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

Research Paper

MS-FL: A FEDERATED LEARNING FRAMEWORK BASED ON MULTIPLE SECURITY STRATEGIES

Dr. M V NARAYANA [1], SYED HAJRA JASMEEN [2], NALAM VIGNESH [3], THUMU YASHWANTH REDDY [4], SHAIK ABDUL ATHIF [5]

[1]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— With the development of data science, AI and data transaction, an increasing number of users are utilizing multi-party data for federated machine learning to obtain their desired models. Therefore, scholars have proposed numerous federated learning frameworks to address practical issues. However, there are still three issues that need to be addressed in current federated learning frameworks: 1) privacy protection, 2) poisoning attack, and 3) protection of the interests of participants. To address these issues, this paper proposes a novel federated learning framework MS-FL based on multiple security strategies. The framework's algorithms guarantee that data providers need not worry about data privacy leakage. At the same time, it can defend against poisoning attack from malicious nodes. Finally, to ensure the interests of all parties are protected, a blockchain protocol is utilized. The theoretical derivation proves the effectiveness of this framework. Experimental results show that the algorithm designed in this paper outperforms other algorithms.

Index Terms – Federated learning, privacy protection, poisoning attack, secure data sharing, multi-party data, machine learning security, decentralized framework, data privacy, participant incentive protection, robust learning.

I. INTRODUCTION

Recent years, due to the presence of sensitive information in the data, enterprises and organizations are regulated by laws and cannot disclose the data. As a result, most of the data are isolated and closed, leading to the formation of numerous data islands and a significant waste of resources. Therefore, the reasonable use of data resources while simultaneously protecting data privacy has become an urgent issue in the current era. Some scholars have proposed the federated learning (FL) [1] method to complete machine learning by utilizing the data of multiple parties involved in machine learning like Fig. 1. However, Fredrikson [2] found that part of data information of model trainers could be inferred according to the model after training, which means that even if no data privacy was leaked in the process of federated learning, there is a risk of data privacy leakage from the model after training.

In practice, a fully homomorphic cryptosystem CKKS is widely used to protect data privacy because it supports: (1) addition and multiplication homomorphism of ciphertext; (2) floating-point arithmetic and evaluating an arbitrary polynomial, which is ideal for privacy-protecting machine learning. Therefore, in this study, we exploit CKKS technology to protect data privacy of FL participants. Except for privacy leak, in the process of gradient aggregation, the adversary intends to inject poisoned (biased or misleading) data into a federated learning system, with the objective of modifying the model's parameters in a way that is beneficial to the attacker. If the aggregation server does not have defense mechanism and directly uses average of aggregate gradients, it has been demonstrated that a single poisoner can control entire training process [4], [5].

In this paper, we mainly focus on three types of representative poisoning attacks: (1) Label-flipping attack [6] (data poisoning). In a data set, each data sample carries a category label. However, malicious nodes can use wrong labels to train machine learning model. (2) Backdoor attack (data poisoning). Malicious nodes aim to seek a set of parameters to establish strong links between trigger and target label while minimizing the impact on classification of benign inputs. In Fig. 2, the trigger is a white block. (3) Arbitrary model attack [8] (model poisoning). If training model locally, malicious nodes can deliver arbitrary wrong gradients to aggregation server to reduce final model accuracy.

In light of the increasing value of data, data trading has experienced substantial growth.

In real life, there is a situation where a company needs specific machine learning models, but lacks or has no data, and the data owners do not need the corresponding machine learning models themselves. For example, an educational research institution needs to train a machine learning model using the academic achievements of students from different schools, but these schools themselves do not need this machine learning model. The main concern of this paper is how to utilize multi-party data to train a reliable machine learning model under the condition of protecting privacy information, and allow both the model requesters and data owners to complete the transaction of data value. In this paper, we construct a novel FL framework MS-FL based on multiple security strategies to solve the problem of the above real-world scenario. MS-FL achieves the following advantages:

Privacy: As prior works have shown, an adversary may recover data owner's sensitive information such as training samples or memberships by inferring shared gradients. To protect data owners' data privacy, we use multiple security protocols and CKKS technology to keep each data owner's local gradients confidential. In addition, after executing protocols of MS-FL, only model requestor has access to the final model.

