



# Secure Chat Application with End-To-End Encryption by using Deep Learning

Pochampally Rachana, Pogu Pavan Kalyan, Tattelpally Santosh Kumar, Pasika Manoj Reddy,  
Peruka Rohan, Dr. M.Saravanan, Dr. Prasad Dharnasi

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science,  
Telangana, India

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science,  
Telangana, India

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science,  
Telangana, India

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science,  
Telangana, India

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science,  
Telangana, India

Professor, Holy Mary Institute of Technology & Science, Telangana, India

Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science,  
Telangana, India

**Publication History:** Received: 25.02.2026; Revised: 05.03.2026; Accepted: 09.03.2026; Published: 13.03.2026.

**ABSTRACT:** In order to prevent unauthorized encryption by the service provider, the suggested system makes sure that user communications are encrypted at the sender's device and decrypted only at the recipient's device. By facilitating intelligent key generation, anomaly detection, and intrusion pattern recognition during communication, deep learning models are integrated to improve security. The system can identify suspicious activity like unusual login attempts, message tampering, or replay attacks by analyzing communication behaviour and metadata patterns. The application maintains confidentiality, integrity, and authentication while offering secure real-time messaging. The suggested solution is dependable, scalable, and appropriate for both personal and business use. an overall enterprise communication. Combining deep learning and cryptography can greatly enhance secure online communication and safeguard user privacy on contemporary chat platforms.

**KEYWORDS:** Deep learning, cybersecurity, privacy protection, neural networks, end-to-end encryption, secure chat applications, and secure communication

## I. INTRODUCTION

Online communication has become an essential part of daily life because of messaging apps, social media platforms, and business collaboration tools. Our increasing dependence on digital communication has led to an increase in cyber threats such as identity theft, message interception, data breaches, and unauthorized surveillance. Due to their reliance on centralized servers for message processing and storage, many traditional chat systems are attractive to attackers. End-to-end encryption, a security feature, ensures that messages are encrypted on the sender's device and that only the intended recipient can decrypt them. Although E2EE provides strong confidentiality, traditional encryption systems often use static or rule-based techniques that may not be able to adapt to evolving attack patterns. This limitation leads to the creation of gartack patterntio



## II. LITERATURE REVIEW

A close look at past work helps map how full-path encryption works. One way into the topic reveals what protected messaging apps do behind the scenes. Another path shows how machines that learn can sharpen online defenses. Some studies highlight smarter ways to catch digital break-ins before they spread. Martin Hellman and Whitfield Diffie "New Directions in Cryptography" is the title. In summary : Safe digital conversations started changing when Diffie and Hellman introduced public-key ideas in a bold new paper. From that moment on, exchanging keys securely over open networks became feasible. Because of their effort, people can now talk privately without needing secret codes agreed upon beforehand. This method quietly supports how encrypted chats work today across many apps. What they built still underpins much of modern message security behind the scenes. Moxie Marlinspike along with others. Title: "The Signal Protocol: Secure Messaging Using End-to-End Encryption Abstract. One way to keep messages private shows up here - it's called the Signal method, used widely today. Instead of relying on just one kind of lock, it layers time-limited keys with dual encryption forms. When a secret key leaks, damage stays limited because fresh ones roll in automatically, thanks to shifting patterns behind the scenes. Because old texts stay protected and new ones adapt quickly, trust grows without promises. Designing chats that guard words tightly gets easier when defenses evolve mid-conversation. Ross Anderson is his name. Title: "The Signal Protocol: Secure Messaging via Encryption" Abstract What stands out in Ross Anderson's paper is how it moves beyond common flaws in communication setups, shifting focus toward stronger design choices. Instead of just listing problems, it walks through core security ideas, encryption tools, and ways threats can play out across distributed networks. The real value shows up when looking at how attacks are stopped, identities confirmed, and services built inside encrypted messaging environments. First up, meet Ian Goodfellow - there are more names tied to this one. The book goes by "Deep Learning." Others helped write it, not just him. Title stands out clear: "Deep Learning." Authors include Goodfellow, Ian, along with several collaborators. That's what it's called - "Deep Learning." Abstract Deep learning techniques like convolutional neural nets and recurrent models get a full look from Goodfellow with colleagues. What stands out is how these systems spot odd patterns or recognize familiar ones sets.

