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 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013

Blockchain Integration with Cloud Storage for Secure and Transparent File Management

Tirupalli Sriya Reddy, Munduri Sohan Krishna, Sangaraju Viswanath, Yeruva Sneha Deepika, 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

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: 30.01.2026; Revised: 18.02.2026; Accepted: 23.02.2026; Published: 28.02.2026.

ABSTRACT: File get handled differently now – encryption handles them in the cloud. Every more afterward shows up on a blockchain log, stuck there forever, cannot be altered later. Actions like sharing, viewing, or editing appear one after without gaps. Permission rules live inside self-executing agreements that watch who does what. Access stays locked down until conditions line up just right. A fresh approach to handling digital files emerges when these tools work together. Because data moves with identifiable markets, trust grows around how files are shared or accessed later. In settings where security matters most – like hospitals, banks, or counts – this method helps meet strict rules without sacrificing speed. What stands out is how each action inside a shared folder leaves a clear mark behind it. Not every idea for online storage brings such clarity on security and openness at once. This method targets reliable handling of files while maintaining openness and safety. It brings together features from separate technologies in a way that works well. The setup helps keep data accurate, private, and supported by clear proof of every action tied to files.

KEYWORDS: Blockchain, Cloud storage, Secure file management, Data integrity, Privacy, Smart contracts.

I. INTRODUCTION

Cloud storage services have brought a revolution in the way people and organizations store and manage their digital data by making it unnecessary to have local storage infrastructure. However, despite the benefits, the centralized cloud storage system has some drawbacks, such as a lack of transparency, the risk of data breaches, and the need to rely on third-party trust. There is no direct way for the user to check whether their data has been modified or accessed illegitimately. The blockchain technology, with its decentralized and immutable ledger, offers a promising solution to these problems. By storing data-related transactions in a blockchain, it is possible to ensure transparency, traceability, and tamper-proofing. This paper proposes a hybrid architecture that combines blockchain technology with cloud storage.

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

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013

II. LITERATURE REVIEW

It looks at the impact of incorporating blockchain tech into cloud storage systems and how that affects the security and transparency in the storage, retrieval, and management of files. From what we look at, the focus shifts from storage of files and more to trust, tracking, and record-keeping. Each study considers the potential in the technology of immutable logs in distributed systems. Some of the studies look at how certain types of encryption and shifts that block the ability to make changes without detection. Others look at the speed versus security trade-offs that are created by the addition of certain types of security checks. Some of the studies look at how control over access to the storage and retrieval system is decentralized. The studies investigate systems in the real world and use simulation models of their hybrids. The results of the studies point to the existence of more effective audit trails, although they also point to longer retrieval times. The trust in the system is also a factor upon which the system in the technology depends, and in certain cases the performance of the system depends on the technology. The lack of scalability of some system designs is also an issue upon which the technology and system depend. The security upgrades in the systems and technologies of the system tend to come at costs that the majority of users fail to see. Persistent developer interest, however, is evident in the system improvements that security upgrades come at costs to users. The earlier systems lacked adaptability, and the newer systems are offering adaptation at a faster pace. The need for privacy is driving innovations in the systems and technologies to control access to the systems and technologies in a more intelligent way. The evolution of the systems and technologies of the system and technology to control access to the systems and technologies lets the history of files become visible without exposing the content of the files. The studies show that the potential of new digital ledgers is strong, despite the limitations of these systems. One way to end this is to look for a study led by Meet Shah on the storage of files in a network using blockchain technology. As opposed to large firms dominating everything, fragments exist on multiple machines across the globe, making it significantly harder to leak information. Since control is distributed, no one machine crashing takes everything down. Internet-connected devices that voluntarily provide storage create networks that share loads far more efficiently than any previous system. Everyone in the network has the same record, so corrections to the record after it has been saved are immediately visible to all. The overall safety of the system increases when changes require the consent of everyone in the network, not just one person at the top. Each file is divided into smaller parts and distributed to separate computers in a network called the InterPlanetary File System (IPFS). Each small part is encrypted before it is sent. Each part is given a unique address that indicates the location of the part. This address is linked to the blockchain where it remains unchangeable. Since no single central server holds all the information, the security of the system is enhanced.

