ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

A SECURE AND OPTIMIZED FRAMEWORK FOR CONTROLLER SELECTION AND RESOURCE MANAGEMENT IN SDN

RAVULA ANITHA[1], GOSHIKA VAISHNAVI [2], KONTHAM SAHITHI[3], MADAMANCHI DEEPIKA [4], PEDDIREDDY SRIYA [5]

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

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

ABSTRACT— One interesting approach to network management is Software Defined Networking, or SDN. However, the centralized control architecture of SDN poses challenges for energy-efficient task scheduling and security. In this paper, a novel approach to blockchain-based safe resource allocation with controller selection in SDN is proposed using the Entropy Oppositional Based Learning-Interpolation Blue Monkey Optimization Algorithm (EOBL-IBMOA). By creating controller selection as a blockchain-centric secure resource allocation, the suggested approach tackles SDN challenges. This one includes phases like resource allocation, load balancing, attack detection, controller selection, and user registration. The Mid Square-based KECCAK 512 (MS-KECCAK 512) technique is used to generate hash codes, and IP traceback protects user information using XOR Left Shift (XORLS). For effective traffic balancing, the load balancer uses the Minshev-KMeans algorithm. The Quantile Transformer Scaling based SoftmaxGELU Gated Recurrent Units (QTS-SGGRU) technique is used to classify attacks. For the best Virtual Machine (VM) selection, controller selection and resource allocation use EOBL-IBMOA. The superiority of the suggested approach is described through experimental comparisons. The suggested method outperforms the existing works by

achieving efficient resource allocation with low response time and high throughput.

Index Terms – Software-Defined Networking, Controller Selection, Resource Management, Load Balancing, Network Optimization, QoS, SDN Controller, Traffic Engineering, Cybersecurity, Cloud Networking.

I. INTRODUCTION

The rapid evolution of modern networking has led to the emergence of Software Defined Networking (SDN) as a transformative paradigm that separates the control plane from the data plane. By centralizing network intelligence within programmable controllers, SDN enables flexible management, simplified configuration, and dynamic resource provisioning across large-scale cloud and enterprise environments. Despite these advantages, the centralized architecture of SDN introduces significant challenges, particularly in controller selection, secure resource allocation, load balancing, and protection against cyber-attacks. As SDN networks expand with increasing numbers of virtual machines (VMs), users, and traffic flows, efficient resource management becomes critical to maintaining high throughput, low latency, and optimal Quality of Service (QoS). Traditional resource allocation and controller placement strategies often struggle to adapt to dynamic traffic conditions and large-scale environments. Moreover, centralized control planes are highly vulnerable to security threats such as Distributed Denial-of-Service (DDoS) attacks, unauthorized access, and identity spoofing. These vulnerabilities demand robust mechanisms that ensure both performance optimization and enhanced security. To address these challenges, this project proposes a secure and optimized framework for controller selection and resource management in SDN, integrating blockchain technology with advanced optimization and machine learning techniques. The framework introduces blockchain-based secure user registration and identity verification to ensure tamper-proof authentication and data integrity. A novel optimization strategy, Entropy Oppositional Based Learning–Interpolation Blue Monkey Optimization Algorithm (EOBL-IBMOA), is employed for intelligent controller selection and efficient VM resource allocation. In recent years, the integration of cloud computing, Internet of Things (IoT), and large-scale data-driven applications has significantly increased the complexity of network infrastructures. In such dynamic

