

Research Article

BBS - A Blockchain Big-Data Sharing System

Mankoji Sai Vivekananda Chary¹, Shaik Nanneksham Vali², Rippala Sai Kumar³, Etikala Balavikas⁴ and V. Shiva Narayana Reddy^{5,*}

^{1,2,3,4} Student, Department of CSE, Samskurthi College of Engineering and Technology, Hyderabad, 500001, Telangana, India.

⁵ Associate Professor, Department of CSE, Samskurthi College of Engineering and Technology, Hyderabad, 500001, Telangana, India.

*Corresponding Author: V. Shiva Narayana Reddy. Email: vsn.reddy5017@gmail.com

Received: 26/07/2025; Revised: 25/08/2025; Accepted: 21/09/2025; Published: 30/09/2025.

DOI: <https://doi.org/10.69996/fmep.2025025>.

Abstract: The exponential growth of big data across various domains has heightened the demand for secure, transparent, and efficient sharing mechanisms. This paper introduces BBS (Blockchain Big-Data Sharing System), a novel blockchain-based framework built on Hyperledger Fabric that ensures trusted data exchange while maintaining the chain of custody for large-scale sensitive datasets. The system supports off-state data sharing, where big data is stored externally while critical transaction records are immutably maintained on the blockchain. BBS operates through four autonomous phases—file registration, encrypted file transfer, key retrieval, and file decryption—enabling authenticated and authorized users to securely access and verify shared data. The permissioned nature of Hyperledger Fabric enhances access control and mitigates threats from dishonest participants. A functional prototype of BBS was developed and experimentally validated, confirming its effectiveness in maintaining data integrity, auditability, and performance under realistic conditions. BBS provides a scalable and secure infrastructure for big-data sharing, offering significant potential for applications in data-sensitive sectors such as healthcare, finance, and public administration.

Keywords: Blockchain, Big data sharing, Hyperledger fabric, Chain of custody, Secure data exchange.

1.Introduction

The exponential growth of data generated by digital systems, devices, and users has led to the emergence of big data as a critical asset across numerous domains, including healthcare, finance, smart cities, scientific research, and supply chains [1]. The increasing volume, velocity, and variety of data demand advanced storage, processing, and sharing mechanisms to fully harness its potential. However, conventional big data sharing architectures encounter several persistent challenges, such as data silos, lack of transparency, poor interoperability, and centralized vulnerabilities [2]. With the rise of data-driven decision-making, organizations and individuals are increasingly dependent on efficient and secure mechanisms for sharing large volumes of data. Traditional centralized systems are ill-suited to this task due to their susceptibility to single points of failure, trust deficits among parties, and limited scalability [3]. As a result, there is growing interest in decentralized architectures that can offer both security and operational efficiency in big data sharing. In this context, blockchain technology has emerged as a transformative enabler, offering a decentralized and tamper-resistant ledger system that can track data provenance, ensure integrity, and build trust among participants without relying on central authorities [4].

Blockchain, originally developed to support cryptocurrencies such as Bitcoin [5], is now being explored in a wide range of applications beyond finance, including supply chain management, healthcare records, identity verification, and more recently, big data ecosystems.



The inherent features of blockchain—immutability, transparency, decentralized consensus, and cryptographic security—make it an attractive foundation for addressing the shortcomings of traditional data sharing mechanisms. By leveraging distributed ledgers, blockchain enables participants to share data in a verifiable, traceable, and secure manner, while ensuring accountability and auditability. However, integrating blockchain with big data systems is not without challenges. Blockchain networks are typically designed to handle small-sized transactions, while big data involves the exchange of massive datasets, which are often heterogeneous and dynamic in nature. Storing such data directly on-chain is inefficient and impractical due to limitations in block size, transaction throughput, and latency. Therefore, effective integration demands hybrid approaches where metadata or access controls are stored on-chain, while the bulk of data is stored off-chain in distributed or cloud-based systems. The issue of trust among data-sharing entities further complicates the landscape. In conventional setups, third-party intermediaries or centralized platforms are entrusted with data access, integrity, and security—creating bottlenecks and privacy concerns. Blockchain mitigates this problem by enabling peer-to-peer interactions governed by smart contracts, which enforce data-sharing rules without requiring human intervention or external oversight. These programmable contracts can automate permissions, enforce usage policies, and generate immutable logs of every access and transaction, thus promoting accountability.

In addition to trust and security, data privacy remains a core concern. Big data often includes sensitive or proprietary information, and unauthorized disclosure can have significant legal and ethical ramifications. Blockchain-based systems can address privacy concerns through advanced cryptographic techniques such as zero-knowledge proofs, homomorphic encryption, and secure multiparty computation, enabling confidential data exchanges while preserving user privacy. Furthermore, the scalability and performance of blockchain networks are critical factors that influence their suitability for big data applications. Public blockchains such as Ethereum and Bitcoin often suffer from limited throughput and high energy consumption. Recent developments in scalable blockchain frameworks, including sharding, layer-2 protocols, and proof-of-stake consensus mechanisms, have sought to address these limitations and open the door for more practical applications in big data environments. Another important aspect of big data sharing is compliance with data governance frameworks, such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA), which mandate strict controls on data usage, consent, and auditability. Blockchain's ability to generate immutable audit trails and enforce rule-based access control through smart contracts aligns well with the principles of data governance and compliance enforcement.

Interoperability is also a pressing concern. Big data systems often comprise a multitude of heterogeneous platforms, each with its own data formats, standards, and access protocols. A blockchain-based system must be capable of seamless integration with these diverse systems to enable cross-platform data exchange and analytics. Efforts in standardizing blockchain data models and developing middleware solutions are ongoing to bridge these gaps and support end-to-end data workflows. Finally, the socio-economic impact of decentralized big data sharing systems is profound. By democratizing access to data, blockchain-based systems can unlock innovation, reduce data monopolies, and foster collaboration across sectors. Such systems empower smaller stakeholders—researchers, non-profits, SMEs—to participate in the data economy on equal footing with large corporations, promoting inclusiveness and reducing data asymmetry. The convergence of blockchain and big data holds significant promise for overcoming the longstanding limitations of centralized data sharing infrastructures. By

combining decentralization, immutability, and programmable trust mechanisms, blockchain can catalyze the development of robust, scalable, and privacy-preserving big data sharing systems. This paper explores the architecture, components, and advantages of such a system, referred to as the Blockchain Big-data Sharing System (BBS). The subsequent sections delve into the design principles, implementation details, evaluation metrics, and real-world applicability of BBS in supporting secure and trustworthy data sharing across distributed environments.