Robustness: The model training process can defend against above three poisoning attacks from malicious nodes.

Fair Transaction: After every round of model training, model parameters will be delivered to model requestor and model requestor must pay to data owners. Smart contract used in MS-FL on blockchain makes this transaction atomic and transparent.

Interest protection: Compared with some existing literature, MS-FL guarantees that data owner will not lose all opportunities to benefit from model requestor just because a portion of submitted gradient components deviates from the majority.

II. RELATED WORK

A. NttpFL: Privacy-preserving oriented no trusted third party federated learning system based on blockchain

In federated learning, multiple parties may use their data to cooperatively train a model without exchanging raw data. Federated learning protects the privacy of users to a certain extent. However, model parameters may still expose private information. Moreover, existing encrypted federated learning systems need a trusted third party to generate and distribute key pairs to connected participants, making them unsuitable for

federated learning and vulnerable to security risks. To mitigate these issues, we propose a privacy-preserving oriented no trusted third party federated learning system based on blockchain (NttpFL). The initiator of the federated learning task and the partners negotiate keys through the conference key agreement and do not need to distribute keys through a trusted third party. We design a double-layer encryption mechanism to ensure privacy. Partners cannot obtain any private information other than their information. The decentralized nature of blockchain suits our system. In addition, blockchain makes the entire process transparent and traceable and avoids the single node failure problem. Experimental results confirm that the proposed method significantly reduces the communication costs and computational complexity compared to existing encrypted federated learning without compromising the performance and security.

B. Research on homomorphic encryption for arithmetic of approximate numbers

We suggest a method to construct a homomorphic encryption scheme for approximate arithmetic. It supports an approximate addition and multiplication of encrypted messages, together with a new rescaling procedure for managing the magnitude of plaintext. This procedure truncates a ciphertext into a smaller modulus, which leads to rounding of plaintext. The main idea is to add a noise following significant figures which contain a main message. This noise is originally added to the plaintext for security, but considered to be a part of error occurring during approximate computations that is reduced along with plaintext by rescaling. As a result, our decryption structure outputs an approximate value of plaintext with a predetermined precision.

We also propose a new batching technique for a RLWE-based construction. A plaintext polynomial is an element of a cyclotomic ring of characteristic zero and it is mapped to a message vector of complex numbers via complex canonical embedding map, which is an isometric ring homomorphism. This transformation does not blow up the size of errors, therefore enables us to preserve the precision of plaintext after encoding. In our construction, the bit size of ciphertext modulus grows linearly with the depth of the circuit being evaluated due to rescaling procedure, while all the previous works either require an exponentially large size of modulus or expensive computations such as bootstrapping or bit extraction. One important feature of our method is that the

precision loss during evaluation is bounded by the depth of a circuit and it exceeds at most one more bit compared to unencrypted approximate arithmetic such as floating-point operations. In addition to the basic approximate circuits, we show that our scheme can be applied to the efficient evaluation of transcendental functions such as multiplicative inverse, exponential function, logistic function and discrete Fourier.

C. *Data quality detection mechanism against label flipping attacks in federated learning*

Federated learning (FL) is an emerging framework that enables massive clients (e.g., mobile devices or enterprises) to collaboratively construct a global model without sharing their local data. However, due to the lack of direct access to clients' data, the global model is vulnerable to be attacked by malicious clients with their poisoned data. Many strategies have been proposed to mitigate the threat of label flipping attacks, but they either require considerable computational overhead, or lack robustness, and some even cause privacy concerns. In this paper, we propose Malicious Clients Detection Federated Learning (MCDFL) to defense against the label flipping attack. It can identify malicious clients by recovering a distribution over a latent feature space to detect the data quality of each client. We demonstrate the effectiveness of our proposed strategy on two benchmark datasets, i.e., CIFAR-10 and Fashion-MNIST, by considering different neural network models and different attack scenarios. The results show that, our solution is robust to detect malicious clients without excessive costs under various conditions, where the proportion of malicious clients is in the range of 5% and 40%.

