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

AASSI: A SELF-SOVEREIGN IDENTITY PROTOCOL WITH ANONYMITY AND ACCOUNTABILITY

MODUKURU PRADEEP [1], DANNAVARAM SHASHANK [2], KOTLA ADITHYA VARDHAN REDDY [3], MALLELA KARTHIK [4], PUTTI AKASH [5]

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

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

ABSTRACT— The concern and opposition to centralized management of user identities by third-party authorities have led to the emergence of Self-Sovereign Identity (SSI). With the help of blockchain, SSI effectively restore users' control over their own identities, but privacy concerns due to blockchain transparency, coupled with the absence of accountability like Know Your Customer (KYC) and Anti-Money Laundering (AML), have cast uncertainties upon the viability of SSI. In this paper, we bridge this gap by introducing AASSI, a pioneering SSI protocol meticulously designed to balance the twin imperatives of privacy and accountability. Specifically, AASSI extends support for anonymity, self-derivation, fine1grained tracing and selective revocation. In the realm of anonymity and self-derivation, AASSI introduces redactable signatures, which empowers users to autonomously derive distinctive credentials for each user1service-provider interaction, effectively improving privacy protection and self-management capabilities. Pertaining to fine-grained tracing, the protocol employs a dual-tag system that facilitates tracing users' real identities as well as a granular historical records of derived credentials. For selective revocation, AASSI leverages dynamic accumulators as a building block to enable the revocation of offending users. Ultimately, we provide functional comparison, which shows that AASSI has robust features, in particular, it supports novel self-derived features that further increase user control over their identity, and fine-grained tracking, which provides more flexibility for tracers.

We demonstrate protocol efficiency through off1chain time-consuming comparison, which show that AASSI dramatically reduces the time overhead of credential verification. Moreover, We test the on-chain communication overhead and experimentally prove the feasibility of AASSI.

Index Terms – Self-Sovereign Identity (SSI), blockchain, identity management, privacy preservation, accountability, redactable signatures, dynamic accumulators, credential verification, selective revocation, fine-grained tracing, decentralized identity (DID), Know Your Customer (KYC), Anti-Money Laundering (AML).

I. INTRODUCTION

Digital identities [1] are identifiers that present individual's real identities as the unique information in the digital world. Today, most digital identities are still authenticated and controlled by a central authority integrated with a service provider, the user provides sensitive personal information that meets the service provider's access controls in order to register an account, then the service provider provides the user with limited access rights. In this model, users digital identities are stored in the central authority's servers, adversaries can maliciously access users' sensitive data simply by attacking the servers, exposing users to the risk of data misuse and privacy leakage. Although the regulatory authorities have introduced laws and regulations to protect personal privacy, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), data leakage continue to occur [2], [3]. To counteract the centralized control of user identity, the federated identity management (FIM) model and the user-centric model were successively introduced. The former proposes to replace a central authority with trust relationships in federated choose a service provider and decide whether to share their identity to another service provider through authorization. Unfortunately, the key issues of identity control and privacy leakage remain unattended. Inspired by blockchain networks and cryptography technologies, a user-controlled decentralized digital identity model, SSI, was proposed [5]. SSI uses decentralized identifiers (DIDs) [6] and verifiable credentials (VCs) [7] as building blocks to enable user to independently create digital identities and have full control over the identity information.

Users can self-create DIDs and manage a number of VCs under their name. By controlling the private keys associated with

DIDs, users can use their VCs as required in online interactions. In a classic SSI scenario, the issuer signs the personal data selected by the user to generate a digital identity, i.e., VC. When access to a service provider, the user can select a compliant digital identity for communication based on the access control of different service providers. Ultimately, the service provider can verify the user's identity by accessing the user's DID, and the data stored in the blockchain related to verifiable credentials. The tamper-proof and distributed nature of blockchain ensures the integrity and decentralization of user's digital identities, while the verifiable credential data model enables users to use their registered identities in perpetuity [8]. While existing SSI protocols have advantages in terms of persistence and control, they face three major problems.

