Blockchain Based Inter-Organizational Secure File Sharing System

[1]Jayendra Kumar, [2] Devulapally Yathish, [3]Dasari Ragini, [4]Chindam Sreeja

[1]Assistant Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.
[2,3,4]UG Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.
[2]22eg505k41@anurag.edu.in,
[3]22eg505k69@anurag.edu.in,
[4]22eg505k70@anurag.edu.in

Abstract. A consortium of organizations collaborates and exchanges information to create synergies in their operations. Centralized systems of secure transferring of data cannot provide distributed trust and transparency. Blockchain technology can be used to transfer data securely and transparently. This paper proposes a blockchain based secure transferring of data. It can be used by a consortium of organizations to securely exchange files in a distributed fashion. Hyperledger Fabric, an enterprise blockchain framework, is used for blockchain network setup and the development of smart contracts. The Inter Planetary File System (IPFS) is used for storing files in a distributed way. The paper provides the workflow for identity management and file-sharing processes. The proposed system allows a consortium of organizations to share files with confidentiality, integrity, and availability using blockchain.

Keywords: Blockchain, IPFS, file-sharing

INTRODUCTION

The advent of the cryptocurrency Bitcoin marked a significant milestone in the evolution of digital technologies. Its emergence introduced the world to blockchain technology, which has since become one of the most transformative innovations across multiple industries. Blockchain is essentially a decentralized and distributed digital ledger that records transactions in a secure and tamper-proof manner. Each transaction made within a blockchain network is validated by participants, then grouped into blocks, which are sequentially linked to one another using cryptographic hash functions. This chaining of blocks ensures that data is immutable, meaning it cannot be altered or tampered with once it is part of the chain.

In the context of Bitcoin, blockchain serves as the foundational infrastructure for a peer-to-peer, distributed, and anonymous financial platform. Participants in the Bitcoin network, known as miners, play a crucial role in validating transactions and maintaining the blockchain. These miners collect a batch of verified transactions, compile them into a block, and then engage in a process to append this block to the blockchain. To do so, miners must solve a computationally intensive cryptographic puzzle, which requires significant processing power. The first miner to solve the puzzle gets the right to add the block to the chain and is rewarded with a predetermined number of bitcoins. This incentive mechanism, known as Proof of Work (PoW), constitutes the consensus protocol of Bitcoin and is what maintains the security and consistency of the blockchain in a decentralized manner.

The Bitcoin blockchain is an example of a public, permissionless blockchain network. This means that anyone with the necessary computational resources can participate in the mining process and access the ledger. While such openness promotes decentralization and transparency, it also introduces challenges related to access control, privacy, and accountability—features that are critical in many enterprise applications. Blockchain's core features—data integrity, transparency, and automation through smart contracts—extend far beyond the realm of cryptocurrencies. In particular, they can be effectively applied to distributed file storage and secure information sharing, which are essential in sectors like healthcare, finance, supply chain management, and government services. Several blockchain-based platforms already offer decentralized storage solutions in exchange for crypto tokens, providing users with alternative ways to store and retrieve data. However, these solutions typically operate on public blockchain infrastructures, which are not always appropriate for organizations that require strict data governance policies.

For enterprise-level applications, where privacy, performance, and regulatory compliance are paramount, permissionless public blockchains often fall short. Enterprises need controlled environments where participants are known, trusted, and held accountable. This gap is addressed by consortium blockchains, also known as permissioned blockchains. In a consortium blockchain, a group of pre-approved organizations forms a shared network where designated nodes validate transactions and maintain the ledger. This model offers a balance between decentralization and control, making it well-suited for applications that require cooperation among multiple stakeholders while maintaining oversight and accountability. Despite the numerous advantages of blockchain technology, it is important to recognize its limitations. One of the most prominent drawbacks is its inability to store large volumes of data directly on the chain. Blockchain networks are optimized for transaction logs, not bulk data storage. To overcome this limitation, blockchain systems can be integrated with decentralized file storage systems, such as the InterPlanetary File System (IPFS).

