Application Mode of Blockchain Technology in User Data Sovereignty and Privacy Protection

Yinfeng Li

Office of Academic Affairs, Zhengzhou University of Technology, Zhengzhou, 450000, China
E-mail: lyfzyyf@outlook.com

Received 10 September 2025; Accepted 31 October 2025

Abstract

In the decentralized Internet environment, growing awareness of user data sovereignty has raised higher requirements for privacy protection in blockchain scenarios. To enhance the security and controllability of data authorization, this study develops a model integrating zero-knowledge proof (ZKP), field disclosure control, and multi-party joint verification. The ZKP ensures verifiable privacy, field disclosure control minimizes data exposure, and multi-party verification strengthens consistency and tamper resistance. Through this collaborative integration, the model forms a unified framework for secure and transparent data authorization. Experimental results on two blockchain datasets show that the model outperforms comparison approaches in authorization accuracy, field matching consistency, and verification efficiency, achieving a minimum verification loss of 0.248 and a true positive rate of 96.8%. Under simulation conditions, it maintains stable performance across different complexity levels, with authorization accuracy of 95.1% and field validation consistency of 96.5%. Compared with traditional

Journal of Cyber Security and Mobility, Vol. 14_5, 1199–1220.
doi: 10.13052/jcsm2245-1439.1457
© 2025 River Publishers

single-mechanism methods, the model delivers comprehensive improvements in privacy strength, verification transparency, and collaborative trust, demonstrating strong potential for application in high-sensitivity blockchain privacy protection scenarios, particularly in privacy-critical domains such as healthcare record management, financial data exchange, and supply chain traceability.

Keywords: Blockchain, privacy protection, data sovereignty, ZKP, DID.

1 Introduction

In the midst of the rapid advancement of digital infrastructure and the widespread adoption of artificial intelligence, data has steadily evolved into a digital asset with well-defined and measurable value [1]. Especially in the context of the current decentralized Internet, users frequently generate multidimensional sensitive data such as identity attributes, transaction records and behavior habits when using various intelligent services. How to ensure privacy protection and boundary control in the information processing process has become an important issue in technological governance [2]. In recent years, related research has explored data authorization, access control, and privacy preference expression [3, 4]. Li et al. proposed a sharing method for civil aviation flight operation data, which ensured identity privacy and data confidentiality while sharing data [5]. Singh et al. proposed a lightweight two factor authentication method for medical IoT environments, which covered multi-dimensional authentication and authorization of users, devices, and data, improving access control accuracy and system security. This method combined physical layer security mechanisms and authentication processes, balancing scalability and resource efficiency [6]. Sharma et al. proposed a sovereignty protection method for indigenous geographic spatial data that did not require a third-party trust mechanism. By embedding encryption and verification functions in the browser, anonymous sharing and authorized access of cloud data were achieved. This method, which combined geographic masking and blockchain hash verification technology, was applied and verified in the study of local management areas [7]. Yin et al. proposed a file retrieval model that combined attribute encryption and proxy re-encryption to optimize the searchability and integrity verification of encrypted data in cloud storage. This method introduced a partially hidden access structure, supported keyword updates and access control, and improved the retrieval efficiency of encrypted data while ensuring privacy and security [8].

To further enhance the manageability of users' information usage process, more and more research is introducing blockchain technology into data sharing and access control scenarios. Blockchain technology has characteristics such as immutability, traceability, and distributed storage, providing structural support for data analysis, permission expression, and auditing mechanisms [9]. Shree et al. proposed a medical IoT data protection architecture that combines blockchain technology. By introducing secret sharing algorithms to achieve distributed data storage, the system's ability to resist key leaks and node attacks was effectively enhanced. This architecture balanced data confidentiality with transparency and scalability, and was prototype validated and demonstrated good performance in medical monitoring scenarios [10]. Lejun et al. proposed a method for detecting and deleting redundant data at edge nodes using blockchain technology, which enabled the identification and dynamic integrity protection of hotspot data without compromising user privacy. This method used ciphertext scanning and content extraction signature mechanism to ensure secure removal of non hot data supported by blockchain, improving the efficiency and credibility of edge storage [11]. Deng et al. proposed a cross platform information dissemination privacy protection protocol based on blockchain and smart contracts, which achieved controllable and auditable management of user information upload and dissemination process through a four stage process. This method combined user privacy preferences to set the propagation range and has the ability to resist multiple types of malicious attacks [12]. Ghani MANU et al. developed a multi-technology fusion system that combined blockchain and distributed computing, aiming to enhance user data protection capabilities without sacrificing recognition accuracy. The system showed higher accuracy and stronger scalability in multiple public dataset tests, demonstrating good potential for practical deployment [13]. Although the above studies have demonstrated the effectiveness of blockchain-assisted privacy protection in specific domains, they generally remain scenario-dependent and technically fragmented. Most methods emphasize either data encryption or access control, but fail to establish a unified framework that simultaneously addresses verifiable privacy, flexible disclosure, and multi-party collaboration. Furthermore, several approaches rely heavily on centralized trust assumptions or static policy configurations, limiting their adaptability, scalability, and interoperability in dynamic decentralized environments.

