
Distributed Storage and Privacy Protection for Educational Blockchain Data

Yufei Che

*College of Education Science, Weinan Normal University, Weinan 714000,
China
E-mail: manshan0606@163.com*

Received 05 June 2026; Accepted 28 July 2026

Abstract

To address the issues of static scheduling strategies, coarse-grained privacy protection, and their mutual independence in distributed storage of educational blockchain data, this study hypothesizes that a collaborative mechanism integrating dynamic closed-loop storage scheduling with adaptive graded desensitization can effectively balance storage efficiency and privacy protection strength. To test this hypothesis, this study conducts experiments on the Open University Learning Analytics Dataset (OULAD) educational dataset with six privacy levels and up to 5000 data blocks to evaluate throughput, latency, energy consumption, and classification accuracy. Key findings include: storage throughput reaching 35.6 MB/s with a write latency of 102.9 ms, response time and floating-point operations optimized to 85.6 ms and 33.5 MFLOP, respectively; encryption throughput of 18.7 MB/s with key generation time of only 3.9 ms; and correct classification of 548 out of 600 samples across six privacy levels with energy consumption of 20.5 J. Ablation studies confirm the irreplaceable roles of Coding Storage Allocation and the

Hybrid-Dimensional Grid, while sensitivity analysis identifies the optimal configurations for the duplicate block count, learning rate, maximum privacy level, and contraction-expansion coefficient as 2, 0.001, 5, and $1.0 \rightarrow 0.5$, respectively. These results demonstrate that the proposed method effectively resolves the trade-off between storage efficiency and privacy protection for educational blockchain data, providing key technical support for trusted data management in education informatization.

Keywords: Educational blockchain, distributed storage, privacy protection, CSA, HDG, QPSO.

1 Introduction

1.1 Background and Recent Advances

Given the deeply integrated relationship between higher education and online education, in addition to satisfying the conditions for long-term storage and traceability of educational blockchain data, the system requires efficient data accessibility, especially when cross-institutional sharing and credit mutual recognition are involved [1, 2]. However, educational data is essentially a high-value privacy asset: once student identity information (name, student ID, ID number) is leaked, it will lead to identity theft risks. Specifically, ‘student ID’ to the school-assigned identification number, and ‘ID number’ to the national identity card number. If grades and teaching evaluation data are tampered with or illegally accessed, it will directly damage educational equity and evaluation credibility [3]. Therefore, establishing an educational blockchain data management system with high reliability and robust privacy security measures is a key issue in educational informatization.

In terms of data storage, to address the problem of high latency in centralized cloud storage for large-scale data, Wu et al. proposed a dual-blockchain-based distributed data management framework, MapChain-D. By mapping the data chain to the index chain to achieve efficient data storage and retrieval, this framework reduces storage and communication overhead and improves system scalability [4]. To address the insufficient security and reliability in distributed data storage, Agrawal et al. proposed a distributed data storage method based on blockchain and fog computing models. Leveraging blockchain attributes such as decentralization and immutability, alongside the low latency of near-source fog computing, this method enables secure and reliable distributed data storage [5]. To address the problems of

data silos, sharing difficulties, and insufficient security in traditional centralized architectures, Jayabalan and Jeyanthi proposed an off-chain storage framework based on blockchain and InterPlanetary File System (IPFS). By storing encrypted system record data in IPFS and using blockchain to record hash indexes and access permissions, it can achieve tamper-proof, scalable, and privacy-preserving distributed data storage [6]. To address the issues of high centralized storage pressure, significant data synchronization latency, and insufficient fault tolerance in port supply chain data storage, Li et al. proposed a blockchain-assisted storage scheme for port supply chain data. By employing an on-chain and off-chain collaborative storage architecture alongside the decentralized and tamper-proof nature of blockchain, combined with dynamic searchable encryption to ensure data verifiability and retrieval efficiency, this scheme achieves secure, reliable, and scalable supply chain data storage [7]. To address the challenges of security, tamper resistance, and long-term accessibility in storing certificate files for higher education credential management, Syaifudin et al. proposed a decentralized credential storage scheme based on Hyperledger Besu and IPFS. By storing certificate files in the IPFS decentralized network with content-based addressing to ensure file integrity, and recording certificate metadata on the blockchain for tamper-proof records, the scheme achieves secure, reliable, and lifelong-accessible storage of academic credentials [8].

