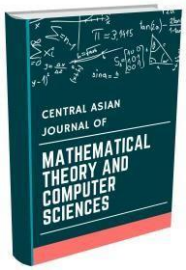


CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.casjournal.org/index.php/cajmtcs
Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5309

Article

A Secure Distributed File Storage Framework Using Cryptographic Hashing and PoW

N. Selvam*[1], M. Mohamed Thariq[2], A. Mohamed Fahadhu[3]

1,2,3. Department of Computer Science and Engineering, Dhaanish Ahmed College of Engineering, Padappai, Chennai, Tamil Nadu, India
* Correspondence: selvamn@dhaanishcollege.in

Abstract: The growing concerns around data security and privacy have highlighted the need for secure, decentralised file storage solutions. This project proposes a Blockchain-Based Secure File Storage System that leverages blockchain technology to ensure the integrity, confidentiality, and immutability of files stored on a distributed network. In this system, files are securely stored by associating them with cryptographic hashes within blocks, creating a tamper-resistant ledger. The Blockchain is responsible for tracking file metadata, such as file names, owners, and timestamps, while ensuring that each file is securely linked to its predecessor, forming a chain of blocks. Each block's validity is maintained using Proof of Work (PoW), ensuring consensus and the integrity of the data stored. The code implementation allows users to add files, store them securely, and verify their integrity via a decentralised ledger. As files are uploaded, they are hashed, and a new block is created on the blockchain. The use of Proof of Work ensures that only valid blocks are added to the chain, preventing malicious tampering or unauthorised access. This system is ideal for scenarios requiring high levels of data security, such as cloud storage, healthcare data management, and legal document storage, where the integrity and authenticity of files need to be guaranteed over time. This project demonstrates how blockchain technology can be adapted beyond cryptocurrency to build a secure, trustworthy file storage framework that offers enhanced protection against data breaches and unauthorised modifications.

Citation: Selvam N., Thariq M. M., Fahadhu A. M. A Secure Distributed File Storage Framework Using Cryptographic Hashing and PoW. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(1), 255-271.

Received: 19th Dec 2025
Revised: 31th Dec 2025
Accepted: 13th Jan 2026
Published: 22nd Jan 2026

Keywords: Data Security, Privacy, Cryptographic, Tracking File, Securely Linked, Blockchain, Cloud Storage, Blockchain Technology, Cryptocurrency, Unauthorised Modifications

1. Introduction

In today's digital world, data is one of the most valuable things for people, businesses, and governments [54]. Every day, a lot of sensitive information is created, saved, and shared since cloud computing, online collaboration tools, and remote access technologies are growing so quickly [29]. This digital transition has made things a lot more efficient and easier to get to, but it has also made data security, privacy, and trust much harder. Most traditional file storage systems are based on centralised architectures, which means that one server or authority stores and manages all the data [42]. Even though many people use these systems because they are easy to use, they have built-in flaws that make them easy targets for hackers, system crashes, and unauthorised access. In centralised storage systems, one point of failure can have terrible effects [33]. If hacking, malware, insider threats, or hardware failure breach a central server, the whole dataset could be made public, damaged, or lost forever. High-profile data breaches over the past

ten years have shown how attackers can use these weaknesses to steal private information, which can cost businesses money, get them in trouble with the law, and hurt their reputation for a long time [58].

Centralised systems also demand users to trust service providers completely, expecting that they would handle data in a way that is ethical, safe, and open. This paradigm built on trust typically doesn't allow for verification, which means that users have no control or awareness over how their data is viewed or changed [31]. The restrictions of traditional storage strategies become clearer as the amount of data grows at an exponential rate. The situation is made worse by challenges with scalability, expensive maintenance costs, and the growing difficulty of managing security [47]. These problems have led researchers and developers to look at different ways of storing data that don't rely on a single governing party and can give higher guarantees of data integrity, availability, and transparency [57]. In this situation, blockchain technology has become a strong and new way to fix many of the problems that come with traditional file storage methods. Blockchain technology is basically a decentralised and distributed ledger system that keeps track of transactions on many different nodes in a network [36]. There is a block for each record, and each block is cryptographically connected to the one before it. This makes an unchangeable chain of data. This architecture makes sure that once information is captured, it can't be changed without the network's agreement [53].

This makes the system very hard to hack or cheat. Blockchain was first used as the technology behind cryptocurrencies like Bitcoin [43]. Since then, it has grown into a flexible platform that can be used in many fields, including banking, supply chain management, healthcare, identity management, cybersecurity, and digital storage [37]. One of the best things about blockchain is that it is not controlled by one person or group. Data is not kept in one place; instead, it is spread out among many participants, each of whom has a copy of the ledger. This gets rid of single points of failure and makes the system more robust [40]. If some nodes go down or are hacked, the other nodes can still work and keep the data safe. Blockchain also uses cryptography to make sure that the data stored in the system is safe, can be checked, and is clear. Because of these traits, blockchain is great for apps that need a lot of trust, accountability, and data integrity. Blockchain provides a new way to protect data when storing files without actually keeping big files on the chain itself [26]. It can be hard to save whole files on a blockchain because of storage limits, performance issues, and high computing expenses. Instead, blockchain can be used to store important file-related information including metadata, cryptographic hash values, timestamps, and information about who owns the file [50]. This way, the system can check that files are real and complete while keeping the actual file content in traditional or decentralised storage systems off-chain.

If someone tried to change a file, the stored hash and the computed hash would not match, which would quickly show that the file had been tampered with [46]. This project looks at the Blockchain-Based Secure File Storage System, which builds on these ideas to show how blockchain may make digital storage safer and more reliable. The project is about making a private blockchain simulation with Python [32]. This will give researchers a controlled space to explore the basic parts of blockchain and how they may be used to keep files safe. The system is not meant to be a production-ready storage platform; instead, it is a conceptual and technological demonstration of how blockchain ideas might be used to solve real-world data security problems. The system's core is a proprietary blockchain structure made up of separate blocks, each of which has information about files [56]. Every block has important information such an index, timestamp, file metadata or hash, the hash of the preceding block, a nonce value, and the block's own cryptographic hash [39]. These parts work together to make sure that blocks are securely connected and that changing the contents of a block would make the whole chain invalid from that point on. The blockchain starts with a genesis block, which is the first block on the chain and sets the system's initial state [52]. The system uses a proof-of-work approach to add new blocks to the blockchain.

Proof-of-work is a way for everyone to agree on something that needs people to solve a hard challenge before a new block can be added.

In this method, a nonce value is changed again and over again until the resulting block hash meets a set difficulty criterion, which is usually shown as a particular amount of leading zeros in the hash [48]. Proof-of-work takes a lot of resources, but it is very important for keeping bad actors from quickly changing the blockchain. This is because any effort to change a block would entail redoing the proof-of-work for that block and any blocks that come after it. A simulated workflow that works like real-world blockchain operations brings file data into the system [34]. When a file is added, its metadata or cryptographic hash is initially put on a list of things that are waiting to be processed. These pending entries are transactions that haven't been confirmed yet and are waiting to be added to the blockchain. When the mining process starts, the data that is waiting is put into a new block and goes through the proof-of-work procedure[41]. After mining is successful, the block is added to the chain, and the list of blocks that are still waiting is cleared. This method shows how blockchain can keep a chronological and auditable record of events connected to files. The chain validation process is a key part of the system because it monitors the blockchain's integrity all the time [27]. Validation functions check that the hash of each block is valid, that each block correctly points to the hash of the preceding block, and that the proof-of-work requirements have been met.

The validation procedure will find inconsistencies if any block is changed or taken away, which could mean that someone is trying to change it [55]. This capacity shows one of blockchain's best features: it can make strong promises about the integrity of data without any outside help. From a cybersecurity point of view, the suggested approach solves a number of important problems that come with standard file storage [45]. It lessens the need for a single trusted authority by decentralising the record of file ownership and integrity. Cryptographic hashing makes it impossible to change files without being noticed, and the immutable ledger keeps a clear record of all file-related operations. These traits are especially useful in places where data integrity and accountability are very important, like healthcare systems, legal document management, academic research repositories, and enterprise data storage [30]. The project also stresses honesty and openness. Everyone in the network can see and verify every block that is added to the chain. This makes sure that file records can't be changed or deleted without anyone knowing. Users can trust the stored data since they can check its authenticity on their own without having to rely on a central administrator [51]. The system can also be expanded with access control methods to keep sensitive data safe and make sure that only authorised users can work with certain files. The current implementation is more about showing basic blockchain ideas, but it also sets the stage for future improvements and real-world implementations [35]. One possible improvement is to integrate decentralised file storage platforms like the InterPlanetary File System, which lets files be stored on a distributed network and accessible by content-based addressing. You may make a completely distributed and secure file storage ecosystem with both data availability and integrity by combining blockchain with decentralised storage.