III. PROBLEM STATEMENT

The conventional cloud storage solution has some issues regarding data security, integrity, transparency, and unauthorized access. As files are stored in a centralized system, they are prone to data tampering, single-point failure, and alack of trust between users and service providers. There is no trustworthy way to check whether the stored data has been tampered with without the users' consent. Thus, there is a requirement for a secure and transparent file management solution that combines blockchain technology with cloud storage solutions. By storing cryptographic hash values and metadata on the blockchain, data integrity can be verified at any time. This approach improves trust, prevents unauthorized modifications, and ensures secure access while maintaining efficient storage management.

IV. EXISITING SYSTEM

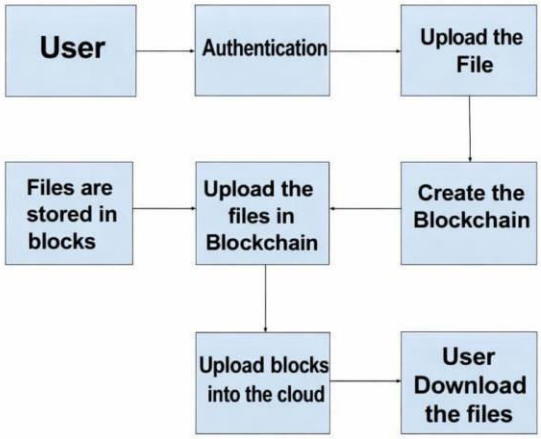
The system currently integrates blockchain and cloud computing to provide secure and transparent file management. To access the system, users must first log in. After logging in, users are able to upload files to the system, at which point the system creates a cryptographic hash value for the file. The system then creates a new block in the blockchain which contains the file metadata, including the hash value, the date, and the user information. However, the system does not store the file on the blockchain; rather, it stores the hash value and the corresponding reference information, while the file itself is stored in the cloud. This design allows for enhanced scalability and efficiency of the system.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

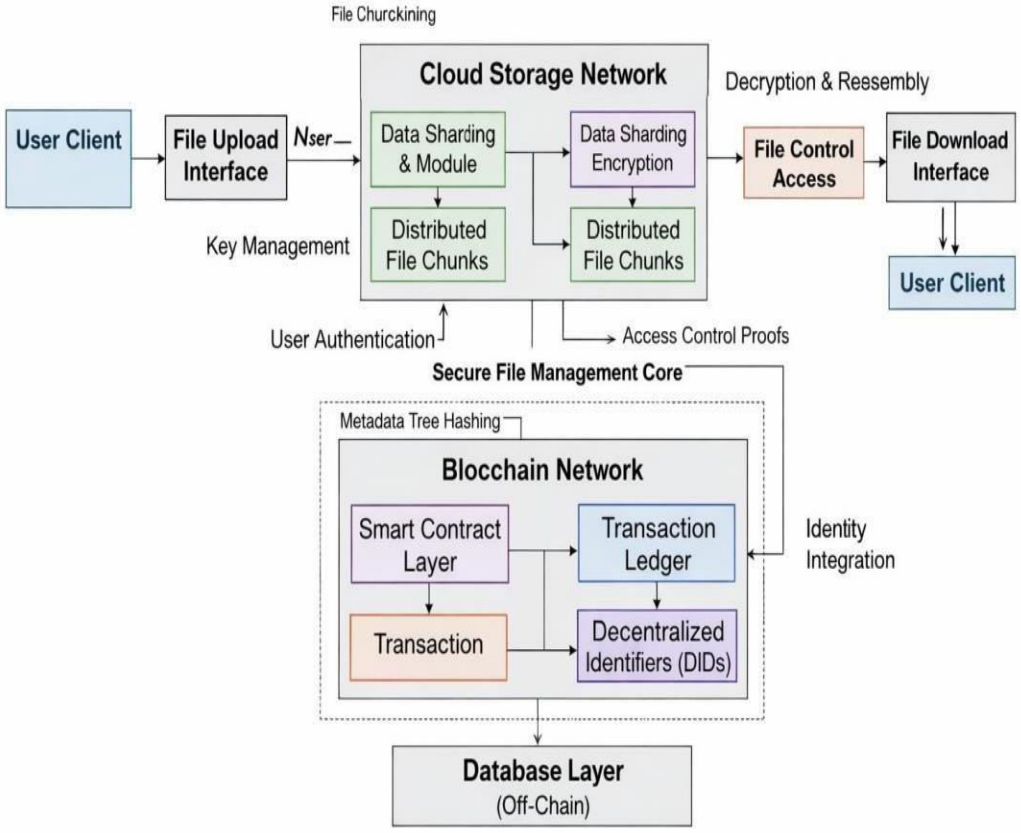
|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013



Whenever a user desires to download a file, the system removes the file's information from the blockchain and then checks the integrity of the file by performing a hash value comparison. If the hash values are found to be equal, then the specified file is downloaded from the cloud storage. This design approach maintains the integrity of the data, does not allow for any unauthorized changes to be made to the files, and maintains transparency and trust in the management of files.