In the aspect of data privacy protection, Liang et al. identified the issue related to plaintext storage and no ownership of data in personal data privacy protection, thereby suggesting a blockchain consortium-based protection scheme called Personal Data Privacy Chain (PDPChain). Through an improved Paillier homomorphic encryption mechanism and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for data encryption, combined with off-chain distributed cluster storage and on-chain transmission collaboration, this scheme reduces the total encryption and decryption time by 25% [9]. To address the privacy leakage problems emerging from data transmission via central servers in the integration of e-healthcare and the industrial Internet of things, Khan et al. introduced an innovative secure architecture using blockchain technology. By utilizing NuCypher threshold re-encryption to encrypt data, chaincode to authenticate and trace transactions, and lightweight multi-consensus protocols with digital signatures, the framework assures the privacy of shared resources [10]. Li et al., addressing the contradiction between civil aviation operational data sharing and privacy protection, proposed a Blockchain-Based Privacy Protection and Security Sharing Scheme of Flight Operation Data (BFOD). Through

hash anonymous identity verification for access permissions, zero-knowledge proofs (zk-SNARKs) to verify data requirements without leaking privacy, and proxy re-encryption to improve sharing efficiency, it can simultaneously meet the requirements of availability and privacy protection [11]. To address insufficient individual privacy protection in medical data sharing and the inadequacy of traditional privacy-preserving techniques in big data and blockchain environments, a blockchain-based secure data sharing scheme named SecureChain using local differential privacy is proposed. By applying local differential privacy perturbation to individual records before data publication and leveraging the low latency and high throughput features of blockchain, the scheme achieves secure and efficient medical data sharing while meeting privacy conditions [12]. To address the issues of insufficient privacy protection, lack of data integrity assurance, and reliance on centralized systems in electronic medical record sharing, Wang et al. proposed a Privacy and Control with Threshold Ring Signatures (PCTRS) framework based on blockchain and threshold traceable ring signatures. By integrating IPFS off-chain storage, elliptic curve ephemeral key exchange, and Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) encryption, combined with smart contracts and threshold ring signatures, the framework achieves a balance between privacy preservation and traceability [13].

In summary, existing research has made significant progress in latency optimization, reliability improvement, and scalability enhancement of distributed storage, and has achieved important breakthroughs in encryption efficiency, fine-grained access control, and identity anonymization in the field of privacy protection. However, most traditional approaches utilize preset criteria and fail to provide adaptive scheduling according to the popularity of accessed educational data, thereby complicating load balancing and efficient storage. In terms of privacy protection, conventional approaches mainly utilize encryption or desensitization in an equal manner without considering multiple dimensions of privacy levels. Moreover, in the context of educational blockchain data, the importance of distributed storage and privacy protection lies in meeting both the high-concurrency access demands of cross-institutional transactions and the differentiated protection of multi-level sensitive information. However, access frequency fluctuates significantly with academic cycles, and different privacy levels require vastly different desensitization intensities. Conventional approaches separate storage from privacy by using static redundancy and uniform encryption, leading to rigid scheduling and inappropriate protection. This fragmented paradigm can no longer adapt to the dynamic evolution of educational data.

1.2 Research Framework and Innovation

The Coding Storage Allocation (CSA) algorithm can achieve fault tolerance and load balancing with lower redundancy overhead by encoding original data into multiple redundant blocks and storing them in a distributed manner, thereby improving the storage reliability of educational blockchain data [14]. Hybrid-Dimensional Grid (HDG) can achieve fine-grained privacy grading and dimension-wise desensitization while maintaining data availability by mapping data to a multi-dimensional hybrid space [15]. Nevertheless, the node distribution algorithm of the CSA technique relies on static preset conditions that cannot adapt dynamically to varying trends in educational data access popularity; furthermore, the desensitization value and factor of the HDG approach are manually configured [16, 17]. Therefore, based on the fundamental logic of CSA and HDG, this study introduces the Asynchronous Advantage Actor-Critic (A3C) algorithm and Quantum Particle Swarm Optimization (QPSO), and ultimately proposes an Educational Blockchain Data Storage and Privacy Model (EBSPM). This study aims to build an educational data security storage framework that integrates adaptive storage and graded desensitization, solving the dual limitations of traditional methods in storage dynamic scheduling and privacy granularity optimization.

