International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902014

Cloud-Based File Sharing App with Data Security

Gayathri Chenchala, Adithya Boini, Sai Charan Challa , Sai Kumar Chinningu , Dasaroju Damodhar Chary, Mr.D.Bhagyaraj Yadav, Dr.M.Saravanan

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

Assistant Professor, Department of Computer Science and Engineering, 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: 23.02.2026; Revised: 10.03.2026; Accepted: 13.03. 2026; Published: 18.03.2026.

ABSTRACT: In today's digital era, data sharing and collaboration have become essential components of both personal and organizational workflows. Traditional file-sharing methods such as USB drives, emails, and local networks are often inefficient, limited in scalability, and vulnerable to data breaches. To overcome these challenges, cloud-based file sharing applications have emerged as a reliable secure, and accessible solution for storing and exchanging digital information. A cloud- based file sharing system alows users to upload, store, and share files over the internet through a centralized cloud server. It enables real-time access to data from any location, at any time, using any device connected to the internet. This flexibility enhances productivity and collaboration among users, especially in distributed and remote environments. However, with the growing volume of sensitive data being shared over the cloud, data security has become a major concern. Unauthorized access, data leakage, and cyberattacks can compromise user privacy and organizational integrity. Therefore, integrating robust security mechanisms-- such as end-to-end encryption, user authentication, role-based access control, and secure data transfer protocols (like HTTPS and SSL/TLS)- is critical to ensure confidentiality, integrity, and availability of shared data The proposed major project aims to design and implement a Cloud-Based File Sharing Application with Data Security, providing users with a secure and user-friendly platform to upload, download, and share files. The system will utilize cloud storage for scalability and employ encryption techniques to safeguard files from unauthorized access. Additionally, the application will include features like file versioning, access permissions, and activity logs to enhance transparency and control over data usage. This project not only addresses the need for efficient and secure data sharing but also contributes to the growing field of cloud computing and cybersecurity by demonstrating how advanced technologies can be integrated to protect user data in a cloud environment.

KEYWORDS: Cloud Computing, File Sharing, Data Security, End-to-End Encryption, Multi-Factor Authentication, Role-Based Access Control, AWS Cloud Services, Scalability, Data Integrity, Secure Data Transmission, Real-Time Accessibility, Encryption Algorithms, Remote Work, Online Collaboration, Performance Optimization.

I. INTRODUCTION

1.1 Overview

Cloud-based file sharing allows users to store files on remote servers and access them through the internet. These systems support collaboration, remote work, and data backup. Despite their benefits, cloud file sharing systems are vulnerable to security threats such as data breaches and unauthorized access. However, with the growing volume of sensitive data being shared over the cloud, data security has become a major concern. Unauthorized access, data leakage, and cyberattacks can compromise user privacy and organizational integrity. Therefore, integrating robust security mechanisms—such as end-to-end encryption, user authentication, role-based access control, and secure data transfer protocols (like HTTPS and SSL/TLS)—is critical to ensure confidentiality, integrity, and availability of shared data. The proposed major project aims to design and implement a Cloud-Based File Sharing Application with Data Security, providing users with a secure and user-friendly platform to upload, download, and share files. The system will utilize cloud storage for scalability and employ encryptiontechniques to safeguard files from unauthorized access. Additionally, the application will include features like file versioning, access permissions, and activity logs to enhance transparency and control over data usage. This project not only addresses the need for efficient and secure data sharing but also contributes to the growing field of cloud computing and cybersecurity by demonstrating how advanced technologies can be integrated to protect user data in a cloud environment.

1.2 Problem Statement

Existing cloud file sharing platforms often lack adequate security mechanisms, leading to risks such as data leakage, unauthorized access, and loss of user privacy. There is a need for a secure file sharing system that protects data at every stage. With the rapid growth of cloud computing and remote collaboration, individuals and organizations increasingly rely on cloud platforms to store and share digital files. However, while cloud-based systems offer convenience, scalability, and accessibility, they also introduce significant security and privacy challenges. Many existing file-sharing solutions fail to ensure full protection of sensitive data, leading to issues such as unauthorized access, data leakage, malware attacks, and loss of confidentiality. Traditional file- sharing methods—such as email attachments, portable storage devices, or unsecured public cloud links—are not suitable for handling confidential or large-scale data sharing. These methods lack encryption and access control mechanisms, making files vulnerable during transmission and storage. Furthermore, users often have limited control over how their shared data is accessed, used, or modified once it leaves their local environment

