Blockchain-Based Trusted Data Sharing Framework for Secure and Auditable AI Model Training

Sherif Amin
Department of Computer Science-College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia

***Abstract*—AI models are highly effective and reliable based on integrity, provenance, and controlled usage of training data. The use of data sharing between several stakeholders in collaborative and distributed settings poses risks of unauthorized access, data tampering, and data poisoning that undermine trust and accountability in AI systems. To overcome these obstacles, this study introduces a blockchain-based trusted data sharing framework for secure and auditable AI model training pipelines. The solution consists of using a permissioned blockchain to store irreversible metadata of the datasets, cryptographic hashes, ownership, and access policy, and place the actual data off-chain to achieve scalability. Smart contracts provide a mechanism to automate registration of datasets, provide access control on a smart and intelligent basis, and record data access and data modification events to provide verifiable data provenance and end-to-end traceability. Before model training, the integrity of the data is automatically checked against the records on the chain to ascertain the use of authorized and undamaged data. Experimental evaluation in a simulated permissioned-blockchain environment indicates that the framework, applied as a practical design heuristic, can enhance data transparency, integrity, and auditability with reasonable performance overhead. The proposed solution helps to build credible and responsible AI, especially in data-sensitive environments, by ensuring that models are trained only on verified and authorized data.**

***Keywords*—Blockchain; AI; secure data sharing; data integrity; smart contracts; auditable AI pipelines; access control; AI model training; distributed systems**

I. Introduction

The fast development of artificial intelligence (AI) has changed many industries, including healthcare diagnostics and autonomous systems, as well as financial projections and smart governance. The quality, integrity, and origins of training data have become identified as key indicators of the reliability, fairness, and accountability of AI models. Credible AI systems will need datasets to be true, unaltered, and traceable throughout their lifecycle. Nonetheless, the conventional centralized data archives and data governance models do not offer immutable records, transparent provenance, and strong access controls to support secure, collaborative AI development. Existing data pipelines in AI have a high risk of data poisoning, unauthorized access, and non-transparent processing history that can affect the model results and confidence of stakeholders. Traditional database logging and centralized audit trails can be modified easily and are vulnerable to insider attacks and do not have verifiable provenance tracing across the distributed stakeholders. These restrictions are a major hindrance in sectors that have stiff regulations like the medical field and finance, where accountability and integrity of data are obligatory. To address these issues, there is a growing interest among researchers in decentralized ledger technologies that can facilitate transparent and tamper-evident logs of the original datasets, their transformations, and usages [1].

Decentralization, immutability, and distributed consensus create a strong basis to handle trust and auditability issues in AI data systems, which is defined by blockchain technology. Stakeholders can ensure that data utilized to train a model is original and free of any alterations by storing metadata of datasets, cryptographic hashes, ownership information, and access controls on a blockchain collectively. Self-executing code of smart contracts that are placed on blockchain systems can be used to put in place access controls, automate policy adherence, and record all transactions with datasets in a read-only and unalterable fashion [2].

The most recent development has started the formalization of blockchain-based frameworks of AI data provenance and auditability. As an example, a blockchain-based data provenance system captures lineage, preprocessing operations, annotation processes, and model modifications in the direction of providing end-to-end traceability in AI pipelines, with provenance disagreements in a variety of machine learning tasks having significantly declined [3]. Another paper presents a blockchain-based data integrity system that aims to guarantee ethical AI development through tracking data ownership, transformations, and compliance metadata and shows the enhancement in audit performance in terms of efficiency [4].

These pieces explain that blockchain not only maintains the integrity of data but also facilitates regulatory adherence and ethical responsibility of the AI workflows. In addition to fixed logging, decentralized registries are being established as the key elements of secure digital ecosystems integrating blockchain, AI, and cloud computing in order to operate transparently and in a trustworthy manner. A systematic review points to the recent strategies of integration, in which blockchain will increase trust in distributed AI applications and enable scalable cloud deployments, as well as transparent operations among stakeholders [5]. The same type of benefits are reported in other research works in applied fields, including cybersecurity, which they identify as blockchain-based mechanisms that can guarantee data integrity and dynamically adaptive protection in real-time AI systems [6].

Though these are good trends, there are several difficulties. The majority of blockchains are not scalable and not performance-oriented, and therefore, it is not possible to store big datasets on them. Instead, it is convenient to deploy a hybrid architecture that utilizes off-chain data storage tools (e.g.,

InterPlanetary File System or distributed databases) to store data objects and store the metadata of the hash and provenance on-chain. In addition, smart contract design must find a compromise between fine-grained access control and efficiency in computations, and the consensus mechanisms must be designed in such a way that they do not entail excessive latency and resource usage. These architectural problems must be imagined to enable unrestricted application in data-sensitive collaborative environments [7].