The core novelty of this research is reflected in breaking through traditional static preset rules, coupling CSA and A3C to model coding storage allocation as a Markov decision process, thereby achieving dynamic closed-loop learning for node allocation. To overcome manual experience constraints, this study constructs a nested optimization framework of QPSO and HDG to transform privacy desensitization parameter selection into a quantum particle swarm optimization problem in a high-dimensional grid space, endowing the model with adaptive level configuration capability and, on this basis, connecting the storage layer and protection layer sequentially to build an end-to-end integrated “storage-protection” paradigm, effectively resolving the fragmentation dilemma of their long-standing mutual independence.

2 Methodology

This section comprises three parts. The first part integrates CSA as the backbone with A3C to develop an intelligent and adaptable scheduling model known as CSA-A3C. In the second part, the backbone will be HDG while QPSO will be combined to develop an optimization privacy protection model named QPSO-HDG. The third part connects CSA-A3C and QPSO-HDG

in sequence to form a distributed storage and privacy protection model for educational blockchain data, named EBSPM. The cascaded modules form an end-to-end “storage-protection” integrated process. It improves both security and storage efficiency of educational blockchain data.

2.1 Distributed Storage Module Based on CSA and A3C

2.1.1 Education data partitioning and node allocation strategy based on CSA

Educational blockchain data contains sensitive information, such as student scores, academic certification documents, and course transcripts. The availability, reliability, and confidentiality of such data have implications for the fairness of educational systems and individual privacy [18]. CSA encodes raw data into multiple redundant blocks and distributes them across different nodes. It achieves fault tolerance and load balancing with low redundancy cost. It also improves system robustness [19]. Therefore, this study applies CSA to data partitioning and node allocation for educational blockchain data to achieve efficient and reliable distributed storage. The structure of CSA is shown in Figure 1.

As shown in Figure 1, CSA encodes raw educational data into several redundant blocks. Then an allocation strategy deploys these blocks to distributed nodes. The encoding process of CSA in educational data partitioning is described below. First, the system reads the raw educational data file and partitions it into fixed-size blocks, generating k original data blocks. Second, based on the finite field $GF(2^8)$, $n - k$ linearly independent coding coefficient vectors are generated to construct the generator matrix. Third,

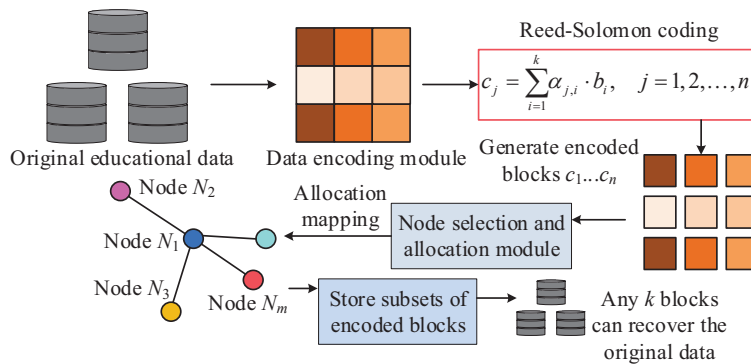


Figure 1 Structure of CSA.

linear combination operations are performed on each original data block to compute $n - k$ parity blocks, which together with the original blocks form n coded blocks. Specifically, let the original data file be F . The system divides it into k original data blocks, denoted as $F = \{b_1, b_2, \dots, b_k\}$. It uses Reed-Solomon coding to generate n encoded blocks. The j -th encoded block is calculated as shown in Equation (1) [20].

$$c_j = \sum_{i=1}^k \alpha_{j,i} \cdot b_i, \quad j = 1, 2, \dots, n \quad (1)$$

where c_j denotes the j -th encoded block, $\alpha_{j,i}$ denotes the coding coefficient from a finite field, b_i denotes the i -th original data block, which satisfies $n > k$. The number of redundant blocks is $n - k$. Define the node set $N = \{N_1, N_2, \dots, N_m\}$. The allocation function $\phi : \{c_j\} \rightarrow N$ maps each encoded block to a storage node [21]. The system ensures that any k encoded blocks can recover the original data F through decoding. For different privacy levels of educational data, such as public schedules and exam transcripts, CSA dynamically adjusts (k, n) . Highly sensitive data uses a larger $n - k$ to enhance fault tolerance [22]. During node allocation, the system prefers nodes with lower load $L(N_p)$ and shorter historical response time $T(N_p)$. This design ensures real-time access and reliability.