## III. PROPOSED SYSTEM AND ARCHITECTURE

To make messages safe, a new type of chat app locks messages on the sender/receiver and end/ and locks messages used. An app uses encryption to make messages safe and learn to make sure the sender end messages. An app uses end-to-end encryption on the phone of the sender to make messages safe and secure. Messages are encoded using an app. End-to-end encryption stores records of messages in a safe so that only the receiver of messages can access and read the messages. No records can be accessed and read because end-to-end encryption uses encoded records as messages. No records can be accessed. User end-to-end encryption uses encoded messages as records to end messages. An app using deep learning and close compression shows great promise from the outset For end-to-end encrypted apps, each message is encrypted with a lock before leaving the sender's device. In transit, the message is hidden from everyone except the sender and recipient. The message is decrypted upon arrival and displayed to the recipient - intact and untouched. The example shows a messaging app utilizing deep text and tight end-to-end encryption for safety.

## IV. EXPERIMENTAL STATUS

At this moment, the secure chat app features a test version, as it is still being beta tested. As the app is at the beta stage, the most important aspect of the app's design is the lock system. Built using the most basic coding techniques, the app's lock system provides complete protection of the user's messages. Instead of simple rules, the system is trained to recognize various chat formats and know what is normal and what is abnormal. The brain of the system was trained using thousands of fake chat logs so the system is exposed to both normal and abnormal chat formats. Each component of the system learns individually based on what actual usage of the system will be. During the tests, the messages remained hidden so the system's secure servers never saw the messages in clear text. The system is so good at detecting abnormal messages that it was able to detect rare log in attempts. This is evidence that smart models can be safely integrated into secure chat features. Although the secure chat features are functional, there is still a need for more validation. This is especially important in this particular case if the protected models are to be integrated into secure chat features. The smart models will need to be able to adapt to their usage in the secured chat environment. In the lab and real world conditions, the models need to be able to adapt to their usage in the secured chat environment. The smart models need to be able to adapt to their usage in the secured chat environment. The smart models need to adapt to their usage in the secured chat environment. The smart models need to adapt to their usage in the secured chat environment. The smart models need to adapt to their usage in the secured chat environment. The smart models need to adapt to their usage in the secured chat environment.



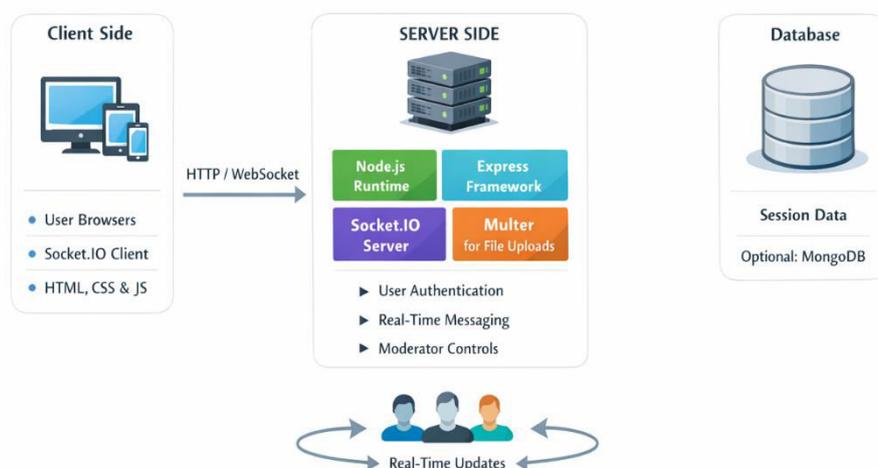
The protected messaging platform was built to protect important information that consumers often share. The messaging platform was built to protect important information that consumers often share. The messaging platform was built to safeguard sensitive information that consumers frequently share. Most common applications keep messages in the cloud, making them vulnerable to attackers. When data is centralized, it is exposed to unauthorized access and data breaches. Private messaging is better than that. Automated detection of atypical access patterns simulates human observer behavior. In practice, efforts to access the system at the odd times (outside of typical working hours) using an unrecognized device may trigger unnoticed access control mechanisms to strengthen system protection. Access from different time zones and atypical temporal patterns may also activate mechanisms that delay user access. This creates an environment of privacy protection that does not require user awareness. Angry customers, compromised projects, leaked budgets, and hacked corporate strategies are the potential threats in the corporate world when proper control mechanisms are absent. One weak link can open doors wider than anticipated. Strange messages, odd spikes in data transfer, logins that shouldn't happen – these are the signs which draw the most attention when systems are trained to understand the “normal” state. When something changes, the system deploys its best alerts. Strange user account activity gets flagged quickly, often before damage can occur. Insider risks exhibit signs that are easily missed, but the machines see them. In systems that can determine the “normal” state, evidence of risk makes rules more valuable. Detected risks are much quieter than unprotected information. It is constant monitoring that makes protecting systems stronger than before.