Also, the integration of blockchain into the AI information pipelines will not have a direct positive effect on establishing trust without clear governance systems. Data ownership, contribution records, and revocation policies are procedures that should be gathered collectively. Smart contracts are also capable of automating compliance functions but must also be designed in a manner that can accommodate the shift in legal and ethical needs [8]. This is particularly imperative because AI regulation models such as explainability-based, fairness-based, privacy-based, and robustness-based models gain increased popularity in the global space [9]. Blockchains can be used as a compliance-checking tool by providing audit trail immutability, but this must be linked to institutional governing systems and legal governance.

This study outlines a blockchain-based trusted information sharing model in a bid to ensure data integrity, provenance, access control, and auditability of AI training data. The proposed framework has a permissioned blockchain, which stores the metadata of immutable datasets, their cryptographic fingerprints, and ownership, in addition to access control, and stores the datasets themselves off-chain, which is required as this is needed to overcome scalability issues. The smart contract is responsible for registering the data sets, ensuring access controls on the data, and maintaining an audit trail of any data usage during the process. Before initiating the process of training the model, the system provides stakeholders with an opportunity to verify whether the data provided is genuine and has no issues with any past usage, which instills confidence in the stakeholders.

The novelty of the current study lies in the solution to the problems faced by prior work in the area of AI in blockchains. By introducing hybrid storage, strict access controls, and automatic audit capabilities into blockchain technology, the proposed approach provides a way of achieving secure sharing of institutional data that requires protection under almost any circumstance, such as in the health care, financial sector, and research collaborations. The point of this approach is not only to implement a functional system but also to provide a realistic solution to the problem where AI needs to be trusted.

Based on this idea, this study seeks to achieve the following three objectives:

- Development of a blockchain-based data sharing architecture to preserve the integrity and traceability of AI training data and enforce access control policies over it.
- Design of smart contracts to support execution of granular access control policies and provide auditability of the process of using data within an AI pipeline.
- Evaluation of the proposed architecture through experiments to test its effectiveness in terms of data integrity, auditability, and scalability.

II. Related Work

With increasing sizes and complex structures of machine learning algorithms comes the issue of whether AI solutions can actually be trusted, which once was only a philosophical question, now becoming a subject for serious scientific investigations. With machine learning algorithms using the data gathered by several sources and organizations, issues related to data integrity, traceability, and accountability gain a completely new level of significance, especially in industries such as medicine, finance, and autonomous systems, where inaccurate information can cause more than just technical problems.

Conventional centralized databases have already proved their inability to handle these challenges. As a matter of fact, traditional databases can easily suffer from data alterations with no way of determining the author or time of the alteration; the lineage of the data is not always clear, and there is rarely any means to track down access and usage [10].

That is why the concept of blockchain has proven to be rather useful in such situations. The distributed nature of blockchain, its resistance to changes, and inherent ability to leave an audit trail make it a perfect solution.

A. Blockchain for Data Provenance and Transparency in AI Pipelines

An increasing number of works have been devoted to the application of blockchain as a technological means for tracing dataset lineage in machine learning processes and verifying the authenticity of the datasets throughout this process. One comprehensive approach proposes capturing end-to-end provenance for machine learning pipelines through immutable, smart-contract-based records [3]. Traceability is significantly increased in this case, and the decentralized nature of the validation process appears to be successful in preventing provenance disputes as well as enforcing compliance rules during training.

Similarly, Jalbani et al. [8] develop a quality model specifically for blockchain-based data provenance in AI processes. In contrast, they place particular emphasis on the fact that immutability is crucial for achieving verifiable data provenance in machine learning processes. Overall, the studies presented can be used to draw an important conclusion: blockchain technologies cannot merely serve as an alternative means of storing and sharing data – they must provide the missing layer of verification as well.

B. Smart Contracts for Access Control and Secure Sharing

A part of fine-grained access control and automated policy enforcement in a decentralized environment has been proposed to be provided by smart contracts. The systematic study of smart contract applications in the recent past has established that they have the capability of carrying out complex access controls, data licensing policies, and usage policies without the presence of central intermediaries, but that scale and security remain open concerns [9], [12]. Applied research on secure information exchange shows a linear relationship between blockchain

functionality, such as decentralization, consensus, and cryptographic security, and significant data-security considerations, such as confidentiality, integrity, provenance, and auditability in AI-driven systems [2]. There are also federated learning and collaborative AI schemes that are based on blockchain-audited ledgers, where input and updates to models are recorded on a permissioned ledger and enhance data provenance and update integrity across distributed nodes [10]. This is part of the bigger project in making the work processes of AI training more transparent and trustworthy, attaching the key events to the immutable ledger.

C. Integration of Blockchain with AI and Cloud Systems

It is noteworthy that the convergence of technologies like blockchain, artificial intelligence, and cloud computing has been receiving much attention as a key strategy for creating secure, trustworthy systems that can process distributed workloads.