In summary, although current research has achieved phased results in data encryption, access control, and identity verification, most solutions have not yet established a closed loop for user data sovereignty protection

centered on blockchain, especially in the areas of multi-agent collaboration and sensitive information disclosure control. Specifically, existing studies often lack scalability to support large-scale data authorization, interoperability across heterogeneous blockchain platforms, and robust performance under real-world constraints such as dynamic access policies and multi-role collaboration. Based on this, an innovative application model for user data sovereignty and privacy protection in the blockchain environment is proposed, which integrates two key mechanisms: Zero-Knowledge Proof (ZKP) and Decentralized Identifier (DID), and constructs a collaborative architecture of multi-attribute disclosure and joint verification mechanism [14, 15]. This method enhances data access privacy and security using ZKP. It enables flexible disclosure of multi-attribute identities through DID. Leveraging blockchain's tamper-proof and auditable features, it balances system deployability with privacy protection accuracy. This approach offers a new pathway for implementing data sovereignty across various scenarios. It is particularly valuable in privacy-sensitive areas like healthcare record management, financial data exchange, and supply chain traceability. Accordingly, this study aims to (1) construct a blockchain-based user data sovereignty protection model integrating ZKP, field disclosure control, and multi-party joint verification; (2) enhance verifiable privacy, controllable disclosure, and collaborative authorization in decentralized environments; and (3) validate the model's effectiveness through comparative experiments on multiple blockchain datasets. The main contributions of this research include proposing a unified framework for secure and transparent data authorization, introducing a multi-level disclosure mechanism for sensitive attributes, and establishing a collaborative verification approach that improves consistency and resistance to tampering.

2 Methods and Materials

2.1 Construction of Data Access Control and Privacy Statement Model Based on ZKP

In the blockchain data sharing environment, access control often faces issues such as permission disclosure, verification process exposure, and privacy leakage, which weaken the privacy protection capability of decentralized trust in blockchain. ZKP allows data owners to prove their access rights without exposing the original declaration content, which is an important mechanism to ensure that data is verifiable but invisible, and enhances the

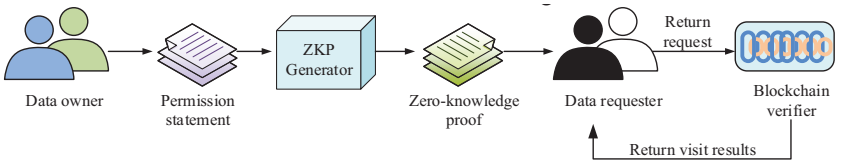

Figure 1 Architecture of the ZKP-based data access control model. (Illustrating the four key components and their interactions, demonstrating how off-chain proof generation and on-chain verification together enable privacy-enhanced access control.)

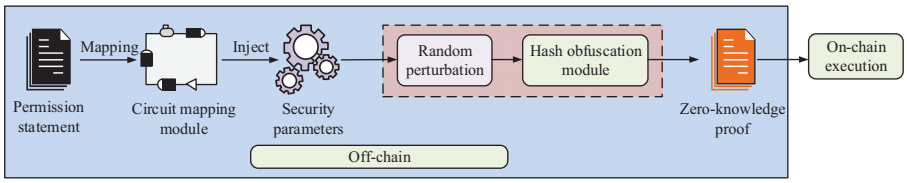

Figure 2 Workflow off-chain statement generation and proof construction. (Showing how access policies are converted into Boolean circuits and constraint logic, highlighting the ZKP module's role in generating verifiable proofs without exposing original data.)

privacy strength of access control [16]. Therefore, the study introduces the ZKP mechanism to construct a data access control and privacy declaration model, in order to achieve data access authorization verification without the need to disclose raw data. The structure of ZKP data authorization model is shown in Figure 1.

As shown in Figure 1, the model consists of four core components, namely the data owner, data requester, ZKP authorization module, and blockchain verification node. Firstly, the data owner generates declaration content based on the access policy. Subsequently, the corresponding access proof is generated in the off chain ZKP module, and the requester carries the access proof to initiate an access request to the blockchain. After verifying the access proof through smart contracts on the chain, the access authorization result is returned. Throughout the entire authorization verification process, measures are consistently taken to ensure that the content of the privacy statement remains concealed from view, while upholding the fundamental principle that the process itself remains verifiable. To further adjust and optimize the ZKP module in the future, a processing flowchart from privacy statement to access proof is constructed, as shown in Figure 2.

From Figure 2, the ZKP modules are all performed off chain, undertaking the key functions of off chain access declaration processing and proof generation. The access policy submitted by the user is converted into a

Boolean circuit structure for subsequent verification within the module, and the corresponding constraint logic is then constructed to form a verifiable computation path [17]. After completing semantic mapping and structural transformation, the module outputs a structured ZKP object, which will be used on the chain to perform validation operations. The entire process is completed off chain, ensuring that the original declaration content is not leaked and providing pre-support for efficient and trustworthy verification on chain, which is an important link in implementing privacy enhancement in the model. The formal representation of the access declaration is shown in Equation (1) [18].

$$\phi = \prod_{i=1}^{n} \psi(a_i \in A_i) \tag{1}$$

In Equation (1), ϕ represents the access permission declaration. $\| \ (\cdot)$ represents indicative function. A indicates the ith access attribute. A_i indicates the allowable range corresponding to the attribute. ψ represents indicative function. n indicates the number of attribute conditions included in the declaration. This product expression is used to construct the overall validity judgment of multi-attribute constraint conditions, ensuring that all attributes meet the authorization requirements before entering the subsequent circuit mapping stage. Its processing logic is shown in Equation (2).

$$C = \mathrm{MapCircuit}(\phi, \lambda) \tag{2}$$

In Equation (2), C represents the set of generated circuit constraints. λ represents safety parameters used to control circuit complexity. Based on the circuit structure, further combining disturbance vectors and hash functions to generate structured proof objects, the specific process is shown in Equation (3).