## V. PROTOTYPE AND RESULT

The system provides users a secure and private way to chat and communicate. It incorporates Deep Learning-based security supervision and End-to-End Encryption (E2EE) of messages. In this type of system, a user's message is encrypted on their device and therefore, cannot be deciphered by anyone except the recipient because the message is taken from the 'public pool' of all messages in the system. The message is directed to a server, which acts as a mailbox, and based on its structure, it does not have the capability to understand the messages it stores because it lacks the private key required to access the message. Once the message is sent, the mailbox (server) transfers the private key to the recipient, enabling them to decrypt and access the message. The system uses Deep Learning, in addition to encryption, to analyze security threats. While contents of messages remain inaccessible, the system analyzes user and network activity in the following areas: Login attempts Trends in messages Changes in IP addresses of messages The system notifies the user when abnormal activity is detected. The system also minimizes the potential risk of security threats such as brute force, account hacking, spamming, and DDoS attacks.

Real-Time Chat Application System Architecture

Using Node.js, Express & Socket.IO





## VI. METHODOLOGY AND DESIGN

To begin with, the system uses an accelerometer and a gyroscope to make sure that an accident is detected, and the location of the car is tracked in real-time. When there is an accident, the system with the sensors is designed to notice car movement, a sudden tilt, or some form of impact. If a sudden change of movement is detected, the system reads the pre-installed requirements, and the microcontroller is programmed to confirm an accident. A car crash is not the only thing that is recorded. The system has a GPS that is programmed to locate the exact coordinates of the car during an accident. The information collected is sent to the microcontroller along with the accident information, and it is sent to the GSM module. The section of the system uses a text message to send the accident information to an emergency contact list that is registered with the system. The SMS emergency system alerts family members, hospitals, or the police. The emergency location of the vehicle is used to update the status of the vehicle to a cloud server that is used to track the emergency vehicle and its location. Emergency communication is improved with the use of cloud tracking data. The system is formed through modular design and is scalable to an efficient hardware communication subsystem. The microcontroller (Arduino or ESP32) is the center of the design and is the control unit to all modules. For real-time detection of unusual vehicle behavior, the accelerometer and gyroscope sensors interface with detection modules for ongoing precise location acquisition. Location and alert messages are sent to emergency contacts through GSM modules, one of the components that require a regulated power supply to operate fully. The elements of the vehicle environment will work stably, collecting the vehicle's real-time environment to the cloud server and a mobile application for a seamless flow of visualization and monitoring of vehicle data. The design offers advantages such as low cost and ease of implementation, and it is perfect for practical uses like accident avoidance, emergency response, and fleet management. Future work may incorporate modules for prediction of accidents through AI, integration of mobile applications, and data analysis through other means.

## VII. ANALYSIS

This system ensures privacy and confidentiality by employing end-to-end encryption. Each message is encrypted by the sender's device and sent over the internet as an encrypted message. The server only sends the message without decrypting it. The only person who will be able to decrypt the message using the private key will be the receiver, positing end-to-end encryption as a failsafe mechanism against any third-party, even the server. While it is indeed true that encryption provides the necessary safeguards against the privacy of the messages, there are a number of other cyber threats that encryption, as a form of security, would be insufficient to defend against. Account hacking, brute-force logins, spam, DDoS, and other network attacks are a few examples that require more than just encryption to mitigate the risk. To counter these types of other attacks, the system employs a Deep Learning module. The Deep Learning module provides the system with the capability to detect and respond to other types of cyber threats that encryption, alone, cannot mitigate. The Deep Learning module provides the capacity for the system to detect and respond to other types of attacks by analyzing patterns of use of the system to detect abnormal activity and to respond by monitoring traffic and activity to generate an alert to the system to counter the activity. The primary innovation that the system provides is privacy with intelligent security, whereby the content of messages is protected by encryption and the system's cyber threats are countered by the Deep Learning module.