Another interesting avenue is the use of smart contracts, which are programs that run on the blockchain and do what they say they would do. Smart contracts might be used to automatically limit access, enforce file-sharing rules, and change rights based on rules that are already in place [38]. This would provide you more control over who can see, change, or share files, which would make the system even more secure and easy to use. There are also scaling methods like sharding or different consensus techniques that might be used to make things run better and handle bigger datasets. In conclusion, this project's Blockchain-Based Secure File Storage System shows how blockchain technology may be used to fix the problems with traditional centralised storage systems [44]. The system has a strong framework for making sure that data is safe, open, and trustworthy by integrating decentralisation, cryptographic security, and immutability. The project uses Python to

make it easy and useful to learn about how blockchain concepts can be used to protect files [28]. Blockchain-based approaches have a lot of promise to change the future of secure storage as digital data becomes more important and larger. This will lead to more reliable, trustworthy, and user-friendly data management solutions [49].

Literature Review

This summary talks about major discoveries in the discipline, new technologies, and how different methods have changed over time [20]. Critical evaluations and comparisons of various methodologies and models provide a valuable foundation for comprehending the current state of the art and identifying potential gaps or opportunities for additional inquiry and innovation [3]. This chapter is important for putting the project in a bigger picture by using what we learnt from earlier studies. Blockchains, which were established in 2008, allow decentralised peer-to-peer networks that don't have a central authority. One of the key uses is decentralised storage, where people rent out unused space and make sure it's safe by using end-to-end encryption [24]. These networks are better than centralised systems at stopping data loss and making sure that providers check file integrity [10]. Research has mostly looked at capacity and efficiency, but security, integrity, and privacy issues still need to be dealt with. This paper talks about blockchain-based storage, how it is different from cloud storage, and looks at networks like SIA, Filecoin, and Storj. We talk about the pros and cons, security risks, and future research areas for decentralised storage [15].

To manage IoT data, you need cloud storage, but it can be risky because of things like data leaks and having to rely on a centralised third-party auditor (TPA). Decentralised storage using blockchain removes the need for a TPA, avoids points of failure, and is cost-effective and fast [8]. This paper introduces IoTChain, a decentralised storage and sharing system that uses Ethereum and IPFS and is built on the blockchain. It uses attribute-based access control (A-BAC), AES encryption, elliptic curve key exchange, and proof-of-authority (PoA) consensus to make things safer and more efficient [4]. IoTChain is a good, cheap way to handle IoT data that works on the Ethereum Rinkeby network. Blockchain is a type of distributed network that keeps data in a decentralised way. Blockchain makes transactions clear and safer by using cryptography [22]. It has features such being unchangeable, decentralised, and auditable that make transactions safe and impossible to change. Decentralisation is becoming more popular as a way to construct apps and store data. This paper has done a survey of Ethereum-based decentralised apps [13]. This research paper also talks about how smart contracts work in Blockchain. The InterPlanetary File System is also used to store and get files in a distributed setting [25].

A reliable product evaluation management (PEM) system is needed to make sure that online buying goes well [6]. This study recommends the implementation of a blockchain-based Product Evaluation Management (PEM) system, wherein product reviews are archived in the InterPlanetary File System (IPFS) and data hashes are preserved on the Ethereum blockchain. Smart contracts make it possible to safely and easily get data back, which stops illegal alterations. It is easier to search for keywords, and there is a way to make money to encourage sustainability. The results of the simulation on Ethereum using Solidity show that the system is very usable and very reliable[1]. In cloud computing, it is very important to have safe distant data storage. Traditional proven data possession (PDP) techniques use RSA or bilinear pairings, which make them very slow and expensive to use [19]. So, we present a private PDP architecture built on blockchain that combines both blockchain and RSA to make things safer and more efficient. We delineate its system and security frameworks and formulate a definitive implementation. Theoretical research and prototype testing show that our plan is safe, works well, and is useful. The InterPlanetary File System (IPFS) is a peer-to-peer system that lets people store and share data across several computers [12]. It uses content-addressing to find unique files with a Content Identifier (CID), which makes it easier to get data more quickly. IPFS

allows users to upload, find, and share content directly across a blockchain-supported network, which makes things faster and removes the need for central servers [16]. This work talks about the advantages of distributed storage over traditional methods, which often don't provide reliable and redundant data. This work also suggests a way to protect data by using several authentication methods. This lets users easily find and manage their information on the IPFS blockchain [21].

A distributed file storage system makes copies of data on multiple nodes, so you don't have to rely on a single server. Using a peer-to-peer network and blockchain technology, it makes things more redundant, strong, and safe [5]. Some examples of use cases are delivering content, transferring files, using dApps, CDNs, and backing up data. There are still problems with data privacy and security [18]. This article shows how to use Ethereum, Solidity smart contracts, MetaMask, React.js, CSS, and Ethers.js to make a decentralised storage plan based on blockchain. More and more, the medical field is using blockchain and IPFS to manage data in a safe and decentralised way [14]. Traditional centralised storage approaches have a 75% accuracy rate, but they put data at danger of being stolen. This study suggests a blockchain-based system with Ethereum smart contracts and consensus mechanisms to improve security and integrity [9]. The medical data is hashed and stored in IPFS with unique content identifiers. This makes sure that the data cannot be changed and is open to everyone. Only registered users can access it, which reduces the chance of unauthorised access [23]. The decentralised strategy avoids single points of failure, which makes the data more reliable and gets 90% accuracy.

In the previous several years, there have been a lot of cyberattacks on the data of global organisations, governments, institutions, and even people [7]. Most of these attacks are aimed at the flaws in centralised storage systems. They say that a new way of storing data needs to be developed to solve problems that have been around for a long time with centralised systems. A practical solution to most of these problems is blockchain technology, which is built on an off-chain ledger [11]. This article aimed to develop and test a decentralised document storage system utilising a private Blockchain network, Ethereum tokens, and the InterPlanetary File System (IPFS). We present a secure, lightweight blockchain-based architecture to solve problems with storage and security in edge computing [2]. First, we come up with a communication model that works better by combining CoAP and MQTT. We also use blockchain and IPFS for decentralised storage to make sure that data is safe and can be traced. In the end, we improve the PBFT consensus method to make the system work faster [17]. The results demonstrate that this method is a possible way to promote blockchain-based edge computing because it is very strong and doesn't add much extra work.

2. Methodology

Project Description

Existing System

Most current file storage solutions use either centralised servers or cloud services from other companies. These technologies are efficient, fast, and scalable, but they raise serious questions about data security, integrity, and transparency [60]. Centralised systems have one point of failure: if they are hacked, have bugs, or are threatened from the inside, all of the data stored on them could be lost or changed. Users also rely on providers for access control, backups, and recovery, which may not meet their privacy or compliance demands [74].

Proposed System

The suggested method uses the built-in features of blockchain technology—decentralization, immutability, and transparency—to make file storage safer. This approach does not use a central server to manage data, which is different from standard

systems. It doesn't store the actual files; instead, it saves metadata about the files, like their names, hash values, and timestamps, in blocks on a blockchain [66]. Before being added to the chain, each new transaction, which is a file activity, is checked using a Proof-of-Work consensus process. This makes sure that the data is real and hasn't been changed [78]. The blockchain structure, which connects each block to the one before it with cryptographic hashes, makes security even better by making it easy to see when modifications are made without permission. This implementation of the blockchain does not contain the actual file content, but it does show how the blockchain can be a safe and reliable way to check file integrity [73]. The code written in Python simulates mining, creating blocks, and validating chains. It shows how blockchain may be used to safely handle files.