2.1.2 A3C-driven data scheduling and CSA-A3C construction

Although redundancy improves the storage reliability of CSA, its resource allocation algorithm relies on static rules that cannot adjust to dynamic changes in data access patterns. A3C uses multi-agent asynchronous parallel learning [23]. Therefore, this study designs an A3C-driven scheduling mechanism to dynamically optimize node allocation and storage decisions in CSA. The structure of A3C is shown in Figure 2.

As shown in Figure 2, A3C includes a global network and multiple parallel actor-critic worker threads. Each worker interacts with the environment. It computes gradients asynchronously and updates global parameters. This process accelerates convergence and improves decision stability [24]. Let us define the state space $S = \{s_t\}$. s_t includes attributes of the current data block c_j , such as size, privacy level, and access frequency, as well as node load $L(N_p)$. The action space $A = \{a_t\}$ represents the selection of storage node N_p . The policy network outputs a probability distribution $\pi(a_t | s_t; \theta)$, where θ denotes policy parameters. The critic network outputs the state value $V(s_t; \theta_v)$, where θ_v denotes value parameters. The advantage function is

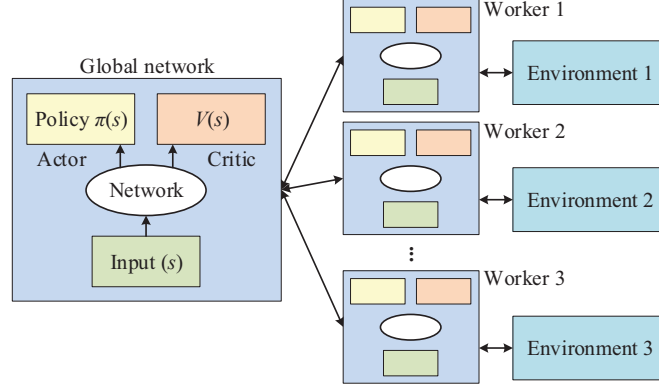


Figure 2 Structure of A3C.

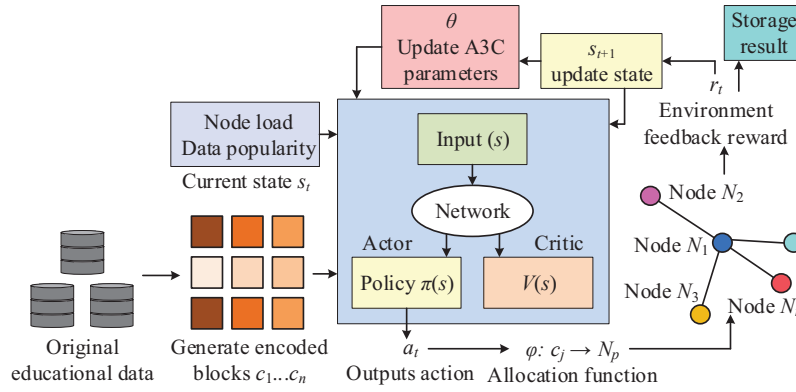


Figure 3 Structure of CSA-A3C.

defined as shown in Equation (2) [25].

$$A(s_t, a_t) = r_t + \gamma V(s_{t+1}; \theta_v) - V(s_t; \theta_v) \quad (2)$$

where r_t denotes the immediate reward after executing action a_t , such as the negative inverse of storage latency and load balancing gain. γ denotes the discount factor, set to 0.9. A3C maximizes cumulative expected reward through asynchronous updates. It dynamically adjusts the allocation function ϕ in CSA. It assigns high-frequency data blocks to low-latency nodes and avoids node overload. Therefore, the structure of the integrated module CSA-A3C is shown in Figure 3.