$$Z_p = \mathrm{GenProof}(C, \vec{r}, H) \tag{3}$$

In Equation (3), Z_p represents the structured zero knowledge proof object. $\vec{r}$ represents disturbance vectors. H represents a hash function. Subsequently, the on chain verification node needs to perform validity judgment on Z_p, and the logical definition of the verification function is shown in Equation (4).

$$\mathrm{Verify}(Z_p, \kappa_{pub}) = \begin{cases} 1, & \text{if } Z_p = C \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

In Equation (4), $\mathrm{Verify}(Z_p, \kappa_{pub})$ represents the on chain validation function. κ_{pub} represents a public authentication key. Considering the actual

system performance requirements, there is a functional relationship between the computational complexity of on chain verification and the circuit scale, and the cost formula is shown in Equation (5).

$$T = \alpha \cdot \log m + \beta \tag{5}$$

In Equation (5), T represents the on chain verification time. m indicates the number of circuit gates. α and β represent system constants. To evaluate the impact of ZKP on system communication burden, the relationship between the proof length and security parameters is shown in Equation (6).

$$L_{Z_P} = \gamma \cdot \lambda^{\frac{3}{2}} + \delta \tag{6}$$

In Equation (6), L_{Z_P} represents the byte length of ZKP. γ and δ indicate system adjustment parameters. Based on the above construction results, further integration of key modules and verification logic is studied to construct the overall process framework of ZKP access control system, as shown in Figure 3.

As shown in Figure 3, the ZKP authorization and verification process consists of two parts: off-chain generation and on-chain verification, including four core steps: permission declaration submission, ZKP generation, blockchain verification execution, and authorization result feedback. Firstly, the data owner defines access declarations locally and generates structured ZKP proof objects by combining security parameters with random perturbation vectors. Subsequently, the data requester carries the proof object to

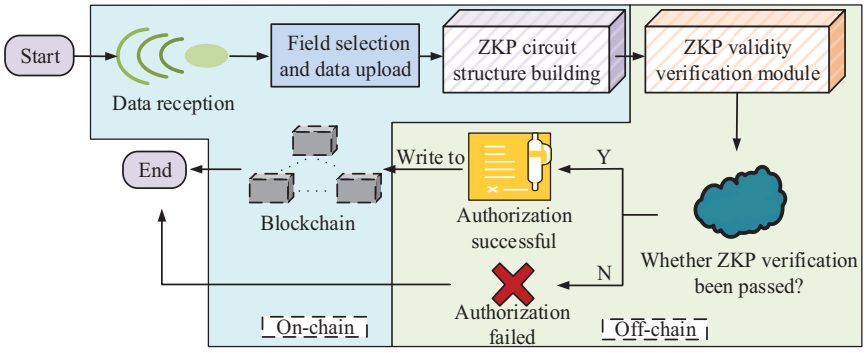

Figure 3 Complete process of ZKP-based authorization and verification. (Presenting the end-to-end authorization flow, emphasizing how the model ensures verifiable yet privacy-preserving access control through off-chain proof generation and on-chain validation.)

initiate an access request to the blockchain, and the on-chain smart contract performs verification operations based on the global verification key to determine whether it meets the access constraints defined in the declaration. If the verification result is not passed, the process will be terminated and recorded on the chain. If the verification is successful, the system returns an access authorization token and allows data to be called within a limited range.

2.2 Optimization of Multi-attribute Disclosure and Joint Verification Mechanism Based on DID

To further enhance the identity management and auditing capabilities of the model in multi-stakeholder data sharing scenarios, after constructing a model that integrates ZKP modules, research continues to introduce DID mechanisms. DID relies on the distributed trust of blockchain to achieve autonomous management and trusted disclosure of user identities. This mechanism binds user identity information to verifiable credentials (VC) in a minimal disclosure manner, and dynamically discloses and verifies on chain based on access request types and policy adaptation [19]. The overall architecture is shown in Figure 4.

As shown in Figure 4, the DID module consists of four parts: DID controller, credential generator, policy mapper, and verification request interface. Users first generate autonomous and controllable DID based on local keys, and can customize disclosure policies for public and private fields. Subsequently, during the data access request process, users selectively disclose relevant fields in VC based on specific requests, forming a dynamic identity package submission chain verification node. The entire DID structure realizes the decoupling design between user identity management and data access requests, no longer relying on central authentication services, and can support multiple types of access requests and policy combinations. This mechanism provides an auditable identity entry point for the data request process, which is a key prerequisite for building a trusted interaction process.

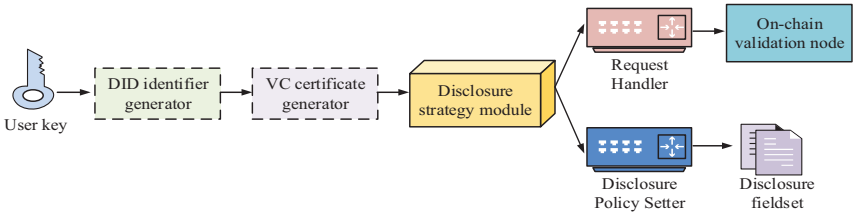

Figure 4 Structure of verifiable identity based on DID.