Proposed Work

General Architecture

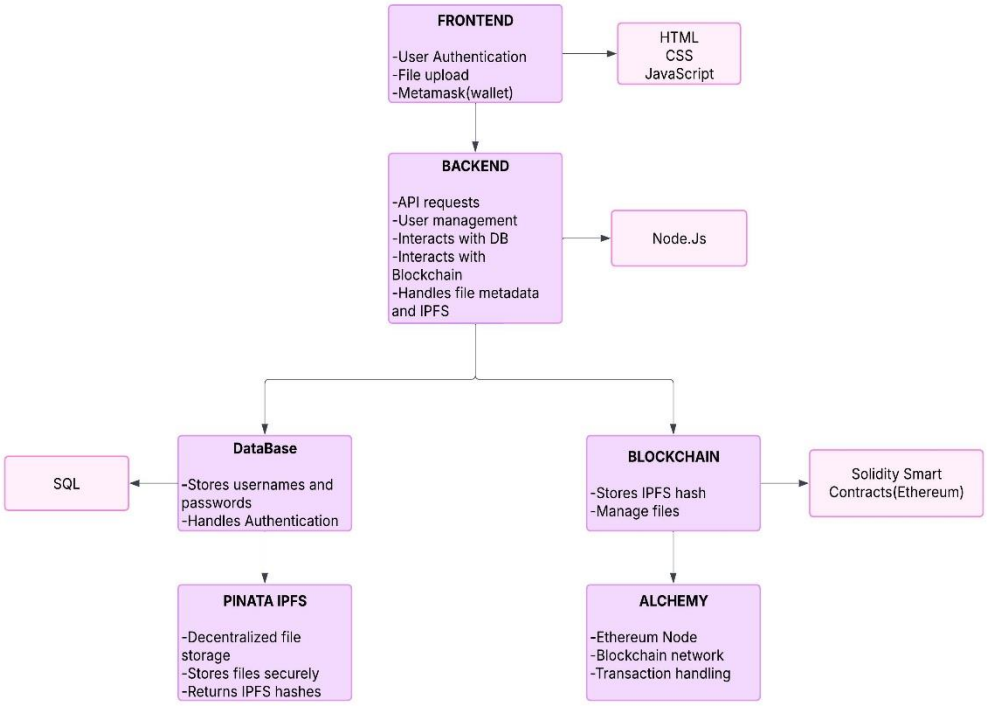


Figure 1. Architecture Diagram.

The diagram shows how a decentralised application (DApp) works by combining blockchain technology, backend infrastructure, and decentralised file storage [68]. A web-based interface made with HTML, CSS, and JavaScript lets end users engage with the system on the front end. It lets users log in, upload files, and connect their wallets with MetaMask [72]. The backend, which is implemented in Node.js, makes it possible to make API requests, log in users, call the database, integrate with the blockchain, and store file metadata and IPFS (InterPlanetary File System) data. The database module keeps track of usernames and passwords for authentication [59]. It works with Pinata IPFS, a decentralised storage system that keeps files safe and sends IPFS hashes. The blockchain layer is very important for processing files and preserving IPFS hashes because it makes sure that everything is clear and can't be changed. Smart contracts written in Solidity on the Ethereum blockchain handle data and process transactions (Figure 1).

Alchemy also provides Ethereum nodes and blockchain network solutions that handle transactions well. The Blockchain-Based Secure File Storage System's design phase is all about figuring out how to leverage blockchain concepts to safely handle file metadata [65]. The system has three primary parts: inputting metadata, managing transactions with mining, and checking the blockchain. When a user sends in file metadata, it is treated as a

transaction and put on a list of things that need to be done [79]. The blockchain engine then uses a Proof-of-Work algorithm to mine this data and make a legitimate block that is added to the chain [69]. Each block is linked to the one before it in a way that makes the data unchangeable. The technology also gives a way to check the integrity of the blockchain by checking hashes and block linkages. Supporting diagrams like DFDs, UML, use case, and sequence diagrams help people see how data flows and how different parts of the system work together [61]. This makes it easier to comprehend, build, and add to the system in future editions.

Data Flow Diagram

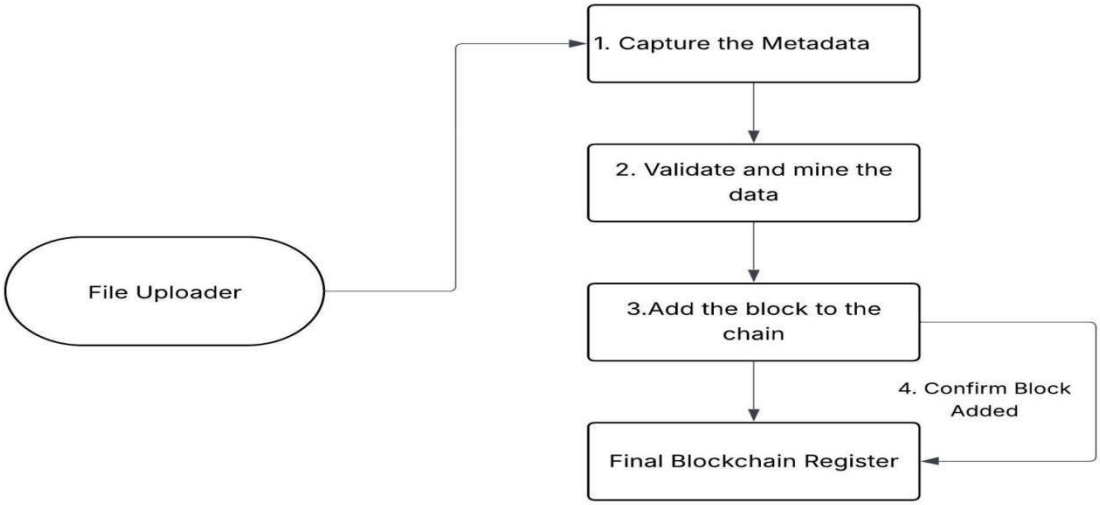


Figure 2. Data Flow Diagram.

Figure 2. The diagram shows how to safely add file metadata to a blockchain ledger. The File Uploader starts the process by getting important metadata, like the file name, size, hash, and timestamp [64]. Then, this metadata goes through a validation and mining process, which includes cryptographic verification (for example, Proof of Work). When mining is successful, the data is put into a block and added to the blockchain, which makes it impossible to change [75]. Finally, the system checks to make sure that the block has been added successfully and is now part of the Blockchain.

Uml Diagram

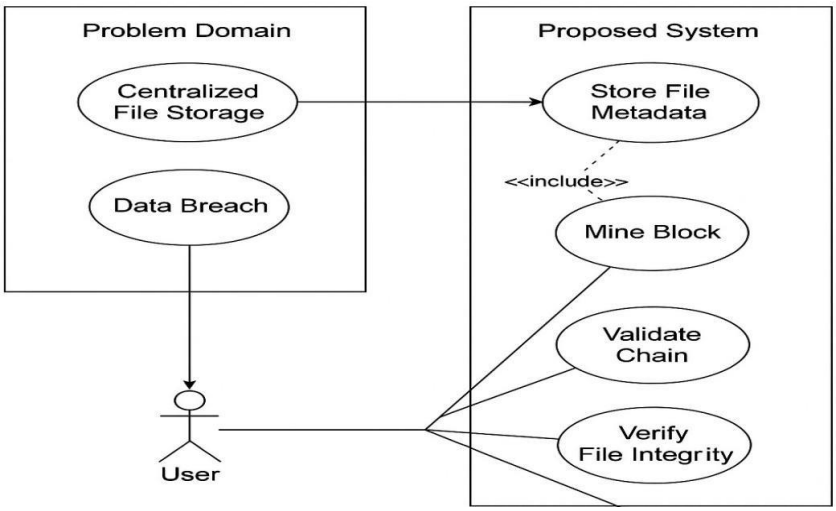


Figure 3. UML Diagram.

Figure 3. depicts a use case model that compares a blockchain-based secure file storage system to traditional centralised storage. On the left, you can see problems like

centralised storage and data breaches [71]. On the right, you can see the proposed solution, which lets users store file metadata, mine blocks, validate the chain, and check the integrity of files [62]. The technology uses the fact that blockchain is decentralised and cannot be changed to make data more secure.