As shown in Figure 3, CSA-A3C tightly connects the static encoding allocation layer of CSA with the dynamic decision layer of A3C. The system

first encodes and partitions educational data through the CSA module to generate redundant encoded blocks. Then, the policy network in A3C outputs optimal node allocation actions based on the current system state, including node load, data privacy level, and historical access frequency. Once the environment executes the action, the system receives an immediate reward to update the actor and critic networks, thereby continuously improving subsequent allocation decisions.

2.2 Privacy Protection Module for Educational Blockchain Data

2.2.1 Privacy classification and desensitization structure based on HDG

Educational blockchain data includes highly sensitive information such as identity, grades, attendance, and rewards and penalties. Once leakage or misuse occurs, it seriously harms personal privacy and may cause educational unfairness and legal risks. Privacy protection is a prerequisite for data sharing and certification [26, 27]. CSA-A3C focuses on the reliability of storage and efficiency of scheduling. Because neither its encoding nor its allocation desensitizes data content, the module cannot resist attacks targeting data access or theft. The HDG approach converts the data into a hybrid space of multiple dimensions. It manages to ensure privacy classification and dimensional desensitization with utility preserved [28]. Therefore, this study introduces HDG to perform privacy classification and dimensional desensitization for educational data. It builds a basic privacy protection structure for educational blockchain. The structure of HDG is shown in Figure 4.

The HDG structure includes a dimension definition layer, a hierarchical mapping layer, and a desensitization execution layer. The system first defines

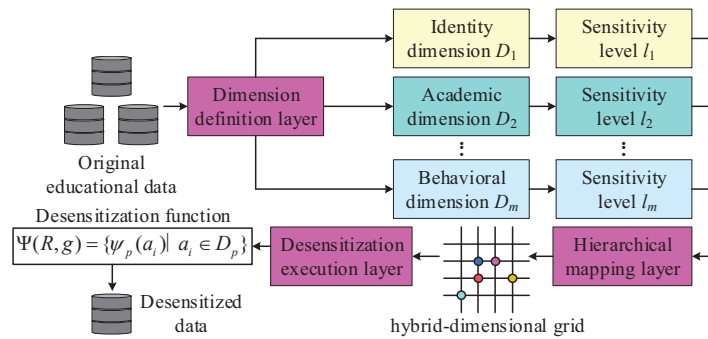


Figure 4 Structure of HDG.

privacy dimensions based on data attributes. Then it maps data in each dimension to grids with different security levels. Finally, it executes desensitization according to strategies [29]. The application process of HDG in privacy protection is as follows. Let a data record be R , which contains d attribute fields $\{a_1, a_2, \dots, a_d\}$. Define a privacy dimension set $D = \{D_1, D_2, \dots, D_m\}$, where each dimension D_p corresponds to a group of related attributes, such as identity dimension including name and student ID. Assign a sensitivity level $l_p \in \{1, 2, \dots, L\}$ to each dimension D_p , where L grid G is the highest level. Construct a hybrid-dimensional grid G as a m -dimensional tensor. Each grid unit $g(v_1, v_2, \dots, v_m)$ stores the desensitization strategy for a specific dimension combination [30]. The desensitization function Ψ is defined as shown in Equation (3).

$$\Psi(R, g) = \{\psi_p(a_i) \mid a_i \in D_p, \text{ according to the policy in } g\} \quad (3)$$

where ψ_p denotes the desensitization operation on the p -th dimension, such as generalization, suppression, or noise addition. The specific operation depends on the predefined level combination in grid unit g [31]. For different data types, the system uses different sensitivity levels. Public course names use a low level $l = 1$ and apply generalization. Transcripts and ID numbers use a high level $l = L$ and apply suppression or strong noise. HDG provides the capability to dynamically adjust the values for desensitization on multiple axes. The grid also enables a multi-level conjunctive query capability, allowing properly authorized users to retrieve information at various granularities.

2.2.2 HDG privacy protection scheme optimized by QPSO

Although HDG supports multidimensional desensitization, its initial configuration relies on manual experience and lacks adaptive optimization. Consequently, HDG alone cannot achieve the optimal privacy-utility trade-off across varying data properties. The QPSO algorithm leverages quantum superposition and swarm intelligence search capabilities. It optimizes solution space and prevents local optima [32]. Therefore, this study designs QPSO to optimize sensitivity levels and desensitization parameters in HDG. It improves adaptability and overall performance of privacy protection. The workflow of QPSO is shown in Figure 5.