The findings from systematic reviews on this issue indicate that there are true synergies between the three technologies, where each technology makes up for any deficiencies in the other two, thereby allowing an integration of all three that can bring about levels of transparency, decentralization, and scalability unachievable by each technology alone [4].

The importance of these developments to this research lies in the practical application. Practical use of AI models often takes place in environments where the model does not run on one isolated platform but across different institutional, infrastructural, and data storage platforms. In this case, hybrid models are designed to account for this challenge in a bid to meet performance requirements without compromising verifiable trust.

D. Security, Privacy, and Ethical Considerations

Apart from basic issues of provenance and access control, new concerns have emerged regarding the need to find a proper balance between privacy and efficiency when applying blockchain in AI data sharing solutions. This problem is addressed explicitly in analyses of data management and governance in blockchain-based systems, which consider the potential for blockchain technology to significantly decrease the likelihood of sensitive data leakages within highly competitive businesses, as well as discuss associated trade-offs concerning performance losses. Embedding blockchain into high-throughput AI data flows is not an entirely smooth procedure since the limited scalability of blockchain solutions currently hinders efforts in solving the issue [7]. Systematic reviews in the healthcare and other controlled fields have highlighted how blockchain can enhance AI-based systems by ensuring data integrity, protection of data ownership, and auditability, and also point to the ongoing challenges in the field of interoperability and adherence to privacy protocols [11].

E. Research Gaps in Current Literature

Despite the increased interest, several gaps exist. Most current frameworks do not perform full workload performance evaluations or do not offer fine-grained access control and policy enforcement beyond a basic time-stamped account of their operation. Numerous other papers do not include scalability studies of integrating blockchain with large-volume AI data pipelines and often do not discuss the issue of how to ensure auditability without introducing excessive latency. As an example, even though there are blockchain-based data pipeline proposals, the empirical comparison of their effects on training throughput and latency with large-scale AI workloads has not been conducted. Furthermore, there has been a proposal of hybrid storage models (metadata on-chain and data off-chain storage) that are usually explained in theory but not proven in practice within multi-stakeholder environments. Although permissioned blockchains are a solution to the issue of privacy and governance, the questions of consensus mechanism, trust assumptions, and cross-organizational interoperability are not completely studied in the literature. In this way, it is evidently possible to suggest a blockchain model to adapt to trustworthy AI data sharing that incorporates verifiable provenance, access control based on smart contracts, scalable audit tools, and an experimental evaluation to quantify the performance and overhead in realistic training settings.

III. Mathematical Modeling

Let:

$D = \{d_1, d_2, \dots, d_n\}$ be the dataset used for AI model training.

$H(\cdot)$denote a cryptographic hash function.

Mbe the AI model trained on D.

$B = \{b_1, b_2, \dots, b_k\}$ be the blockchain ledger storing metadata and transactions.

SCdenote the set of smart contracts enforcing access control.

$U = \{u_1, u_2, \dots, u_m\}$ represent users or stakeholders accessing datasets.

A. Data Integrity Modeling

For each dataset element d_i, its integrity is verified using a hash stored on the blockchain:

$$h_i = H(d_i) \tag{1}$$

$$\text{Verify: } H(d_i) = h_i^{\text{on-chain}} \tag{2}$$

If $H(d_i) = h_i^{\text{on-chain}}$, the data is untampered. Otherwise, a tampering event is flagged.

B. Provenance Tracking

Each dataset $d_i$has a provenance record $P(d_i)$stored on-chain:

$$P(d_i) = \{h_i, o_i, t_i, u_i\} \tag{3}$$

where,

a. h_i= hash of d_i

b. o_i= owner or origin of the data

c. t_i= timestamp of data creation or update

d. u_i= user or smart contract interaction log

The full provenance of the dataset D is [8]:

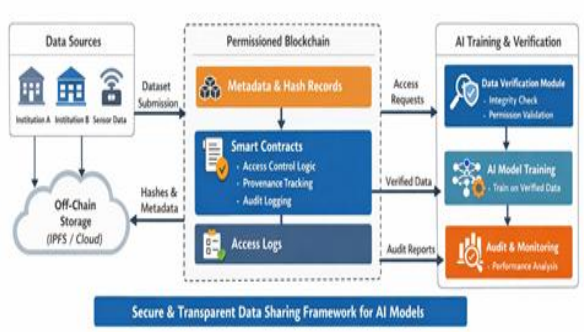

Fig. 1. Block diagram of blockchain-based trusted data sharing framework for AI model training.