Firstly, the user's DID is generated by a local key pair and constructed as a globally unique identity identifier through hash mapping, expressed in Equation (7) [20].

$$DID_u = H(PK_u \| Meta_u) \tag{7}$$

In Equation (7), DID_u represents the decentralized identity identifier of the user u. PK_u represents the user's public key. $Meta_u$ represents identity metadata, such as registration time, institution code, etc. After receiving data requests, users need to construct corresponding disclosure attribute sets as the basis for on chain verification. The definition of the disclosure strategy mapping function is shown in Equation (8).

$$\nu_u = P(DID_u, R_q) \tag{8}$$

In Equation (8), ν_u represents the set of attributes disclosed by the user. $P(\cdot)$ represents the policy mapping function. R_q indicates the scope or role type of data accessed by the requester, used to determine which attribute fields need to be disclosed. Subsequently, the on chain verification node performs matching verification on the fields disclosed in ν_u, and the verification function is shown in Equation (9) [21].

$$S_i = \sum_{j=1}^{\mu} \frac{1}{\mu} w_i \cdot \xi(b_j, \hat{b}_j) \tag{9}$$

In Equation (9), S_i represents the total score of the ith user in the joint verification phase. w_i represents the weight coefficients of disclosure fields. b_j indicates the actual field values disclosed by the user. $\hat{b}_j$ indicates the expected field value on the verification agency side. $\xi(\cdot)$ represents the field consistency function. μ indicates the maximum number of fields for the current user's DID disclosure, used to control the joint verification dimension. If the user discloses attributes that cover access verification requirements, the verification will pass. To further enhance the robustness and tamper resistance of identity verification, the system introduces a joint verification mechanism involving multiple verification nodes based on single node attribute matching. The overall process is shown in Figure 5 [22].

As shown in Figure 5, after completing DID generation and attribute disclosure, the system further supports multi-node collaborative verification mechanism. The specific process is as follows: firstly, the user generates a DID locally and binds it with a VC. Then, the policy mapping module extracts the required attribute fields for the current access request and constructs a disclosure set. Subsequently, the disclosure set is sent along with

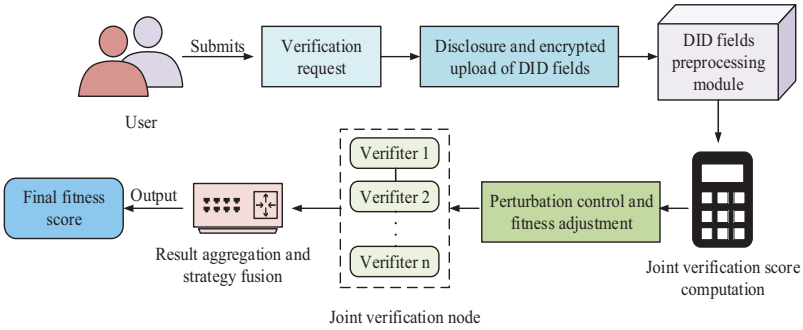

Figure 5 Workflow of multi-party joint verification. (Showing the collaborative verification and voting aggregation process across multiple nodes, enhancing objectivity and resistance to manipulation in decentralized identity validation.)

the request to the on chain verification node group, where different nodes execute verification tasks in parallel. Joint verification is divided into two layers of logic. The first layer is basic field consistency verification to ensure that the disclosed attributes meet the minimum trusted identity requirements defined by the requester. The second layer is context policy verification, which determines whether the disclosure field matches the request type, role permissions, etc. The verification results of each node are aggregated through a voting mechanism to form a global judgment. If the majority of nodes unanimously approve the verification, the system grants data access permission. This process effectively enhances the objectivity and resistance to attacks of identity verification, and is suitable for data sharing scenarios involving cross organizational and multi institutional collaboration. On the basis of implementing joint verification logic, further research is conducted to model the voting process and policy decision function. Firstly, assuming that among N validation nodes, each node returns a single validation judgment $J_i \in \{0, 1\}$, the global judgment result is determined by the majority voting function in Equation (10).

$$\mathrm{V}_{final} = \begin{cases} 1, & \sum_{i=1}^{N} J_i \geq T \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

In Equation (10), V_{final} represents the final joint validation result. J_i indicates the judgment result of the ith verification node. T represents the voting threshold, which determines the number of nodes required for majority

agreement. To address the issue of identity and permission coupling in complex request scenarios, a policy adaptation function is introduced for dynamic policy evaluation, as shown in Equation (11).

$$S_q = f_{match}(\nu_u, E_q, \theta) \tag{11}$$

In Equation (11), S_q represents the strategy matching score. E_q indicates the context of the access request. θ indicates a slight sensitivity factor used to control the accuracy of strategy adaptation. Finally, to balance the efficiency of identity verification and blockchain load balancing, a verification cost function is introduced, as shown in Equation (12).

$$t_{DID} = \eta \cdot |\nu_u| + \rho \tag{12}$$

In Equation (12), t_{DID} represents the time required for DID authentication. $|\nu_u|$ indicates the number of disclosure fields. η indicates the validation time for unit fields. ρ represents fixed expense items. To achieve unified protection of user data sovereignty and access control, further integration of ZKP access authorization mechanism and DID joint authentication mechanism is studied, and a complete ZKP-DID joint model is constructed. The overall process is shown in Figure 6.