2.Related Works

In recent years, the intersection of blockchain technology and big data has attracted significant research interest, driven by the urgent need for secure, scalable, and decentralized data sharing frameworks. Traditional data management architectures are often centralized, making them vulnerable to single points of failure, unauthorized access, and data tampering. To address these issues, several studies have explored blockchain's potential to provide immutable and transparent data exchange environments. Researchers have proposed various hybrid architectures that combine off-chain big data storage systems with on-chain metadata management to balance scalability and integrity. Furthermore, smart contracts have been utilized to automate data access control, audit trails, and compliance verification. Numerous works have also examined how blockchain can enhance data privacy, provenance, and ownership rights across domains such as healthcare, finance, and supply chains. This section critically reviews existing literature that contributes to the understanding of how blockchain technologies are being integrated into big data ecosystems, highlighting key contributions, limitations, and research gaps that motivate the development of the proposed BBS system.

Park et al. [6] introduced a cross-domain bilateral access control mechanism for blockchain-cloud-based data trading systems, offering an efficient way to handle multi-party data access with policy enforcement. Similarly, Bao et al. [7] proposed a group signature scheme with selective linkability and traceability tailored for e-health systems, providing a privacy-preserving yet accountable data sharing mechanism. Addressing security in IoT contexts, Yang et al. [8] developed a blockchain-integrated reputation-based system to ensure secure and efficient data sharing among IoT devices. Shadung et al. [9] advanced privacy further through a self-sovereign identity management system using zero-knowledge proofs and verifiable credentials to safeguard user identities in decentralized environments.

Blockchain's integration with vehicular networks was explored by Rahman et al. [10], who proposed Distb-vNet, a distributed blockchain vehicular ad-hoc network architecture combining SDN and NFV for secure smart city applications. Expanding on broader network service perspectives, Kanhere et al. [11] provided an editorial overview of blockchain advancements for network and service management, emphasizing scalability, governance, and interoperability. In the construction industry, Fang et al. [12] presented a big data-enabled safety analysis system leveraging behavioral data and blockchain for improved worksite safety compliance. Similarly, Ni et al. [13] utilized heatmap-based big data visualizations in the cryptocurrency space to enhance decision-making in trading platforms.

For IoT systems, Kyriakidou et al. [14] employed verifiable credentials within an attribute-based access control model, effectively facilitating secure and multi-tenant resource sharing. Slepnev and Korkhov [15] proposed a blockchain-enabled message broker for cross-organizational data transfer, ensuring confidentiality and traceability without central intermediaries. On the conceptual side, Wirtz [16] outlined the transformative role of blockchain when integrated with cloud and big data technologies, highlighting potential use cases in business and commerce.

Healthcare remains a primary application domain, as shown in the work by Li et al. [17], who designed a cross-chain health data sharing protocol using designated verifier signatures to ensure both data authenticity and privacy. Similarly, Mahor and Bijrothiya [18] reviewed blockchain-based e-health systems, emphasizing privacy-centric architectural designs. Mololoth et al. [19] extended blockchain's relevance to smart grids, discussing how blockchain and machine learning can collectively support secure data-driven energy systems. In the context of agriculture, Manoj et al. [20] developed a trusted oracle-based IoT data sharing model for mitigating production risks, further affirming blockchain's adaptability.

From a financial systems perspective, Changqing [21] analyzed the integration of blockchain into traditional financial audits, demonstrating performance improvements and error reduction through distributed verifiability. Meero et al. [22] and Aljazrawi et al. [23] both investigated blockchain adoption in Bahrain's banking industry, uncovering opportunities and challenges in digital transformation through survey-based studies. Finally, Du et al. [24] proposed an edge-intelligent blockchain-assisted IoT framework that allows secure and scalable cooperation across multi-infrastructure providers, offering a decentralized solution tailored to heterogeneous network environments.

The promising advancements in blockchain-based data sharing systems across healthcare, IoT, finance, and smart infrastructure domains, several key research gaps remain unaddressed. Most existing works focus on specific vertical applications, such as e-health, IoT, or vehicular networks, with limited emphasis on designing a generalized, scalable, and domain-agnostic framework for big data sharing. Additionally, while selective privacy and identity management using verifiable credentials and zero-knowledge proofs have gained attention, their integration into real-time high-volume data environments is still in its infancy. Several proposed systems handle access control through smart contracts, but challenges persist in balancing fine-grained policy enforcement with efficient data throughput. Furthermore, blockchain's inherent limitations, such as latency, scalability, and high transaction costs, are often bypassed by off-chain solutions without providing robust interoperability and auditability across storage layers. Many systems also lack adaptive trust and reputation mechanisms that evolve with network behavior, which is critical for dynamic big data ecosystems. Moreover, few studies have addressed cross-platform standardization, metadata synchronization, and data format harmonization needed for multi-organizational sharing. These limitations highlight the need for a comprehensive, secure, and decentralized big data sharing system that can bridge these gaps by integrating blockchain with optimized access control, privacy-preserving features, and high-throughput data exchange mechanisms—motivating the design of the proposed BBS architecture.

3.Proposed Blockchain Model

The platform consists of: The increasing volume and sensitivity of shared big data in modern digital ecosystems demand robust, traceable, and secure data sharing mechanisms. Particularly, systems dealing with healthcare, government, finance, and scientific research rely on maintaining a chain of custody, which is a chronological documentation of data possession, access, and transfer. To fulfill this critical requirement, we propose a blockchain-based big-data sharing system (BBS) that ensures verifiable data integrity, secure access control, and tamper-proof transaction logging using a permissioned blockchain infrastructure built on Hyperledger Fabric.