D. *TDFL: Truth discovery based Byzantine robust federated learning*

Federated learning (FL) enables data owners to train a joint global model without sharing private data. However, it is vulnerable to Byzantine attackers that can launch poisoning attacks to destroy model training. Existing defense strategies rely on the additional datasets to train trustable server models or trusted execution environments to mitigate attacks. Besides, these strategies can only tolerate a small number of malicious users or resist a few types of poisoning attacks. To address these challenges, we design a novel federated learning method TDFL, T ruth Discovery based Federated Learning, which can defend against multiple poisoning attacks without additional datasets even when the Byzantine users are ≥50%.

Specifically, the TDFL considers different scenarios with different malicious proportions. For Honest-majority setting (Byzantine <50%), we design a special robust truth discovery aggregation scheme to remove malicious model updates, which can assign weights according to users' contribution; for Byzantine-majority setting (Byzantine ≥50%), we use maximum clique-based filter to guarantee global model quality. To the best of our knowledge, this is the first study that uses truth discovery to defend against poisoning attacks. It is also the first scheme which can achieve strong robustness under multiple kinds of attacks launched by high proportion attackers without root datasets. Extensive comparative experiments are designed with five state-of-the-art aggregation rules under five types of classical poisoning attacks on different datasets. The experimental results demonstrate that TDFL is practical and achieves reasonable Byzantine-robustness.

III. PROPOSED METHODOLOGY

The main concern of this paper is how to utilize multi-party data to train a reliable machine-learning model under the condition of protecting privacy information, and allow both the model requesters and data owners to complete the transaction of data value. In this paper, we construct a novel FL framework MS-FL based on multiple security strategies to solve the problem of the above real-world scenario.An adversary may recover data owner's sensitive information such as training samples or memberships by inferring shared gradients. To protect data owners' data privacy, we use multiple security protocols and CKKS techenology to keep each data owner's local gradients confidential. In addition, after executing protocols of MS-FL, only model requestor has access to the final model.

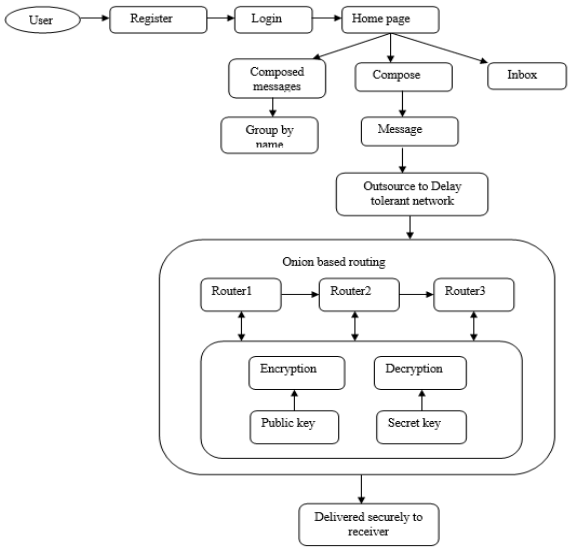
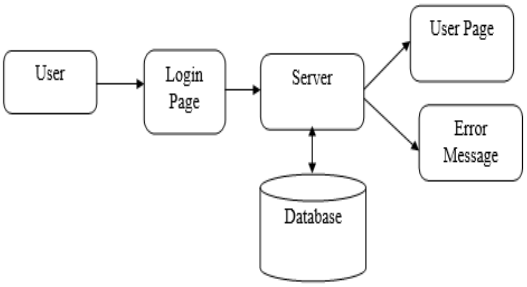