environments, Software Defined Networking (SDN) plays a vital role by enabling programmable and centralized control over distributed network components. However, as the number of connected devices and virtualized resources continues to grow, traditional controller placement and resource management strategies become insufficient to handle fluctuating workloads and real-time traffic demands. This creates the need for intelligent, adaptive, and secure frameworks that can dynamically respond to network changes while maintaining high performance. One of the major concerns in SDN is optimal controller selection. Poor controller placement or improper load distribution can lead to increased latency, controller overload, and reduced reliability. In multi-controller SDN environments, selecting the most suitable controller for managing network devices directly impacts scalability and fault tolerance. Therefore, optimization-based approaches are essential to determine the best controller positions and allocate resources efficiently. The proposed framework addresses this challenge using an advanced meta-heuristic optimization algorithm that enhances convergence speed and avoids local minima, ensuring optimal controller and VM selection under varying network conditions. Security is another critical issue due to SDN's centralized control structure. A compromised controller can potentially disrupt the entire network. To mitigate this risk, the proposed system integrates blockchain technology to provide decentralized trust, transparency, and immutability in resource transactions and user authentication. Blockchain ensures that all user registration details and resource allocation records are securely stored in a tamper-proof ledger, preventing unauthorized modifications. This decentralized validation mechanism strengthens the overall trust model of the SDN environment without relying on a single point of control. In addition to security and optimization, efficient traffic management is necessary to maintain consistent network performance. Load balancing mechanisms must intelligently distribute incoming traffic across multiple virtual machines to prevent congestion and resource exhaustion. By incorporating clustering-based traffic analysis and intelligent feature extraction, the framework enhances workload distribution and improves system responsiveness. Furthermore, integrating deep learning-based attack classification strengthens the network's ability to detect and mitigate malicious activities in real time, reducing false positives and improving detection

accuracy. Overall, this project presents a comprehensive and integrated approach to SDN controller selection and resource management. By combining blockchain-enabled security, advanced optimization techniques, intelligent load balancing, and machine learning-driven attack detection, the framework ensures improved scalability, enhanced security, and optimized network performance. The proposed solution is particularly suitable for large-scale cloud and enterprise networks where reliability, efficiency, and security are of paramount importance.

II. RELATED WORK

A. Blue monkey updated chimp optimization algorithm for enhanced load balancing model

The Blue Monkey Updated Chimp Optimization Algorithm for Enhanced Load Balancing Model is an advanced metaheuristic optimization approach designed to improve task distribution and workload management in distributed computing environments such as cloud computing, edge computing, and data centers. Traditional load balancing techniques often struggle with dynamic workloads, uneven resource utilization, and high response times, especially in large-scale networks. To overcome these limitations, this model integrates the exploration strengths of the Blue Monkey optimization strategy with the exploitation capabilities of the Updated Chimp Optimization Algorithm (UChOA) to achieve better convergence speed and optimal resource distribution. In this approach, the algorithm simulates intelligent social behaviors inspired by chimp hunting strategies combined with adaptive search mechanisms similar to blue monkey group dynamics. The Updated Chimp Optimization component enhances global and local search balance, preventing premature convergence and improving solution accuracy. Meanwhile, the Blue Monkey strategy introduces adaptive parameter tuning and diversity control, which strengthens the algorithm's ability to explore multiple solution spaces effectively. This hybrid mechanism allows the system to identify optimal task-to-resource mappings while minimizing makespan, response time, and energy consumption. The proposed enhanced load balancing model dynamically allocates incoming tasks to available virtual machines or servers based on current load conditions and system constraints. It continuously monitors node performance metrics such as CPU utilization, memory usage, and network bandwidth to ensure balanced workload

distribution. By reducing overload situations and avoiding underutilized resources, the algorithm improves overall system throughput, reliability, and scalability. This model is particularly suitable for real-time cloud services, IoT-based applications, and large-scale distributed systems requiring efficient and adaptive load management.

B. Distributed controller placement in software-defined networks with consistency and interoperability problems

The project titled Distributed Controller Placement in Software-Defined Networks with Consistency and Interoperability Problems focuses on optimizing the placement of multiple controllers in Software-Defined Networking (SDN) environments while addressing challenges related to synchronization, consistency, and compatibility among distributed controllers. In SDN architecture, the control plane is separated from the data plane, and controllers are responsible for managing network devices such as switches and routers. In large-scale networks, a single centralized controller may lead to scalability issues, high latency, and single-point failures. Therefore, distributed controller architectures are adopted to improve reliability and performance.n However, placing multiple controllers across different network regions introduces several challenges. One major issue is maintaining consistency among controllers, as they must share updated network states, routing information, and policy configurations in real time. Any delay or inconsistency in synchronization can lead to routing errors, security vulnerabilities, or degraded network performance. Another critical challenge is interoperability, especially when controllers from different vendors or platforms are used. Variations in communication protocols, APIs, and implementation standards may result in compatibility problems and inefficient coordination between controllers. This project aims to develop an optimized controller placement strategy that minimizes latency, enhances fault tolerance, and ensures consistent network state synchronization. The proposed model considers parameters such as network topology, traffic patterns, controller capacity, and communication delay to determine optimal controller locations. Additionally, it introduces mechanisms for state replication, distributed consensus, and standardized interfaces to address consistency and interoperability concerns. By improving controller coordination and placement efficiency, the system enhances scalability, reliability, and