V. PROPOSED SYSTEM



International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

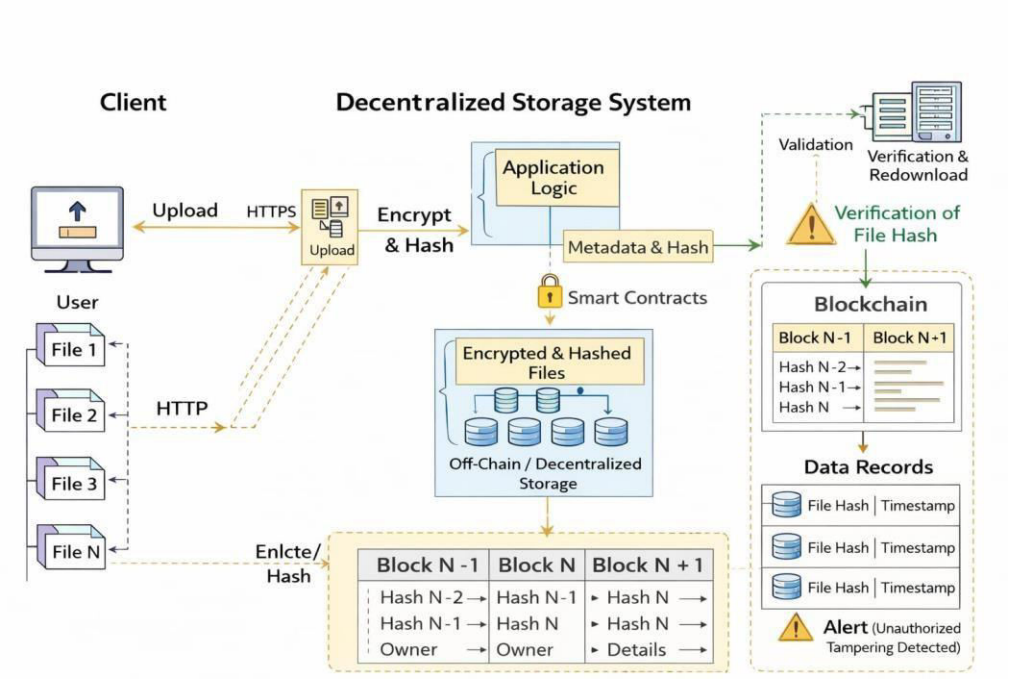
|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013

The paper proposes a system for cloud storage that uses a decentralized system and blockchain for enhanced security and privacy. Our system has four primary layers. The User Interaction Layer, The Cloud Storage Network Layer, The Secure File Management Core Layer, and the Blockchain and Database Layer. The User Interaction Layer allows clients to upload and download files securely with access verification and download verification. The Cloud Storage Network Layer is responsible for the Cloud storage network and uses a technique referred to as file \chunking" that fragments files into smaller "chunks" that are encrypted individually and stored across several cloud storage servers. This allows for greater confidentiality and increases the system's tolerance to the loss of a server. The Secure File Management Core Layer is the primary orchestration layer for the system that handles authentication, access control, and the hashing of the file metadata into a digital signature stored in a hash tree for additional security. The blockchain layer provides storage for integrity proofs and has decentralized identifiers for resolving identity non-availability in the database for the non-key file metadata and index that are used for cloud storage cost reduction. When files are uploaded, they are encrypted, divided into several duplicates of the same chunk".