(1) Privacy: The verification requires users to disclose some sensitive information on the blockchain, but the transparency of the blockchain makes user information easily accessible to blockchain participants, which brings the risk of user privacy leakage.

(2) Over-reliance: Although SSI implements self-control of user identity, users need to interact frequently with issuers in order to obtain credentials about different attributes, which increases the user's reliance on the issuer, and increases the difficulty of the issuer's work.

(3) Accountability: Laws such as KYC and AML state that some financial institutions should have the right to know the private information and true identity of users involved in any transaction, which is contrary to the need for complete privacy. Therefore, how to balance the relationship between privacy and accountability is an important question.

In order to solve the above problems, this paper proposes AASSI, a SSI protocol that can simultaneously support privacy, low dependency, and accountability. In terms of privacy and low reliance, AASSI introduces redactable signatures as building blocks. It enables users to derive derived signatures containing partly attributes from a master signature, and the derivation process does not require the participation of the issuer, effectively reducing the user's reliance on the issuer. In addition, the verification of derived signatures does not involve knowledge of other attributes except for partly attributes, which can greatly protect the privacy of users. Combined with zero-knowledge proofs, users can prove that they meet access control without revealing specific attributes.

For example, the user is over 18. In terms of accountability, on the one hand, the protocol employs a dual-tag system that facilitates tracing users' real identities as well as a granular historical records of derived credentials. on the other hand, AASSI leverages dynamic accumulators to enable the revocation of offending users. The following summarizes the paper's major contributions:

We proposed AASSI, a new SSI protocol that can balance privacy and accountability. Specifically, AASSI extends support for anonymity, self-derivation, fine-grained tracing, and selective revocation. In general mode, users can derive credentials that contain only the required attributes, and the derivation process does not require the issuer to be involved. In addition, no one can learn the true identity of a general user just by observing the blockchain and interacting online. In accountability mode, a tracer can trace the true identity of the offending user and can perform fine-grained tracking of that user's historical behaviour. The protocol also supports an optional revocation feature that enables the revocation of illegal user.

We formalized the components, threat model and security model of AASSI protocol. It is demonstrated that the protocol satisfies the security requirements of correctness, unforgeability, anonymity, and traceability. We implemented AASSI and analysed its performance. First, we computed its complexity, and compared the functionalities and time overhead of AASSI with existing SSI protocols. Second, we evaluated its feasibility and efficiency from off-chain and on-chain experiments. Experimental results show that AASSI has feasibility, robust features and low time overhead in credential verification.

II. RELATED WORK

A. Big data supply chain analytics: Ethical, privacy and security challenges posed to business, industries and society

This study conducted a comprehensive review of big data supply chain analytics (BDSCA). The paper explored the application of big data in supply chain management and its benefits for organisations and society. The paper also examined the ethical, security, privacy and operational challenges of big data techniques, as well as the potential reputational damages to businesses. The review outlined four principal facets, namely: Big data analytics, applications, ethics and privacy issues, and how organizations employed this emerging tool to anticipate and even predict the future

and direct their operations. These principle facets are built across the multiple levels and unique conceptual standpoints indicated by 7 themes and 14 sub-themes. These themes were generated based on 120 articles (2005−2020) drawn mainly from leading academic journals. Overall, there is a considerable consensus across current literature that big data analytics extend far beyond just reinventing the supply chain. It has the potential to support more responsive next-generation of global companies who are operating in an increasingly challenging and uncertain environment.

B. *Privacy-preserving identity management system on blockchain using zk-SNARK*

Privacy plays a crucial role in the internet era, where many applications allow people to communicate and use their services through the internet. Privacy-preserving Identity Management (PPIdM) system is a scheme that helps manage users' identities and protects users' privacy by enabling users to authenticate themselves without disclosing their real identities. The PPIdM system also allows users to reveal some minor identity attributes while others remain secret selectively. However, anonymity also encourages malicious users to break the system's policy and commit crimes since their real identities are anonymous. Existing PPIdM systems use the identity provider (IP) as a medium to verify users' identity attributes, record all users' real identities, and ensure that malicious users' identities are traceable. Therefore, users' identities are hidden from all entities but the IP. However, the user's privacy is vulnerable because there is nothing to guarantee that the IP is always honest and not curious about their users' activities and private information. This paper proposes a PPIdM system on the blockchain that helps users manage their identity attributes and keeps their real identities secret from all entities, including the IP. Still, the system's consensus can trace malicious users' real identities if they violate the system's policy. The PPIdM's security requirements are analyzed and proved informally using the game-based proof scheme. The main idea of this study is to combine zk-SNARK, a type of zero-knowledge proof (ZKP), Shamir's secret sharing (SSS), and several other cryptographic techniques.