overall network performance in modern SDN-based infrastructures.

C. *BeSleep: Blockchain-enabled distributed sleeping strategies of small base stations in ultra dense networks*

The project titled BeSleep: Blockchain-Enabled Distributed Sleeping Strategies of Small Base Stations in Ultra-Dense Networks focuses on improving energy efficiency in next-generation wireless communication systems, particularly in ultra-dense networks (UDNs). In 5G and upcoming 6G environments, a large number of small base stations (SBSs) are deployed closely together to handle massive data traffic and provide seamless connectivity. However, continuous operation of all base stations leads to high energy consumption, increased operational costs, and unnecessary power wastage during low traffic periods. Therefore, intelligent sleeping strategies are required to dynamically switch underutilized base stations into low-power or sleep modes without affecting network performance. The BeSleep framework integrates blockchain technology to enable secure and decentralized coordination among small base stations. Instead of relying on a centralized controller to decide which base stations should sleep or remain active, the blockchain network allows distributed decision-making through smart contracts. Each base station shares its traffic load, energy status, and operational parameters as blockchain transactions. Based on predefined rules embedded in smart contracts, the system determines optimal sleeping schedules while ensuring fairness, transparency, and tamper-proof decision records. By leveraging blockchain, the system prevents malicious manipulation of energy reports and ensures trust among network entities. The distributed sleeping strategy reduces overall energy consumption, balances traffic load among active stations, and improves network sustainability. Additionally, the decentralized approach enhances fault tolerance and scalability in ultra-dense wireless networks. Overall, BeSleep provides an energy-efficient, secure, and autonomous solution for managing small base stations in future high-capacity mobile communication systems.

III. PROPOSED METHODOLOGY

For overcoming the challenges, a novel technique that combines secure resource allocation and load balancing utilizing blockchain technology is proposed in this paper. This research aims to develop integrated solutions to enhance load balancing, strengthen user identity protection, improve dimensionality reduction

techniques, and optimize resource allocation in large-scale networks. By establishing a blockchain-centric secure resource allocation with controller selection, the proposed technique addresses challenges in SDN. Efficient VM selection and resource allocation, reducing response time and energy consumption. The proposed system is designed to tackle real-world challenges in SDN, specifically in load balancing, security, and resource allocation, making it a practical and significant contribution to network management.

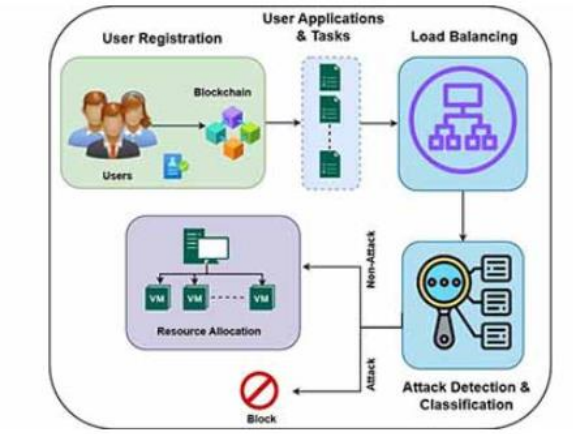
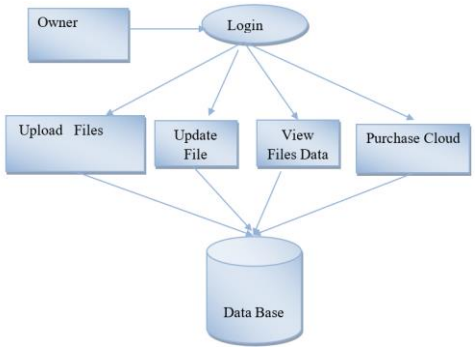