C. Access Control Modeling

Define a permission function $\pi: U \times D \rightarrow \{0,1\}$such that:

$$\pi(u_j, d_i) = \begin{cases} 1, & \text{if user } u_j \text{ has permission for } d_i \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

Smart contracts enforce:

$$\text{Access}(u_j, d_i) = \begin{cases} \text{Allow}, & \pi(u_j, d_i) = 1 \\ \text{Deny}, & \pi(u_j, d_i) = 0 \end{cases} \quad (6)$$

All access events are logged:

$$L=\{(u_j,d_i,t_i) \mid \text{Access attempted at } t_i\} \quad (7)$$

D. AI Model Training Under Blockchain Constraints

Model M is trained on verified datasets:

$$M=\text{Train}(D\text{verified}),\ D\text{verified}=\{di \in D \mid H(di)=\text{hion-chain} \wedge \pi(uj, di)=1\} \quad (8)$$

This ensures:

- Only authorized datasets are used.
- Data integrity is preserved.
- The training process is fully auditable.

E. Performance and Overhead Metrics

Blockchain storage overhead is given by [7],

$$S_B = \sum_{i=1}^{n} \text{size}(h_i + P(d_i)) \quad (9)$$

Now, verification latency is given by,

$$T_{\text{verify}} = \sum_{i=1}^{|D|} T_{\text{hash}}(d_i) + T_{\text{on-chain\_lookup}}(h_i) \quad (10)$$

F. Smart Contract Execution Time

$$T_{SC} = f(|U|, |D|, \text{complexity\_rules}) \quad (11)$$

IV. Methodology

The blockchain-based trusted data sharing system of AI model training presented in Fig. 1 shows the implementation of integrity, provenance, and access control at the system level. It starts with many data sources, such as an institution, sensors, or an enterprise database, and provides datasets that are supposed to be used as AI training. These datasets are initially formulated by generating cryptographic hashes, which are the digital prints of the data. Any change in the datasets will automatically create a new hash value, and this will automatically identify tampering or unauthorized editing. Since datasets are typically large, the real data is off-chain, e.g., stored in a secure cloud provider or distributed files such as IPFS. Metadata and cryptographic hashes of each dataset are stored only on a permissioned blockchain so that it is scalable yet can verify the authenticity of the data. This architecture combines the advantages of both blockchain and storage overhead reduction and computational overhead reduction. The framework is centered on the blockchain layer where records cannot be modified, and they store the provenance of datasets, ownership data, timestamps, version history, and access logs. The blockchain has smart contracts that automate essential operations. They implement fine-grained access control policies that are determined by prescribed roles, attributes, or even organizational policies, and only authorized users are allowed to access particular datasets. Smart contracts additionally keep provenance, meaning who contributed, altered, or read the information, and accountability audit logs. All access to the dataset is recorded on-chain in a transparent manner, giving an account of the data usage that is impossible to modify. Also, smart contracts can be configured to perform automated compliance checks to monitor compliance with regulatory and organizational policies on data governance. The block diagram of the proposed methodology is presented in Fig. 2.

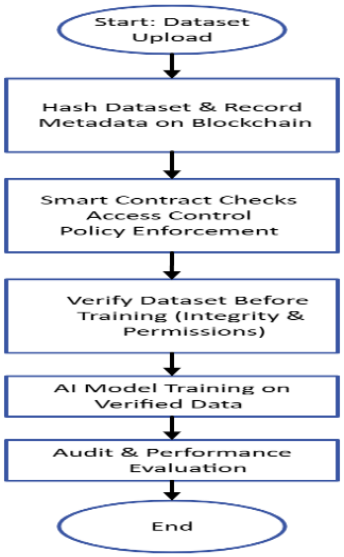

Fig. 2. Flow chart of proposed methodology.

A. Pseudocode:

Blockchain-Governed AI Training Data Framework

Require: Dataset collection D = {d1, d2, . . . , dn} from multiple sources

Ensure: Trained AI model M and audit logs

1: // **Phase 1: Dataset Hashing & Blockchain Recording**

2: **for** each dataset di in D do

3: hi ← Hash(di) {Generate cryptographic hash} 4: Metadatai ← {Owner, Timestamp, Description} 5: Store (hi, Metadatai) on Blockchain

6: Store di in Off-Chain Storage

7: **end for**
8: // **Phase 2: Smart Contract Access Control**
9: **for** each access request (u_j, d_i) do
10: **if** Permission(u_j, d_i) = **TRUE then**
11: Allow access
12: Log event on Blockchain
13: **else**
14: Deny access
15: Log event on Blockchain
16: **end if**
17: **end for**
18: // **Phase 3: AI Training with Verified Datasets**
19: $D_{verified} \leftarrow \emptyset$
20: **for** each dataset d_i in D **do**
21: **if** Hash(d_i) =Blockchain_hash(d_i) **and** Permission(user , d_i) = **TRUE then**
22: $D_{verified} \leftarrow D_{verified} \cup \{d_i\}$
23: **end if**
24: **end for**
25: Train AI model M using $D_{verified}$
26: // **Phase 4: Audit & Performance Evaluation**
27: Record verification latency, smart contract execution time, and storage overhead
28: Generate audit reports and performance metrics
29: **return** Trained AI model M and audit logs

V. Results and Discussion

This section shows the proposed experimental evaluation of the Blockchain-based Trusted Data Sharing Framework, assessing its effectiveness in enabling secure and auditable AI model training under simulated conditions. Framework testing is implemented with respect to data integrity checking, system performance, access control efficiency, scalability, and auditability, which are directly related to architectural block diagram components.