C. *Security analysis of coconut, an attribute based credential scheme with threshold issuance*

Coconut is an attribute-based credential scheme with threshold issuance. We analyze its security properties. To this end, we define

an ideal functionality for attribute-based access control with threshold issuance. We describe a construction that realizes our functionality. Our construction follows Coconut with a few changes. In particular, it modifies the protocols for blind issuance of credentials and for credential show so that user privacy holds against computationally unbounded adversaries. The modified protocols are slightly more efficient than those of Coconut. Our construction also extends the public key, which seems necessary to prove unforgeability.

D. Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability

The traditional system designed by incorporating the (WSN) suffers from important issues such as centralization of information, single source of trust, and fails to provide a trusted data-auditing solution due to the involvement of Third Party Auditor (TPA). This article proposes a novel solution by leveraging the concept Blockchain and (DDSS) system to mitigate the issues mentioned above. In our model, Sensor Nodes are accountable for their activity because the blockchain permanently records the logs of sensor nodes. The proposed solution provides the decentralized authentication of sensor nodes and the information stored in the fully distributed system. Furthermore, a decentralized data-auditing scheme without involving the TPA is also suggested, which finally benefits the user in terms of bandwidth and money. The formal verification of the proposed protocol is done using the Scythe simulator tool, which indicates that the protocol is safe and can protect against the relevant attacks with 100% accuracy. We have estimated the proposed scheme's time complexity and computational efficiencies and compared them with the existing one. The computation and communication overhead of the proposed method is reduced by 22.143% and 12.5% compared with the Khalid et al. (2020) scheme. Lastly, the platform simulates our solution, confirming that less than USD 2 is required to execute the proposed solution.

III. PROPOSED METHODOLOGY

In this paper, we bridge this gap by introducing AASSI, a pioneering SSI protocol meticulously designed to balance the twin imperatives of privacy and accountability. Specifically, AASSI extends support for anonymity, self-derivation, fine-grained tracing and selective revocation. For selective revocation, AASSI leverages dynamic accumulators as a building block to enable the revocation of offending users.

Ultimately, we provide functional comparison, which shows that AASSI has robust features, in particular, it supports novel self-derived features that further increase user control over their identity, and fine-grained tracking, which provides more flexibility for tracers. We demonstrate protocol efficiency through off-chain time-consuming comparison, which show that AASSI dramatically reduces the time overhead of credential verification. Moreover, We test the on-chain communication overhead and experimentally prove the feasibility of AASSI.

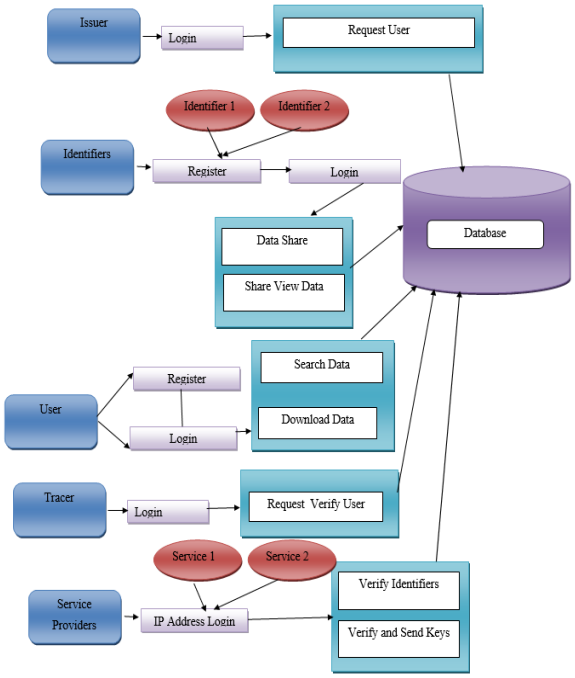
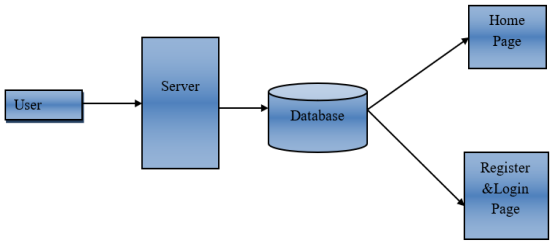