1.3 Objectives of the Project

To design a secure cloud-based file sharing system . To implement user authentication and authorization.To ensure data confidentiality using encryption . To provide secure file upload and download. The main objective of this project is to develop a cloud-based file sharing application that enables users to securely upload, store, and share files over the internet while ensuring the confidentiality, integrity, and availability of data. To achieve this, the project focuses on the following specific objectives: To design and develop a cloud-based platform that allows users to store, access, share files anytime and anywhere through an internet connection. To implement strong data security mechanisms such as encryption (for data at rest and in transit), authentication, and authorization to protect files from unauthorized access. To provide user authentication and role-based access control, ensuring that only authorized users can view, upload, or download files. To ensure secure data transfer between the client and the cloud server using secure communication protocols (e.g., HTTPS, SSL/TLS). To incorporate file management features like upload, download, delete, and version control for efficient file organization. To maintain data integrity by preventing unauthorized modification or corruption of files during storage and transfer. To implement activity logs and audit trails to track file sharing activities and enhance system transparency and accountability. . To create a user-friendly interface that simplifies file sharing and management, ensuring accessibility for both technical and non-technical users.

II. LITERATURE SURVEY

The study titled *Cloud Based File Sharing System with Network Security* by Ruby Angel T. G. et al. presents a secure cloud file sharing architecture that integrates authentication mechanisms, encrypted data transfer protocols such as HTTPS and SFTP, and access control techniques to enhance security in cloud environments. Similarly, Chetan Vijaykumar Dalave et al., in *Secure the File Storage on Cloud Computing Using Hybrid Cryptography Algorithm*, explore the use of hybrid cryptographic methods, including algorithms like Blowfish, to ensure confidentiality and protection of files stored in the cloud. The paper *CloudLock: Secure Data Sharing Using a Hybrid Cryptosystem in Multi-Cloud Data Storage* proposes a hybrid ChaCha20-Poly1305 based encryption framework designed to provide secure data sharing across multi-cloud platforms, offering improved performance and resilience.

Jeetendra Singh Yadav and Ashish Pandey, in *Implementing an Advanced and Secure Framework for Data Sharing in Mobile Cloud Platforms*, introduce a hybrid encryption model that ensures strong end-to-end security for file sharing in mobile cloud environments. Another approach is presented in *Secure Cloud File Sharing Scheme Using Blockchain and Attribute-Based Encryption*, which combines blockchain smart contracts with Attribute-Based Encryption (ABE) to achieve fine-grained and decentralized file sharing security. Kandra Keerthi and A. Murali Mohan Kumar, in *Sharing Files on Cloud Storage Using a Group Key Management Protocol*, propose a hybrid encryption technique integrated with a group key management protocol to secure shared files within cloud systems.

Furthermore, Muthi Reddy P., Manjula S. H., and Venugopal K. R., in *Secure Data Sharing in Cloud Computing: A Comprehensive Review*, provide an extensive survey of encryption methods, key management techniques, and data sharing security schemes in cloud storage. Lastly, Rohith Karthikeya and D. Murali, in *WEB CLOUD: Web-Based*

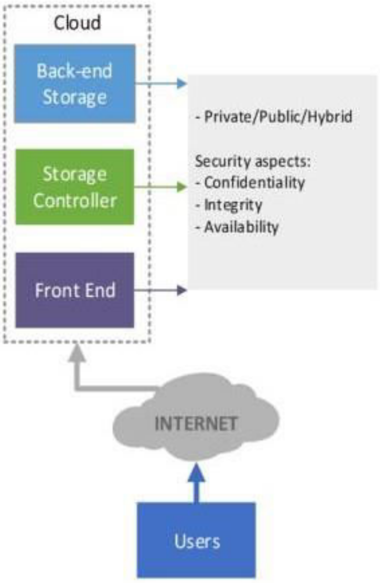
| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902014

Cloud Storage for Secure Data Sharing Across Platforms, discuss a web-based cloud storage model that supports cross-platform secure file sharing through encryption mechanisms and collaborative features. Together, these studies highlight various cryptographic, architectural, and decentralized approaches aimed at enhancing security, confidentiality, and reliability in cloud-based file sharing systems.