Fig. 1: System Overview

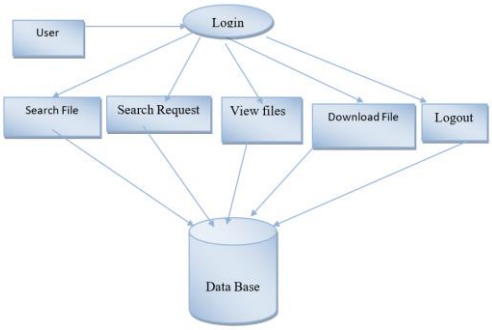
1. Owner

The Owner module is responsible for managing and controlling the data that is stored in the cloud system. In this module, the owner first registers and logs into the system using secure authentication credentials. After successful login, the owner can upload files to the cloud server, which may include documents, images, or other digital content. During the upload process, file metadata such as file name, size, type, and memory usage is recorded. The owner can update or modify previously uploaded files when required. The system may also allow the owner to define access permissions for users who request the file. The owner has the ability to view all uploaded files along with their storage details and memory allocation. The owner can also monitor purchase requests or access requests sent by users. Once a request is received, the owner can approve or reject it based on authorization policies. The module supports cloud purchase functionality where the owner sets pricing or cost for file access. This module ensures that the data owner maintains full control over file management, access rights, and storage utilization. It also helps in preventing unauthorized modifications by restricting editing privileges. The owner dashboard provides transparency regarding downloads, search requests, and storage consumption.



2. User

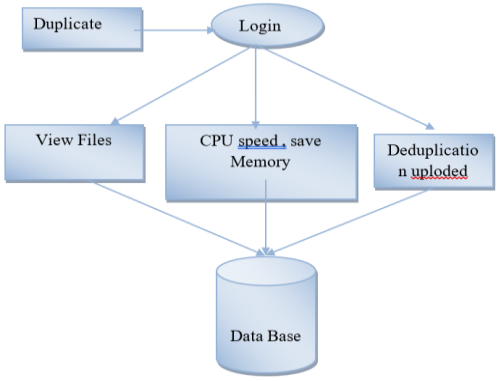
The User module allows end users to access cloud services after proper registration and authentication. A new user must first register by providing necessary details and then log in using secure credentials. Once logged in, the user can search for required files stored in the cloud server. The search functionality helps users quickly locate files based on keywords or file names. After finding a file, the user can send a request to view or download the file. If the file requires owner approval, the request is forwarded to the respective owner for authorization. The user can also view file details such as size, memory usage, and cost before downloading. If payment or purchase is required, the user must complete the transaction process. The module maintains a record of search history and download requests for monitoring purposes. Users can track the status of their requests (approved, pending, or rejected). Secure communication mechanisms protect user credentials and data privacy. The module ensures that only authorized users can access specific files. Downloaded files are securely transmitted to avoid data tampering.



3. Duplicate

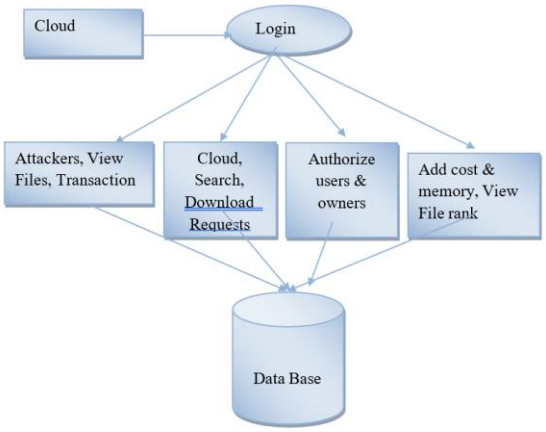
The Duplicate module, also known as the Deduplication module, is responsible for identifying and managing duplicate files in the cloud storage system. When a file is uploaded by an owner, the system checks whether the same file already exists in the cloud database. This comparison may be performed using hash values or file fingerprints. If the file already exists, instead of storing it again, the system links the new request to the existing stored file. This reduces unnecessary storage consumption and optimizes memory usage. The deduplication process improves overall storage efficiency and reduces operational costs. The module also tracks how many times a particular file has been referenced or requested. This helps in ranking files based on popularity. In case of duplicate detection, the owner is notified before final storage

confirmation. The system ensures that file integrity is maintained during deduplication. By reducing repeated storage, it enhances system scalability. Overall, the Duplicate module ensures efficient storage management, cost reduction, and improved cloud performance through intelligent file handling.