Fig. 1: System Overview

1. User Interface Design

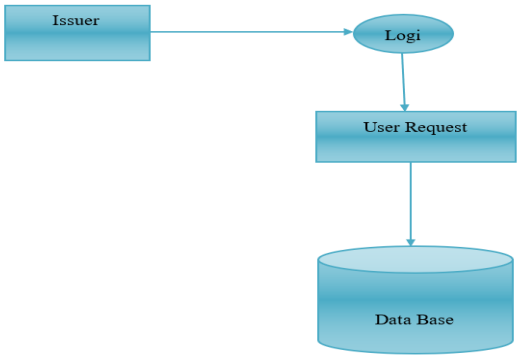
In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server.

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.



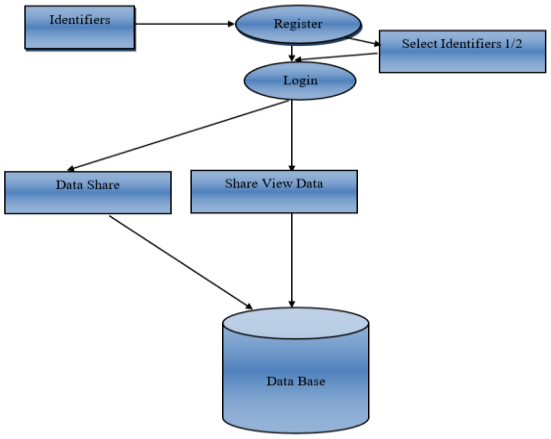
2. Issuer

This is the first module issuer. issuer can login from a user id and password and generated port no. Issuer can get a user request the issuer has to approve a request.



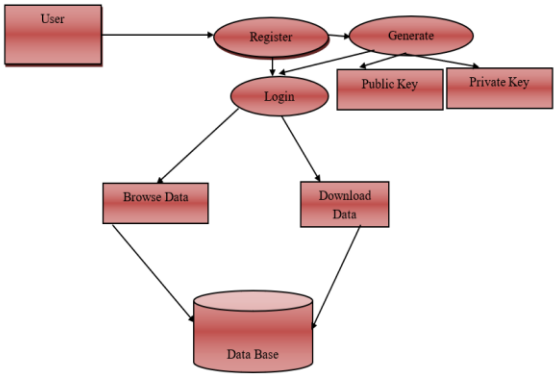
3. Identifiers

This is the third module of this project. In this project identifiers has a register with all details and login with a user id and password. The identifiers has a upload a file the file has a upload with a text or doc file to the data. The identifiers has a share a data it can be view from a database.



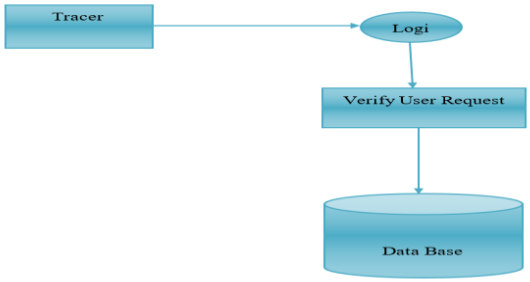
4. User

This is the fourth module of this project. User has a register with all details and then login with a email id and password. The user has a generate a public key and a private keys. The public key and private keys it will be deleted after the approve request. User has a Browse the identifier has a store we can search a data. User has a key verification the keys are verify the correct then it will have a decrypt a file download.