As shown in Figure 6, the overall process of the ZKP-DID joint model constructed in this study is mainly divided into four stages: off chain declaration and identity construction, on chain access request submission, joint verification execution, and access feedback. Firstly, users generate access permission declarations and DID locally. They construct the minimum disclosure field set through the policy mapper, generate structured proofs and verifiable

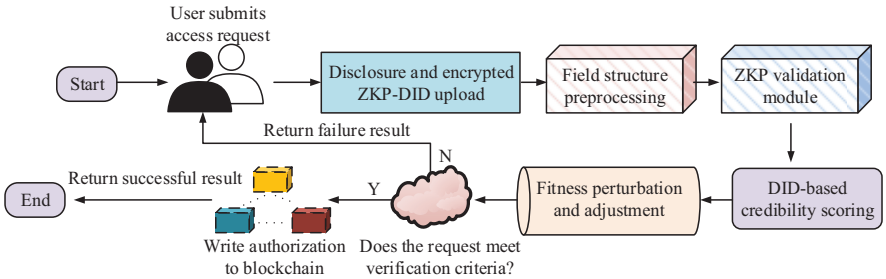

Figure 6 Integrated workflow of the dual-mechanism privacy protection model. (Depicting the integrated process of off-chain statement construction and on-chain joint verification, reflecting how the ZKP-DID model achieves coordinated user data sovereignty and privacy protection.)

identity packages VC, and undertake the role of permission proof and identity support. Subsequently, the data requester submits the structured proof and disclosure field set along with the access request to the blockchain network, and the on chain smart contract triggers the ZKP verification and DID joint verification modules respectively. During the verification process, the system first completes the compliance determination of permission constraints based on structured proofs, and then calls distributed verification nodes to perform joint verification on the attribute fields in the field set. The verification node generates a global verification result through a voting mechanism. If both ZKP and DID verifications pass, the system issues an authorization token and opens data access;If any step fails, record the abnormal operation and terminate the request process.

3 Results

3.1 ZKP-DID Joint Model Performance Test

To evaluate the comprehensive performance of the ZKP-DID joint model constructed for the study, a local multi-threaded environment was built with Intel Xeon Platinum 8358 CPU, NVIDIA RTX 6000 Ada GPU, and Debian 11.6 LTS operating system. The test data sources include two representative open-source datasets, namely the Amazon Public Blockchain Data (AWS-BC) and the Bitcoin Transaction subgraph Dataset (Elliptic-Sub) published by Elliptic. The AWS-BC dataset covers transaction structures, block header information, and contract call logs on the Bitcoin and Ethereum chains, and is suitable for experimental simulations of on chain access control and ZKP verification. The Elliptic-Sub dataset contains 203769 timestamped Bitcoin transaction records and address class annotations, with high-dimensional heterogeneous structural characteristics, suitable for disclosure field control, joint scoring function construction, and privacy protection model performance evaluation. The study further determined the optimal hyperparameter combination for model operation, and conducted hyperparameter selection testing on the security parameter λ of ZKP module and the upper limit μ of the number of fields disclosed by DID module. The test results are shown in Figure 7.

Figure 7(a) shows the results of the value selection test for security parameter λ, and Figure 7(b) shows the results of the value selection test for the field disclosure upper limit μ. From Figure 7(a), when $\lambda = 8$ and $\lambda = 16$, the final validation loss of the model was relatively high, stabilizing at around

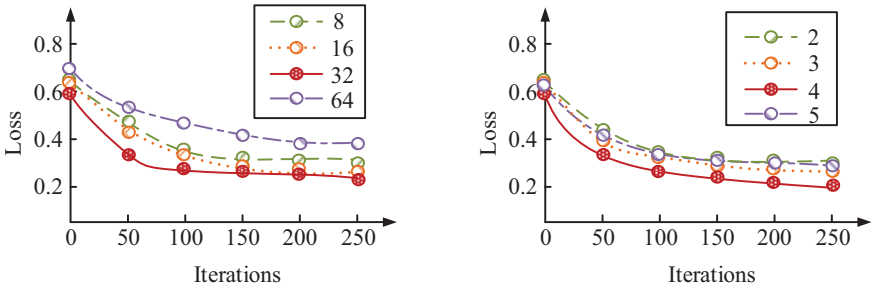

Figure 7 Hyperparameter test results.

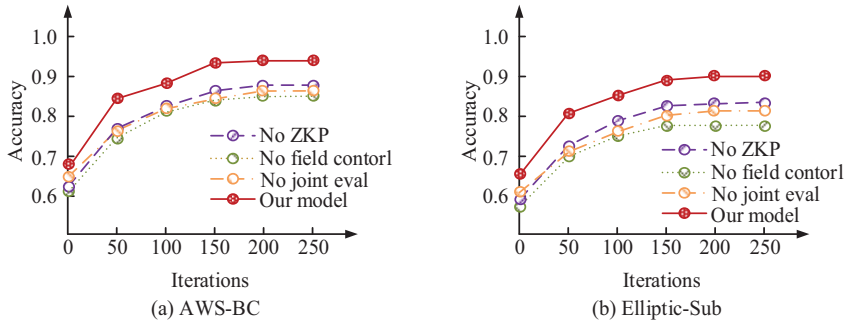

Figure 8 Ablation test results on two datasets.

0.335 and 0.305, respectively, indicating that a too low security level may affect the expression accuracy of the ZKP structure. When $\lambda = 64$, although the security level was improved, the final loss value of the model actually increased. In contrast, when $\lambda = 32$, the model consistently maintained the lowest validation loss value over multiple iterations, ultimately stabilizing at 0.248. According to Figure 7(b), when the upper limit of segment disclosure μ was 4, the loss value reached its lowest point of 0.268. When μ further increased to 5, although the amount of information further increased, the validation loss slightly increased, indicating that too many field inputs may introduce redundant noise and affect the stability of the model. In summary, the study ultimately determined the hyperparameter combination as $\lambda = 32$ and $\mu = 4$, and applied it as the default configuration in the training and testing process of the complete model architecture in subsequent experiments. The study continued to conduct ablation tests on two datasets, and the results are shown in Figure 8.