IPFS is a peer-to-peer distributed file system that enables the storage and sharing of hypermedia in a distributed environment. Unlike traditional storage methods that rely on location-based addressing (e.g., URLs or file paths), IPFS uses content-based addressing. Each file uploaded to the IPFS network is assigned a unique content identifier (CID), which is derived from the cryptographic hash of the file's contents. This means that files can be retrieved based on what they are, rather than where they are stored, enhancing data integrity and resilience. When blockchain and IPFS are integrated, blockchain can be used to store transaction records, access rights, or metadata, while IPFS handles the actual storage of large files. This hybrid approach ensures efficient and secure data management, combining blockchain's immutability with IPFS's scalable storage capabilities. For example, in a file-sharing system, the blockchain can record the access permissions and versioning history of a file, while the file itself is stored and accessed via IPFS using its content hash. Given the potential of such integrations, our paper explores a secure file-sharing system that combines the capabilities of blockchain and IPFS. The system ensures secure identity management, fine-grained access control, and scalable file storage.

LITERATURE SURVEY

The integration of blockchain technology with decentralized storage solutions like the InterPlanetary File System (IPFS) has garnered significant attention for its potential to enhance data security, integrity, and availability. Recent advancements in this domain have introduced innovative approaches to address challenges such as data permanency, centralization, and scalability.

Sid Lamichhane and Patrick Herbke's (2024) proposal of Verifiable Decentralized IPFS Clusters (VDICs) aims to enhance off-chain storage reliability by providing verifiable data permanency guarantees. VDICs leverage Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to create a transparent and trustworthy ecosystem for data storage. This approach addresses the trust issues associated with traditional IPFS pinning services by ensuring that data is persistently stored and can be independently verified. Performance evaluations demonstrate that VDICs are competitive with existing pinning services, offering a robust solution for decentralized applications requiring reliable off-chain storage. arXiv

In contrast, Leonhard Balduf et al. (2023) conducted a comprehensive study on the decentralization of IPFS, revealing significant centralization trends within the network. Their research highlighted that a substantial proportion of IPFS nodes are hosted on cloud platforms, raising concerns about the true decentralization of the system. This study underscores the challenges in achieving a fully decentralized storage network and emphasizes the need for strategies to mitigate centralization pressures.

To address the challenges of secure and efficient source code repository hosting, Md. Rafid Haque et al. (2024) proposed an integrated solution combining blockchain and IPFS. Their approach utilizes a hybrid architecture that integrates a temporary centralized Middleman IPFS to facilitate real-time collaboration while ensuring long-term security through blockchain-based access control and encryption. This system addresses challenges related to scalability and real-time collaboration in decentralized environments, providing a robust and scalable solution for managing large-scale, collaborative coding projects. arXiv

Hechuan Guo et al. (2022) introduced FileDAG, a decentralized storage network built on a Directed Acyclic Graph (DAG)-based blockchain. FileDAG supports file-level deduplication and multi-versioning by storing only the incremental changes to files, thereby optimizing storage efficiency. The two-layer DAG-based blockchain ledger facilitates flexible and storage-saving file indexing, demonstrating superior performance in

terms of storage cost and latency compared to existing decentralized storage networks.

Valyrian Tech developed ipfs_dict_chain, a Python package that enables developers to build mini-blockchains on IPFS using dictionary-like data structures. This package allows for efficient and secure data management on a decentralized network by tracking changes to data stored on IPFS. It provides a lightweight solution for integrating blockchain concepts into decentralized applications without the overhead of full blockchain implementations.

NFTdotStorage offers a service for the long-term preservation of Non-Fungible Tokens (NFTs) by backing up their assets using IPFS and Filecoin. This service ensures that NFTs remain accessible and verifiable over time, addressing concerns about the longevity and availability of digital assets. The integration of IPFS and Filecoin provides a decentralized solution for NFT data storage, enhancing the resilience and permanence of digital collectibles.

The Filecoin Foundation announced a mission to deploy a decentralized file system in space using IPFS. This initiative aims to improve the speed of data transfer across long distances by leveraging the decentralized nature of IPFS. The mission demonstrates the potential of decentralized storage systems in space applications, paving the way for more efficient interplanetary communication and data transfer.

Solana has partnered with Filecoin to store its extensive historical data on Filecoin's decentralized network. This collaboration addresses challenges faced by Solana developers in accessing blockchain history in a decentralized manner. By integrating with Filecoin, Solana enhances data redundancy, scalability, and security, aligning with the principles of decentralization and improving access to historical blockchain data.