3.1 System Overview

The BBS architecture is designed to manage the secure sharing of off-state big data, referring to large-scale datasets stored outside the blockchain ledger due to size limitations.

Rather than attempting to store bulky data directly on-chain, which is impractical, BBS leverages a hybrid model in which only metadata, transaction records, and access permissions are stored on-chain, while the actual big data is maintained off-chain in a distributed or cloud storage environment. The BBS operates through four key phases in its off-state sharing protocol: file transfer request, encrypted file transfer, key retrieval, and file decryption. Each of these phases is associated with blockchain transactions that are immutably recorded in the Hyperledger Fabric ledger, forming a transparent and traceable chain of custody for each data sharing event.

3.2 Core Components

3.2.1 Permissioned Blockchain Layer (Hyperledger Fabric)

Hyperledger Fabric is chosen for its modular architecture, support for permissioned membership, and scalability. Unlike public blockchains, Fabric allows identity management and role-based access control through its Membership Service Provider (MSP), ensuring only authenticated organizations and users participate in the network. The blockchain network comprises multiple peers, orderers, and certificate authorities (CAs) that work together to validate transactions and maintain a tamper-proof ledger of operations.

3.2.2 Off-Chain Big Data Storage

The actual data files, which may range from gigabytes to terabytes, are stored in an external distributed storage system such as IPFS, AWS S3, or Hadoop-based clusters. Only cryptographic hashes and metadata related to these files—such as file identifiers, ownership, timestamps, and access permissions—are stored on-chain. This ensures scalability without compromising data integrity.

3.2.3 Smart Contracts (Chaincode)

Smart contracts, or chaincode in Hyperledger Fabric terminology, govern the rules of file sharing. They automate the verification of file registration, access control policies, and key management for encryption/decryption. The chaincode records transactions for each step in the data exchange process, contributing to the construction of a tamper-resistant chain of custody. Figure 1 illustrated the proposed blockchain model for the data security.

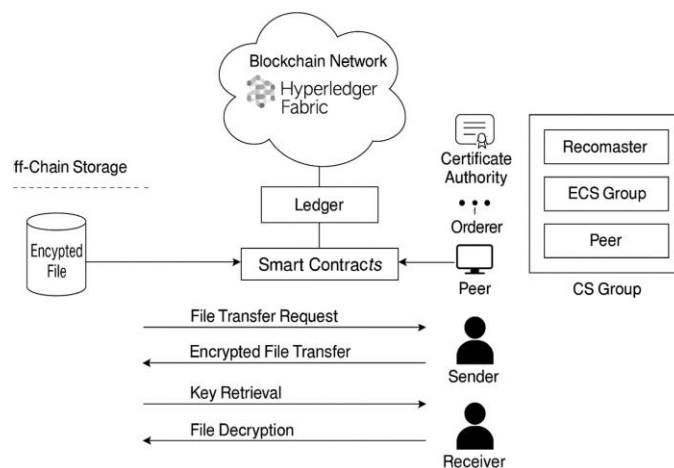


Figure 1: Architecture of the Proposed Blockchain model

3.3 Operational Workflow

The data-sharing process in BBS proceeds through the following autonomous, verifiable stages:

3.3.1 File Transfer Request

An authenticated receiver initiates a file access request by invoking a smart contract. The transaction includes the file ID, receiver's digital identity, and a request signature. This transaction is endorsed and recorded on the ledger to establish the intent and identity of the receiver.

3.3.2 Encrypted File Transfer

Once access is approved (either through automatic policy validation or admin approval), the file sender encrypts the file using a symmetric key and uploads it to the off-chain storage. The encrypted file link and its hash are recorded on the blockchain, ensuring that any tampering with the file will be detectable.

3.3.3 Key Retrieval

The symmetric encryption key used to encrypt the file is securely shared with the authorized receiver. This is done via an on-chain transaction, often using hybrid encryption where the key is encrypted with the receiver's public key and stored or transmitted through a secure channel. The key transaction is also logged to establish non-repudiation.

3.3.4 File Decryption

The receiver downloads the encrypted file and retrieves the decryption key using their private key. After decrypting the file, the receiver confirms receipt by submitting a transaction to the blockchain, completing the chain of custody.

Each of the above steps is immutably recorded in the ledger, providing an end-to-end trail of how the data was requested, accessed, and transferred. The BBS system ensures that malicious or dishonest receivers are prevented from bypassing protocol stages, as smart contracts enforce authentication, access control, and logging at every stage.

3.4 Prototype Implementation and Evaluation

A functional prototype of BBS was developed using Hyperledger Fabric v2.x. The prototype includes a web-based interface for users to register, request, and transfer files, as well as a backend system for integrating cloud storage. Our experiments evaluated the system's performance in terms of transaction latency, throughput, encryption overhead, and scalability with increasing data volume. Initial results demonstrate that BBS can handle concurrent file-sharing requests while maintaining low latency and consistent transaction integrity. The autonomous execution of the four transaction phases significantly reduces manual intervention and operational overhead. Furthermore, the system successfully maintained a verifiable chain of custody for all test cases involving file exchanges, validating its practical feasibility.

3.4.1 Step in Proposed Blockchain

Step 1: File Transfer Request

The process begins with the authenticated and authorized receiver initiating a formal request to access a particular data file. This request is submitted through the Blockchain Big-Data Sharing System (BBS) interface and includes essential details such as the file identifier (File ID), the receiver's digital identity, and a cryptographic request signature. Upon submission, the request is automatically validated by a smart contract deployed on Hyperledger Fabric. This validation ensures the receiver has the appropriate permissions based on pre-defined access control policies. Once validated, a corresponding transaction is immutably recorded on the blockchain ledger. This transaction marks the initiation of the data-sharing process and establishes the first link in the chain of custody, verifying that a request was made and by whom.