Use Case Diagram

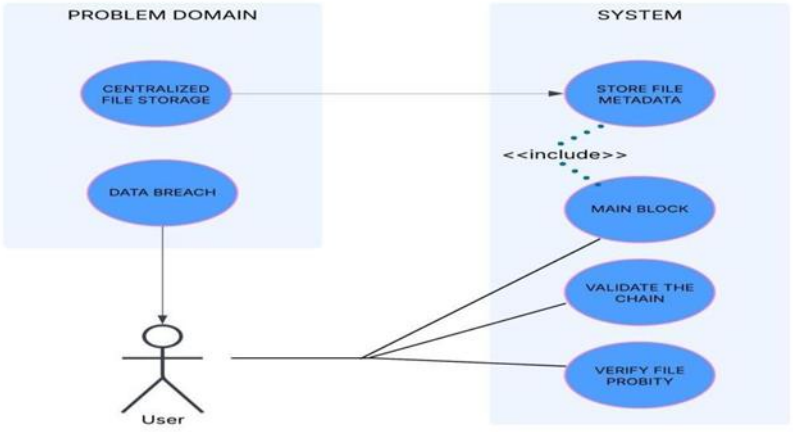


Figure 4. Use Case Diagram.

The diagram in **Figure 4.** shows how a user and a Blockchain-Based Secure File Storage System work together [76]. The user can do three main things: upload a file, download a file, and check the file's integrity. The blockchain processes and protects the metadata of a file when it is submitted [67]. Downloading gives you access to files that are already stored, and integrity checking makes sure that the file hasn't been changed by using the blockchain's immutability. The technology works behind the scenes to handle these transactions and keep the blockchain ledger safe.

Sequence Diagram

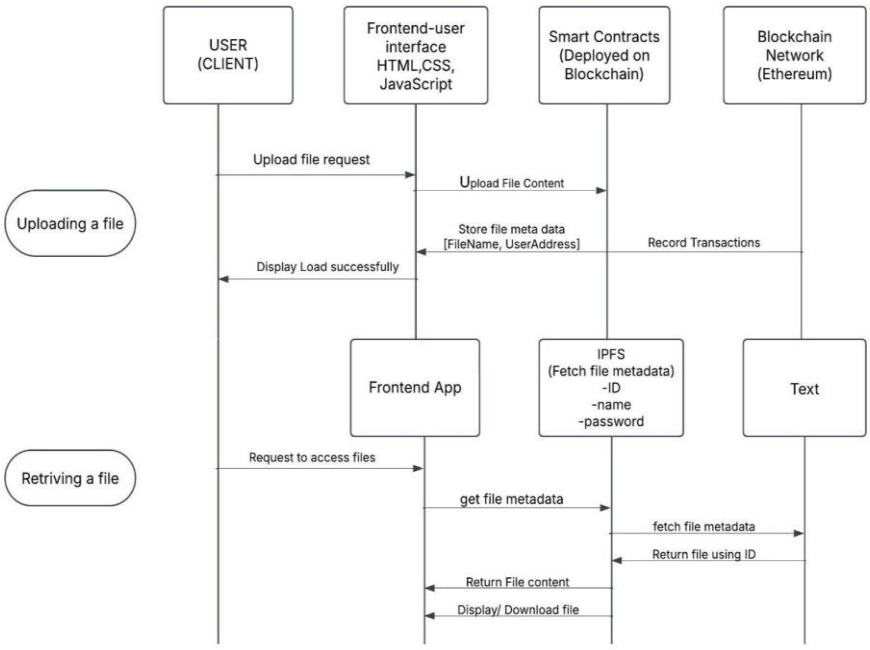


Figure 5. Sequence Diagram.

Figure 5. shows how the main parts of a blockchain-based file storage system work together when files are uploaded and downloaded [70]. When a user uploads a file through

the frontend, it goes to a decentralised storage network like IPFS, which sends back a unique content identifier (CID). A smart contract records this CID, along with file metadata and the user's wallet address, on the blockchain. This makes sure that the data is safe and can't be changed. A success message is provided to the user once the confirmation is received [63]. The frontend asks the smart contract for the file's metadata and hash, which it gets from the blockchain. The frontend then uses the CID to get the file from IPFS so that the user can see or download it [77]. This procedure shows how blockchain-based storage solutions are safe, open, and not controlled by any one person.

Module Description

The Blockchain-Based Secure File Storage System is built in a modular way, so that each portion of the system can do a specific job that is important for keeping file-related data safe. The modular structure also makes it possible to scale up, fix bugs more easily, and add new features in the future [83]. There are three key parts to the system right now: File Metadata Handling, Blockchain Transaction & Mining, and Blockchain Validation & Integrity Checking.

Module 1. File Metadata Handling.

This module is where users can start interacting with the system. Its main job is to gather and keep track of metadata about files that users have uploaded. Instead of saving the original file, the system makes or accepts a SHA-256 hash of the file's contents. This hash works as a unique fingerprint to make sure the file is real [88]. The user gives basic file information including the filename, timestamp, and hash value. This information is then put into a transaction structure and sent to the transaction pool. This module makes sure that all user input is organised, formatted correctly, and ready to be processed on the blockchain [93]. It is very important for keeping a consistent and tamper-proof view of files in the system.

Module 2. Transaction Pool Management and Mining.

The second module is in charge of handling pending transactions and doing mining work. A transaction pool temporarily stores all incoming file metadata until it is aggregated and added to a block [90]. This module starts the mining process by utilising a Proof of Work (PoW) algorithm that keeps making hash values until they reach a specific level of difficulty (for example, a hash that starts with a certain amount of zeros). In this process, a nonce is given to the block, and its hash is recalculated until it is legitimate. The block is added to the blockchain once it has been mined successfully [87]. This module is the most important part of how blockchain works. It makes sure that all transactions kept on the blockchain are permanent and safe. It stops unauthorised additions and makes sure that every transaction can be checked.

Module 3. Blockchain Validation and Integrity Checking.

The third module checks the whole blockchain structure to make sure that no changes have been made [94]. It checks the blockchain from the first block to the most recent one to make sure that the hash values are valid, that the blocks are consistent with each other, and that the difficulty level is set correctly. The system will know that the chain has been compromised if any block is changed, even a little bit [82]. This module is very important for keeping trust and openness because it lets users or administrators check the integrity of their saved files at any moment. It also makes it easier to do frequent chain audits and might be used as a base for adding version control or rollback functionality in future versions of the system. This module is also set up in a way that makes it easy to add more nodes or connect to a dispersed network in the future.

Step 2. Processing of File Metadata.

This step is when the system takes in and processes the metadata from the files that users send in. The system doesn't upload the whole file; instead, it processes metadata including the file name, file size, and, most significantly, a cryptographic hash (usually

SHA-256) of the file's contents [86]. This hash is like a fingerprint for the file because it is unique to it. The metadata is checked for structure and format when it is sent in, and then it is sent to the transaction pool. This stage makes sure that the data is consistent and ready to be safely added to the blockchain [91]. Until the mining phase begins, validated entries are kept as pending transactions [97]. The whole procedure is made easier to protect metadata and make sure that blockchain entries are correct.

Step 3. Mining and Block Creation.

In machine learning, this step is called "building the model." In blockchain, it means making and checking a block. The system starts mining when there are a set of transactions that are ready to go. The Proof of Work algorithm is used to create a cryptographic hash for the block that meets a certain level of difficulty. The system keeps changing the nonce value until the hash starts with a certain number of zeros [84]. When the requirement is met, the block is valid and is added to the blockchain. This step makes the file metadata permanent and tamper-proof, making sure that the data is safely logged and can be checked at any time [95].

Verifying and Validating the Blockchain

At this point, the system checks the entire blockchain to make sure it is still legitimate. It is necessary to check the hash of the preceding block every time a block is mined and added. The system checks to see if the stored hash for each block matches the recalculated hash and if all the linkages between blocks are still there [80]. This step of validation stops changes or data corruption that aren't allowed. Changing any one piece of metadata in any block makes the whole chain invalid, which shows how the system is designed to be tamper-evident [96]. This step is very important for keeping user trust and system transparency, especially as the blockchain gets bigger.