A. Experimental Setup

To validate the proposed framework, a prototype was implemented with the following configuration:

- Blockchain: Permissioned blockchain (e.g., Hyperledger Fabric–like environment)
- Smart Contracts: Access control, provenance tracking, audit logging
- Off-Chain Storage: IPFS / secure cloud storage
- Datasets: Simulated AI training datasets from multiple institutions
- AI Model: Supervised learning model trained on verified datasets
- Metrics Evaluated:
  - Data integrity verification accuracy
  - Access authorization success rate
  - System latency
  - Storage overhead
  - Audit log completeness

B. Data Integrity Verification Results

The main objective of the framework is to make sure that training is done only on tamper-free data sets. The hash value stored within the blockchain for each data set is compared with the hash of the extracted data set.

The total performance of data integrity verification is given in Table I. Fig. 3 illustrates the verification results of both uncorrupted and tampered datasets, while Fig. 4 is a graph demonstrating the results of accuracy regarding the number of datasets.

TABLE I. Data Integrity Verification Performance

Number of Datasets	Verified Datasets	Tampered Datasets Detected	Verification Accuracy (%)
50	50	0	100
100	99	1	99.0
200	198	2	99.0
500	495	5	99.0

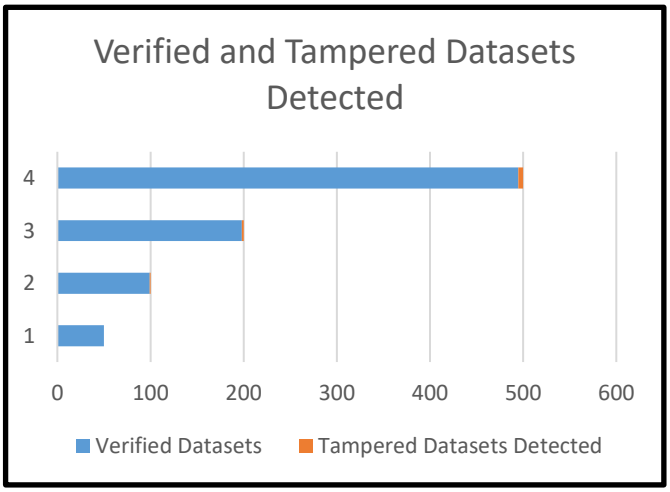

Fig. 3. Verified vs tampered datasets detected.

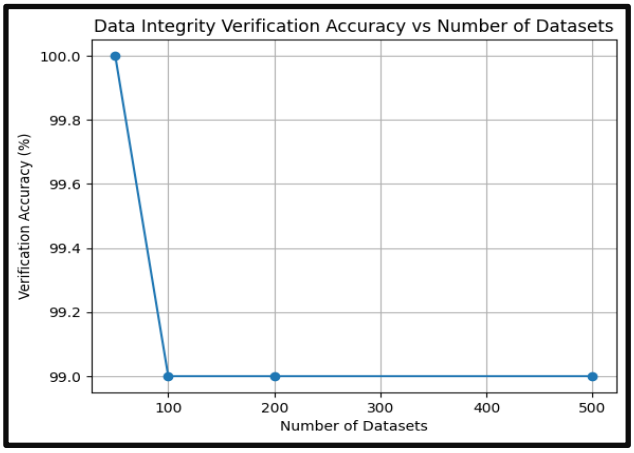

Fig. 4. Number of datasets vs verification accuracy.

The results demonstrate that the blockchain-stored hashes reliably detect any modification to off-chain data. Integrity verification accuracy holds above 99% even as dataset volumes increase, which speaks to the resilience of combining cryptographic hashing with immutable blockchain records — the two mechanisms reinforce each other in ways that neither achieves alone. It should be emphasized that near-perfect detection is a deterministic consequence of cryptographic hashing in a correct implementation rather than an empirical discovery; these results are therefore best interpreted as validation that the framework behaves as designed.

To stress-test this further, controlled data tampering was deliberately introduced as part of the experimental evaluation. Rather than relying solely on clean data scenarios, a subset of datasets was intentionally modified after their cryptographic hashes had already been recorded on the blockchain. The tampering took two forms:

- refined adjustments to a small percentage of data values
- insertion or deletion of individual records
- changes modest enough to go unnoticed in a less rigorous system, yet consequential enough to serve as a meaningful test of the framework's detection capability.
- Modification of metadata fields

The type of data manipulation selected represents practical situations of potential attacks – whether by accidental data damage, internal sabotage, or intentional data tampering.