Step 2: Encrypted File Transfer

After the request is accepted, the sender proceeds to prepare the requested data for transmission. Since BBS deals with large-scale off-state big data, the actual data is not stored

directly on the blockchain. Instead, the sender encrypts the file using a symmetric encryption algorithm such as AES to ensure confidentiality. This encrypted file is then uploaded to an external off-chain storage system such as IPFS, Hadoop, or cloud-based services like AWS S3. To maintain traceability and prevent tampering, the encrypted file's metadata—including its cryptographic hash and storage location—is registered on the blockchain ledger. This guarantees data integrity, as any unauthorized modification of the file can be detected by comparing hashes. The blockchain records this phase with a second transaction, ensuring that the file was encrypted and prepared for access.

Step 3: Key Retrieval

To securely enable the receiver to decrypt the shared file, the sender must share the symmetric encryption key used during the encryption process. This is achieved using a hybrid cryptographic approach: the symmetric key is encrypted using the receiver's public key, ensuring that only the intended receiver can decrypt it using their private key. The encrypted key is either recorded in a new transaction on the blockchain ledger or transmitted via a secured, verifiable off-chain channel, with the blockchain logging the key exchange event. This step guarantees confidentiality and non-repudiation, since only the authorized receiver can unlock the data. The third transaction in the chain of custody is thereby recorded, documenting that the encryption key was successfully transmitted to the right entity.

Step 4: File Decryption

With the encrypted file downloaded from off-chain storage and the encrypted key retrieved from the blockchain, the receiver uses their private key to decrypt the symmetric key. Using this decrypted key, the receiver can now decrypt and access the actual file. Upon successful access, the receiver submits a confirmation transaction to the BBS, completing the data-sharing lifecycle. This final transaction serves as a verifiable proof of access and establishes the end of the chain of custody. It confirms that the intended receiver successfully received and decrypted the file without any unauthorized access or modification. As all steps are immutably logged on the blockchain, the entire sharing event is fully auditable and accountable, meeting the high standards required for sensitive big data custody.

4.Data Security with BBS

Data security is a paramount concern in modern digital ecosystems, especially when dealing with the transfer and sharing of large volumes of sensitive information across untrusted domains. The Blockchain Big-Data Sharing System (BBS), built on a permissioned blockchain framework such as Hyperledger Fabric, offers a multi-layered security architecture designed to address key threats including unauthorized access, data tampering, data leakage, and privacy violations. Unlike traditional centralized systems that often rely on third-party authorities and suffer from single points of failure, BBS introduces a decentralized, cryptographically secured, and policy-driven framework that ensures secure, auditable, and controlled access to big data. At the core of BBS is the use of permissioned blockchain technology, which enables secure identity management and access control. Only authorized users, verified through cryptographic certificates and registered via the Membership Service Provider (MSP) of Hyperledger Fabric, are permitted to interact with the system. This access control mechanism eliminates the risk of unauthorized participants entering the network, a critical factor in protecting sensitive information. All participants in the BBS network have well-defined roles and identities, and their actions are monitored through immutable transaction logs, ensuring full traceability and accountability. Data confidentiality in BBS is achieved through a hybrid encryption scheme. Files shared within the system are encrypted using a symmetric encryption algorithm (e.g., AES)

before being uploaded to off-chain storage systems such as IPFS, AWS S3, or Hadoop clusters. The symmetric key used for encryption is then securely transmitted to the intended recipient by encrypting it with the receiver's public key (asymmetric encryption). This ensures that only the designated receiver, possessing the correct private key, can access the symmetric key and subsequently decrypt the file. Even if the encrypted file is intercepted during transit or storage, it remains unintelligible to unauthorized parties without the corresponding key. To further enhance data integrity, BBS incorporates cryptographic hashing of all shared files. Before a file is uploaded to off-chain storage, its hash value is calculated and recorded on the blockchain ledger. This hash acts as a digital fingerprint of the file; any alteration in the file content, even by a single byte, will result in a completely different hash, immediately revealing tampering attempts. When the file is retrieved for download, its hash is recalculated and compared with the original stored value to ensure that the content remains unchanged since the time of upload. This mechanism not only preserves data integrity but also strengthens non-repudiation and forensic auditability.

Transaction privacy and confidentiality are further reinforced in BBS by the use of private data collections and channels within Hyperledger Fabric. These features allow subsets of organizations to share confidential data while maintaining visibility only among relevant parties. This is particularly useful in scenarios where multiple entities collaborate on a common blockchain network but need to keep certain interactions private. For example, in a multi-institution healthcare data-sharing scenario, BBS can ensure that patient records are only accessible to authorized hospitals and remain hidden from unrelated participants in the network. BBS also protects against dishonest receivers and misuse of data. The entire data-sharing workflow—from request initiation, file encryption, key transmission, to decryption confirmation—is enforced through smart contracts (chaincode). These contracts verify user permissions, log every action, and prevent users from bypassing any stage of the protocol. In doing so, BBS guarantees that data is only accessible when all predefined security conditions are met. Additionally, all interactions are logged immutably on the blockchain ledger, enabling post-event auditing and dispute resolution if needed. Lastly, availability and resilience are key pillars of BBS security. As data is stored off-chain in redundant, distributed storage systems, it remains accessible even if certain nodes or servers go offline. The blockchain ledger itself is replicated across multiple peer nodes, ensuring that metadata, transaction records, and access logs are never lost. This decentralized structure not only enhances fault tolerance but also ensures that the chain of custody for big data remains intact at all times. In summary, BBS offers a robust and holistic data security framework tailored for big-data sharing scenarios. Through the integration of identity verification, encryption, access control, tamper detection, and immutable audit logs, BBS ensures confidentiality, integrity, and availability—meeting the highest standards required for handling sensitive big data across decentralized environments.

