information is shared only with verified individuals. Furthermore, the administrator is responsible for confirming and validating the integrity of the data, maintaining system security and reliability. By overseeing identity verification and file approvals, the administrator enforces strict access control, prevents unauthorized access, and ensures that users can securely interact with 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 open-source web application securely manages digital assets using the PD-CP-ABE encryption scheme, providing fine-grained access control and privacy protection. Functional testing confirms reliable will creation, storage, and authorized data sharing across multiple platforms. The system also supports portability, allowing users to switch service providers without losing access to their encrypted data.

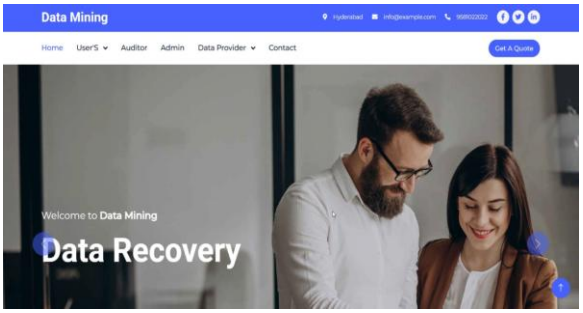


Fig. 2: Home Page

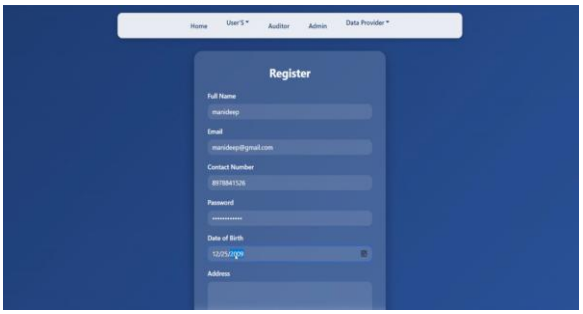


Fig. 3: Registration

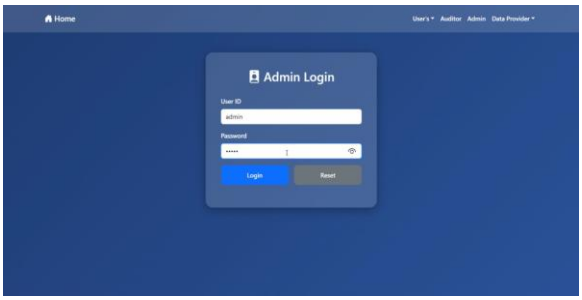


Fig. 4: Login

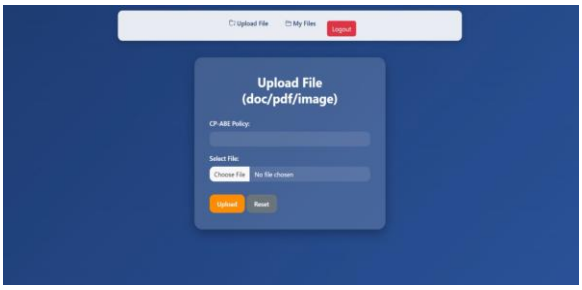


Fig. 5: Upload File

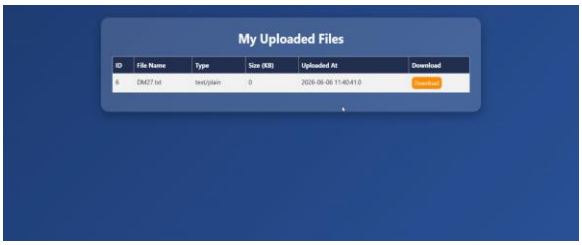


Fig. 6: Uploaded Files

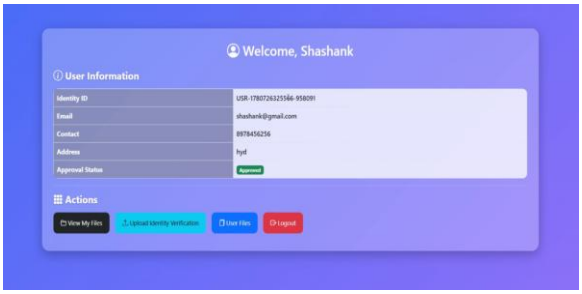


Fig. 7: User Information

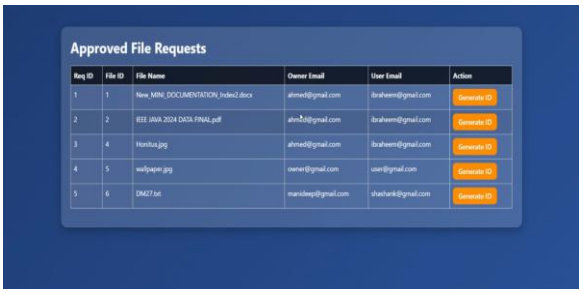


Fig. 7: Approved Files

V. CONCLUSION

This paper presents an open-source and Privacy Enhancing Technology (PET) for a third-party digital will management solution. 'Beyond Life' securely and efficiently manages the posthumous distribution of users' digital assets at content-level granularity, leveraging a novel and efficient version of CP-ABE called PD-CPABE. We take a step forward to address technological gaps identified in the most recent studies (e.g., [3]) and devise a solution that addresses requirements specified for a working solution, including cross-platform support, decentralization, and portability. Leveraging blockchain technology and multi-cloud storage mechanisms, we bring transparency and control to address users' trust concerns when using a third-party solution for digital will management. The solution supports various deployment models, allowing users to customize their will's generation, storage, and processing (e.g., local or remote service).

We have not studied legal and usability issues associated with 'Beyond Life'. Further, we acknowledge the proposed solution required further technological refinements and extensions to optimise the user experience. From a security perspective, we believe there is a need to design solutions against various protocols and threat models in this domain before third-party digital will management solutions can be used at scale and in the real world. As the first opensource solution for digital will management, 'Beyond Life' facilitates faster progress towards addressing gaps by helping research to be less theoretical and more pragmatic.