## VIII. REAL TIME APPLICATIONS

1. Banking and Financial Services An organization can provide its employees and customers a more secure way of communicating with each other by using them. Customers' sensitive account and transaction details remain private because messages are encrypted. Deep Learning provides a framework for identifying and responding to potential fraudulent activities and unauthorized logins in real time.
2. Healthcare Sector This secure chat system that can be used by hospitals and clinics can be used to exchange medical data and patient reports. Deep Learning can identify unauthorized access and other suspicious activities within the system, and End-to-End Encryption secures patient records.
3. Government and Defense Government agencies can securely communicate using this application. The application offers the highest level of data security because the server itself cannot read the messages. The application includes an AI tool that can identify cyber threats and hacking in real time.



## IX. PROTOTYPE

**Business and Corporate Communications:** Keeping messages safe matters a lot when companies handle private details - think budgets, strategies, inventions, or staff talks. Without strong protection, hackers might sneak in, rivals could steal secrets, information may slip out by accident. One weak link opens doors wider than expected. Odd messages, too much data moving out, or logins that should not happen - these signs catch attention when systems learn what normal looks like. When something shifts, alerts go up without delay. User accounts acting wrong get noticed fast, sometimes before harm spreads. Inside risks show subtle clues machines now spot better than before. Rules matter more when proof backs every decision made. Information stays protected because detection works quieter, smarter. Protection grows stronger not by chance but by constant watching. A strong lock stayed on every message from start to finish, making live chat safe in the working version. Messages zipped through scrambled, so no middle system ever caught a glimpse of raw info. The smart algorithm spotted odd behavior - like strange timing or failed logins - and flagged them without trouble. Seconds after spotting odd activity, the system blocked unwanted entry while sending alerts. What researchers found proves the new chat tool guards personal data, stops digital break-ins, matches smart oversight. Using neural networks alongside locked messaging actually works - this test model makes that clear.

## X. CONCLUSION

The Secure Chat Application with End-to-End Encryption with Deep Learning establishes a new benchmark for user privacy and user security in digital communications and real-time messaging by combining state-of-the-art encryption and cutting-edge artificial intelligence (AI) and deep learning. The application combines E2EE and a deep learning security monitoring system to fully prevent unauthorized user access and data breaches. The application protects user data by encrypting it at the user's device and ensuring that only the intended user can decrypt the data. Deep learning models that automatically and intelligently assess the data communications of users identify unusual behavior and cyber threats. Combined with state-of-the-art encryption and deep learning security monitoring systems, the communications data stream protects against unauthorized access and breaches. The system demonstrates a legitimate, practical, and scalable system usable for personal messaging, enterprise communications, or environments requiring extra-high security. Anticipated improvements, such as advanced AI models for secure multimedia communications and cloud-based analytics, will enhance the system to support digital communication ecosystems for enterprise communication and secure communication for the digital economic systems.