As shown in Figure 5, the workflow includes population initialization, fitness evaluation, local attractor update, quantum potential well contraction, and global best iteration. Each particle represents a candidate solution. The swarm searches for the global optimum through quantum behavior [33].

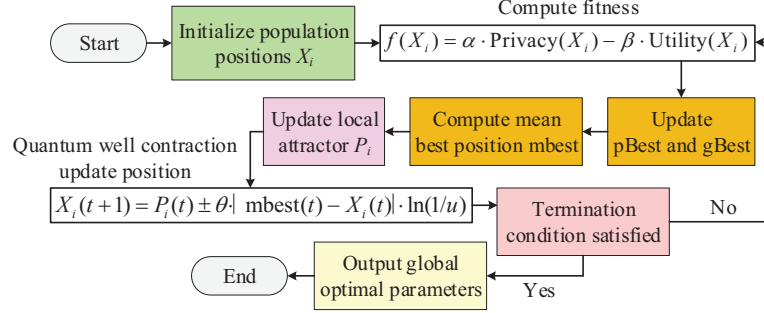


Figure 5 Workflow of QPSO.

QPSO encodes sensitivity level combinations and desensitization parameters in HDG as particle position vectors. Let the population size be M . The position of the i -th particle at iteration t is $X_i(t) = (x_{i1}, x_{i2}, \dots, x_{iZ})$. Z denotes the number of parameters to optimize, including dimension levels l_p and desensitization thresholds. The fitness function is defined as shown in Equation (4).

$$f(X_i) = \alpha \cdot \text{Privacy}(X_i) - \beta \cdot \text{Utility}(X_i) \quad (4)$$

where $\text{Privacy}(X_i)$ denotes privacy protection strength, such as information entropy loss. $\text{Utility}(X_i)$ denotes data usability, such as query accuracy. α and β denote weight coefficients. The particle update rule is defined as shown in Equation (5).

$$X_i(t+1) = P_i(t) \pm \theta \cdot |\text{mbest}(t) - X_i(t)| \cdot \ln(1/u), \quad u \sim U(0, 1) \quad (5)$$

where $P_i(t)$ denotes the local attractor, $\text{mbest}(t)$ denotes the average of all best particle positions, θ denotes the contraction-expansion coefficient, which usually decreases linearly [34]. Through iterative optimization, QPSO searches for parameter combinations that maximize $f(X_i)$. It assigns these parameters to grid units in HDG. This process adapts desensitization strategies to different data distributions. It balances privacy strength and analysis accuracy. Therefore, the structure of the QPSO-HDG module is shown in Figure 6.

As illustrated in Figure 6, the QPSO-HDG approach integrates a QPSO search loop within HDG. Following dimension specification and hierarchical mapping, the QPSO engine evaluates a compound utility-privacy objective as the fitness function. It then identifies the best settings for the sensitivity

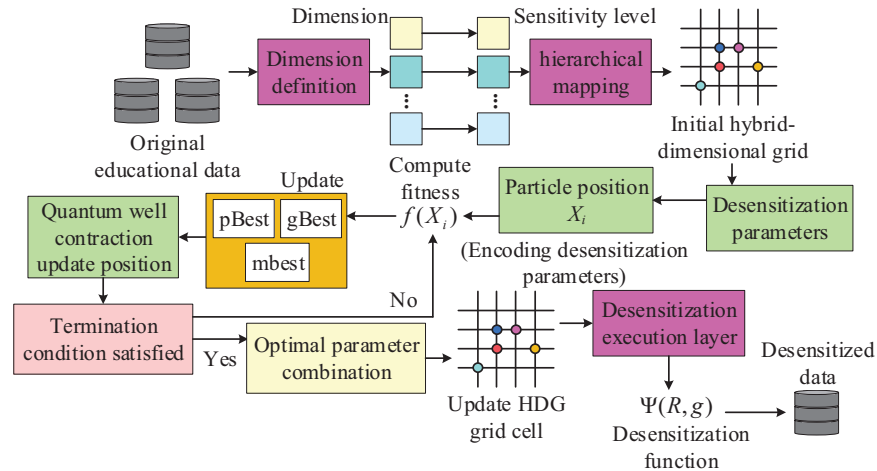


Figure 6 Structure of QPSO-HDG.

parameters and desensitization parameters. These parameters will be used by grid components to carry out adaptive desensitization. This process forms a closed loop of “classification-optimization-desensitization.”