Fig. 1: System Overview

3.1 User Interface Design

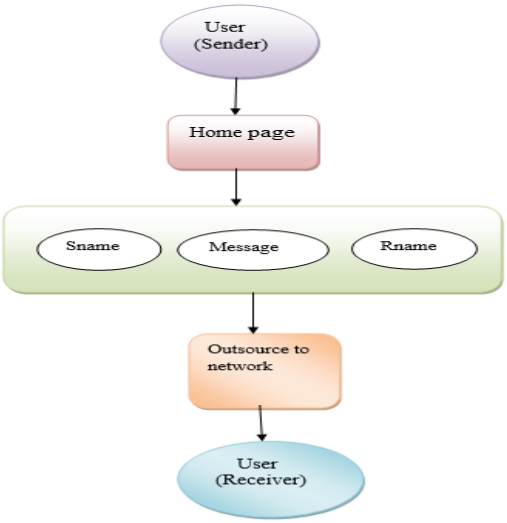
To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else, user must register their details such as username, password, Email id, City and

Country into the server. Database 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. It will search the query and display the query.



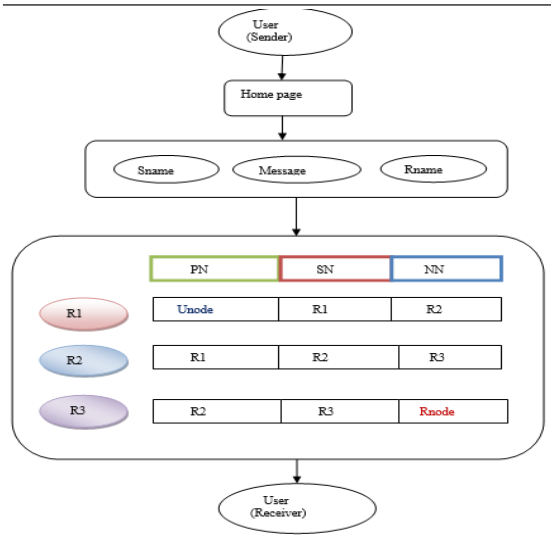
3.2 Message Sending Process

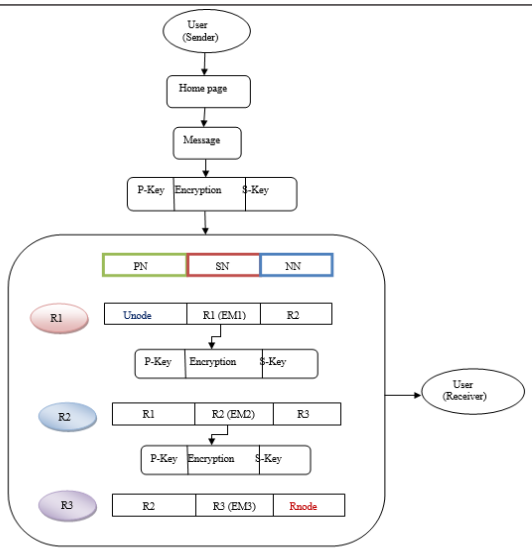
This is the second module of the project. In this the user acts like a sender that he/she needed to send some information to other user of the application. For sending a message must and should metadata will be needed just like sender, message and receiver. This metadata helps to route the packet data in the network for deliver to the receiver. Data user have data and they are curious about others' privacy. Some of them are malicious, who will poison in the model training.



3.3 Routing

This is the third module of the project. This module work happens after successfully outsource a message to the network. Routing is nothing but transmitting the data from one node to its neighbor node. In this project we are using routers for transmitting the data. Due to these anonymous routing happens in the network. Routers not known the metadata (sender, receiver) but knows only the previous node information and next neighbor node.