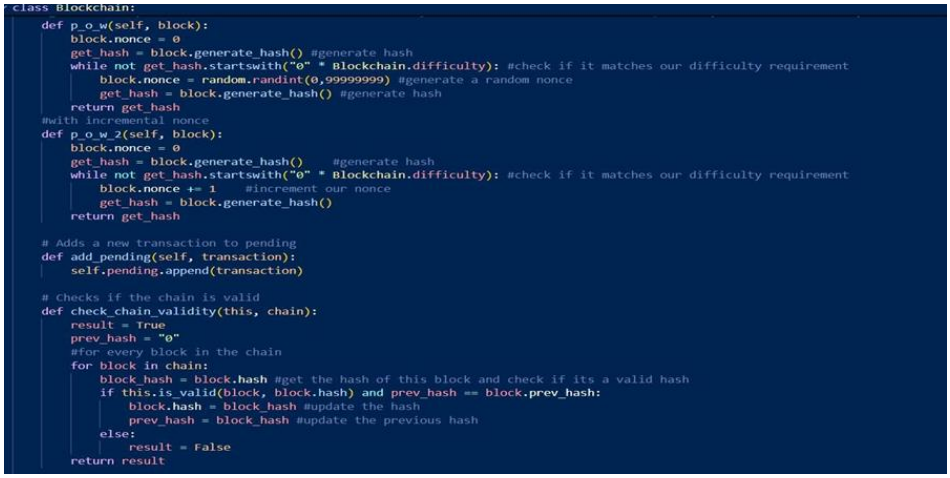
In this case, a sample dataset is a set of example metadata that was used during testing. For example, this data is not the file itself but its digital fingerprint. This means that if the file is changed later, its hash will change, showing that it has been tampered with. These samples are used to check block formation, mining accuracy, and validation integrity while the system is running [92]. These data entries are what make up the main part of each block and assist make sure that the system is safe, consistent, and easy to track.

Implementation And Testing

Input And Output

Image - Uploading of File in User Interface

The user starts the procedure by choosing a file from the system's web-based interface. Users can choose from a variety of file types (PDF, TXT, JPG, etc.) using this easy-to-use upload platform [85]. After the file is uploaded, it is processed and added to a new block. This block is then mined and added to the blockchain (Figure 6).



```
class Blockchain:
    def p_o_w(self, block):
        block.nonce = 0
        get_hash = block.generate_hash() #generate hash
        while not get_hash.startswith("0" * Blockchain.difficulty): #check if it matches our difficulty requirement
            block.nonce = random.randint(0,99999999) #generate a random nonce
            get_hash = block.generate_hash() #generate hash
        return get_hash
    #with incremental nonce
    def p_o_w_2(self, block):
        block.nonce = 0
        get_hash = block.generate_hash()    #generate hash
        while not get_hash.startswith("0" * Blockchain.difficulty): #check if it matches our difficulty requirement
            block.nonce += 1    #increment our nonce
            get_hash = block.generate_hash()
        return get_hash

    # Adds a new transaction to pending
    def add_pending(self, transaction):
        self.pending.append(transaction)

    # Checks if the chain is valid
    def check_chain_validity(this, chain):
        result = True
        prev_hash = "0"
        #for every block in the chain
        for block in chain:
            block_hash = block.hash #get the hash of this block and check if its a valid hash
            if this.is_valid(block, block.hash) and prev_hash == block.prev_hash:
                block.hash = block_hash #update the hash
                prev_hash = block_hash #update the previous hash
            else:
                result = False
        return result
```

Figure 6. The Unit Testing Process for File Upload and Encryption.

Integration Testing

Integration testing makes sure that all the parts of the Blockchain-Based Secure File Storage System work together perfectly. In this system, integration testing means making sure that the file upload, encryption, and blockchain procedures all work together appropriately [81]. Once a file is uploaded, it has to be encrypted, and the encrypted information should be put to the blockchain as a new block. Integration testing makes sure that data moves correctly through each process and that nothing is lost or corrupted when these parts interact with each other [89]. This makes sure that the complete system works well (Figure 7).

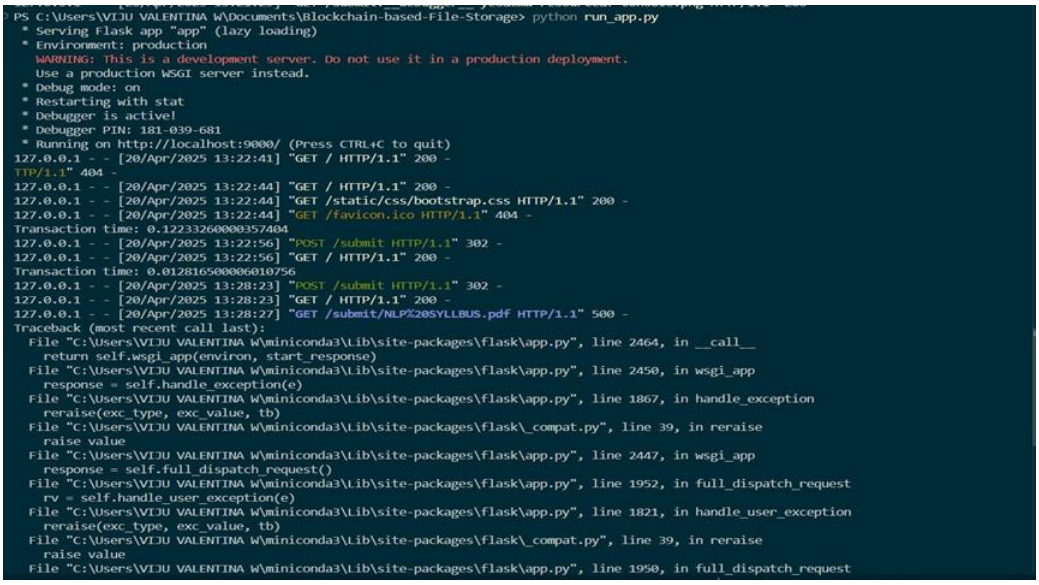


Figure 7. Integration Testing Process for File Upload and Blockchain Interaction.

Test Result

- Files are successfully uploaded and encrypted before being added to the blockchain.
- The blockchain mining process finishes without any problems, and blocks are added correctly.
- You can get files back from the blockchain and decrypt them without losing or corrupting any data.

3. Results And Discussions

Efficiency of the Proposed System

The suggested blockchain-based approach is very good at protecting file metadata and making sure that data is correct. It doesn't actually store files, but it does give you a reliable way to check if a file has been changed by comparing its current hash to the one stored in the blockchain [99]. This makes sure that users can find out if something has been changed without having to rely on someone else. From a computational point of view, the proof-of-work mechanism is set up with customisable difficulty, which lets the system act like real mining without taking too long to process [98]. This mix between safety and speed makes it useful for both academic and prototype use.

Efficiency Highlights

- Data Security: Makes ensuring that file metadata is stored in a way that can't be changed.
- Hash-based Verification: This method uses SHA-256 to produce file hashes that are like fingerprints for each file.

- Mining and Validation: The efficient proof-of-work algorithm mines and checks blocks in just a few seconds.
- Chain Consistency: Keeps blocks linked correctly with as little processing overhead as possible.
- Light on resources: It can run on PCs with basic hardware specs without any problems.
- Tamper Detection: Any change to block data breaks the chain, which shows that the validation procedures are quite powerful.

The current prototype isn't set up for industrial-scale performance or network-wide consensus, but it does show how blockchain works in a small, efficient space.

Comparison of Existing and Proposed Systems

The existing centralised file storage systems and the proposed blockchain-based system differ fundamentally in their design, operation, and security model. Traditional systems offer convenient storage and high-speed access but fall short in terms of trust, transparency, and tamper resistance. In contrast, the proposed blockchain system sacrifices some speed and simplicity in favour of enhanced data integrity and auditability.

4. Conclusion

The Blockchain-Based Secure File Storage System shows how blockchain technology can make file-related data much safer, more open, and more honest. The system uses a bespoke Python-based blockchain to store crucial metadata like file names, cryptographic hashes, and timestamps. This makes sure that the data can't be changed and can be verified by proof-of-work consensus. This framework stops people from making changes without permission and makes sure that all recorded information stays safe. The project fixes big problems with existing centralised storage systems, like being easy to hack, losing data, letting people in without permission, and not being able to trace data. The system doesn't yet support real file uploads, decentralised storage, or advanced access control measures, but it does a good job at simulating key blockchain functions. There are clear examples of how to do things like create blocks, add transactions, mine with nonce calculations, link blocks with hashes, and validate the whole chain. These basic properties help us understand how blockchain can be a strong base for safe file storage solutions. The project also makes it possible to make future improvements, such as adding smart contract-based access controls, making it easier to handle large amounts of data, and switching to more energy-efficient consensus mechanisms like Proof-of-Stake. This initiative shows that blockchain has the ability to change the way digital data is protected.