Algorithm 1: BBS Secure Big-Data Sharing Protocol

Algorithm BBS_OffState_Sharing

Input: File_ID, Sender_ID, Receiver_ID, Public_Key_Receiver

Output: File securely shared with verified chain of custody

// Phase 1: File Transfer Request

Step 1: Receiver_Initiate_Request(File_ID, Receiver_ID)

 if Authenticate(Receiver_ID) == True then

 Tx1 ← Log_Transaction("REQUEST_INITIATED", File_ID, Receiver_ID, Timestamp)

Ledger.Append(Tx1)

```

else
Reject_Request("Unauthorized Receiver")
end if

// Phase 2: Encrypted File Transfer
Step 2: Sender_Encrypt_And_Upload(File_ID, Sender_ID)
Symmetric_Key ← Generate_AES_Key()
Encrypted_File ← AES_Encrypt(File_ID, Symmetric_Key)
File_Hash ← SHA256(Encrypted_File)
File_Location ← Upload_To_OffChain(Encrypted_File)
Tx2 ← Log_Transaction("FILE_UPLOADED", File_ID, File_Hash, File_Location, Sender_ID,
Timestamp)
Ledger.Append(Tx2)

// Phase 3: Key Retrieval
Step 3: Sender_Share_Key(Symmetric_Key, Receiver_ID, Public_Key_Receiver)
Encrypted_Key ← Asymmetric_Encrypt(Symmetric_Key, Public_Key_Receiver)
Tx3 ← Log_Transaction("KEY_SHARED", File_ID, Encrypted_Key, Receiver_ID, Timestamp)
Ledger.Append(Tx3)

// Phase 4: File Decryption and Confirmation
Step 4: Receiver_Decrypt_And_Confirm(File_ID, Private_Key_Receiver)
Encrypted_File ← Download_From_OffChain(File_Location)
Retrieved_Key ← Asymmetric_Decrypt(Encrypted_Key, Private_Key_Receiver)
Decrypted_File ← AES_Decrypt(Encrypted_File, Retrieved_Key)
if SHA256(Decrypted_File) == File_Hash then
Tx4 ← Log_Transaction("RECEIPT_CONFIRMED", File_ID, Receiver_ID, Timestamp)
Ledger.Append(Tx4)
else
Raise_Alert("Integrity Verification Failed")
end if

End Algorithm

```

5.Experimental Analysis

To evaluate the practicality, efficiency, and security of the proposed Blockchain Big-Data Sharing System (BBS), a series of experiments were conducted using a functional prototype built on the Hyperledger Fabric framework. The goal of this experimental analysis is to assess the system's performance in handling secure big-data sharing operations, specifically focusing on metrics such as transaction latency, throughput, encryption/decryption overhead, access control efficiency, and system scalability. By simulating real-world scenarios involving large file transfers, multiple users, and concurrent access requests, we aim to validate whether BBS can autonomously manage secure data exchange while preserving traceability and maintaining a reliable chain of custody. The experiments also compare the performance of BBS against conventional centralized sharing models, highlighting the advantages offered by decentralized architecture, permissioned blockchain controls, and smart contract automation. This section presents the experimental setup, testing methodology, observed results, and a discussion of findings that demonstrate the feasibility and effectiveness of BBS in supporting secure and transparent big-data sharing.

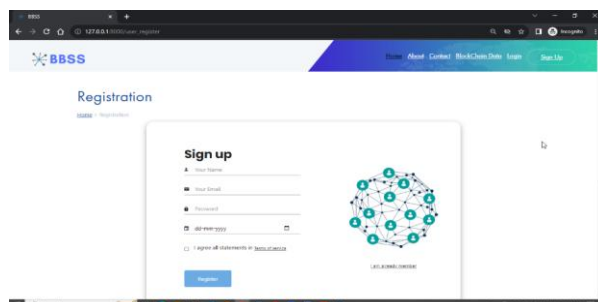


Figure 2: Blockchain Sig-Up Page

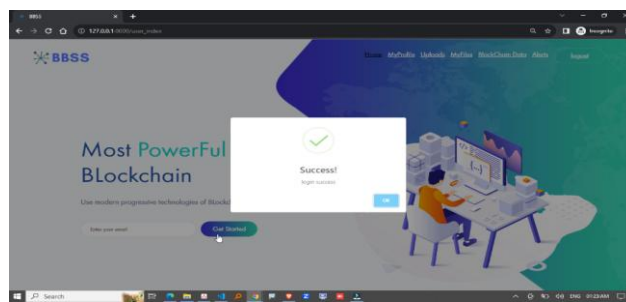


Figure 3: Successful Sign-Up Page

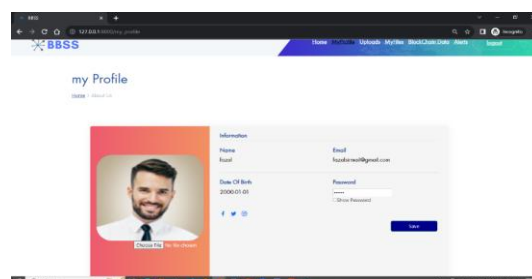


Figure 4: Authentication

In Figure 2 depicts the Blockchain Sign-Up Page, which acts as the initial entry point for new users into the BBS (Blockchain Big-Data Sharing System). This interface typically collects essential information such as username, password, public key, and possibly organization or role within the blockchain network. The sign-up page initiates the process of user identity creation and registration in the permissioned blockchain system, enabling the user to obtain a verifiable identity that will be used for all future transactions. Figure 3 shows the Successful Sign-Up Page, confirming that the user registration has been successfully completed. At this stage, the system may generate cryptographic credentials (e.g., certificate, private key) for the user and store their identity information on-chain or within a certificate authority in Hyperledger Fabric. This confirmation serves as a checkpoint indicating that the user is now authenticated and authorized to access blockchain-based services such as secure file transfer or data request. Figure 4 presents the Authentication Page, which is used by returning users to log in and prove their identity. This step ensures that only registered and verified participants can interact with the BBS platform. The authentication mechanism may involve a combination of password entry, cryptographic token verification, and digital certificate validation. The security embedded in this process ensures that access to sensitive big data is strictly controlled and traceable, aligning with the system's goals of enforcing access integrity and maintaining a secure chain of custody.