5. Tracer

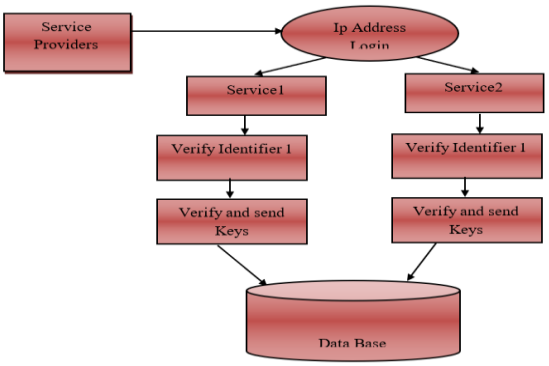
This is the first module issuer. Tracer has a generated with a randomly user id and password. Tracer can login from a user id and password. Tracer can send a keys to the user. The tracer has a get a private keys the private keys it will be forward to user.



6. Service Providers

The service providers it was login with a system original ip address of a system. The service providers has a divided into a two

services. The service one has to verify identifier1 the request. The Service two has a verify a identifier 2 request. The services has a interlinking two each other. The service providers has a verify and send a keys to user. Then the user has a download a file.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed AASSI protocol effectively balances privacy and accountability in Self-Sovereign Identity (SSI) systems. By integrating redactable signatures, dynamic accumulators, and a dual-tag tracing mechanism, the protocol supports anonymity, self-derived credentials, fine-grained tracing, and selective revocation. Performance evaluations demonstrate reduced credential verification time and low on-chain communication overhead compared to existing SSI approaches.