REFERENCES

[1] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, “Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment,” IEEE Access, vol. 10, no. 4, pp. 36978–36994, 2022.

[2] R. Banoth and M. B. Dave, “A survey on decentralized application based on blockchain platform,” in 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022.

[3] Z. Zhou, M. Wang, Z. Ni, Z. Xia, and B. B. Gupta, “Reliable and sustainable product evaluation management system based on blockchain,” IEEE Trans. Eng. Manage., vol. 71, no. 12, pp. 12259–12271, 2024.

[4] P. Jothilingam, “Towards autonomous commissioning: Integrating digital twins, artificial intelligence and smart sensors for next-generation process control systems,” Certified Journal of International Research (CJIR), vol. 5, no. 1, pp. 1-8, Mar. 2025.

[5] P. Jothilingam, “Edge computing for industrial automation and control: Enabling real-time processing, scalable architectures and secure operations,” Certified Journal of International Research (CJIR), vol. 5, no. 1, pp. 1–8, Mar. 2025.

[6] D. R. Janardhana, K. Shivanna, M. Ghouse Shukur, C. P. Vijay, H. R. Mahalingegowda, and H. V. Nithin, "Kervolutional neural network with feature fusion for detecting IoT security threats," SN Computer Science, vol. 6, no. 8, p. 979, 2025.
[7] J. D. Rangappa, A. P. Manu, S. Kariyappa, S. K. Chinnababu, G. H. Lokesh, and F. Flammini, "A lightweight blockchain to secure data communication in IoT network on healthcare system," International Journal of Safety & Security Engineering, vol. 13, no. 6, pp. 1015–1024, 2023.
[8] K. Shivanna, H. P. Hema, D. R. Janardhana, and P. M. Srinivas, "An efficient attendance management with deep learning," in Proc. 2024 Int. Conf. on Computing, Semiconductor, Mechatronics, Intelligent Systems and Communications (COSMIC), Nov. 2024, pp. 18–23.
[9] N. S. Jayanna and R. M. Lingaraju, "Estimating coconut yield production using hyperparameter tuning of long short-term memory," International Journal of Advanced Computer Science and Applications, vol. 15, no. 4, pp. 764–771, 2024.
[10] P. K. P. Monappa and R. M. Lingaraju, "Effective skip-based residual network algorithm for detection and classification of areca plant diseases," International Journal of Intelligent Engineering Systems, vol. 18, no. 4, pp. 260–271, 2025.
[11] D. Narasappa, "Integrating Zero Trust Architecture with Automation and Analytics for Resilient Cybersecurity," 2025 3rd International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2025, pp. 1-6.
[12] D. Narasappa, "AI-Driven Security Measures for IoT Networks Utilizing Machine Learning for Anomaly Detection," 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC), GB Nagar, Gwalior, India, 2025, pp. 134-139.
[13] S. Rani, J. Singh, and S. Devi, "Comment on 'Evaluating Protein Liquid Supplementation for Enhanced Protein Intake and Adherence at Short-Term After Metabolic and Bariatric Surgery: A Pilot Randomized Controlled Trial,'" Obesity Surgery, Sep. 2025.
[14] S. Rani, J. Singh, and S. Devi, "Comment on 'Oncologic and perioperative outcomes following robot-assisted radical prostatectomy in morbidly obese patients: a systematic review and meta-analysis,'" Journal of Robotic Surgery, vol. 19, no. 1, Sep. 2025.
[15] I. Ganie and S. Jagannathan, "Adaptive control of robotic manipulators using deep neural networks," Proc. 6th IFAC Conf. Intell. Control Autom. Sci. (ICONS), vol. 55, no. 15, pp. 148–153, 2022.
[16] I. Ganie and S. Jagannathan, "Continual online learning-based optimal tracking control of nonlinear strict-feedback systems: Application to unmanned aerial vehicles," Complex Eng. Syst., vol. 4, no. 1, 2024.
[17] I. Ganie and S. Jagannathan, "Continual optimal adaptive tracking of uncertain nonlinear continuous-time systems using multilayer neural networks," Proc. 2023 Amer. Control Conf. (ACC), San Diego, CA, USA, 2023, pp. 3395–3400.
[18] H. R. Laskar, "Adoption of fintech and digital financial services (DFS) by young professionals," Int. J. Adv. Res. Eng. Technol., vol. 11, no. 1, pp. 537–561, 2020.
[19] H. R. Laskar, "Factors influencing saving and investment behavior of government and private sector employees," Indian Journal of Economics and Business, vol. 20, no. 1, pp. 1168–1192, 2021.
[20] S. Roushon and H. R. Laskar, "Influence of Neural Behaviour on Decision Making," IOSR Journal of Humanities and Social Science, vol. 29, no. 5, ser. 13, pp. 35–42, May 2024.
[21] Z. Alam and H. R. Laskar, "The Influence of Neural Behavior on Individuals' Financial Decisions," Journal of Economics, Finance and Management Studies, vol. 7, no. 6, pp. 3298–3306, Jun. 2024.
[22] S. Laskar, H. R. Laskar, and M. N. I. Barbhuyan, "Perception of Women Entrepreneurs Regarding Social Media Marketing," Bangladesh Journal of Multidisciplinary Scientific Research, vol. 9, no. 5, pp. 10–18, Nov. 2024.
[23] A. Dhanai, H. S. Bagde, R. Gera, K. Mukherjee, C. Ghildiyal, and H. Yadav, "Case report on irritational fibroma," Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S960–S962, Feb. 2024.
[24] H. Bagde, A. Dhopte, F. Bukhary, N. Momenah, F. Akhter, O. Mahmoud, K. P. Shetty, M. A. Shayeb, H. Abutayyem, and M. K. Alam, "Monkeypox and oral lesions associated with its occurrence: a systematic review and meta-analysis," F1000Research, vol. 12, p. 964, Mar. 2024.
[25] H. Bagde, R. S. Karki, S. Husain, S. Khan, V. Haripriya, and P. Purwar, "Evaluation of microbiological flora in endo-perio lesions before and after treatment," Journal of Pharmacy and Bioallied Sciences, vol. 17, suppl. 2, pp. S1707–S1709, Jun. 2025.

[26] B. Shyamsukha, H. Bagde, A. Sharan, M. Choudhary, A. Duble, and A. V. Dhan, “Evaluating the potential of ChatGPT as a supplementary intelligent virtual assistant in periodontology,” Journal of Pharmacy and Bioallied Sciences, vol. 17, suppl. 2, pp. S1415–S1417, Jun. 2025.

[27] H. S. Bagde, M. K. Alam, A. K. A. Alhamwan, H. M. H. Aljubab, F. F. A. Alrashedi, D. H. M. Aljameeli, and M. G. Sghaireen, “The effect of a low-carbohydrate diet on periodontal health and inflammation in patients with type 2 diabetes,” Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S641–S643, Feb. 2024.

[28] H. S. Bagde, M. K. Alam, Y. E. M. Almohammed, S. M. M. Almaqawid, A. W. N. Alanazi, F. T. F. Alanazi, and M. G. Sghaireen, “The efficacy of platelet-rich plasma as an adjunct to bone grafting in alveolar ridge preservation following tooth extraction,” Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S564–S566, Feb. 2024.

[29] S. B. Mangalekar, H. S. Bagde, M. Sale, S. V. Jambhekar, C. Patil, and C. V. Deshmukh, “Comparing laser-assisted and conventional excision in the management of oral soft lesions: a prospective clinical study,” Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S859–S861, Feb. 2024.

[30] M. K. Alam, H. S. Bagde, A. K. A. Alhamwan, H. M. H. Aljubab, F. F. A. Alrashedi, D. H. M. Aljameeli, and M. G. Sghaireen, “Comparing the long-term success rates of immediate implant placement vs delayed implant placement in patients with periodontally compromised teeth,” Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S626–S628, Feb. 2024.

[31] H. S. Bagde, M. K. Alam, Y. E. M. Almohammed, S. M. M. Almaqawid, K. K. Ganji, and M. G. Sghaireen, “Comparing the clinical and radiographic outcomes of two different surgical approaches for treating infrabony defects in chronic periodontitis patients,” Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 1, pp. S567–S569, Feb. 2024.

[32] A. Sharan, B. Pawar, H. Bagde, T. K. Chawla, A. V. Dhan, B. Shyamsukha, and S. Sharma, “Comparative evaluation of dentin hypersensitivity reduction over one month after a single topical application of three different materials: a prospective experimental study,” Journal of Pharmacy and Bioallied Sciences, vol. 16, suppl. 4, pp. S3405–S3407, Dec. 2024.