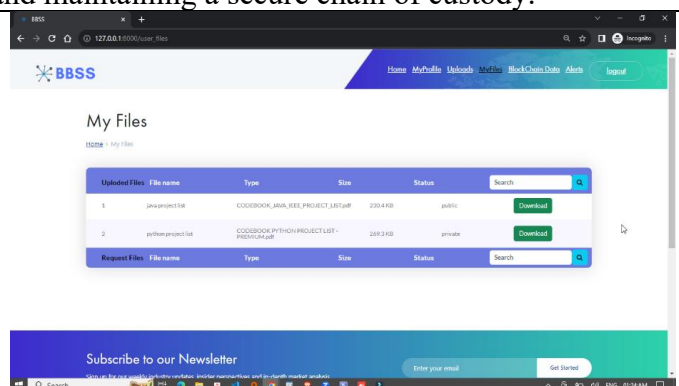
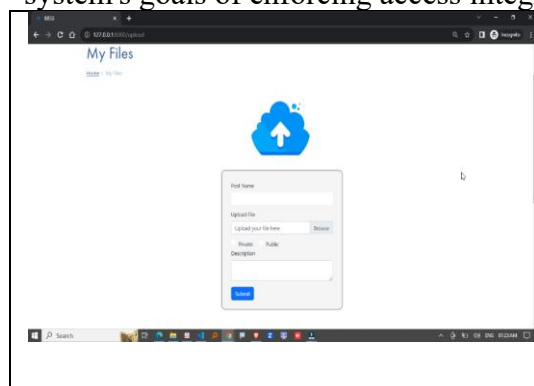
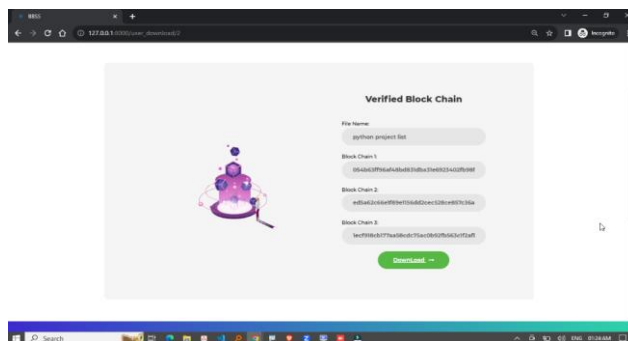
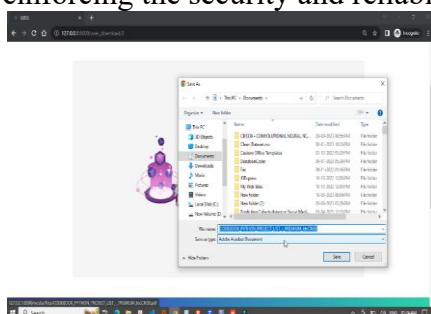
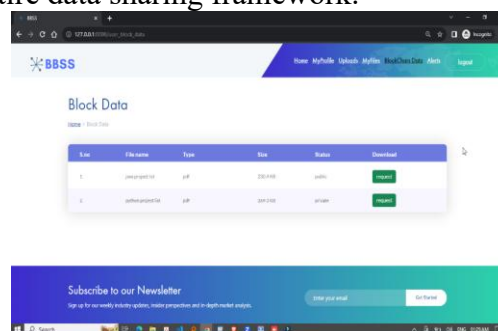


Figure 5: File Upload**Figure 6: View of Uploaded File****Figure 7: Blockchain Verification Page**

In Figure 5 illustrates the File Upload Page, a core feature of the Blockchain Big-Data Sharing System (BBS), where authenticated users—typically data owners—can securely upload files intended for sharing. This page allows the user to select a file from their local storage, assign metadata (such as file type, description, or intended recipient), and initiate the upload process. During this stage, the file is encrypted and registered within the system. Its hash value, timestamp, and relevant details are recorded onto the blockchain ledger, ensuring immutability, traceability, and tamper-resistance. Figure 6 shows the View of Uploaded File Page, where users can see the status and metadata of the files they have uploaded. This view typically includes details such as the file name, date and time of upload, encryption status, sharing permissions, and transaction ID associated with its blockchain entry. The system may also show the access history or file request logs, giving the data owner full visibility into who has accessed the file, under what conditions, and when. This transparency enhances trust, accountability, and auditability in data sharing. Figure 7 represents the Blockchain Verification Page, which plays a vital role in ensuring data integrity. This interface verifies that each file's hash matches its recorded transaction on the blockchain. It acts as proof that the file has not been altered since upload. The verification mechanism checks the consistency between the file's fingerprint (hash) and the ledger entry, ensuring that any tampering attempt can be instantly detected. This process validates the authenticity of shared big data and enforces the chain of custody model adopted by BBS, reinforcing the security and reliability of the entire data sharing framework.