Table 1 Comparison of access control performance across models

Data Set	Method	Rejection Rate/%	Anonymity Score/%	False Acceptance Rate/%
AWS-BC	No ZKP	12.5	82.4	7.8
	No field control	14.7	79.3	9.2
	No joint eval	11.6	84.1	6.7
	Our model	7.2	91.5	4.1
Elliptic-Sub	No ZKP	15.3	77.9	8.6
	No field control	17.4	74.2	10.3
	No joint eval	13.1	80.5	7.2
	Our model	8.5	89.7	4.9

Figure 8(a) shows the ablation test results on the AWS-BC dataset, and Figure 8(b) shows the ablation test results on the Elliptic-Sub dataset. As shown in Figure 8(a), the complete model maintained a high authorization accuracy throughout the entire iteration process, ultimately stabilizing at around 0.94. In contrast, the model without ZKP module showed a significant decrease in performance, with a final authorization accuracy of only 0.88. After removing the field disclosure control module, the final accuracy decreased to 0.85. After removing the joint validation structure, the final accuracy of the model was 0.87. Similarly, in 8(b), the authorization accuracy rate of the complete model finally stabilized at 0.90, significantly ahead of the other three baseline models with a module removed. The results indicated that the ZKP mechanism, field disclosure control strategy, and joint verification structure played an irreplaceable role in constructing a high-precision and robust data sovereignty protection model. The combination of the three forms the core foundation for the rationality and performance improvement of the complete model structure. The study further compared the performance of several baseline models and the complete model constructed in the study on multidimensional indicators, as shown in Table 1.

As shown in Table 1, the ZKP-DID joint model constructed in the study exhibited significant performance advantages in both types of datasets. In terms of authorization rejection rate, the complete model achieved 7.2% and 8.5% on the AWS-BC and Elliptic-Sub datasets, respectively, which was nearly 50% lower than the version without ZKP or field control module. Meanwhile, in terms of anonymous disclosure ratings, the complete model scored 91.5% and 89.7% respectively, significantly better than other structures. For the critical misjudgment rate, the complete model was

controlled at 4.1% and 4.9%, significantly lower than the structure without integrated joint verification mechanism. In summary, the ZKP-DID joint model enhanced anonymity and reduced the risk of false authorization while ensuring authorization accuracy.

3.2 ZKP-DID Joint Model Simulation Test

To further verify the adaptability and stability of the ZKP-DID joint model constructed in the real blockchain data environment, three types of simulation scenarios were designed based on the aforementioned two datasets, representing application scenarios with low, medium, and high data structure complexity. The study selected three representative models in the current direction of blockchain data privacy protection as comparison baselines, namely the Distributed Policy Based Access Model (DPAM), Lightweight Threshold Cryptographic Validator (LTCV), and Graph sensitive subgraph Aggregation (GSSA), to compare with the research models. Using authorization accuracy as an indicator, the test results are shown in Figure 9.

Figures 9(a), 9(b), and 9(c) respectively show the authorization accuracy test results of four models in three different complexity levels of blockchain data environments. From Figure 9(a), in low complexity environments, the performance differences between the four models were small, but the ZKP-DID joint model had the highest authorization accuracy, reaching 93.6%. In the same complexity environment as Figure 9(b), the authorization accuracy value of the research model was further improved to 95.1%. In the high complexity scenario shown in Figure 9(c), the performance of most models fluctuated significantly, but the authorization accuracy of the research model still remained at 91.2%, which was better than the other three types of models. The study continued to select Field Match Consistency (FMC) as the evaluation metric, and the test results are shown in Figure 10.

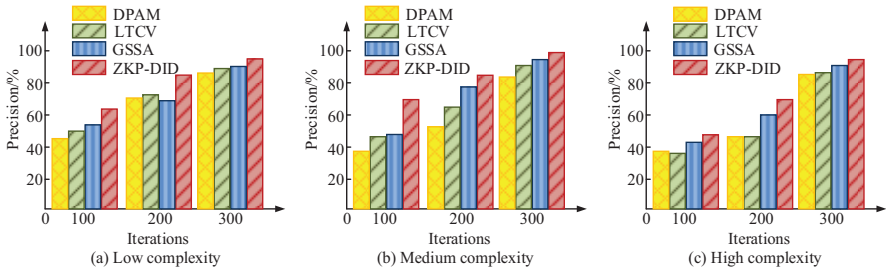

Figure 9 Authorization precision performance across simulation complexity levels.

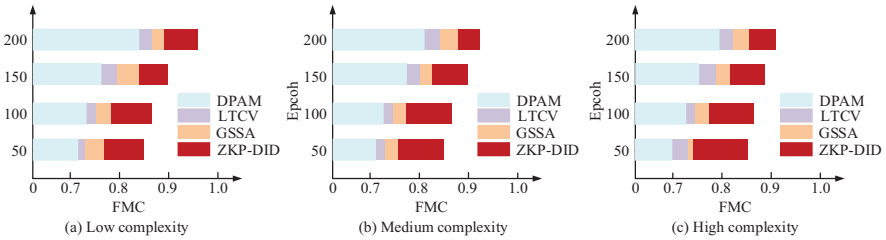

Figure 10 FMC under variable complexity levels.