III. SYSTEM ARCHITECTURE



The architecture of the Cloud-Based File Sharing System with Data Security consists of multiple integrated layers that work together to ensure confidentiality, integrity, and secure access to stored files. The Client Layer serves as the entry point of the system, allowing users to interact through a web or mobile interface. This user interface provides functionalities such as registration, login, file upload, file download, file sharing, and file management. It is designed to be user-friendly while maintaining secure communication with the backend server through HTTPS protocols. The File Upload and Download Module within this layer manages the transfer of files between the user’s device and the server. During upload, the selected file is securely transmitted to the application server, and during download, encrypted files are retrieved and delivered securely after proper authorization.

The Application Server acts as the core processing unit of the system and handles all business logic and security mechanisms. The Authentication Module verifies user credentials using secure methods such as password hashing and optional multi-factor authentication to prevent unauthorized access. Once authenticated, users are granted secure session tokens for continued interaction. The Encryption and Decryption Module ensures data confidentiality by encrypting files before they are stored in the cloud and decrypting them only when authorized users request access. Typically, a hybrid encryption approach can be used, where symmetric encryption algorithms secure the file data and asymmetric encryption protects the encryption keys. The Access Control Manager further strengthens security by enforcing role-based or attribute-based access control policies. It determines which users are permitted to view, download, edit, or share files and maintains logs for monitoring and auditing purposes.

The Database Server is responsible for storing structured information related to users and files. It securely maintains user credentials in encrypted or hashed form to prevent exposure of sensitive data. In addition to credentials, the database stores file metadata such as file names, upload timestamps, ownership details, storage paths, and permission settings. This metadata enables efficient file management, retrieval, and monitoring without exposing the actual file content.

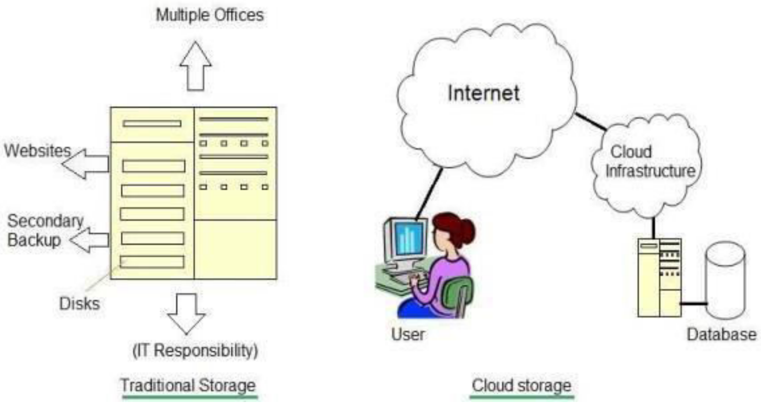
Cloud Storage forms the final layer of the architecture and is used to store the actual encrypted files. Only encrypted versions of files are stored in the cloud, ensuring that even if unauthorized access occurs at the storage level, the data remains unreadable. The cloud storage system also includes backup and replication mechanisms to support disaster recovery and prevent data loss due to hardware failure or cyber-attacks.

The working flow of the system begins when a user logs in securely through the client interface. The authentication module verifies the credentials, and upon successful validation, access is granted. When a user uploads a file, the system encrypts the file before transmitting it to cloud storage, ensuring that no plain-text data is stored externally. The encrypted file is then saved in the cloud, while relevant metadata is stored in the database. When an authorized user requests to download the file, the system first checks access permissions. If authorization is confirmed, the encrypted file is retrieved from the cloud, decrypted securely by the application server, and then delivered to the user through a secure connection. This end-to-end secure workflow ensures that data remains protected throughout storage, transmission, and access, making the system reliable and resistant to security threats.

.

IV. EXISTING SYSTEM

Existing cloud file sharing systems primarily focus on providing convenient storage, easy access, and fast file sharing over the internet. These systems allow users to upload files to remote servers, access them from multiple devices, and share them with others using links or permissions. While this functionality improves collaboration and accessibility, many traditional cloud platforms emphasize usability and storage efficiency more than comprehensive security mechanisms. As a result, security is often implemented at a basic level rather than as a core architectural component.In many conventional systems, files are stored directly in the cloud without strong end-to-end encryption. Although some providers may use encryption during transmission (such as SSL/TLS), the files themselves may be stored in a format that can potentially be accessed by the service provider or exposed if the storage infrastructure is compromised. Without proper encryption before uploading, sensitive information such as personal data, financial records, research documents, and confidential business files becomes vulnerable to unauthorized access. If attackers gain access to cloud servers through hacking, misconfigurations, or insider threats, unencrypted or weakly protected files can be easily exploited. Authentication mechanisms in traditional systems are often limited to simple username and password verification. Weak passwords, password reuse, and lack of multi-factor authentication increase the risk of account compromise. Brute-force attacks, phishing attacks, and credential stuffing are common threats that exploit these weak authentication methods. Without additional layers such as OTP verification, biometric authentication, or token-based session management, user accounts remain susceptible to intrusion