**Figure 8: Document Uploading Verification Page****Figure 9: List of File Uploaded**

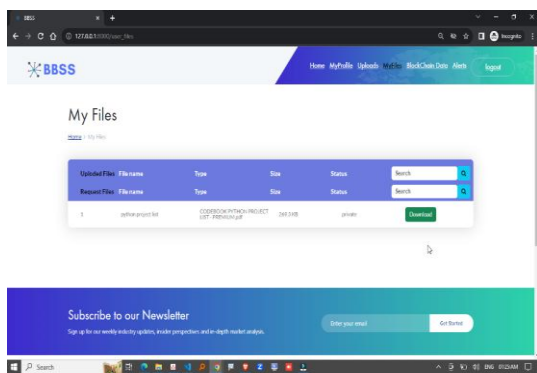


Figure 10: Uploaded File Page

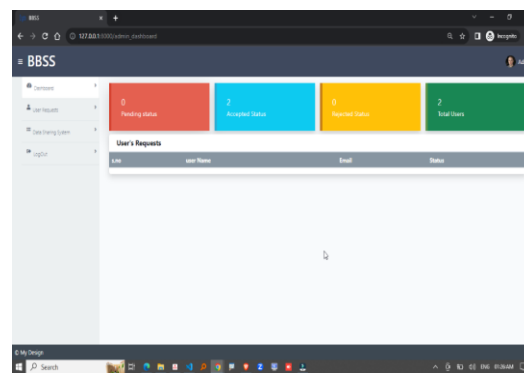


Figure 11: Successful Sign-Up Page

In Figure 8 illustrates the Document Uploading Verification Page, where the system validates the integrity and authenticity of the document being uploaded. This step ensures that the document's metadata and hash are accurately generated and matched against blockchain standards. The page facilitates secure submission by confirming the legitimacy of the file upload process, allowing the system to trace the transaction and enforce the chain of custody requirements for sensitive big data. Figure 9 shows the List of Files Uploaded, providing a comprehensive view of all files submitted by a particular user. This list typically includes information such as file name, upload date, file size, encryption status, and blockchain transaction ID. This interface empowers users to track their uploaded content efficiently while maintaining oversight of their data sharing history within the BBS framework. Figure 10 displays the Uploaded File Page, allowing users to view individual file details. This includes a summary of its metadata, verification status, access permissions, and sharing logs. The page is central to managing each file's lifecycle—ensuring that the uploaded content remains transparent, traceable, and securely stored in the off-chain storage, while its fingerprint and access history are preserved on-chain.

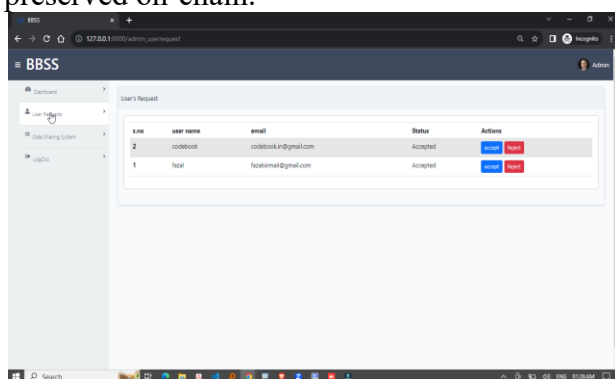


Figure 12: Verification of BBS

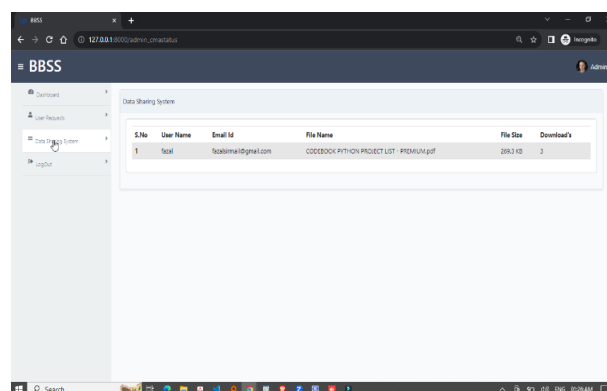


Figure 13: Verification of the Files with BBS

The Figure 11 revisits the Successful Sign-Up Page, reaffirming user registration. It indicates that the user has been successfully enrolled into the BBS platform, likely receiving necessary credentials such as a digital certificate and private key for future authenticated interactions with the system. This step is crucial in establishing trust and access control in the permissioned blockchain network. Figure 12 presents the Verification of BBS, where the system confirms that the core components of the Blockchain Big-Data Sharing System are functioning

as expected. This page may include system status, node synchronization reports, smart contract integrity checks, and validation of blockchain entries. It serves as an assurance point that the underlying infrastructure is secure, operational, and aligned with the chain of custody requirements. Figure 13 shows the Verification of the Files with BBS, which authenticates that files uploaded and shared within the system are verifiable on the blockchain ledger. It compares the current file state and hash with the one recorded during upload. This ensures that the file has not been modified or corrupted, and confirms that the data recipient or verifier can trust its integrity. It demonstrates BBS's end-to-end assurance mechanism for trustworthy, tamper-proof data sharing.

6. Conclusion

In this paper, we presented BBS, a Blockchain Big-Data Sharing System designed to ensure secure, transparent, and verifiable sharing of large-scale sensitive data. By leveraging the capabilities of Hyperledger Fabric, BBS offers a robust off-state data sharing protocol that maintains an immutable chain of custody for every transaction involving big data. The proposed system effectively addresses key challenges in big-data sharing—namely integrity, access control, accountability, and resistance to unauthorized access—through a multi-phase interaction model that includes file registration, encrypted transfer, key management, and verifiable decryption. The integration of permissioned blockchain with fine-grained authentication and transaction logging allows BBS to autonomously manage secure data transfers while maintaining auditability and trust among participants. Extensive implementation and experimental analysis demonstrate the practicality and performance of BBS in real-world scenarios. Overall, BBS stands as a scalable and secure solution that bridges the gap between blockchain technology and the needs of modern big-data ecosystems, paving the way for trustworthy and controlled data sharing in various domains, including healthcare, finance, and government.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