Table 2 Model evaluation results under simulated conditions

Complexity	Method	TAR/%	FAR%	ART/s
Low complexity	DPAM	84.3	10.7	13.5
	LTCV	86.2	9.9	12.2
	GSSA	89.7	8.4	16.8
	Our model	96.8	2.1	11.1
Medium complexity	DPAM	80.5	12.8	14.4
	LTCV	83.1	11.5	13.3
	GSSA	87.2	4.7	17.2
	Our model	92.3	7.9	11.8
High complexity	DPAM	75.6	15.3	15.6
	LTCV	77.4	14.6	14.7
	GSSA	83.2	12.1	18.5
	Our model	90.9	5.0	12.3

Figures 10(a), 10(b), and 10(c) are horizontal bar charts comparing the field consistency of four models under three different operating conditions. According to Figure 10, the ZKP-DID joint model maintained high consistency at all complexity levels, with values of 96.5%, 93.0%, and 90.6%, respectively. In contrast, the consistency of the other three models decreased significantly in high complexity environments. Specifically, in high complexity environments, the field validation consistency of the research model was improved by about 10% compared to other models, indicating that the research model still had strong stability and robustness in complex data environments. The study further compared the four models under three levels of complexity in terms of three key metrics – True Acceptance Rate (TAR), False Acceptance Rate (FAR), and Average Response Time (ART). The results are shown in Table 2.

According to Table 2, the ZKP-DID joint model exhibited performance advantages in all three scenarios. The highest true positive rate was 96.8%,

the lowest false authorization rate was 2.1%, and the verification efficiency was the best, with an average delay of 11.1 seconds, which verified its better practicality and deployment value under multiple security verification and privacy balance objectives. In summary, the ZKP-DID joint model that integrated ZKP mechanism and field disclosure control performed the best in simulation testing, with good transferability and generalization ability, and was more suitable for dynamic authorization management needs in complex data sovereignty scenarios.

4 Conclusion

A privacy protection authorization model that integrated ZKP mechanism, field disclosure control, and DID was studied and constructed to address key issues such as ambiguous data usage permission determination and lack of multi-party verification and collaboration mechanism in the context of blockchain user data sovereignty. The hyperparameter test results on the AWS-BC and Elliptic-Sub blockchain datasets showed that when the security parameter was set to 32 and the field disclosure upper limit was 4, the model validation loss was the lowest, and the convergence speed and stability performance were the best. The ablation test further proved that the absence of any core module would lead to significant degradation of overall performance. In the simulation conditions, the fusion model achieved authorization accuracies of 93.6%, 95.1%, and 91.2% at three different complexities, respectively. Meanwhile, the true positive rate was 96.8%, the false authorization rate was 2.1%, and the average delay was 11.1 seconds, which was significantly better than the three comparison models. Overall, the model constructed in the study achieved a high-precision, multi-dimensional and controllable data sovereignty authorization process in static scenarios, with strong structural scalability and cross platform migration potential. Theoretically, it advanced blockchain-based privacy protection by unifying verifiable privacy, controllable disclosure, and collaborative verification into a single model. Practically, beyond technical contributions, the proposed model provided a practical framework for implementing user data sovereignty and privacy compliance in decentralized ecosystems. It offered valuable guidance for secure data authorization, multi-party collaboration, and the construction of trustworthy digital infrastructures across diverse application scenarios such as healthcare, finance, and government digital identity. However, further consideration is still needed for cross-platform identity behavior changes, multi-data source collaborative verification mechanisms,

and policy convergence issues under attack scenarios. In addition, when transitioning from experimental validation to real-world deployment, several practical barriers must be addressed, including scalability constraints under massive user traffic, compliance with heterogeneous regulatory frameworks, and the computational cost associated with privacy-preserving cryptographic operations. These factors may affect the model's responsiveness, resource efficiency, and legal adaptability in large-scale blockchain ecosystems. In the future, research can continue to enhance the model's practical performance in multi-role collaborative and low-trust environments by incorporating federated learning frameworks or graph neural network architectures. Further optimization of its scalability, compliance adaptability, and cost-effectiveness is needed to improve its governance value for data sovereignty in the context of the decentralized Internet.

Fundings

The research is supported by Research and Practice Project of Research Teaching Reform in Undergraduate Universities in 2022, Henan Province, China (No.: 2022SYJXLX122); Higher Education Teaching Reform Research and Practice Project, Henan Province, China (No.: 2024SJGLX0207); Education and Teaching Reform Research and Practice Project, Zhengzhou University of Technology, China (No.: ZGJG202455B); Yellow River Culture Education Special Series Project Teaching Reform Project, Zhengzhou University of Technology, China (No.: ZGJG202405HJA).

References

[1] Gheisari M, Hamidpour H, Liu Y, Saedi P, Raza A, Jalili A, Rokhsati H, Amin R. Data Mining Techniques for Web Mining: A Survey. Artificial Intelligence and Applications, 2023, 1(1): 3–10. DOI: 10.47852/bonviewAIA2202290.

[2] Akash T R, Lessard N D J, Reza N R, Islam M S. Investigating Methods to Enhance Data Privacy in Business, Especially in sectors like Analytics and Finance. Journal of Computer Science and Technology Studies, 2024, 6(5): 143–151. DOI: 10.32996/jcsts.2024.6.5.12.