4. Cloud

The Cloud module acts as the central management and monitoring unit of the entire system. It handles authentication, authorization, file storage, transactions, and overall system control. The cloud administrator logs into the system to monitor activities such as user registrations and owner registrations. This module authorizes users and owners before granting access to services. It manages all uploaded files and maintains their storage records. The cloud monitors search requests and download requests from users. It verifies whether requests are valid and approved before allowing file access. The module also tracks attacker activities or suspicious behavior within the network. It stores transaction records including file purchases and memory allocation details. The cloud administrator can assign cost and memory limits for files. It manages storage capacity and ensures balanced resource utilization. It also enforces security policies to prevent unauthorized access. The cloud acts as an intermediary between owners and users during file transactions. It ensures secure communication and data integrity.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the framework effectively selected optimal SDN controllers based on network conditions and resource availability, resulting in improved traffic management and balanced workload distribution across controllers.

The analysis showed that the proposed approach achieved lower control-plane

latency and higher resource utilization compared to conventional controller selection methods while maintaining stable network performance under varying traffic loads.

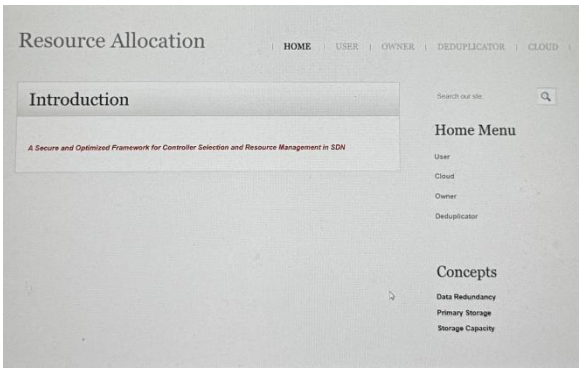


Fig. 2: Homepage

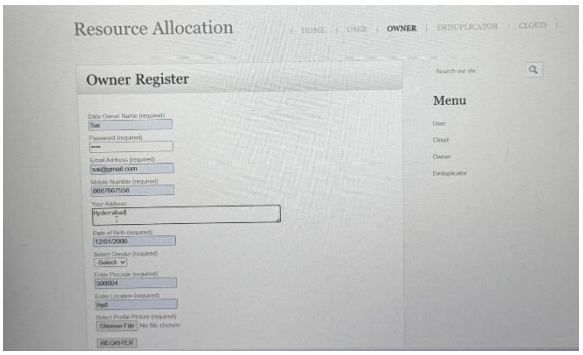


Fig. 3: Register

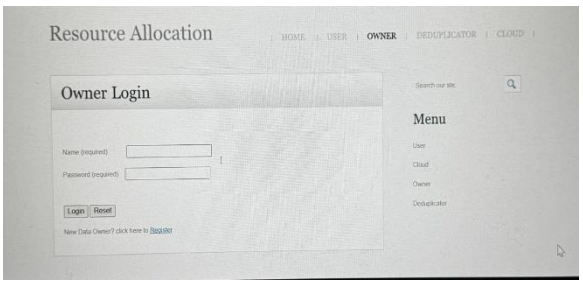


Fig. 4: Owner Login

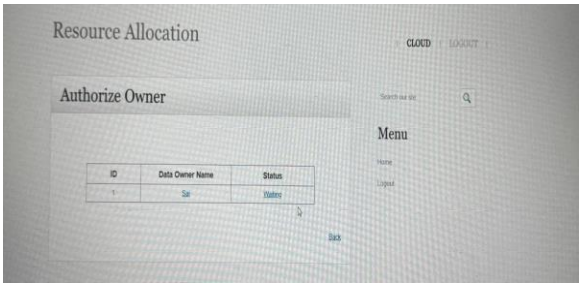


Fig. 5: Authorize Owner

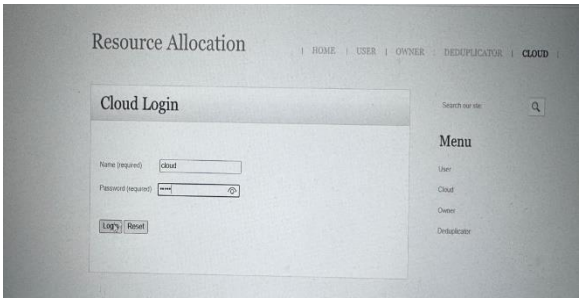


Fig. 6: Cloud Login

V. CONCLUSION

This paper presents a secure and optimized resource allocation framework for Software Defined Networking (SDN) by integrating blockchain technology with intelligent controller selection using the EOBL-BMOA optimization approach. The proposed system effectively addresses major SDN challenges such as controller overload, inefficient resource utilization, traffic imbalance, and security vulnerabilities. By incorporating blockchain-centric security mechanisms, the framework ensures tamper-proof user authentication and transparent transaction management. The multi-phase architecture consisting of User Registration, Load