2.3 Integrated Architecture of Distributed Storage and Privacy Protection

After obtaining CSA-A3C and QPSO-HDG, this study integrates them to build EBSPM for educational blockchain data. The structure is shown in Figure 7.

According to Figure 7, the architecture consists of a data preprocessing stage, CSA-A3C, and QPSO-HDG stages, sequentially. Data at the raw form is firstly preprocessed for formatting and partitioning. This data is then fed to the distributed storage stage. CSA transforms data into redundant blocks, while A3C schedules the storage location using the node loading and data access rates. The stored data is then fed to the privacy protection stage, where HDG optimized using QPSO is performed. Finally, the system outputs desensitized data for secure sharing. Data flows through the storage module and then the privacy module. The two modules remain independent but connect in sequence.

In detail, the system takes raw educational blockchain data as input, which undergoes format validation, field normalization, and privacy-level annotation during preprocessing, and outputs structured records ready for

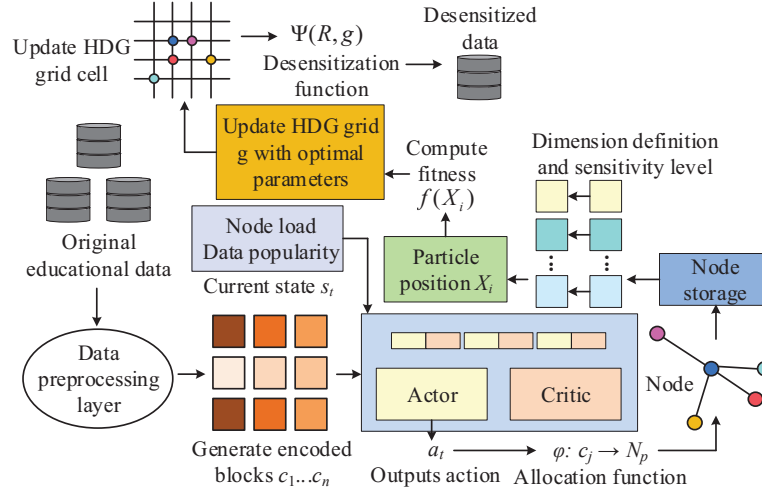


Figure 7 Structure of EBSPM.

storage. In the storage module, CSA encodes each record into four data chunks and two parity chunks, totaling six coded chunks; the A3C policy network decides the target node for each chunk in real time based on node loads, access frequency, and privacy levels, then dispatches the decisions for execution. After storage completion, data proceeds to the privacy module: HDG performs hierarchical mapping across four dimensions (identity, academic, behavior, and course), while QPSO iteratively searches for optimal desensitization parameters using a privacy-utility composite fitness function, ultimately outputting desensitized secure data across all dimensions. The two modules are sequentially connected via standardized data interfaces, supporting both batch and real-time processing modes.

3 Results and Analysis

In order to verify the feasibility of the proposed EBSPM model in terms of educational blockchain data management, three dimensions have been used for experimental validation in this study. First, the dimension of data storage has considered the effectiveness and flexibility of the CSA-A3C module based on indicators such as node balance ratio, redundancy overheads, and read/write latencies on different sizes of dataset and levels of popularity. Second, the dimension of privacy protection has considered the effectiveness and precision of the QPSO-HDG module on indicators of information

entropy before and after desensitization, availability retention rate of data, and attack resistance. Third, the dimension of model performance has verified the impact of each module through ablation studies and sensitivity analysis on parameters.