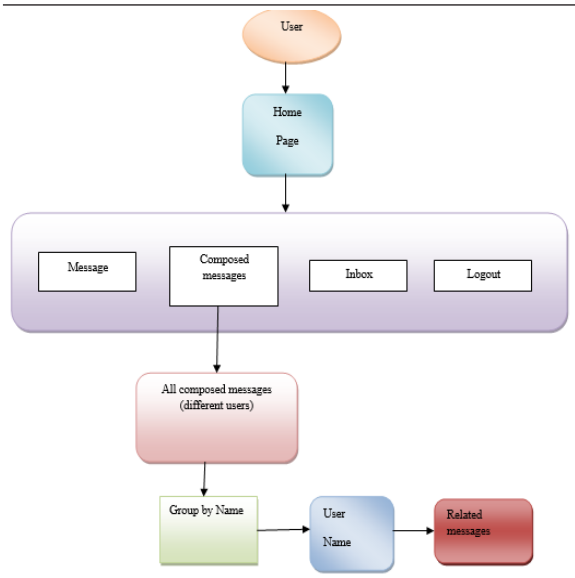
3.4 Data Security analysis

This is the fourth module of the project. Normally the main issue of the network is security why because there is a chance of fetch the outsourced data by the malicious users. To avoid this we convert the data which is going to outsource in the network into cipher text. Symmetrical way (single key for encrypt and decrypt) is not secure. So, we are using onion based anonymous routing. In this encryption done with public key and a corresponding secret key will be generated which will helps to decrypt. Same process will be going on in different layers i.e., routers.

3.5 Composed Data Analysis:

This is the fifth module of the project. Actually it is the enhancing module of the project. If users want to know the information which he/she shared with a particular user then he has to recollect all the information till to known he share. It is hard to check one – by-one and it will takes lot of time .So, to avoid that we are using data analysis concept in this user need to give an input that is the name of the user which he needed to know all the shared information till to now. Easily fetch the shared information in a series manner from the database related to that user only.

International Journal of Engineering Research and Science & Technology



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed **MS-FL framework** performs better than existing federated learning methods in terms of security and overall model performance. The framework effectively protects user data privacy during training and reduces the risk of information leakage. It also demonstrates strong resistance against **poisoning attacks** by identifying and limiting the impact of malicious participants. The integration of **blockchain technology** helps ensure fairness, trust, and protection of the interests of all parties involved in the federated learning process.