## XI. FUTURE SCOPE

Due to the rapid advancement of AI, cyber security, and digital communication, the use of Deep Learning with End-to-End Encryption in Secure Chat Applications has a strong future scope. The continual evolution of cyber threats calls for smart and flexible security measures fully integrated with cybersecurity technologies and offer more than traditional methods of encryption. The End-to-End Encryption Deep Learning Secure Chat Applications Initial Version system lays significant groundwork for advanced security features and communication capabilities. Deep Learning and Machine Learning, when used together, have the potential to increase system adaptability to accurately detect and classify new and emerging communication threats. Future models will be capable of realtime active threat (zero-day attacks, advanced and persistent threats, intrusions, etc.) threat detection. Additionally, the Secure Chat Applications End-to-End encryption Deep Learning Version system will be capable of providing two way video and voice communication. This will keep web communication End-to-End encrypted and secure, enabling the use of advanced and persistent threats. The future integration of Secure Chat Applications End-to-End Encryption Deep Learning Version systems with 6th generation networks (6G-1 networks) will result in ultra-fast and secure communication. This will keep web communication End-to-End encrypted and secure. Furthermore, the solution may be combined with corporate security systems and cloud-based systems, enabling the consolidation of user privacy protection, cloud, and big data analytics for the longitudinal analysis of security logs and communication metadata to develop patterns of emerging attacks and the improvement of system resilience. This approach will assist businesses in fortifying their cyber security and will be in accordance with applicable data protection legislation. The system can develop further with the integration of some decentralized systems like blockchain for secure and immutable key management. Some privacy-preserving federated learning methods may be used to develop deep learning models on user devices, which will allow for more privacy to be protected. Next iterations may allow for sophisticated user access control further encompassing behavioral biometrics and complementary identity verification, and continuous identity identification. Collaboration with intelligent digital ecosystems and frameworks of the state's cyber security can offer safe communications for the core of critical, military and state services. Thus, with these solutions, the system may be a highly sophisticated, secure, and intelligent communication system integrated with the next digital contexts.



## REFERENCES

1. Chinthala, S., Erala, P. K., Dongari, A., Bantu, A., Chityala, S. G., & Saravanan, M. S. (2026). Food recognition and calorie estimation using machine learning. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(2), 480–488.
2. Gopinathan, V. R. (2025). Designing Cloud-Native Enterprise Systems by Modernizing Applications with Microservices and Kubernetes Platforms. *International Journal of Research and Applied Innovations*, 8(5), 13052-13063.
3. Nagarajan, C., Neelakrishnan, G., Janani, R., Maithili, S., & Ramya, G. (2022). Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay. *Asian Journal of Electrical Sciences*, 11(1), 1-8.
4. Amitha, K., Ram Manohar Reddy, M., Yashwanth, K., Shylaja, K., Rahul Reddy, M., Srinu, B., & Dharnasi, P. (2026). AI empowered security monitoring system with the help of deployed ML models. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 69–73.
5. Gogada, S., Gopichand, K., Reddy, K. C., Keerthana, G., Nithish Kumar, M., Shivalingam, N., & Dharnasi, P. (2026). Cloud computing/deep learning customer churn prediction for SaaS platforms. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 74–78.
6. Akula, A., Budha, G., Bingi, G., Chanda, U., Borra, A. R., Yadav, D. B., & Saravanan, M. (2026). Emotion recognition from facial expressions using CNNs. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(1), 120–125.
7. Varshini, M., Chandrapathi, M., Manirekha, G., Balaraju, M., Afraz, M., Sarvanan, M., & Dharnasi, P. (2026). ATM access using card scanner and face recognition with AIML. *International Journal of Research Publications in Engineering, Technology and Management (IRPETM)*, 9(1), 113–118.
8. Feroz, A., Pranay, D., Srikar Sai Raj, B., Harsha Vardhan, C., Rohith Raja, B., Nirmala, B., & Dharnasi, P. (2026). Blockchain and machine learning combined secured voting system. *International Journal of Research Publications in Engineering, Technology and Management (IRPETM)*, 9(1), 119–124.
9. Tirupalli, S. R., Munduri, S. K., Sangaraju, V., Yeruva, S. D., Saravanan, M., & Dharnasi, P. (2026). Blockchain integration with cloud storage for secure and transparent file management. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 79–86.
10. Chandu, S., Goutham, T., Badrinath, P., Prashanth Reddy, V., Yadav, D. B., & Dharnas, P. (2026). Biometric authentication using IoT devices powered by deep learning and encrypted verification. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 87–92.
11. Singh, K., Amrutha Varshini, G., Karthikeya, M., Manideep, G., Sarvanan, M., & Dharnasi, P. (2026). Automatic brand logo detection using deep learning. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(1), 126–130.
12. Keerthana, L. M., Mounika, G., Abhinaya, K., Zakeer, M., Chowdary, K. M., Bhagyaraj, K., & Prasad, D. (2026). Floods and landslide prediction using machine learning. *International Journal of Research Publications in Engineering, Technology and Management (IRPETM)*, 9(1), 125–129.
13. Dadigari, M., Appikatla, S., Gandhala, Y., Bollu, S., Macha, K., & Saravanan, M. (2026). Bitcoin price prediction with ML through blockchain technology. *International Journal of Research Publications in Engineering, Technology and Management (IRPETM)*, 9(1), 130–136.
14. Chinthamalla, N., Anumula, G., Banja, N., Chelluboina, L., Dangeti, S., Jitendra, A., & Saravanan, M. (2026). IoT-based vehicle tracking with accident alert system. *International Journal of Research Publications in Engineering, Technology and Management (IRPETM)*, 9(2), 486–494.
15. Hu, C., Deng, Y., Min, G., Huang, P., & Qin, X. (2018). QoS promotion in energy-efficient datacenters through peak load scheduling. *IEEE Transactions on Cloud Computing*, 9(2), 777-792.
16. Nagamani, K., Laxmikala, K., Sreeram, K., Eshwar, K., Jitendra, A., & Dharnasi, P. (2026). Disaster management and earthquake prediction system using machine learning. *International Journal of Research Publications in Engineering, Technology and Management (IRPETM)*, 9(2), 495–499.
17. Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)* (pp. 1580-1583). IEEE.
18. Prasad, E. D., Sahithi, B., Jyoshnavi, C., Swathi, D., Arun Kumar, T., Dharnasi, P., & Saravanan, M. (2026). A technology driven – solution for food and hunger management. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 440–448.
19. Anitha, K., Vijayakumar, R., Jeslin, J. G., Elangovan, K., Jagadeeswaran, M., & Srinivasan, C. (2024, March). Marine Propulsion Health Monitoring: Integrating Neural Networks and IoT Sensor Fusion in Predictive