[3] Zhan Z Y, Wang X, Liu Y S, Sun Z L, Gu C H. Integration and Optimization Strategy of Blockchain-Enabled Edge Computing System

for Internet of Vehicles. Journal of Cyber Security and Mobility, 2025, 14(2): 391–432. DOI: 10.13052/jcsm2245-1439.1426.

[4] Zhang L. Implementing RGCN Model in Network Security Big Data Analysis. Journal of Cyber Security and Mobility, 2025, 14(2): 505–530. DOI: 10.13052/jcsm2245-1439.14210.

[5] Li X, Zhao H, Deng W. BFOD: Blockchain-based privacy protection and security sharing scheme of flight operation data. IEEE Internet of Things Journal, 2023, 11(2): 3392–3401. DOI: 10.1109/JIOT.2023.3296460.

[6] Singh N, Das A K. TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor. The Journal of Supercomputing, 2024, 80(1): 865–914. DOI: 10.1007/s11227-023-05507-6.

[7] Sharma P, Martin M, Swanlund D, Latham C, Anderson D, Wood W. A cloud-based solution for trustless indigenous data sovereignty: Protecting Mâori biodiversity management data in Aotearoa New Zealand. Transactions in GIS, 2024, 28(4): 836–857. DOI: 10.1111/tgis.13153.

[8] Yin S, Li H, Teng L, Laghari A A, Estrela V V. Attribute-based multiparty searchable encryption model for privacy protection of text data. Multimedia Tools and Applications, 2024, 83(15): 45881–45902. DOI: 10.1007/s11042-023-16818-4.

[9] Shahidinejad A, Abawajy J. An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT. ACM Computing Surveys, 2024, 56(7): 1–38. DOI: 10.1145/364508.

[10] Shree S, Zhou C, Barati M. Data protection in internet of medical things using blockchain and secret sharing method. The Journal of Supercomputing, 2024, 80(4): 5108–5135. DOI: 10.1007/s11227-023-05657-7.

[11] Lejun Z, Minghui P, Shen S, Weizheng W, Zilong J, Yansen S. Redundant data detection and deletion to meet privacy protection requirements in blockchain-based edge computing environment. China Communications, 2024, 21(3): 149–159. DOI: 10.23919/JCC.Fa.2021-0815.202403.

[12] Deng X, Shao J, Chang L, Liang J. A blockchain-based privacy protection protocol using smart contracts in LEO satellite networks. Peer-to-Peer Networking and Applications, 2024, 17(2): 800–818. DOI: 10.1007/s12083-023-01614-6.

[13] Ghani M A N U, She K, Rauf M A. Enhancing security and privacy in distributed face recognition systems through blockchain and GAN technologies. Computers, Materials & Continua, 2024, 79(2): 2609–2623. DOI: 10.32604/cmc.2024.049611.

[14] Li D, Ke X, Zhang X. A trusted and regulated data trading scheme based on blockchain and zero-knowledge proof. IET Blockchain, 2024, 4(4): 443–455. DOI: 10.1049/blc2.12070.

[15] Sharma P, Wilfred Godfrey W, Trivedi A. When blockchain meets IoT: a comparison of the performance of communication protocols in a decentralized identity solution for IoT using blockchain. Cluster Computing, 2024, 27(1): 269–284. DOI: 10.1007/s10586-022-03921-8.

[16] Lu T, Wei C, Yu R. Cuzk: Accelerating zero-knowledge proof with a faster parallel multi-scalar multiplication algorithm on gpus. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023, 2023(3): 194–220. DOI: 10.46586/tches.V2023.I3.194-220.

[17] Konkin A, Zapechnikov S. Zero knowledge proof and ZK-SNARK for private blockchains. Journal of Computer Virology and Hacking Techniques, 2023, 19(3): 443–449. DOI: 10.1007/s11416-023-00466-1.

[18] Kaur J, Rani R, Kalra N. Attribute-based access control scheme for secure storage and sharing of EHRs using blockchain and IPFS. Cluster Computing, 2024, 27(1): 1047–1061. DOI: 10.1007/s10586-023-04038-2.

[19] Fang J, Feng T, Guo X, Ma R; Lu Y. Blockchain-cloud privacy-enhanced distributed industrial data trading based on verifiable credentials. Journal of cloud computing, 2024, 13(1): 30. DOI: 10.1186/s13677-023-00530-7.

[20] Liu H, Han D, Cui M, Li K C, Souri A, Shojafar M. Idenmultisig: Identity-based decentralized multi-signature in internet of things. IEEE Transactions on Computational Social Systems, 2023, 10(4): 1711–1721. DOI: 10.1109/TCSS.2022.3232173.

[21] Rani P, Sachan R K, Kukreja S. BT-CNV: A distributed and decentralized solution for certificate notarization and verification for academia using public blockchain. Peer-to-Peer Networking and Applications, 2025, 18(1): 1–26. DOI: 10.1007/s12083-024-01889-3.

[22] Xiong R, Ren W, Hao X, He J, Choo K K R. Bdim: A blockchain-based decentralized identity management scheme for large scale internet of things. IEEE Internet of Things Journal, 2023, 10(24): 22581–22590. DOI: 10.1109/JIOT.2023.3303922.

Biography

Yinfeng Li obtained her Master Degree in Economic Law (2013) from Central China Normal University. Presently, she is working as a Lecturer in the Academic Affairs Office, Zhengzhou University of Technology, Henan Province. She has published more than 6 articles and 3 books. Her areas of interest include Intellectual property, economic law and pedagogy.