VI. METHODOLOGY AND DESIGN

The Blockchain Integration with Cloud Storage for Secure and Transparent File Management system employs a modular system design and methodology to address the security, transparency, and efficiency concerns for file handling operations. The system offers a web interface for users to upload and access files, while the backend server processes requests and handles authentication and validation. For confidentiality and the generation of proof of integrity, files are encrypted and hashed prior to being stored. To achieve scalability and cost efficiency in blockchain storage, the encrypted file data is placed in off-chain cloud storage or decentralized storage, while the essential metadata (file hash, owner information, and timestamps) are stored on the blockchain.



While downloading files, the app checks the hash of the file and compares it with the hash value on the blockchain to ensure integrity. This way, the app can verify that the file has not been altered in an unauthorized way. Access control policies can be implemented via smart contracts, which can prevent unauthorized users from downloading or sharing files. This provides users with trust to verify operations through an audit trail that shows all operations of the files. This is not possible on traditional cloud storage. The app employs a multi-tiered architecture where all UI, app logic, storage, and blockchain parts are separated from one another in order to provide more robust security. The client layer offers an interface for users, while the application layer provides file upload, encryption, and storage and blockchain communication. The storage layer contains all of the files in encrypted form, while the blockchain layer contains all of the file metadata with an unaltered and traceable audit trail. This architecture enables the app to be expanded easily to include new features such as storage, new encryption methods, and new enterprise access control systems.

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 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013

ANALYSIS

It has also been noted that integrating blockchain technology with cloud storage services can greatly improve the security, transparency, and trustworthiness of a data storage system. In this approach, data is stored on the cloud, while blockchain technology is used to store the metadata. It can be further explained as follows: in a blockchain-based approach, data is stored on the cloud, while at the same time, blockchain technology stores the metadata or hashes of the stored files. Access to the data, as well as modifications made thereto, can be fully tracked, thus enhancing the data integrity objective. This is due to the fact that in the event of any modification or unauthorized access to the stored data, it can be easily tracked using the hash function. On the other hand, in a cloud storage system, there are risks of a host of data loss due to any unauthorized user. All these risks are eliminated when integrating blockchain with cloud storage. However, as noted in one document, integrating blockchain technology with cloud storage results in an increase in latency. However, this increase in latency in a blockchain-based approach is considered worthwhile in the end, considering that it improves the security, transparency.

VII. REAL TIME APPLICATIONS

Blockchain-Based Secure Distributed File Storage (IPFS / Decentralized Cloud):
A research project and implemented framework where blockchain is combined with decentralized file storage (e.g., IPFS) to improve security, transparency, and reliability compared with traditional cloud systems. Files are broken into shards, hashed, and distributed across nodes with smart contract usage for access agreements.

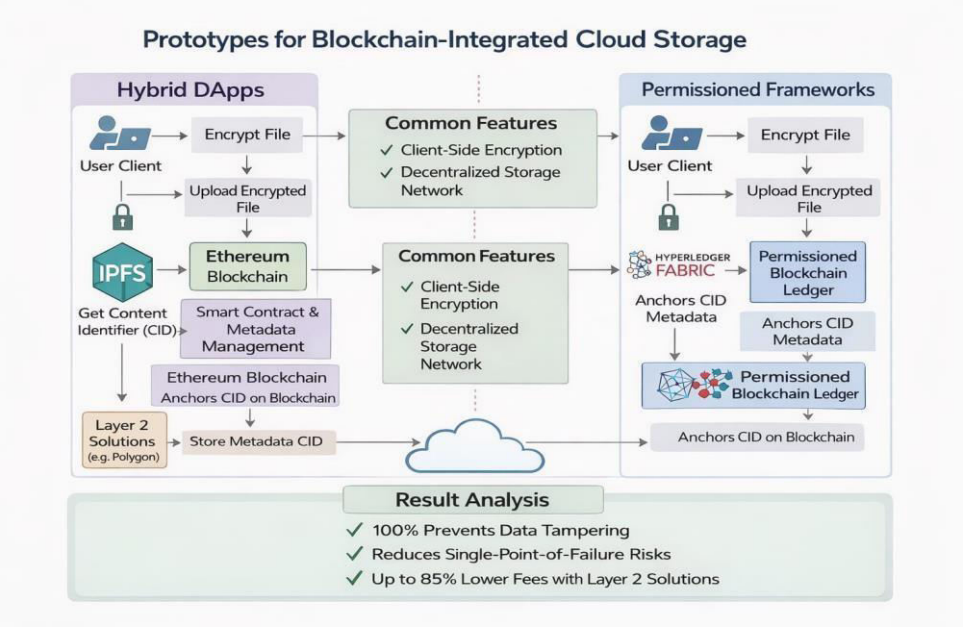
Secure Real-Time File Sharing Using Blockchain Technology:
Academic application presenting a real-time secure file sharing system using blockchain to log actions immutably, with encryption to protect file contents, and a backend developed (e.g., Flask/Python) for upload/download workflows.