[33] J. Prakash, T. Sinha, H. Bagde, N. Rajegowda, S. Bhat, A. Dhopte, M. Cicciù, and G. Minervini, “Evidence-based assessment of temporomandibular disorders in complete denture versus partial denture users: a systematic review,” Minerva Dental and Oral Science, Sep. 2025.

[34] J. R. Rogers, Y. Wang, N. F. Khan, K. Mott, V. K. Nomula, D. Wang, P. C. Fiduccia, M. Burcu, and X. Liu, “Landscape assessment of clone-censor-weight methodology application in real-world data studies: A scoping review,” in Proceedings of the Pharmacoepidemiology and Drug Safety Conference, vol. 33, pp. 424–424, Nov. 1, 2024.

[35] I. A. Mohammed, "Artificial Intelligence in Supplier Selection and Performance Monitoring: A Framework for Supply Chain Managers," Educational Administration: Theory and Practice, vol. 29, no. 3, pp. 1186–1198, 2023.

[36] I. A. Mohammed, "The Role of Artificial Intelligence in Enhancing Business Efficiency and Supply Chain Management," Journal of Information Systems Engineering and Management, vol. 10, no. 10s, pp. 509–518, Feb. 2025.

[37] I. A. Mohammed, "AI-Powered Risk Management Frameworks for Ensuring Supplier Quality in Carbon Capture and Energy Storage Supply Chains," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 1, pp. 854–, Dec. 2023.

[38] I. A. Mohammed, "Optimizing Carbon Capture Supply Chains with AI-Driven Supplier Quality Management and Predictive Analytics," Journal of Next-Generation Research 5.0, Dec. 2024.

[39] I. A. Mohammed, "Machine Learning-Driven Predictive Models for Enhancing Supplier Reliability in Renewable Energy Storage Supply Chains," International Journal of Intelligent Systems and Applications in Engineering, pp. 767–770, 2022.

[40] N. Gupta, M. Adawadkar, I. A. Mohammed, S. Verma, and M. Dubey, "Predictive Insights: Leveraging Artificial Intelligence for Strategic Business Decision-Making," Advances in Consumer Research, vol. 2, pp. 98–105, 2025.

[41] Kumar, P.R., Mohammad, G.B., Narsimhulu, P., Narasappa, D., Maguluri, L.P. et al. (2025). Computer Modeling Approaches for Blockchain-Driven Supply Chain Intelligence: A Review on Enhancing Transparency, Security, and Efficiency. Computer Modeling in Engineering & Sciences, 144(3), 2779–2818.

[42] R. M. Lingaraju, C. S. Pillai, and A. B. Jayachandra, “Object recognition using Lucas–Kanade technique and support vector machine based classification in video surveillance systems,” International Journal of Engineering and Advanced Technology, vol. 9, no. 1, pp. 2219–2224, Oct. 2019.
[43] P. M. Srinivas, K. Shivanna, D. R. Janardhana, and S. Samarth, “SAAI—Smart automated anti-violence intervention,” in Proc. 2024 Int. Conf. on Computing, Semiconductor, Mechatronics, Intelligent Systems and Communications (COSMIC), Nov. 2024, pp. 82–87.
[44] D. R. Janardhana, K. Shivanna, and A. P. Manu, “Security and privacy in military application using blockchain,” in Artificial Intelligence for Military Applications with Blockchain. Boca Raton, FL, USA: CRC Press, 2025, pp. 1–18.
[45] D. R. Janardhana, A. P. Manu, K. Shivanna, and K. C. Suhas, “Malware analysis and its mitigation tools,” in Malware Analysis and Intrusion Detection in Cyber-Physical Systems. Hershey, PA, USA: IGI Global, 2023, pp. 263–284.
[46] P. Jothilingam, “Advancing cybersecurity in industrial control systems: Frameworks, threat modeling, and resilience strategies,” International Journal of Supportive Research (IJSR), vol. 2, no. 2, pp. 69–75, Jul. 2024.
[47] P. Jothilingam, “Cybersecurity in water and wastewater systems: Protecting critical infrastructure from emerging threats and ensuring operational resilience,” in Proc. International Conference on Recent Advances in Science, Engineering, Technology and Management, India, Mar. 2024, pp. 550–558.
[48] K. Chitra, S. S. Priscila, E. S. Soji, R. Rajpriya, B. Gayathri, and A. Chitra, “Transforming electrical simulation and management with smart grid technologies,” International Journal of Engineering Systems Modelling and Simulation, vol. 16, no. 4, pp. 241–253, 2025.
[49] M. V. Soosaimariyan, H. L. Allasi, K. Chitra, and J. B. Gnanadurai, “Enhanced EMG-based hand gesture recognition by using generalized deep infomax networks,” Journal of Sensors, vol. 2025, no. 1, p. 9496890, 2025.
[50] K. Lakshmi and K. Chitra, “Stress Net: Multimodal stress detection using ECG and EEG signals,” Journal of Data Science, vol. 2024, no. 59, pp. 1–8, 2024.
[51] S. Rishabh, K. Chitra, and C. S. Yap, “A study on non-fungible tokens marketplace for secure management,” INTI Journal, vol. 2024, no. 18, pp. 1–8, 2024.
[52] S. Shreyash, S. Gaur, K. Chitra, and M. Y. N. Zuhaili, “EasyLearnify – A student study portal,” INTI Journal, vol. 2024, no. 17, pp. 1–6, 2024.
[53] S. K. R. Padur, “Intelligent Resource Management: AI Methods for Predictive Workload Forecasting in Cloud Data Centers,” J. Artif. Intell. Mach. Learn. & Data Sci., vol. 1, no. 1, pp. 2936–2941, 2022.
[54] S. K. R. Padur, “Online Patching and Beyond: A Practical Blueprint for Oracle EBS R12.2 Upgrades,” Int. J. Sci. Res. Sci. Eng. Technol., vol. 2, no. 3, pp. 75–87, 2016.
[55] S. K. R. Padur, “Engineering Resilient Datacenter Migrations: Automation, Governance, and Hybrid Cloud Strategies,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 2, no. 1, pp. 340–348, 2017.
[56] S. K. R. Padur, “From Centralized Control to Democratized Insights: Migrating Enterprise Reporting from IBM Cognos to Microsoft Power BI,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 6, no. 1, pp. 218–225, 2020.
[57] S. K. Somayajula, "Enterprise Data Migration Success Patterns: Lessons from Large-Scale Transformations," International Journal of Research in Computer Applications and Information Technology (IJRCAIT), vol. 8, no. 1, pp. 757-776, Jan.-Feb. 2025.
[58] S. K. Somayajula, "Demystifying Modern Data Warehousing: From Traditional to Cloud-Native Solutions," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2025.
[59] S. K. Somayajula, "Building a Career in Enterprise Data Architecture: A Practical Guide," International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), vol. 7, no. 1, Jan. 2025.
[60] S. K. Somayajula, "Advanced ETL Optimization: A Framework for Next-Generation Data Integration," International Journal of Computer Engineering and Technology (IJCET), vol. 16, no. 1, pp. 381-406, Jan.-Feb. 2025.
[61] S. Somayajula and A. Orlovsky, "Proof, Truth and Contradiction in the System and Meta-System: Comprehensive Mathematical Solutions and Implementation Framework," 2025.