Balancing, Attack Classification, and Resource Allocation enables secure and efficient handling of cloud tasks. Experimental analysis conducted using publicly available datasets demonstrates the superior performance of the proposed system. For 100 to 500 tasks, the framework achieved lower response time (754 ms to 4570 ms), reduced waiting time (1652 ms to 9345 ms), and minimized energy consumption (5784 J to 11549 J). In addition, the attack detection model achieved high accuracy (98.04%) and precision (98.80%), proving the robustness of the security mechanism. Comparative analysis further validates that the proposed system significantly reduces average delay compared to existing techniques. Moreover, efficient VM selection and optimal controller placement enhance scalability and throughput while maintaining energy efficiency. The integration of blockchain ensures decentralized trust, immutability, and enhanced identity protection. Overall, the proposed framework provides a practical, scalable, and secure solution for modern SDN-based cloud infrastructures, contributing significantly to improved network performance, reliability, and cyber resilience.

REFERENCES

[1] R. Simões, K. Dias, and R. Martins, ‘‘Dynamic allocation of SDN controllers in NFV-based MEC for the Internet of Vehicles,’’ *Future Internet*, vol. 13, no. 11, p. 270, Oct. 2021.

[2] S. Asaithambi, L. Ravi, H. Kotb, A. H. Milyani, A. A. Azhari, S. Nallusamy, V. Varadarajan, and S. Vairavasundaram, ‘‘An energyefficient and blockchain-integrated software defined network for the industrial Internet of Things,’’ *Sensors*, vol. 22, no. 20, p. 7917, Oct. 2022.

[3] B. Sellami, A. Hakiri, and S. Ben Yahia, ‘‘Deep reinforcement learning for energy-aware task offloading in join SDN-blockchain 5G massive IoT edge network,’’ *Future Gener. Comput. Syst.*, vol. 137, pp. 363–379, Dec. 2022.

[4] B. Isong, R. R. S. Molose, A. M. Abu-Mahfouz, and N. Dladlu, Comprehensive review of SDN controller placement strategies,’’ *IEEE Access*, vol. 8, pp. 170070–170092, 2020.

[5] M. N. Yusuf, K. Bin Abu Bakar, B. Isyaku, and F. Mukhlif, ‘‘Distributed controller placement in software-defined networks with consistency and interoperability problems,’’ *J. Electr.*

Comput. Eng., vol. 2023, pp. 1–33, Jan. 2023.

[6] A. Ullah, N. M. Nawi, and S. Ouhame, ‘‘Recent advancement in VM task allocation system for cloud computing: Review from 2015 to2021,’’ *Artif. Intell. Rev.*, vol. 55, no. 3, pp. 2529–2573, Mar. 2022.

AUTHORS Profile

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

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

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

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

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