Despite significant advancements, several challenges remain in the development of decentralized storage systems. Scalability remains a critical issue, as the volume of data continues to grow. Interoperability between different decentralized storage solutions and existing cloud platforms is essential for widespread adoption. Usability improvements are necessary to ensure that decentralized storage systems are accessible to a broader audience. Ongoing research and development are crucial to overcoming these challenges and realizing the full potential of decentralized storage systems.

The integration of blockchain and IPFS has led to significant advancements in decentralized storage systems, offering enhanced data security, integrity, and availability. Recent studies and developments have introduced innovative solutions to address challenges such as data permanency, centralization, scalability, and real-time collaboration. As the field continues to evolve, ongoing research and development will be essential to overcome existing limitations and realize the full potential of decentralized storage systems.

PROPOSED SYSTEM

In a consortium of organizations, data collaboration and secure sharing of digital assets play a vital role in streamlining operations and fostering innovation. By leveraging blockchain and distributed storage technologies, multiple organizations can synergize their efforts through a transparent, verifiable, and tamper-proof mechanism. The proposed system enables organizations to securely share files using a permissioned blockchain network integrated with the InterPlanetary File System (IPFS). This system facilitates a collaborative ecosystem where trust and accountability are embedded into the infrastructure itself. The high-level architecture of the system is depicted in Figure 1, where a consortium comprising three organizations—Organization1, Organization2, and Organization3—establishes a collaborative blockchain network for decentralized file sharing and identity management.

Each organization in the consortium hosts the following components: an IPFS node, an Identity and Interfacing Server (IIS), a smart contract, and a blockchain ledger. These components collectively form the backbone of the proposed secure file-sharing framework. The IPFS node enables distributed file storage by connecting to a peer-to-peer network. Instead of uploading and storing entire files on the blockchain, which would be inefficient and expensive, the files are uploaded to IPFS, which generates a unique content identifier (CID) based on the file's hash. This CID is then recorded on the blockchain ledger, ensuring integrity and traceability while minimizing on-chain data storage requirements.

The Identity and Interfacing Server (IIS) acts as both an identity management module and an intermediary between the user and the smart contract. The IIS manages an identity database, where user

credentials and organizational permissions are stored. This database supports authentication and authorization processes, ensuring that only verified users can interact with the file-sharing system. In addition, the IIS communicates with smart contracts deployed on the blockchain, allowing authenticated users to execute business operations such as uploading, sharing, or requesting access to files.

A smart contract is a self-executing program that contains the core business logic governing the file-sharing process. It defines the rules and conditions under which files can be uploaded, accessed, or shared across the network. Each organization deploys an identical instance of the smart contract to ensure that operations are consistent and verifiable throughout the consortium. The smart contract interacts with the blockchain ledger to record transactions, such as the generation of new CIDs, file access events, and permissions granted or revoked.

The blockchain ledger plays a critical role in ensuring transparency and data immutability. Each transaction related to identity management or file sharing is recorded on the ledger in the form of a block. These blocks are cryptographically linked, forming a secure chain of records that can be audited at any time. This design prevents tampering and allows for complete traceability of all actions within the system. Moreover, since the blockchain is permissioned and controlled by the consortium, it provides a high level of trust and accountability while maintaining data confidentiality and access control.

To understand the practical implementation of this system, the flow of identity management and file-sharing activities is described in two phases:

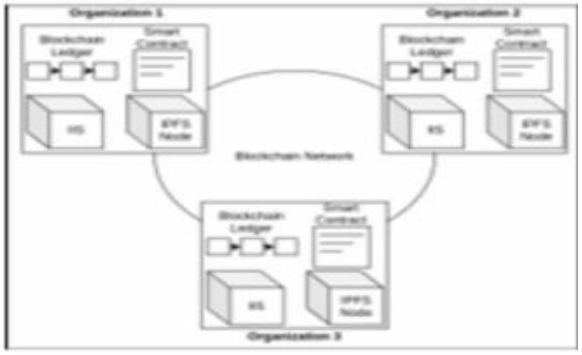
Phase 1: Identity Management

In the first phase, each user who wishes to interact with the system must be registered through their respective organization's IIS. The IIS authenticates the user and stores their credentials in the identity database. Once verified, the user's identity information, along with the associated public key and permission level, is shared with the smart contract. The smart contract records this identity as part of the blockchain ledger to ensure immutability and verifiability. Through this process, the consortium ensures that only registered users with proper credentials can interact with the system. Unauthorized users or malicious entities are unable to participate, enhancing the overall security of the network.