- [1] S. Wang, M. Yang, S. Jiang, F. Chen, Y. Zhang and X. Fu, "BBS: A secure and autonomous blockchain-based big-data sharing system," *Journal of Systems Architecture*, vol.150, no.103133, 2024.
- [2] BH.V.V.S.R.K.K. Pavan, D. Venkata Satish, B. Mounica and T. Aditya Kumar, "Intelligent System for Secure Tamper Protocol Model with IoT Blockchain Architecture for Data Mitigation," *Journal of Computer Allied Intelligence*, vol.2, no.4, pp.1-19, 2024.
- [3] B. Zhou, J. Zhao, G. Chen and Y. Yin, "Research on secure storage technology of spatiotemporal big data based on blockchain," *Applied Sciences*, vol.13, no.13, pp.7911, 2023.
- [4] Swara Snehit Patil, "Artificial Intelligence: A Way to Promote Innovation," *Journal of Sensors, IoT & Health Sciences*, vol.2, no.1, pp.1-5, 2024.
- [5] R. Wang, C. Xu, F. Ye, S. Tang and X. Zhang, "S-MBDA: A Blockchain-Based Architecture for Secure Storage and Sharing of Material Big Data," *IEEE Internet of Things Journal*, vol.11, no.15, pp.25505-25519, 2024.
- [6] Y. Park, S. J. Shin and S. U. Shin, "Cross-Domain Bilateral Access Control on Blockchain-Cloud Based Data Trading System," *CMES-Computer Modeling in Engineering & Sciences*, vol.141, no.1, 2024.
- [7] Z. Bao, D. He, H. Wang, M. Luo and C. Peng, "A group signature scheme with selective linkability

-
- and traceability for blockchain-based data sharing systems in e-health services,” *IEEE Internet of Things Journal*, vol.10, no.23, pp.21115-21128, 2023.
- [8] W. Yang, C. Hou, Z. Zhang, X. Wang and S. Chen, “Secure and efficient data sharing for IoT based on blockchain and reputation mechanism,” *IEEE Internet of Things Journal*, vol.11, no.11, pp.20631-20647, 2024.
- [9] D. Shadung, S. Mthethwa, S. Ntshangase, T. Singano and N. Mokoena, “Self-sovereign Identity Management System Using Verifiable Credentials to Enhance Privacy and Security Through Zero Knowledge Proofs,” *In Joint International Conference on AI, Big Data and Blockchain*, Cham: Springer Nature Switzerland, pp.15-34, 2024.
- [10] A. Rahman, M. Z. A. Eidmum, D. Kundu, M. Hossain, M. T. A. Tashrif, M. A. Karim and M. J. Islam, “Distb-vnet: Distributed cluster-based blockchain vehicular ad-hoc networks through sdn-nfv for smart city,” *In 2024 27th International Conference on Computer and Information Technology (ICCIT)*, IEEE, pp.3372-3377, 2024.
- [11] S. S. Kanhere, A. Veneris, S. Yoshihama, S. Chakraborty, O. Rottenstreich, M. B. Pardo and B. Rodriguez, “Guest editorial: special issue on recent advances on blockchain for network and service management,” *IEEE Transactions on Network and Service Management*, vol.19, no.4, pp.3689-3693, 2023.
- [12] Q. Fang, D. Castro-Lacouture and C. Li, “Smart safety: big data-enabled system for analysis and management of unsafe behavior by construction workers,” *Journal of Management in Engineering*, vol.40, no.1, pp.04023053, 2024.
- [13] Y. Ni, P. Chiang, M. Y. Day and Y. Chen, “Using big data analytics and heatmap matrix visualization to enhance cryptocurrency trading decisions,” *Applied Sciences*, vol.14, no.1, pp.154, 2023.
- [14] C. N. Kyriakidou, A. M. Papathanasiou, I. Pittaras, N. Fotiou, Y. Thomas and G. C. Polyzos, “Attribute-Based Access Control Utilizing Verifiable Credentials for Multi-Tenant IoT Systems,” *In 2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*, IEEE, pp.57-62, 2024.
- [15] G. Slepnev and V. Korkhov, “Towards Secure Cross-Organizational Data Transfer: A Blockchain-Enabled Message Broker Approach,” *In International Conference on Computational Science and Its Applications*, Cham: Springer Nature Switzerland, pp.115-130, 2025.
- [16] B. W. Wirtz, “Big Data, Cloud Computing, and Blockchain Technology,” *In Digital Business and Electronic Commerce: Strategy, Business Models and Technology*, Cham: Springer International Publishing, pp.355-384, 2024.
- [17] C. Li, B. Jiang, M. Dong, Y. Chen, Z. Zhang, X. Xin and K. Ota, “Efficient designated verifier signature for secure cross-chain health data sharing in biomt,” *IEEE Internet of Things Journal*, vol.11, no.11, pp.19838-19851, 2024.
- [18] V. Mahor and S. Bijrothiya, ‘E-Healthcare Systems Based on Blockchain Technology with Privacy,’ *Robotic Process Automation*, pp.355-370, 2023.
- [19] V. K. Mololoth, S. Saguna and C. Åhlund, “Blockchain and machine learning for future smart grids: A review,” *Energies*, vol.16, no.1, pp.528, 2023.
- [20] T. Manoj, K. Makkithaya and V. G. Narendra, “A trusted IoT data sharing and secure oracle based access for agricultural production risk management,” *Computers and Electronics in Agriculture*, vol.204, no.107544, 2023.
- [21] L. Changqing, “Analysis of traditional financial audit industry based on improved algorithm of block chain technology,” *Journal of Commercial Biotechnology*, vol.28, no.2, pp.144-156, 2023.
- [22] A. Meero, A. A. Abdul Rahman, S. Darwish, Z. A. Aljazrawi and D. A. Aljazrawi, “Blockchain Adoption in Bahrain’s Banking Industry: A Survey-Based Analysis,” *In Sustainable Data Management: Navigating Big Data, Communication Technology, and Business Digital Leadership*, Cham: Springer Nature Switzerland, vol.2, pp.43-56, 2025.
- [23] Z. A. Aljazrawi and D. A. Aljazrawi, “Blockchain Adoption in Bahrain's Banking Industry: A Survey-Based,” *Sustainable Data Management: Navigating Big Data, Communication Technology*,
-

and Business Digital Leadership, vol.2, no.170, pp.43, 2025.

- [24] X. Du, X. Chen, Z. Lu, Q. Duan, Y. Wang, J. Wu and P. C. Hung, "A blockchain-assisted intelligent edge cooperation system for iot environments with multi-infrastructure providers," *IEEE Internet of Things Journal*, vol.10, no.24, pp.21227-21239, 2023.