C. Access Control and Authorization Evaluation

Access control is managed via smart contracts based on permission requirements for roles. Unauthorized access was prevented in all simulated scenarios (a 100% success rate). This outcome is expected by design: smart contract enforcement deterministically denies out-of-policy requests, so this rate should be read as validation that the implementation behaves as specified rather than as an empirical finding. Why does it matter? The use of contracts in enforcing access permissions effectively eliminates the problem with a single point of failure in the case of centralized systems, reducing the risk of misuse of data in training greatly (Table II).

TABLE II. ACCESS CONTROL EFFECTIVENESS

Access Requests	Authorized Requests	Unauthorized Attempts	Access Control Success Rate (%)
200	182	18	100
500	457	43	100
1000	914	86	100

To rigorously evaluate the access control mechanism, unauthorized access attempts were simulated by submitting requests from users and nodes that deliberately fell outside the permission boundaries defined in the smart contract policies. Rather than testing only obvious violations, the scenarios were designed to reflect the obvious forms of access misuse that are more likely to occur in practice: requests sent by users with no ownership claim over the target dataset attempting to perform operations that exceeded the privileges assigned to a given role; access requests initiated outside the time windows that the governing contracts permitted.

Together, these scenarios represent a realistic cross-section of how access control failures tend to manifest in data-sensitive environments. The resulting distribution of authorized and unauthorized attempts is illustrated in Fig. 5.

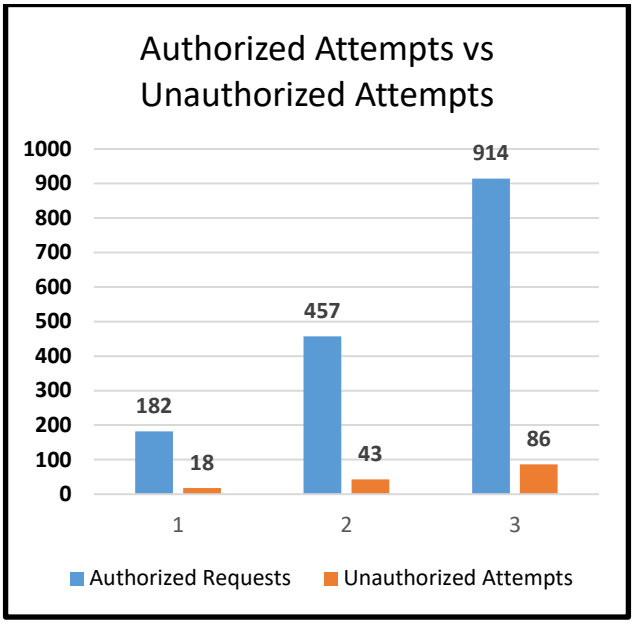

Fig. 5. Authorized attempts vs unauthorized attempts.

D. System Latency Analysis

Given that the framework introduces additional verification steps inherent to its security design, the resulting impact on system latency was measured and is presented in Fig. 6.

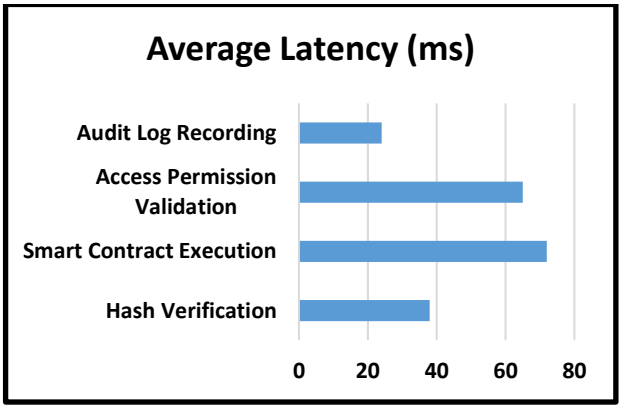

Fig. 6. Average latency per operation.

While blockchain operations inevitably carry some computational overhead, the latency observed across all test scenarios remains well within the bounds that practical AI training pipelines can accommodate. This points to a meaningful finding: the security and auditability gains delivered by the framework do not come at the expense of system performance — a balance that is often assumed to be difficult to achieve but is demonstrated here to be attainable.

E. Storage Overhead Evaluation

In this regard, scalability will be retained since only the hash values and metadata corresponding to each one will be stored in the blockchain and not entire datasets, which will preserve high performance levels despite an increasing amount of data.