Due to these limitations, traditional cloud file sharing systems become vulnerable to various cyber threats, including data breaches, ransomware attacks, insider misuse, man-in-the-middle attacks, and unauthorized third-party access. Data leakage not only results in financial losses but can also damage organizational reputation and violate data protection regulations. Therefore, while existing systems provide convenience and accessibility, they often lack the advanced security architecture required to protect sensitive information in modern cloud environments.

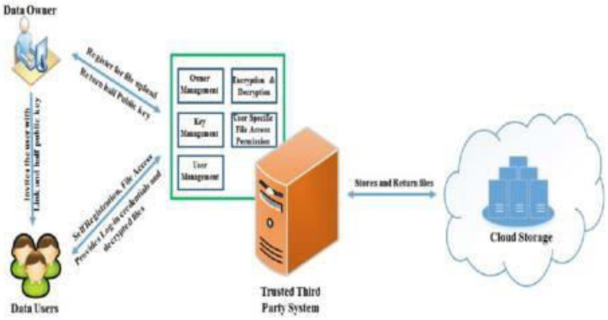
V. PROPOSED SYSTEM

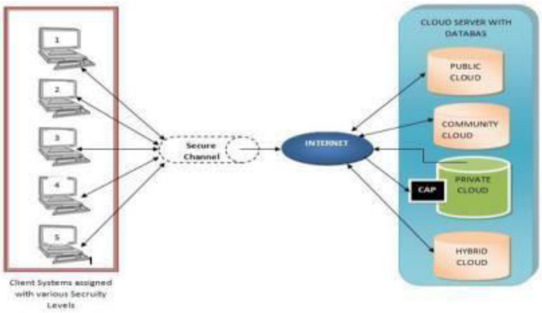
The proposed system introduces a highly secure cloud-based file sharing application designed to address the security gaps found in traditional cloud storage platforms. Unlike conventional systems that prioritize storage and accessibility over protection, this model integrates strong cryptographic techniques and advanced authentication mechanisms directly into its architecture. The primary objective of the proposed system is to ensure data confidentiality, integrity, and controlled accessibility throughout the entire file lifecycle from upload to storage and download.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902014


Data Owner
Register for file upload
Return half Public key
Invites the user with Link and half public key
Owner Management
Encryption & Decryption
Key Management
User Specific File Access Permission
User Management
Self Registration, File Access
Provides Log-in credentials and decrypted files
Data Users
Trusted Third Party System
Stores and Return files
Cloud Storage



The proposed system also incorporates Role-Based Access Control (RBAC) to manage user permissions efficiently. RBAC ensures that users are assigned specific roles—such as administrator, file owner, or viewer—and each role has predefined access privileges. This prevents unauthorized actions such as editing, deleting, or sharing files without proper permission. By enforcing structured access policies, the system minimizes insider threats and prevents privilege escalation. Access rights are dynamically verified each time a user attempts to interact with a file, ensuring continuous authorization enforcement.In addition to encryption and access control, the system implements secure login authentication mechanisms. User credentials are protected using password hashing and salting techniques, preventing storage of plain-text passwords. Multi-factor authentication (MFA) can be integrated to add an extra layer of protection, requiring users to verify their identity through OTP or secondary authentication methods. Secure session management techniques are also employed to prevent session hijacking and replay attacks.

To further enhance security, the system includes activity monitoring and auditing features. Every significant user action—such as login attempts, file uploads, downloads, sharing activities, and permission changes—is recorded in system logs. These logs help administrators detect suspicious behavior, investigate security incidents, and maintain accountability. Real-time monitoring can also trigger alerts in case of unusual access patterns or repeated failed login attempts.The system verifies file integrity using hashing techniques to ensure that stored or transmitted files have not been tampered with. Before and after upload, cryptographic hash values can be generated and compared. If any alteration occurs, the system detects the mismatch and prevents corrupted or modified files from being accessed. This guarantees data integrity alongside confidentiality.