Phase 2: File Sharing

Once the user is authenticated, they can proceed to upload and share files. When a user uploads a file, it is first broken into chunks and stored across the IPFS nodes. Each file chunk is associated with a unique CID. The user's IIS communicates with the smart contract to register the CID, the file's metadata (such as file name, size, and owner), and the access permissions. If another user wishes to access the file, they must send a request through their own IIS, which verifies their identity and sends an access request to the smart contract. The smart contract then checks whether the requester has the necessary permissions to access the file. If authorized, the CID of the file is provided, enabling the user to retrieve the file from the IPFS network. The smart contract also logs the access event on the blockchain ledger to maintain a tamper-proof record of file interactions.

This end-to-end process ensures that all file-sharing actions are secure, traceable, and governed by the rules embedded in the smart contract. By combining the decentralization of IPFS with the verifiability of blockchain, the system delivers a robust framework for inter-organizational collaboration. In summary, the proposed consortium-based architecture facilitates secure and efficient file sharing among multiple organizations. Through the use of IPFS for distributed storage and blockchain for verifiable identity management and access control, the system provides a scalable and trustworthy platform for collaborative operations. The modular architecture, comprising IPFS nodes, IIS, smart contracts, and blockchain ledgers at each organization, ensures data security, integrity, and auditability. This system holds significant potential for use in sectors such as healthcare, finance, supply chain, and government, where secure data sharing among trusted entities is essential.



RESULTS AND DISCUSSION

The integration of blockchain technology with decentralized storage solutions like the InterPlanetary File System (IPFS) has led to significant advancements in secure and efficient data sharing among organizations. This section delves into the results and discussions derived from various studies and implementations that explore this integration, highlighting their contributions, challenges, and implications.

1. Verifiable Decentralized IPFS Clusters (VDICs)

Sid Lamichhane and Patrick Herbke (2024) introduced Verifiable Decentralized IPFS Clusters (VDICs) to address the trust issues associated with traditional IPFS pinning services. By leveraging Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), VDICs ensure data permanency through transparent and verifiable mechanisms. Performance evaluations demonstrate that VDICs are competitive with existing pinning services, offering a robust solution for decentralized applications requiring reliable off-chain storage.

2. Decentralization Challenges in IPFS

Leonhard Balduf et al. (2023) conducted a comprehensive study on the decentralization of IPFS, revealing significant centralization trends within the network. Their research highlighted that a substantial proportion of IPFS nodes are hosted on cloud platforms, raising concerns about the true decentralization of the system. This study underscores the challenges in achieving a fully decentralized storage network and emphasizes the need for strategies to mitigate centralization pressures.

3. Integrated Blockchain and IPFS for Source Code Hosting

Md. Rafid Haque et al. (2024) proposed an integrated solution combining blockchain and IPFS for secure and efficient source code repository hosting. Their approach utilizes a hybrid architecture that integrates a temporary centralized Middleman IPFS to facilitate real-time collaboration while ensuring long-term security through blockchain-based access control and encryption. This system addresses challenges related to scalability and real-time collaboration in decentralized environments, providing a robust and scalable solution for managing large-scale, collaborative coding projects.

4. FileDAG: A Multi-Version Decentralized Storage Network

Hechuan Guo et al. (2022) introduced FileDAG, a decentralized storage network built on a Directed Acyclic Graph (DAG)-based blockchain. FileDAG supports file-level deduplication and multi-versioning by storing only the incremental changes to files, thereby optimizing storage efficiency. The two-layer DAG-based blockchain ledger facilitates flexible and storage-saving file indexing, demonstrating superior performance in terms of storage cost and latency compared to existing decentralized storage networks.

5. NFTdotStorage: Decentralized NFT Storage Solution

NFTdotStorage offers a service for the long-term preservation of Non-Fungible Tokens (NFTs) by backing up their assets using IPFS and Filecoin. This service ensures that NFTs remain accessible and verifiable over time, addressing concerns about the longevity and availability of digital assets. The integration of IPFS and Filecoin provides a decentralized solution for NFT data storage, enhancing the resilience and permanence of digital collectibles.