[62] P. Nutalapati, "Automated Incident Response Using AI in Cloud Security," Journal of Artificial Intelligence, Machine Learning and Data Science, vol. 2, no. 1, pp. 1301–1311, 2024
[63] P. Nutalapati, "Data Leakage Prevention Strategies in Cloud Computing," European Journal of Advances in Engineering and Technology, vol. 8, no. 9, pp. 118–123, 2025.
[64] P. Nutalapati, "Security Considerations for Hybrid Cloud Deployments in Fintech Using Blockchain," Journal of Artificial Intelligence, Machine Learning and Data Science, vol. 1, no. 1, URF Publishers, 2025.
[65] P. Nutalapati, "Zero Trust Architecture in Cloud-Based Fintech Applications," Journal of Artificial Intelligence & Cloud Computing, vol. 2, no. 1, pp. 1–8, 2023.
[66] P. Nutalapati, J. R. Vummadi, S. Dodda and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," 2025 International Conference on Data Science and Its Applications (ICoDSA), Jakarta, Indonesia, 2025.
[67] P. Nutalapati, S. M. Dhavale, A. Shrivastava, R. V. S. Praveen, H. K. Vemuri and R. RiadHwsein, "IoT and Machine Learning-Enhanced Energy Management in Enabled Smart Grids for Predictive Load Balancing," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025.
[68] P. Nutralapati, "Disaster Recovery and Business Continuity Planning in Cloud-Blockchain Infrastructures," SSRN Electron. J., Jun. 2020. Available: https://ssrn.com/abstract=5219038.
[69] S. Arul Krishnan, V. P. Rameshkumaar, K. Prakash, and D. Sugandaran, "Impact of celebrity endorsement on cause-related marketing and purchase intention of FMCG consumers in Chennai," Journal of Statistics & Management Systems, vol. 26, no. 7, pp. 1627–1641, 2023.
[70] S. Arul Krishnan, V. P. Rameshkumaar, R. Sathya Aarthi, and S. Karthikeyan, "Role of job design on institutional support and work-life equilibrium of women teachers in Chennai," Journal of Statistics & Management Systems, vol. 26, no. 7, pp. 1549–1563, 2023.
[71] S. Karthikeyan, V. P. Rameshkumaar, and B. Balaji, "Subscribers of Indian Mobile Telecom: Satisfaction with Experience and Loyalty," International Journal of Management, vol. 11, no. 9, Oct. 15, 2020.
[72] S. Pundir, V. G. Murugan, P. Raman, V. P. Rameshkumaar, and P. Sudharsan, "Automatic Stock Price Prediction and Classification Based on Hybrid with AI Feature Selection Method," in Proc. 2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), pp. 149–154, Apr. 9, 2024. IEEE.
[73] V. Kumar, P. P. Devi, T. N. Babu, A. S. Nader, A. A. S. Mohammed and R. Saravanakumar, "AI-Powered Recruitment Marketing Enhancing Candidate Experience and Employer Branding," 2025 IEEE International Conference on Emerging Technologies and Applications (MPSec ICETA), Gwalior, India, 2025, pp. 1-6.
[74] V. P. Rameshkumaar, D. Ganesan, S. Revathy, R. Karthikeyan, and P. P. Devi, "Evaluating the impact of artificial intelligence on logistics and supply chain efficiency," Indian Journal of Natural Sciences, vol. 15, no. 88, pp. 88823–88828, Feb. 2025.
[75] Y. A. Abduvakhob Kizi, P. Praba Devi, S. Mahadevan, and S. D. S. Ugli, "Words and algorithms: The intersection of linguistic and artificial intelligence," AIP Conference Proceedings, vol. 3306, no. 1, p. 050005, 2025.
[76] S. G. K. Peddireddy, "Advancing Threat Detection in Cybersecurity through Deep Learning Algorithms," FMDB Transactions on Sustainable Intelligent Networks., vol.1, no. 4, pp. 190–200, 2024.
[77] S. G. K. Peddireddy, "Integrating AI for Proactive Network Defense against Emerging Security Vulnerabilities," FMDB Transactions on Sustainable Computer Letters., vol. 2, no. 4, pp. 232–241, 2024.
[78] S. G. K. Peddireddy, "Optimizing Resource Allocation in Multi-Cloud Environments for Cost Efficiency and Scalability," FMDB Transactions on Sustainable Computing Systems., vol. 2, no. 4, pp. 167–177, 2024.
[79] V. Hiremath, "Quantum Networking: Strategic Imperatives for Enterprises and Service Providers in the Emerging Quantum Era," Journal of Computational Analysis and Applications (JoCAAA), vol. 31, no. 3, pp. 617–631, Dec. 2023.
[80] V. Hiremath, "AI-Optimized Adaptive Routing for High-Performance Data Centers: A Predictive Framework for Dynamic Network Optimization," 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC), GB Nagar, Gwalior, India, 2025.
[81] V. Hiremath, "Optimizing SDN Controller Placement for Enhanced Performance and Scalability in Large-Scale Networks," 2025 International Conference on Intelligent Communication Networks and Computational Techniques (ICICNCT), Bidar, India, 2025.

[82] D. Sumathi and P. Poongodi, "Scheduling Based on Hybrid Particle Swarm Optimization with Cuckoo Search Algorithm in Cloud Environment," IIOAB Journal, vol. 7, no. 9, pp. 358-366, 2016.
[83] D. Sumathi and P. Poongodi, "Secure medical information processing in cloud: Trust with swarm based scheduling," Journal of Medical Imaging and Health Informatics, vol. 6, no. 7, pp. 1636-1640, 2016.
[84] V. B. Gowda, M. T. Gopalakrishna, J. Megha, and S. Mohankumar, "Foreground segmentation network using transposed convolutional neural networks and up sampling for multiscale feature encoding," Neural Netw., vol. 170, pp. 167–175, 2024.
[85] V. B. Gowda, G. M. Thimmaiah, M. Jaishankar, and C. Y. Lokkondra, "Background-foreground segmentation using Multi-scale Attention Net (MA-Net): A deep learning approach," Rev. Intell. Artif., vol. 37, no. 3, pp. 557–565, 2023.
[86] A. K. Joshi and S. B. Kulkarni, "Flow analysis of vehicles on a lane using deep learning techniques," J. Adv. Inf. Technol., vol. 14, no. 6, pp. 1354–1364, 2023.
[87] A. K. Joshi, V. Shirol, S. Jogar, P. Naik, and A. Yaligar, "Credit card fraud detection using machine learning techniques," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 6, no. 3, pp. 436–442, 2020.
[88] A. K. Joshi and S. B. Kulkarni, "Multi-modal information fusion for localization of emergency vehicles," Int. J. Image Graph., vol. 24, no. 1, Art. no. 2550050, 2024.
[89] A. Srivastava, "Securing PHI Data in Healthcare," Sci. Data Learn. Mach. Intell. Artif. J., vol. 2, no. 4, pp. 1678–1679, Oct. 2024.
[90] A. Srivastava, "Use of AI/ML in Data Security," J. Artif. Intell. Mach. Learn. Data Sci., vol. 2, no. 2, pp. 1–3, 2024.
[91] A. Srivastava, "WFH Impact on Work Culture and Future of Work Place," Int. J. Innov. Res. Creat. Technol., vol. 8, no. 6, pp. 1–8, Nov. 2020.
[92] A. Srivastava, "Impact of AI on Social Media and its Implication Mental Health," Int. J. Sci. Res. Eng. Manag., vol. 7, no. 7, 2023.
[93] A. Srivastava, "WFH Impact on Work Culture and Future of Work Place," Int. J. Innov. Res. Creat. Technol., vol. 8, no. 6, pp. 1–8, 2022.
[94] A. K. Joshi and S. B. Kulkarni, "Multimodal deep learning information fusion for fine-grained traffic state estimation and intelligent traffic control," Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 3, pp. 1020–1029, 2023.
[95] V. S. A. Anala, A. R. Pothu, and S. Chintapalli, "Enhancing Preventive Healthcare with Wearable Health Technology for Early Intervention," FMDB Transactions on Sustainable Health Science Letters., vol.2, no.4, pp. 211–220, 2024.
[96] R. Boina, "Assessing the Increasing Rate of Parkinson's Disease in the US and its Prevention Techniques"," International Journal of Biotechnology Research and Development, vol. 3, no. 1, pp. 1–18, 2022.
[97] V. S. A. Anala and S. Chintapalli, "Scalable Data Partitioning Strategies for Efficient Query Optimization in Cloud Data Warehouses," FMDB Transactions on Sustainable Computer Letters., vol. 2, no. 4, pp. 195–206, 2024.
[98] Md S. Miah and Md S. Islam, "Big Data Analytics Architectural Data Cut off Tactics for Cyber Security and Its Implication in Digital forensic," in Proc. 2022 Int. Conf. Futuristic Technol. (INCOFT), Belgaum, India, 2022.
[99] M. A. Obaida, Md S. Miah, and Md. A. Horaira, "Random Early Discard (RED-AQM) Performance Analysis in Terms of TCP Variants and Network Parameters: Instability in High-Bandwidth-Delay Network," Int. J. Comput. Appl., vol. 27, no. 8, pp. 40–44, Aug. 2011.