ADVANTAGES

□ The system significantly **reduces hardware and maintenance costs** because organizations do not need to maintain local servers. Cloud providers handle infrastructure management, updates, and system reliability.

□ It also provides **automatic backup and disaster recovery**, ensuring that data is not permanently lost due to hardware failure, accidental deletion, or cyber incidents. This improves reliability and business continuity.

□ The system ensures **file integrity and confidentiality** by combining encryption with hashing techniques. Users can trust that their files are authentic and have not been tampered with.

□ Another major advantage is **fast and secure file sharing**. Optimized cloud infrastructure
enables quick file transfers while maintaining strong security standards.

□ The system maintains **user activity logs and monitoring**, which increases transparency and accountability. Administrators can track login attempts, file access, and sharing activities, helping detect suspicious behavior early.

□ It is highly suitable for **education, corporate, healthcare, and banking sectors**, where sensitive data must be protected according to strict privacy regulations.

□ Overall, the biggest advantage is comprehensive **protection against data breaches and
cyber attacks**. By integrating encryption, authentication, access control, monitoring, and backup mechanisms, the system provides a complete security framework rather than just basic cloud storage functionality

VI. CONCLUSION

The Cloud-Based File Sharing Application with Data Security provides a secure and reliable solution for storing and sharing files over the cloud. By integrating encryption techniques such as AES and RSA with secure authentication and access control mechanisms, the system ensures data confidentiality, integrity, and availability. Compared to traditional cloud storage systems, the proposed model enhances security while maintaining usability. Future enhancements may include blockchain integration and multi-factor authentication for stronger protection. In addition to encryption, the system incorporates secure authentication methods and role-based access control mechanisms to verify user identity and restrict access according to predefined permissions. This structured security approach guarantees data confidentiality, maintains file integrity through verification techniques, and ensures availability through reliable cloud storage and backup mechanisms. User activity monitoring further strengthens accountability and helps detect suspicious behavior. Compared to traditional cloud storage models, the proposed system significantly enhances overall security without sacrificing usability or performance. It offers remote accessibility, scalability, and cost-effectiveness while maintaining strong protection standards. Future enhancements may include blockchain integration for tamper-proof transaction records, multi-factor authentication for stronger identity verification, AI-based threat detection, and advanced key management techniques to further improve resilience against emerging cyber threats. Overall, the system represents a comprehensive and future-ready approach to secure cloud-based file sharing.

VII. FUTURE SCOPE

The future enhancement of the proposed secure cloud-based file sharing system includes the implementation of Multi-Factor Authentication (MFA) to further strengthen user verification. By requiring additional authentication factors such as one-time passwords, security tokens, or biometric confirmation, the system can significantly reduce the risk of unauthorized account access even if passwords are compromised. Another major improvement is the integration of blockchain technology to secure file transactions. Blockchain can provide decentralized verification, tamper-proof transaction records, and transparent auditing of file sharing activities, thereby enhancing trust and security in cloud environments.

The system can also incorporate AI-based threat detection and intrusion prevention mechanisms to proactively identify suspicious behavior, abnormal login patterns, or potential cyber-attacks. Artificial intelligence algorithms can continuously monitor system activity and automatically respond to threats in real time, improving overall resilience. Implementing End-to- End Encryption (E2EE) will further enhance privacy by ensuring that only the sender and intended recipient can decrypt the data, preventing even the cloud service provider from accessing file contents.Biometric authentication methods such as fingerprint scanning and facial recognition can be introduced to improve both security and user convenience, especially in mobile environments. Additionally, adopting a Zero-Trust security architecture would ensure that no user or device is trusted by default, requiring continuous verification before granting access to resources. This approach minimizes internal and external security risks.

REFERNECES

1. 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.
2. 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.
3. 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.
4. 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 (IJRPETM), 9(1), 113–118.
5. 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 (IJRPETM), 9(1), 119–124.
6. 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.
7. 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.
8. 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.
9. 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 (IJRPETM), 9(1), 125–129.
10. 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 (IJRPETM), 9(1), 130–136.