6. Filecoin Foundation's Space Mission

The Filecoin Foundation announced a mission to deploy a decentralized file system in space using IPFS. This initiative aims to improve the speed of data transfer across long distances by leveraging the decentralized nature of IPFS. The mission demonstrates the potential of decentralized storage systems in space applications, paving the way for more efficient interplanetary communication and data transfer.

7. Solana's Integration with Filecoin

Solana has partnered with Filecoin to store its extensive historical data on Filecoin's decentralized network. This collaboration addresses challenges faced by Solana developers in accessing blockchain history in a decentralized manner. By integrating with Filecoin, Solana enhances data redundancy, scalability, and security, aligning with the principles of decentralization and improving access to historical blockchain data.

8. ipfs_dict_chain: A Python Package for Mini-Blockchains

Valyrian Tech developed ipfs_dict_chain, a Python package that enables developers to build mini-blockchains on IPFS using dictionary-like data structures. This package allows for efficient and secure data management on a decentralized network by tracking changes to data stored on IPFS. It provides a lightweight solution for integrating blockchain concepts into decentralized applications without the overhead of full blockchain implementations.

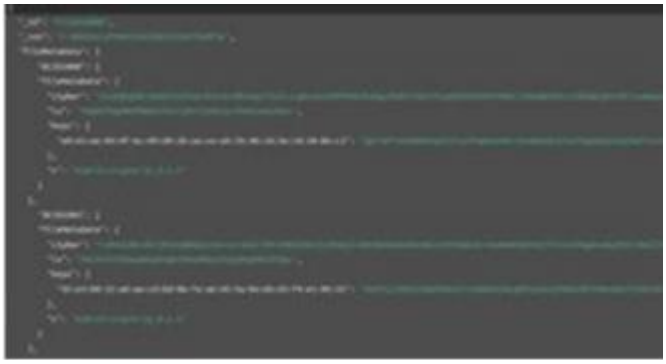
9. Consortium-Based Architecture for Secure File Sharing

A consortium-based architecture facilitates secure and efficient file sharing among multiple organizations. By hosting IPFS nodes, Identity and Interfacing Servers (IIS), smart contracts, and blockchain ledgers, each organization can contribute to a decentralized storage network. The IIS manages identity details and interfaces with smart contracts, while the blockchain ledger records transactions, ensuring transparency and immutability. This architecture supports collaborative operations and enhances data security and integrity.

Discussion

The integration of blockchain and IPFS offers a promising approach to decentralized data storage and sharing. While advancements have been made in enhancing data permanency, scalability, and real-time collaboration, challenges remain in achieving full decentralization and interoperability among different systems. The studies and implementations discussed herein highlight the potential of combining blockchain's immutability with IPFS's distributed storage capabilities to create robust and secure data-sharing ecosystems. However, further research and development are needed to address existing limitations and realize the full potential of decentralized storage systems.

In conclusion, the proposed consortium-based architecture, along with the advancements in Verifiable Decentralized IPFS Clusters, FileDAG, and integrated blockchain solutions, provides a comprehensive framework for secure and efficient data sharing among organizations. By leveraging the strengths of blockchain and IPFS, these systems offer enhanced data security, integrity, and availability, paving the way for more collaborative and decentralized operations across various sectors.