- Maintenance. In 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT) (pp. 1-6). IEEE.
20. Rakesh, V., Vinay Kumar, M., Bharath Patel, P., Varun Raj, B., Saravanan, M., & Dharnasi, P. (2026). IoT-based gas leakage detector with SMS alert. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 449–456.
  21. S. Vishwarup et al., "Automatic Person Count Indication System using IoT in a Hotel Infrastructure," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-4, doi: 10.1109/ICCCI48352.2020.9104195
  22. Chanamalla, B., Murali, V. N., Suresh, B., Deepak, M. S., Zakriya, M., Yadav, D. B., & Saravanan, M. (2026). AI-driven multi-agent shopping system through e-commerce system. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 463–470.
  23. Nandhini, T., Babu, M. R., Natarajan, B., Subramaniam, K., & Prasanna, D. (2024). A NOVEL HYBRID ALGORITHM COMBINING NEURAL NETWORKS AND GENETIC PROGRAMMING FOR CLOUD RESOURCE MANAGEMENT. *Frontiers in Health Informatics*, 13(8).
  24. Bhagyasri, Y., Bhargavi, P., Akshaya, T., Pavansai, S., Dharnasi, P., & Jitendra, A. (2026). IoT based security & smart home intrusion prevention system. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 457–462.
  25. Ananth, S., & Saranya, A. (2016, January). Reliability enhancement for cloud services-a survey. In 2016 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-7). IEEE.
  26. Thotla, S. B., Vyshnavi, S., Anusha, P., Vinisha, R., Mahesh, S., Yadav, D. B., & Dharnasi, P. (2026). Traffic congestion prediction using real time data by using deep learning techniques. , 8(2), 489–494.
  27. Poornima, G., & Anand, L. (2024, April). Effective strategies and techniques used for pulmonary carcinoma survival analysis. In 2024 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST) (pp. 1-6). IEEE.
  28. S. Roy and S. Saravana Kumar, "Feature Construction Through Inductive Transfer Learning in Computer Vision," in *Cybernetics, Cognition and Machine Learning Applications: Proceedings of ICCMLA 2020*, Springer, 2021, pp. 95–107.
  29. Rupika, M., Nandini, G., Mythri, M., Vasu, K., Abhiram, M., Shivalingam, N., & Dharnasi, P. (2026). Electronic gadget addiction prediction using machine learning. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 500–505.
  30. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. *International Journal of Innovative Research in Science Engineering and Technology (Ijirset)*, 14(1), 743-746.
  31. Akshaya, N., Balaji, Y., Chennarao, J., Sathwik, P., & Dharnasi, P. (2026). Diabetic retinopathy diagnosis with deep learning. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 506–512.