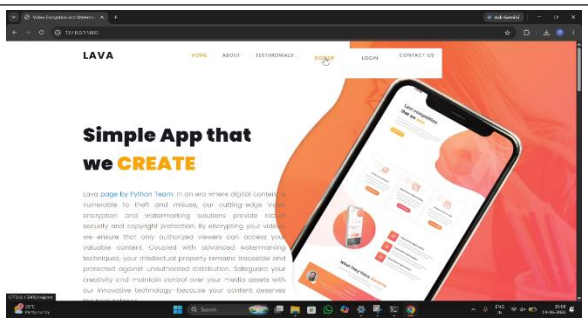


Fig. 2: Home Page

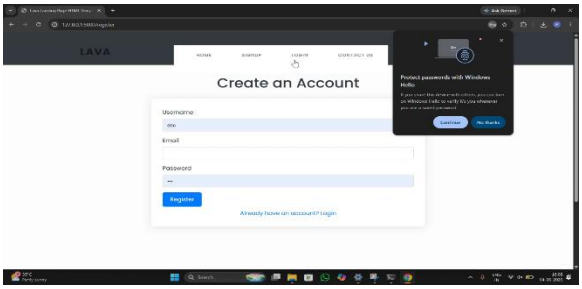


Fig. 3: Registration

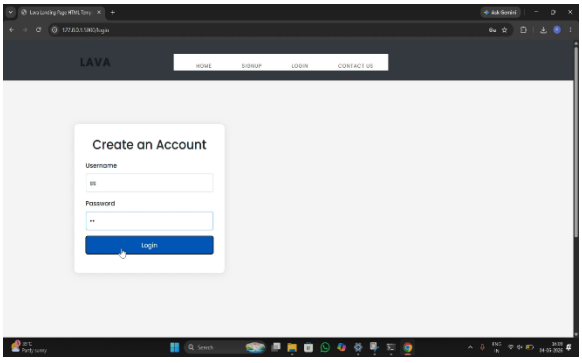


Fig. 4: Login

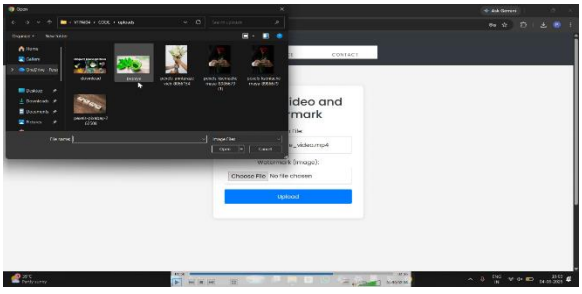


Fig. 5: Upload Image

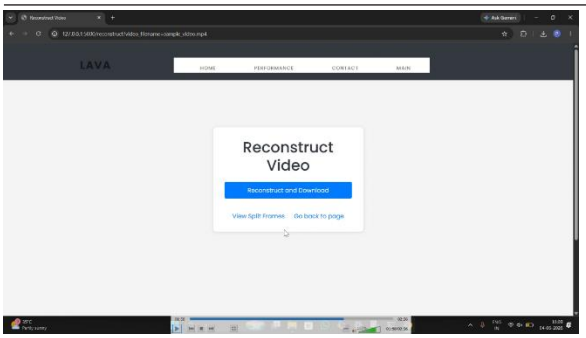


Fig. 6: Reconstruct Video



Fig. 6: Reconstruct Video Results

V. CONCLUSION

In this paper, a novel federated learning framework MS-FL based on multiple security strategies has been proposed for data application scenario, in which the model requestor and the data owner are separated. This framework has been proved secure for privacy of model requestor and data owners. Moreover, it is capable of protecting interests of participants of FL and the aggregation algorithm of MS-FL has ability to defend typical byzantine poisoning attacks. At the end of this paper, the experimental results demonstrate comparable performance of aggregation algorithm of MS-FL in terms of accuracy and robustness.

REFERENCES

1. S. Bai, G. Yang, G. Liu, H. Dai and C. Rong, "NttpFL: Privacy-preserving oriented no trusted third party federated learning system based on blockchain", IEEE Trans. Netw. Service Manage, vol. 19, no. 4, pp. 3750-3763, Dec. 2022.

2. M. Fredrikson, S. Jha and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures", Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security, pp. 1322-1333, Oct. 2015.

3. D. D, A. K. K and R. M, "Research on homomorphic encryption for arithmetic of approximate numbers", Proc. Int. Conf. Intell. Syst. Commun. IoT Security (ICISCoIS), pp. 409-437, Feb. 2023.

4. P. Blanchard, E. Mahdi E. Mhamdi, R. Guerraoui and J. Stainer, "Machine learning with adversaries: Byzantine tolerant gradient descent", Proc. Adv. Neural Inf. Process. Syst., vol. 30, pp. 1-11, 2017.

5. M. Nasr, R. Shokri and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box

inference attacks against centralized and federated learning", Proc. IEEE Symp. Security Privacy (SP), pp. 739-753, May 2019.

6. Y. Jiang, W. Zhang and Y. Chen, "Data quality detection mechanism against label flipping attacks in federated learning", IEEE Trans. Inf. Forensics Security, vol. 18, pp. 1625-1637, 2023.

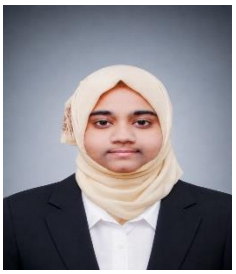
7. E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin and V. Shmatikov, "How to backdoor federated learning", Proc. Int. Conf. Artif. Intell. Statist, pp. 2938-2948, Jun. 2020.

8. C. Xu, Y. Jia, L. Zhu, C. Zhang, G. Jin and K. Sharif, "TDFL: Truth discovery based Byzantine robust federated learning", IEEE Trans. Parallel Distrib. Syst., vol. 33, no. 12, pp. 4835-4848, Dec. 2022.

AUTHORS Profile



Dr. M V Narayana received his Bachelor of Engineering (B.E.) degree in Computer Science in 2004 from JNTU Kakinada, India. He completed his Master of Technology (M.Tech) degree in Computer Science in 2010 from JNTU Hyderabad, India, and was awarded his Ph.D. in Computer Science in 2017 from JNTU Kakinada, India. With over 20 years of dedicated experience in academia and research, he currently serves as a Professor and Head of the Department (HoD) in the CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India. His research interests encompass various areas within computer science, and he has contributed significantly to the field throughout his career.



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



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



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



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