CONCLUSION

In conclusion, the integration of blockchain technology with decentralized storage systems like IPFS presents a transformative solution for secure, transparent, and efficient file sharing among multiple organizations within a consortium. This innovative architecture leverages the strengths of both blockchain and IPFS to address pressing issues such as data integrity, trust, decentralization, and long-term accessibility. By enabling each organization in the consortium to host its own IPFS node, Identity and Interfacing Server (IIS), smart contract, and blockchain ledger, the system ensures that operations remain autonomous yet synchronized through a common governance model. The blockchain ledger, being tamper-proof and auditable, maintains an immutable record of all transactions, while the IPFS network provides scalable and distributed storage for actual data content. The smart contracts deployed across the consortium serve as the backbone of the system's logic, enabling role-based access control, audit trails, and conditional data sharing that reduces the need for manual oversight. The IIS serves as the bridge between users and the blockchain network, managing user identities and permissions, thereby enforcing accountability and minimizing unauthorized access. Together, these components form a robust and decentralized framework suitable for sectors where data privacy, verifiability, and collaborative operations are critical, such as finance, healthcare, legal, and public governance. Furthermore, studies and experimental implementations, including Verifiable Decentralized IPFS Clusters (VDICs), FileDAG, and blockchain-IPFS integrated source code repositories, underscore the system's real-world applicability, scalability, and efficiency in handling sensitive and voluminous data. Challenges like IPFS centralization tendencies, interoperability issues, and network latency still persist but are actively being addressed through research and hybrid architectural approaches. The adoption of verifiable credentials, directed acyclic graph models, and decentralized identity standards continues to enhance the ecosystem's reliability and user trust. Ultimately, this system embodies the principles of decentralization, trustlessness, and transparency, aligning with the broader goals of Web3 and the next generation of internet technologies. As the digital landscape evolves, the proposed consortium-based blockchain and IPFS integrated system stands out as a forward-thinking model for secure, scalable, and cooperative data sharing, laying the groundwork for future innovations in decentralized applications and enterprise-grade solutions. Through continued research, optimization, and wider adoption, such systems hold immense potential to redefine how data is shared and

secured in collaborative, multi-stakeholder environments.

REFERENCES

1. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
2. Murthy, G. V., Kumar, C. P., & Kumar, V. V. (2017, December). Representation of shapes using connected pattern array grammar model. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 819-822). IEEE.
3. Krishna, K. V., Rao, M. V., & Murthy, G. V. (2017). Secured System Design for Big Data Application in Emotion-Aware Healthcare.
4. Rani, G. A., Krishna, V. R., & Murthy, G. V. (2017). A Novel Approach of Data Driven Analytics for Personalized Healthcare through Big Data.
5. Rao, M. V., Raju, K. S., Murthy, G. V., & Rani, B. K. (2020). Configure and Management of Internet of Things. *Data Engineering and Communication Technology*, 163.
6. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
7. Chithanuru, V., & Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions–A review. *Concurrency and Computation: Practice and Experience*, *35*(22), e7724.
8. Prashanth, J. S., & Nandury, S. V. (2015, June). Cluster-based rendezvous points selection for reducing tour length of mobile element in WSN. In *2015 IEEE International Advance Computing Conference (IACC)* (pp. 1230-1235). IEEE.
9. Kumar, K. A., Pabboju, S., & Desai, N. M. S. (2014). Advance text steganography algorithms: an overview. *International Journal of Research and Applications*, *1*(1), 31-35.
10. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
11. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
12. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
13. Mahammad, F. S., Viswanatham, V. M., Tahseen, A., Devi, M. S., & Kumar, M. A. (2024, July). Key distribution scheme for preventing key reinstallation attack in wireless networks. In *AIP Conference Proceedings* (Vol. 3028, No. 1). AIP Publishing.
14. Lavanya, P. (2024). In-Cab Smart Guidance and support system for Dragline operator.
15. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
16. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7).
17. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, *255*.
18. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
19. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, *33*, 179-184.
20. Reddy, P. R. S., & Ravindranadh, K. (2019). An exploration on privacy concerned secured data sharing techniques in cloud. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 1190-1198.
21. Raj, R. S., & Raju, G. P. (2014, December). An approach for optimization of resource management in Hadoop. In *International Conference on Computing and Communication Technologies* (pp. 1-5). IEEE.
22. Ramana, A. V., Bhoga, U., Dhulipalla, R. K., Kiran, A., Chary, B. D., & Reddy, P. C. S. (2023, June). Abnormal Behavior Prediction in Elderly Persons Using Deep Learning. In *2023 International*

Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3) (pp. 1-5). IEEE.

23. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
24. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
25. Dastagiraiah, C., Krishna Reddy, V., & Pandurangarao, K. V. (2018). Dynamic load balancing environment in cloud computing based on VM ware off-loading. In *Data Engineering and Intelligent Computing: Proceedings of IC3T 2016* (pp. 483-492). Springer Singapore.
26. Swapna, N. (2017). „Analysis of Machine Learning Algorithms to Protect from Phishing in Web Data Mining". *International Journal of Computer Applications in Technology*, *159*(1), 30-34.
27. Moparthi, N. R., Bhattacharyya, D., Balakrishna, G., & Prashanth, J. S. (2021). Paddy leaf disease detection using CNN.
28. Balakrishna, G., & Babu, C. S. (2013). Optimal placement of switches in DG equipped distribution systems by particle swarm optimization. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *2*(12), 6234-6240.
29. Moparthi, N. R., Sagar, P. V., & Balakrishna, G. (2020, July). Usage for inside design by AR and VR technology. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.
30. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
31. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.
32. Amarnadh, V., & Rao, M. N. (2025). A Consensus Blockchain-Based Credit Risk Evaluation and Credit Data Storage Using Novel Deep Learning Approach. *Computational Economics*, 1-34.
33. Shailaja, K., & Anuradha, B. (2017). Improved face recognition using a modified PSO based self-weighted linear collaborative discriminant regression classification. *J. Eng. Appl. Sci*, *12*, 7234-7241.
34. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*.
35. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
36. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
37. Tejaswi, S., Sivaprashanth, J., Bala Krishna, G., Sridevi, M., & Rawat, S. S. (2023, December). Smart Dustbin Using IoT. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 257-265). Singapore: Springer Nature Singapore.
38. Moreb, M., Mohammed, T. A., & Bayat, O. (2020). A novel software engineering approach toward using machine learning for improving the efficiency of health systems. *IEEE Access*, *8*, 23169-23178.
39. Ravi, P., Haritha, D., & Niranjan, P. (2018). A Survey: Computing Iceberg Queries. *International Journal of Engineering & Technology*, *7*(2.7), 791-793.
40. Madar, B., Kumar, G. K., & Ramakrishna, C. (2017). Captcha breaking using segmentation and morphological operations. *International Journal of Computer Applications*, *166*(4), 34-38.
41. Rani, M. S., & Geetavani, B. (2017, May). Design and analysis for improving reliability and accuracy of big-data based peripheral control through IoT. In *2017 International Conference on Trends in Electronics and Informatics (ICEI)* (pp. 749-753). IEEE.
42. Reddy, T., Prasad, T. S. D., Swetha, S., Nirmala, G., & Ram, P. (2018). A study on antiplatelets and anticoagulants utilisation in a tertiary care hospital. *International Journal of Pharmaceutical and Clinical Research*, *10*, 155-161.
43. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
44. AC, R., Chowdary Kakarla, P., Simha PJ, V., & Mohan, N. (2022). Implementation of Tiny Machine Learning Models on Arduino 33–BLE for Gesture and Speech Recognition.

45. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
46. Nagaraj, P., Prasad, A. K., Narsimha, V. B., & Sujatha, B. (2022). Swine flu detection and location using machine learning techniques and GIS. *International Journal of Advanced Computer Science and Applications*, *13*(9).
47. Priyanka, J. H., & Parveen, N. (2024). DeepSkillNER: an automatic screening and ranking of resumes using hybrid deep learning and enhanced spectral clustering approach. *Multimedia Tools and Applications*, *83*(16), 47503-47530.
48. Sathish, S., Thangavel, K., & Boopathi, S. (2010). Performance analysis of DSR, AODV, FSR and ZRP routing protocols in MANET. *MES Journal of Technology and Management*, 57-61.
49. Siva Prasad, B. V. V., Mandapati, S., Kumar Ramasamy, L., Boddu, R., Reddy, P., & Suresh Kumar, B. (2023). Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *64*(3), 658-671.
50. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.
51. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
52. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*.
53. Balaraju, J., Raj, M. G., & Murthy, C. S. (2019). Fuzzy-FMEA risk evaluation approach for LHD machine–A case study. *Journal of Sustainable Mining*, *18*(4), 257-268.
54. Thirumoorthi, P., Deepika, S., & Yadaiah, N. (2014, March). Solar energy based dynamic sag compensator. In *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)* (pp. 1-6). IEEE.
55. Vinayasree, P., & Reddy, A. M. (2025). A Reliable and Secure Permissioned Blockchain-Assisted Data Transfer Mechanism in Healthcare-Based Cyber-Physical Systems. *Concurrency and Computation: Practice and Experience*, *37*(3), e8378.
56. Acharjee, P. B., Kumar, M., Krishna, G., Raminenei, K., Ibrahim, R. K., & Alazzam, M. B. (2023, May). Securing International Law Against Cyber Attacks through Blockchain Integration. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2676-2681). IEEE.
57. Ramineni, K., Reddy, L. K. K., Ramana, T. V., & Rajesh, V. (2023, July). Classification of Skin Cancer Using Integrated Methodology. In *International Conference on Data Science and Applications* (pp. 105-118). Singapore: Springer Nature Singapore.
58. LAASSIRI, J., EL HAJJI, S. A. Ï. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, *15*(1).
59. Prasad, D. V. R., & Mohanji, Y. K. V. (2021). FACE RECOGNITION-BASED LECTURE ATTENDANCE SYSTEM: A SURVEY PAPER. *Elementary Education Online*, *20*(4), 1245-1245.
60. Dasu, V. R. P., & Gujjari, B. (2015). Technology-Enhanced Learning Through ICT Tools Using Aakash Tablet. In *Proceedings of the International Conference on Transformations in Engineering Education: ICTIEE 2014* (pp. 203-216). Springer India.
61. Reddy, A. M., Reddy, K. S., Jayaram, M., Venkata Maha Lakshmi, N., Aluvalu, R., Mahesh, T. R., ... & Stalin Alex, D. (2022). An efficient multilevel thresholding scheme for heart image segmentation using a hybrid generalized adversarial network. *Journal of Sensors*, *2022*(1), 4093658.
62. Srinivasa Reddy, K., Suneela, B., Inthiyaz, S., Hasane Ahammad, S., Kumar, G. N. S., & Mallikarjuna Reddy, A. (2019). Texture filtration module under stabilization via random forest optimization methodology. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(3), 458-469.
63. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
64. Sirisha, G., & Reddy, A. M. (2018, September). Smart healthcare analysis and therapy for voice