11. Chinthala, S., Erla, 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.
12. 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 (IJRPETM), 9(2), 486–494.
13. 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 (IJRPETM), 9(2), 495–499.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. Pavan Kumar, T., Abhishek Goud, T., Yogesh, S., Manikanta, V., Dinesh, P., Srinu, B., & Dharnasi, P. (2026). Smart attendance system using facial recognition for staff using AI/ML. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 513–519. https://doi.org/10.15662/IJRPETM.2026.0902005
22. Reddy, V. N., Rao, P. H. S., Singh, N. S., Kumar, V. S. S., Reddy, Y. B., & Dharnasi, P. (2026). Face recognition using criminal identification system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 520–527.
23. Rachana, P., Kalyan, P. P., Kumar, T. S., Reddy, P. M., Rohan, P., Saravanan, M., & Dharnasi, P. (2026). Secure chat application with end-to-end encryption using deep learning. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 472–478.
24. Krishna, G., Rajesh, B., Dinesh, B., Sravani, B., Rajesh, G., Dharnasi, P., & Sarvanan, M. (2026). Smart agriculture system using IoT with help of AI-techniques. International Journal of Computer Technology and Electronics Communication, 9(2), 479–487.
25. Reddy, N. H. V., Reddy, N. T., Bharath, M., Hemanth, N., Dharnasi, D. P., Nirmala, B., & Jitendra, A. (2026). AI based learning assistant using machine learning. International Journal of Engineering & Extended Technologies Research, 8(2), 495–504.
26. Vangara, N., Bhargavi, P., Chandu, R., Bhavani, V., Yadav, D. B., & Dharnasi, P. (2026). Machine learning based intrusion detection system using supervised and unsupervised learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 505–511.
27. Yadamakanti, S., Mahesh, Y., Rathnam, S. A., Praveen, V., Jitendra, A., & Dharnasi, P. (2026). Unified Payments Interface fraud detection using machine learning. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 488–497.
28. Basha, S. A., Krishna, V. S. B., Shanker, S. S., Sravya, R., Shivalingam, N., & Dharnasi, P. (2026). AI-powered price prediction for agriculture markets. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 512–515.
29. Sanjay, P., Vardhan, Y. H., Raja, S. Y., Krishna, V. M., Nirmala, B., & Dharnasi, P. (2026). Disaster management and earthquake tsunami prediction system using machine learning and deep learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 516–522.
30. Varsha, P., Chary, P. K., Sathvik, P., Varma, N. V., Rahul, S., Saravanam, M., & Dharnasi, P. (2026). IoT-based fire alarm and location tracking system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 528–532.
31. Priya, B. A., Gayathri, D., Maheshwari, B., Nikhitha, C., Sravanam, D., Yadav, D. B., & Saravanan, M. (2026). Fake news

detection using natural language processing. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 498–505.

32. Prasad, K., Rakesh, K., Vishnu, G., Raju, G., Vardhan, K., Sarvanan, M., Dharnasi, D. P., & Alaparth, A. J. (2026). Handwritten character recognition using neural networks. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 532–541.
33. Harish, G., Venkatesh, M., Venkatesh, M., Sandeep, G., Mustaffa, M., Sarvanan, M., Dharnasi, D. P., & Alaparth, A. J. (2026). Heart disease prediction using ML and pandas. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 506–515.
34. Vishwanath, M. Y., Ganapathi, K., Krupa, K. D., Bharat Kumar, K. L. N., Reddy, K. S., Saravanan, M., & Dharnasi, P. (2026). Online election system to avoid fraud voting by using cybersecurity techniques with the help of ML techniques. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 516–526.
35. Nithin, A., Harish, B., Prashanth, B., Shirisha, C. H., Raviteja, C. H., Prasad, D., & Saravanan, M. (2026). One stop personalized career and educational advisor. International Journal of Engineering & Extended Technologies Research, 8(2), 542–550.
36. Naresh, D., Anand, P., Harish, M., Vamshi, A., Kethan, A., Nirmala, B., & Saravanan, M. (2026). Face recognition door lock system with IoT & AI. International Journal of Computer Technology and Electronics Communication, 9(2), 526–534.
37. Dharnasi, P. (2025). A Multi-Domain AI Framework for Enterprise Agility Integrating Retail Analytics with SAP Modernization and Secure Financial Intelligence. International Journal of Humanities and Information Technology, 7(4), 61-66.
38. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. Circuits Syst., 7, 3807-3817.
39. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4111-4115.
40. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4111-4115.