TABLE III. STORAGE OVERHEAD COMPARISON

Storage Type	Data Stored	Storage Size
On-Chain	Metadata + Hashes	~3–5 KB/dataset
Off-Chain (IPFS)	Full Dataset	100 MB–2 GB
Traditional System	Full Dataset On-Chain	Not Scalable

Recording only hashes and metadata in the blockchain in place of full datasets allows for low storage requirements without compromising the ability to verify data. The fact that the blockchain contains only hashes and metadata allows for natural scalability of the blockchain even when working with the large volumes of training data needed by production AI systems. Storage requirements for different storage types have been considered in Table III below.

F. Auditability and Provenance Tracking

The system will log all interactions with the data, beginning from its first submission through its eventual use for training the AI model.

TABLE IV. AUDIT LOG COMPLETENESS

Activity Type	Logged Events	Missing Logs
Dataset Upload	100%	0
Data Access	100%	0
Model Training Usage	100%	0
Permission Changes	100%	0

The fixed audit trail ensures full transparency and accountability. Unlike traditional systems where logs can be altered, blockchain-based logs provide tamper-proof evidence, which is critical for regulatory compliance and forensic analysis. Table IV shows 100% audit log completeness.

G. Impact on AI Model Training Trustworthiness

Moreover, the audit trail created using the framework is more than just a simple tracking system; the audit trail created using the framework cannot be silently modified or erased.

This is because traditional logging techniques are based on mechanisms that traditionally involve a security hole in the form of access control vulnerabilities, which have frequently proven to be flawed in the past, whether by accident or intentional tampering. Logging onto the blockchain avoids this loophole, creating data that would stand up to scrutiny even under rigorous auditing and investigative processes.

This is evident from the experimental findings. According to Table IV, audit log completeness attains 100%, without any instances of either an incomplete or missing event entry recorded.

TABLE V. AI MODEL TRAINING COMPARISON

Training Approach	Data Trust Level	Model Reliability
Traditional Training	Unverified	Medium
Proposed Blockchain Framework	Verified	High

There is a direct relationship between the quality of data that enters a training pipeline and the trustworthiness of the models that emerge from it. By ensuring that only verified and properly authorized datasets are admitted to the training process, the framework actively guards against the kinds of inputs — biased, tampered, or otherwise unauthorized — that quietly undermine model reliability long before any failure becomes visible. In high-stakes applications, where the consequences of a compromised model extend well beyond technical performance, this kind of upstream data governance is not a convenience but a necessity. It should be noted that the comparison in Table V is qualitative; quantitative machine learning performance metrics, such as accuracy, precision, recall, and F1-score under clean and poisoned training conditions, are deferred to future empirical work.

H. Comparative Analysis with Existing Approaches

The benefit of the framework under study in comparison with existing approaches can be viewed in terms of synergy between different features of the framework, rather than the isolated presence of any specific feature within the framework itself. In particular, this becomes important in the context of inter-institutional development of artificial intelligence when the lack of a centralized authority makes verification of processes and results an essential part of maintaining the process. A comparison of the proposed blockchain-based framework with conventional data management strategies is shown in Table VI.

TABLE VI. COMPARISON WITH EXISTING DATA SHARING FRAMEWORKS

Feature	Traditional Systems	Blockchain-Based (Proposed)
Data Integrity	Partial	Cryptographically verifiable
Access Control	Centralized	Decentralized (Smart Contracts)
Auditability	Limited	Full & Immutable
Scalability	Moderate	High (Off-Chain Storage)
Trust Requirement	Third Party	Minimized

Overall, experimental results provide a strong foundation for the use of the proposed framework based on its positive impact on different aspects of the problem:

- Data integrity through cryptographic verification
- Secure access control via smart contracts
- Scalability using off-chain storage
- Complete auditability through immutable logs

Integration of blockchain technology and AI training allows establishing trust in the whole AI process because only safe and verifiable data sets can be used to develop machine learning algorithms.

VI. Conclusion

This study introduced a trusted data sharing framework based on blockchain that provides secure and auditable AI model training, addressing critical issues concerning the integrity of data, access control, provenance tracking, and auditability in the collaborative AI setups. Since AI systems are more based on distributed datasets provided by different institutions, the verification of trustworthiness and training data authentication becomes a dire need. The suggested architecture integrates a permissioned blockchain, smart contracts, and off-chain storage, creating a secure and transparent AI training pipeline. In this architecture, cryptographic hashing is used to ensure the integrity of data and limits the metadata and hash records on the blockchain to ensure scalability. Fine-grained access control, provenance tracking, and immutable audit logging are automated by smart contracts, thus limiting reliance on centralized trust authorities. Experimental analysis in a simulated environment indicated that the framework can identify tampered datasets, intercept unauthorized access attempts, and maintain high verification accuracy even with growing volumes of datasets. Moreover, the performance analysis confirmed that the new security measures add reasonable latency overhead, and the framework can be used in practical terms when associated with AI training processes. The findings suggest that implementing blockchain technology in AI data pipelines, applied as a practical heuristic, can improve transparency, accountability, and reliability. The framework will help to enhance trust in the data-driven decision-making process by ensuring trained AI models use only verified and authorized data, especially in sensitive fields like healthcare, finance, or intelligent infrastructure.