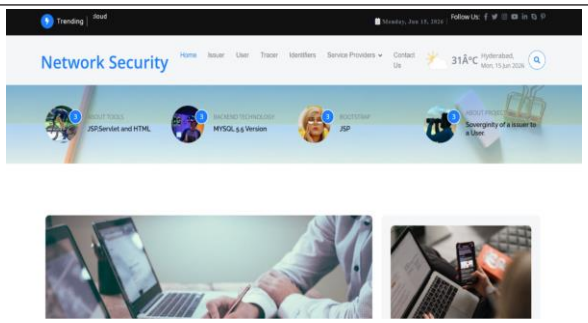


Fig. 2: Home Page

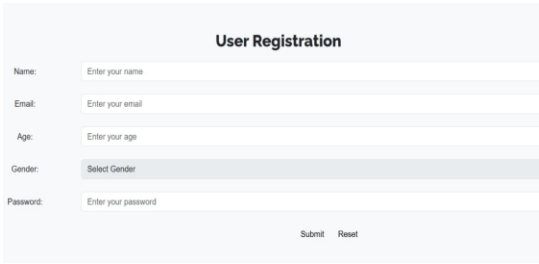


Fig. 3: Registration

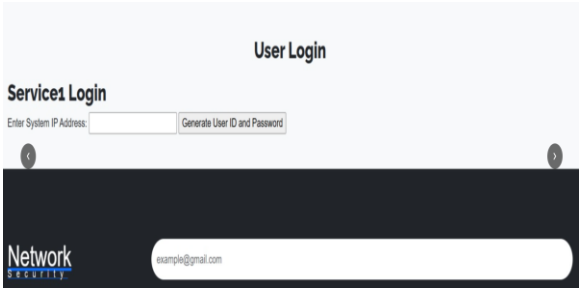


Fig. 4: Login



Fig. 5: Tracer Login

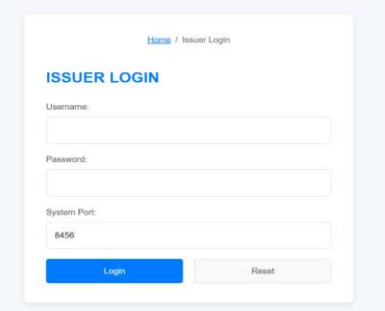


Fig. 6: Issuer Login

V. CONCLUSION

In this work, we have presented a pioneering SSI protocol meticulously designed to balance the twin imperatives of privacy and accountability. Specifically, AASSI extends support for anonymity, self-derivation, fine-grained tracing and selective revocation. In the general mode, no one can learn the privacy attributes and true identity of a general user just by observing the blockchain and interacting online. In accountability mode, there is a tracer that can trace users' real identities as well as a granular historical records of derived credentials, and the issuer can selectively revoke offending users. Innovatively, AASSI supports two novel features, self-derivation and fine-grained tracking, the former effectively improves privacy protection, and user control over their identity, as the user can autonomously derive distinctive credentials for each user-service-provider interaction, the latter provides tracers with more flexible tracking options. We propose the specific structure of AASSI and demonstrate that it satisfies the security requirements of correctness, anonymity, unforgeability and traceability. Finally, we analyze the complexity and compare the functionality of AASSI with existing SSI. We evaluate its computational efficiency and feasibility through off-chain and on-chain experiments, respectively.

REFERENCES

[1] A. J. Zwitter, O. J. Gstrein, and E. Yap, ''Digital identity and the blockchain: Universal identity management and the concept of the 'selfsovereign' individual,'' Frontiers Blockchain, vol. 3, p. 26, May 2020.

[2] N. J. Ogbuke, Y. Y. Yusuf, K. Dharma, and B. A. Mercangoz, ''Big data supply chain analytics: Ethical, privacy and security challenges posed to business, industries and society,'' Prod. Planning Control, vol. 33, nos. 2–3, pp. 123–137, Feb. 2022.

[3] B. Hu, Q. Yan, and Y. Zheng, ''Tracking location privacy leakage of mobile ad networks at scale,'' in Proc. IEEE INFOCOM Conf. Compute. Commun. Workshops, Apr. 2018, pp. 1–2.

[4] A. A. Malik, H. Anwar, and M. A. Shibli, ‘‘Federated identity management (FIM): Challenges and opportunities,’’ in Proc. Conf. Inf. Assurance Cyber Secure. (CIACS), Dec. 2015, pp. 75–82.

[5] C. Allen. (2016). The Path to Self-Sovereign Identity. [Online]. Available:. html

[6] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, ‘‘Distributed- Ledger-based authentication with decentralized identifiers and verifiable credentials,’’ in Proc. 2nd Conf. Blockchain Res. Appl. for Innov. Netw. Services (BRAINS), Sep. 2020, pp. 71–78.

[7] WWW Consortium. (2019). Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web. [Online]. Available: https://www.w3.org/TR/vc-data-model/?#core-data-mode

[8] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, ‘‘Digital identities and verifiable credentials,’’ Bus. Inf. Syst. Eng., vol. 63, no. 5, pp. 603–613, Oct. 2021.

[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

[10] Garapati, R. S., Aitha, A. R., Yandamuri, U. S., Gottimukkala, V. R. R., Nagubandi, A. R., & Kolla, S. H. (2026, March). Cloud-Native Orchestration of Multi-Counterparty Derivatives and Collateral in Manufacturing Enterprises via AI-Assisted Financial Audit Engines. In 2026 IEEE International Conference on AI Engineering and Innovations (AIEI) (pp. 1-6). IEEE.

[11] Boyapati, P. K., Susarla, R. S., & Kandula, S. T. R. (2025, April). Revolutionizing Fraud Detection in Real-Time Financial Transactions Using AI-Based Boundary-Integrated Neural Networks with Starfish Optimization Algorithm. In International Conference on Computer Vision and Robotics (pp. 75-87). Cham: Springer Nature Switzerland.

[12] Akinapalli, S. (2025). Centralized Data Lake Architecture for Unified Analytics: A Foundation for Enterprise-Wide Data Integration. Journal Of Engineering And Computer Sciences, 4(8), 414-422.

AUTHORS Profile



Mr. MODUKURU PRADEEP has received his B. Tech from JNTUK, Kakinada in 2013, M. Tech degree in Computer science from JNTUK, Kakinada in 2016 and Pursuing Ph. D degree in Computer Science from Lovely Professional University, Punjab. He is dedicated to teaching field from the last 10 years. His research area Deep Learning. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



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



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



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



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