REFERENCES

[1] R. Gulotta, A. Kelliher, and J. Forlizzi, "Digital systems and the experience of legacy," in *Proceedings of the 2017 Conference on Designing Interactive Systems*, Edinburgh, United Kingdom, 2017, pp. 663–674. Available: https://doi.org/10.1145/3064663.3064731

[2] A. Shaghaghi, P. Scolyer-Gray, and D. Ashenden, "Digging your own digital grave: How should you manage the data you leave behind," *The Conversation*, Aug. 2020. [Online]. Available: - should-you-manage-the-data-you-leave-behind-143755. [Accessed: Nov. 21, 2023].

[3] A. Reeves, A. Shaghaghi, S. Krebs, and D. Ashenden, ”Data after death: Australian user preferences and future solutions to protect posthumous user data,” *arXiv*. [Online]. Available: https://arxiv. org/abs/2407.01282. [Accessed: Aug. 01, 2024].

[4] J. Jargon, ”A plan for your digital life after death,” *The Wall Street Journal*, Apr. 2023. [Online]. Available: https://archive.md/ yffGZ#selection-109.5-109.45. [Accessed: Nov. 20, 2023].

[5] M. E. Locasto, M. Massimi, and P. J. DePasquale, ”Security and privacy considerations in digital death,” in *Proceedings of the 2011 New Security Paradigms Workshop*, New York, NY, USA, 2011, pp. 1–10. Available:

[6] J. Connor, ”Digital life after death: The issue of planning for a person’s digital assets after death, ” *Texas Tech Law School Research Paper (2011-02)*, SSRN, 2010. Available: https://doi. org/10.2139/ssrn.1811044. [Accessed: Nov. 21, 2023].

[7] J. C. Shah, M. Bhagwat, D. Patel, M. Conti, ”Crypto-wills: Transferring digital assets by maintaining wills on the blockchain,” in *Communication and Intelligent Systems, ICCIS 2019. Lecture Notes in Networks and Systems, vol. 120*, B. Bansal, M. Gupta, H. Sharma, and B. Agarwal, Eds., Springer, Singapore, 2020, pp. 1-10. Available: https://doi.org/10.1007/978-981 15-3325-9 31.

[8] W. Entriken, D. Shirley, J. Evans, and N. Sachs, ”Ethereum improvement proposals,” 2018. [Online]. Available: https://eips. ethereum.org/EIPS/eip-721. [Accessed: Apr. 21, 2024].

[9] Nico, ” Ethereum, ” 2024. [Online]. Available: en/developers/docs/standards/tokens/erc-20/. [Accessed: July. 03, 2024].

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



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



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



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



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