Secure Cloud File Sharing & Access Control (Blockchain + Attribute-Based Encryption):
Published research in Computer Standards & Interfaces focused on using blockchain along with advanced encryption (attribute-based) and smart contracts to handle secure file sharing and access control in cloud contexts.

Inter-Organization Secure File Sharing with Hyperledger & IPFS:
This project proposes using a permissioned enterprise blockchain (Hyperledger Fabric) in combination with IPFS for decentralized and authenticated file sharing across organizations — addressing trust, transparency, and integrity.

VIII. PROTOTYPE

Prototypes of blockchain-enabled cloud storage systems usually belong to one of the following categories: Hybrid



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

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013

Dapp's (Decentralized Applications), which rely on Ethereum smart contracts for metadata management in combination with the IPFS (Interplanetary File System) for off-chain storage, and Permissioned Frameworks such as Hyperledger Fabric, which are designed specifically for enterprise-grade data privacy without the need for public cryptocurrency transaction costs. In a standard hybrid prototype, a file is encrypted on the client side, uploaded to a decentralized network to obtain a distinct Content Identifier (CID), and finally, the CID is anchored to a blockchain ledger for the purpose of its immutability and traceability. Analysis of results from these prototypes has consistently shown a 100% success rate in protecting against unauthorized data manipulation and a marked decrease in single-point-of-failure risks. While performance analysis has revealed a slight increase in latency times compared to standard centralized cloud storage systems (1.2s vs. 0.9s for document uploads), the data has clearly shown that the use of Layer 2 scaling solutions such as Polygon can lower transaction costs by as much as 85%, making the system both economically feasible and greatly superior in terms of providing transparent audit trails.

IX. CONCLUSION

Combining cloud storage and blockchain technology will allow for greater security and transparency when managing files. The solution will allow greater security of files by allowing the fragmentation and encryption of files to be stored on a variety of different nodes, while the blockchain will store the proof and access rights to guarantee that files will not be modified in a malicious manner and that only authorized individuals will be able to access the files. Overall, the solution will provide greater privacy, integrity, and trust, though improvements in speed, cost, and scalability will be needed to allow for widespread use in cloud storage. The proposed answer also offers a greater solution for user trust through the integrity of data and access through decentralization. Smart contracts will provide a greater solution to access control by allowing automated administrative controls to be exercised with little to no human touch. On the other hand, with all the advantages that come with the use of cloud and blockchain technology, the problems of latency, storage costs, and diminished scalability continue to exist. For a greater use of the technologies, improvements must be made regarding the speed of blockchains, the cost of the system, and the lack of friction between the cloud and blockchain storage systems. Research will show that the fused technologies will have a greater impact.

X. FUTURE SCOPE

Integrating blockchain with cloud storage will allow us to move away from the present model of "rented" data storage to a world in which we will have decentralized data sovereignty. Today, we rely on a small number of large companies who control our data, leading to a world with a "single point of failure." This means that a single data breach, or a single change in contractual terms, could put billions of data files in jeopardy. With the advent of blockchain technology, we will be able to move away from centralized storage. Instead of large farm-based storage solutions, data will be divided, encrypted, and distributed across many independent nodes around the world. Smart contracts will act as 'digital notaries,' allowing users to prove that their data exists, that it is not altered, and that it is available in a 2026-accessible way: unencumbered and with no intermediary. The combination of Zero-Knowledge Proofs (ZKPs) and Artificial Intelligence (AI) is necessary in this area. The rising tide of generative AI and the fake content it generates, means that data storage solutions will have to be integrated with blockchain to be trustworthy data sources. By the year 2026, we expect to see the introduction of the "Content Passport" service, which integrates the metadata of a file (such as its creator, the date, and the edit history of the file) onto a blockchain, while the content of the file is stored in a decentralized cloud storage system. This makes the storage blockchain technology files which proves the files' authenticity. This is particularly useful in the legal, medical, and governmental fields where the value of a document may not equal the value of the file. In addition to this, DePIN (Decentralized Physical Infrastructure Networks) is changing the economic landscape of cloud storage. DePIN creates a highly efficient "spot market" for storage. Picture a world where your smart fridge, your self-driving car, or your office PC can automatically rent its unused terabytes to the system in exchange for tokens that can then be used to purchase your encrypted storage. This is a closed-loop, self-reinforcing economic system that significantly decreases the price of storage by utilizing previously "dormant" storage across the globe. The decentralized system will be the only way to manage the vast quantity of data in a cost-efficient manner as we approach the "Metaverse" and high-bandwidth IoT environments.