disorder using cloud and edge computing. In *2018 4th international conference on applied and theoretical computing and communication technology (iCATccT)* (pp. 103-106). IEEE.

65. Reddy, A. M., Yarlagadda, S., & Akkinen, H. (2021). An extensive analytical approach on human resources using random forest algorithm. *arXiv preprint arXiv:2105.07855*.
66. Kumar, G. N., Bhavanam, S. N., & Midasala, V. (2014). Image Hiding in a Video-based on DWT & LSB Algorithm. In *ICPVS Conference*.
67. Naveen Kumar, G. S., & Reddy, V. S. K. (2022). High performance algorithm for content-based video retrieval using multiple features. In *Intelligent Systems and Sustainable Computing: Proceedings of ICISSC 2021* (pp. 637-646). Singapore: Springer Nature Singapore.
68. Reddy, P. S., Kumar, G. N., Ritish, B., SaiSwetha, C., & Abhilash, K. B. (2013). Intelligent parking space detection system based on image segmentation. *Int J Sci Res Dev*, *1*(6), 1310-1312.
69. Naveen Kumar, G. S., Reddy, V. S. K., & Kumar, S. S. (2018). High-performance video retrieval based on spatio-temporal features. *Microelectronics, Electromagnetics and Telecommunications*, 433-441.
70. Kumar, G. N., & Reddy, M. A. BWT & LSB algorithm based hiding an image into a video. *IJESAT*, 170-174.
71. Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., & Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. *Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, Bhadrappa Haralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International*, *44*(3), 18261-18271.
72. Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for Improved Brain Tumor Detection and Classification. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1603-1609). IEEE.
73. Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
74. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.
75. Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.
76. Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1-6). IEEE.
77. Praveen, R. V. S., Hemavathi, U., Sathya, R., Siddiq, A. A., Sanjay, M. G., & Gowdish, S. (2024, October). AI Powered Plant Identification and Plant Disease Classification System. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1610-1616). IEEE.
78. Dhivya, R., Sagili, S. R., Praveen, R. V. S., VamsiLala, P. N. V., Sangeetha, A., & Suchithra, B. (2024, December). Predictive Modelling of Osteoporosis using Machine Learning Algorithms. In *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)* (pp. 997-1002). IEEE.
79. Kemmannu, P. K., Praveen, R. V. S., Saravanan, B., Amshavalli, M., & Banupriya, V. (2024, December). Enhancing Sustainable Agriculture Through Smart Architecture: An Adaptive Neuro-Fuzzy Inference System with XGBoost Model. In *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)* (pp. 724-730). IEEE.
80. Praveen, R. V. S. (2024). *Data Engineering for Modern Applications*. Addition Publishing House.