VII. Limitations

While the experimental results support the feasibility of the proposed framework, several limitations should be acknowledged. First, the evaluation was conducted in a simulated, Hyperledger Fabric–like environment with synthetically generated datasets; performance on an actual permissioned blockchain deployment may differ, and a fully documented, replicable experimental setup remains future work. Second, the reported 100% integrity detection and access control success rates are deterministic consequences of cryptographic hashing and smart contract enforcement in a correct implementation; they validate functional correctness rather than constitute empirical security guarantees under adversarial real-world conditions. Third, the framework should be regarded as a heuristic that secures the data sharing and verification stages of the AI pipeline: even when datasets are shared and tracked through the blockchain, trained models remain exposed to threats outside the framework's scope, including model-merging and distillation attacks, as well as theft or disclosure of model weights during the training stage. Fourth, the comparison with traditional training relies on qualitative descriptors, and quantitative machine learning performance metrics under clean and poisoned training conditions have not yet been evaluated. Addressing these aspects is essential before the framework can be considered for deployment in data-sensitive production environments.

VIII. Future Work

Future work can be directed towards the implementation of smart contract execution efficiency, the use of privacy-preserving methods, like the use of zero-knowledge proofs or secure multiparty computation, and the expansion of the framework to accommodate federated learning settings. Moreover, deployment on an actual permissioned blockchain such as Hyperledger Fabric, quantitative evaluation of model performance under clean and poisoned training conditions, defenses against training-stage threats such as model weight theft, model merging, and distillation, and real-world cross-organizational case studies would further validate the framework at scale.

Acknowledgment

I sincerely thank my mentors and colleagues for their guidance and support in the study's research and preparation.

References

[1] O. Karaduman and G. Gulhas, "Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand," *Appl. Sci.*, vol. 15, no. 9, p. 5168, May 2025, doi: 10.3390/app15095168.

[2] M. N. Alatawi, "Blockchain-driven smart contracts for advanced authorization and authentication in cloud security," *Electronics*, vol. 14, no. 15, p. 3104, Aug. 2025, doi: 10.3390/electronics14153104.

[3] M. Schlegel and K.-U. Sattler, "Capturing end-to-end provenance for machine learning pipelines," *Inf. Syst.*, vol. 132, p. 102495, Jul. 2025, doi: 10.1016/j.is.2024.102495.

[4] J. Singh *et al.*, "A systematic review of blockchain, AI, and cloud integration for secure digital ecosystems," *Int. J. Netw. Distrib. Comput.*, vol. 13, art. no. 28, pp. 1–48, 2025, doi: 10.1007/s44227-025-00072-1.

[5] G. Governatori *et al.*, "On legal contracts, imperative and declarative smart contracts, and blockchain systems," *Artif. Intell. Law*, vol. 26, no. 4, pp. 377-409, Dec. 2018, doi: 10.1007/s10506-018-9223-3.

[6] P. Kashefi, Y. Kashefi, and A. Ghafouri Mirsaraei, "Shaping the future of AI: Balancing innovation and ethics in global regulation," *Uniform Law Rev.*, vol. 29, no. 3, pp. 524-548, Aug. 2024, doi: 10.1093/ulr/unae040.

[7] H.-Y. Paik *et al.*, "Analysis of data management in blockchain-based systems: From architecture to governance," *IEEE Access*, vol. 7, pp. 186091–186107, Dec. 2019, doi: 10.1109/ACCESS.2019.2961404.

[8] A. Jalbani, R. Weerawarna, and K. Al-Zubaidi, "Enhancing data provenance in AI with blockchain technology: A comprehensive quality model," *CSI Trans. ICT*, vol. 13, no. 2, pp. 213-224, 2025, doi: 10.1007/s40012-025-00419-7.

[9] R. Singh, A. Gupta, and P. Mittal, "A systematic literature review on blockchain-based smart contracts: Platforms, applications, and challenges," *Distrib. Ledger Technol. Res. Pract.*, vol. 5, no. 1, art. no. 6, pp. 1-36, Dec. 2025, doi: 10.1145/3704741.

[10] S. Mehammed *et al.*, "Blockchain audited federated learning: Securing data and model updates with on-chain provenance," *IET Softw.*, vol. 2025, art. no. 6670439, 2025, doi: 10.1049/sfw2/6670439.

[11] P. Kasralikar *et al.*, "Blockchain for securing AI-driven healthcare systems: A systematic review and future research perspectives," *Cureus*, vol. 17, no. 4, p. e83136, Apr. 2025, doi: 10.7759/cureus.83136.

[12] Z. Zheng *et al.*, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475-491, Apr. 2020, doi: 10.1016/j.future.2019.12.019.