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

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013

REFERENCES

1. Lakshmi, A. J., Dasari, R., Chilukuri, M., Tirumani, Y., Praveena, H. D., & Kumar, A. P. (2023, May). Design and implementation of a smart electric fence built on solar with an automatic irrigation system. In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1553–1558). IEEE.
2. 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.
3. Sugumar, R. (2025). Explainable AI-driven secure multi-modal analytics for financial fraud detection and cyber-enabled pharmaceutical network analysis. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, 8(6), 13239–13249.
4. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. *International Journal of Innovative Research in Computer and Communication Engineering*, 7(1), 49–63.
5. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder–decoder architecture. *Biomedical Signal Processing and Control*, 108, 107932.
6. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. *Circuits and Systems*, 7, 3807–3817.
7. Prasanna, D., & Manishvarma, R. (2025, February). Skin cancer detection using image classification in deep learning. In *2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1–8). IEEE.
8. 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.
9. Inbavalli, M., & Arasu, T. (2015). Efficient analysis of frequent item set association rule mining methods. *International Journal of Scientific & Engineering Research*, 6(4).
10. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep learning-driven visual analytics framework for next-generation environmental monitoring. *Journal of Applied Science and Technology Trends*, 114–122.
11. Kiran, A., Rubini, P., & Kumar, S. S. (2025). Comprehensive review of privacy, utility and fairness offered by synthetic data. *IEEE Access*.
12. 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.
13. Sakthivel, T. S., Ragupathy, P., & Chinnadurai, N. (2025). Solar system integrated smart grid utilizing hybrid coot-genetic algorithm optimized ANN controller. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 1–24.
14. Madheswaran, M., Dhanalakshmi, R., Ramasubramanian, G., Aghalya, S., Raju, S., & Thirumaraiselvan, P. (2024, April). Advancements in immunization management for personalized vaccine scheduling with IoT and machine learning. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1566–1570). IEEE.
15. Poornachandar, T., Latha, A., Nisha, K., Revathi, K., & Sathishkumar, V. E. (2025, September). Cloud-based extreme learning machines for mining waste detoxification efficiency. In *2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 1348–1353). IEEE.
16. Aashiq Banu, S., Sucharita, M. S., Soundarya, Y. L., Nithya, L., Dhivya, R., & Rengarajan, A. (2020). Robust image encryption in transform domain using duo chaotic maps—A secure communication. In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020* (pp. 271–281). Springer.
17. 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.
18. Karthikeyan, K., & Umasankar, P. (2025). A novel buck-boost modified series forward (BBMSF) converter for enhanced efficiency in hybrid renewable energy systems. *Ain Shams Engineering Journal*, 16(10), 103557.
19. 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.

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

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901013

20. 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.
21. Yashwanth, K., Adithya, N., Sivaraman, R., Janakiraman, S., & Rengarajan, A. (2021, July). Design and development of pipelined computational unit for high-speed processors. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–5). IEEE.
22. Prasanna, D., Ahamed, N. A., Abinesh, S., Karthikeyan, G., & Inbatamilan, R. (2024, November). Cloud-based automatically human document authentication processes for secured system. In *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)* (pp. 1–7). IEEE.
23. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. *International Journal of Innovative Research in Computer and Communication Engineering*, 7(1), 49–63.
24. Saravanan, M., Kumar, A. S., Devasaran, R., Seshadri, G., & Sivaganesan, S. (2019). Performance analysis of very sparse matrix converter using indirect space vector modulation. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 4756–4762.
25. Karthikeyan, K., Umasankar, P., Parathraju, P., Prabha, M., & Pulivarthy, P. Integration and analysis of solar vertical axis wind hybrid energy system using modified zeta converter.