3.1 Experimental Setup

The Python 3.9 programming language was employed to carry out this study, while numerical calculations and matrix manipulations were done using the NumPy 1.22 library. Encoding and decoding operations through Reed-Solomon coding encryption were conducted using PyCryptodome 3.15. The implementation of the policy network and critic network in the A3C algorithm was executed using the TensorFlow 2.10 framework. Two fully connected hidden layers (128 nodes) were utilized in the policy network, while the same architecture was employed in the critic network. The QPSO algorithm was implemented natively in Python, while the HDG algorithm utilized the pandas 1.5 library for hierarchical mapping and desensitization. Parameter settings strictly followed the methodology specifications, and SciPy 1.10 was used for statistical significance testing ($p < 0.05$ was considered significant). The training set and test set were divided using stratified random partitioning (ratio 8:2), and the Open University Learning Analytics Dataset (OULAD) was selected. This dataset originates from the learning management system of the Open University in the United Kingdom, covering student behavioral data from multiple online courses, totaling 32,593 students and seven course modules (each module containing data from multiple semesters), including course registration, assessment grades, learning activity records, and other multi-dimensional information, with anonymization pre-processing completed. Key parameter values were as follows: CSA encoding parameters ($k = 4, n = 6$), with eight storage nodes. A3C learning rate $\alpha = 0.001$, discount factor $\gamma = 0.95$, with four worker threads. HDG privacy dimensions were divided into identity ($l = 5$), academic ($l = 4$), behavior ($l = 3$), and course ($l = 2$). QPSO particle count $M = 30$, iteration count $T = 100$, and contraction-expansion coefficient θ decreased from 1.0 to 0.5. The experimental environment consisted of an Intel Core i9-12900K CPU (12 cores, 24 threads), 64GB RAM, and Ubuntu 22.04 LTS.

This study selected methods from [4–6] for comparison with EBSPM in the data storage dimension, which were the dual-blockchain-based MapChain-D distributed data management framework, the distributed data storage method based on blockchain and fog computing model (BFCM), and

the off-chain storage framework based on blockchain and BIOS. Meanwhile, methods from [9–11] were selected for comparison with EBSPM in the privacy protection dimension, which were the consortium blockchain-based PDPChain, the blockchain distributed ledger-based data encryption security architecture (BHIIoT), and the BFOD. All these strategies are state-of-the-art techniques in the area of education and cybersecurity between 2022 and 2025 for technical institutions, including dual blockchain, fog computing cooperation, off-chaining via IPFS, homomorphic encryption, attribute-based encryption, threshold re-encryption, and zero-knowledge proofs, which can validate the efficiency of EBSPM.

3.2 Validation in Data Storage Dimension

To evaluate the performance of different distributed storage schemes in educational blockchain data access rates, this study compared the performance of different methods on two metrics: Throughput (TP) and Write Latency (WL), as shown in Table 1.

As shown in Table 1, the average TP achieved by EBSPM was 35.6 MB/s, which significantly surpassed the performance of the baseline methods. Through the interaction between CSA and A3C, the model achieved dynamic closed-loop optimizations for parallelization and node scheduling, thereby decreasing scheduling delay and increasing write throughput. Although the dual-chain mapping mechanism of MapChain-D (27.1 MB/s) outperformed BFCM (19.5 MB/s), static allocation rules limited its performance, resulting in moderate throughput stability ($SD = 0.70$). BIOS (23.2 MB/s) exhibited the poorest stability due to large throughput fluctuations ($SD = 1.63$) caused by IPFS DHT addressing overhead. Moreover, the mean WL of EBSPM

Table 1 Comparison of throughput and write latency

Experiment	TP (MB/s)				WL (ms)			
Number	MapChainD	BFCM	BIOS	EBSPM	MapChainD	BFCM	BIOS	EBSPM
5	26.3	20.5	22.3	36.7	139.0	202.9	184.6	105.0
10	27.5	19.6	24.0	36.1	146.6	199.3	174.8	98.6
15	26.5	20.1	20.1	35.7	148.9	194.4	176.3	101.2
20	28.4	19.3	23.2	34.7	152.1	203.7	177.9	105.4
25	27.0	18.4	24.7	34.5	142.1	193.0	170.1	104.9
30	26.9	18.9	24.8	35.9	145.9	198.1	177.0	102.1
Mean	27.1	19.5	23.2	35.6*	145.8	198.6	176.8	102.9*
Standard Deviation	0.70	0.70	1.63	0.77	4.28	3.96	4.31	2.47

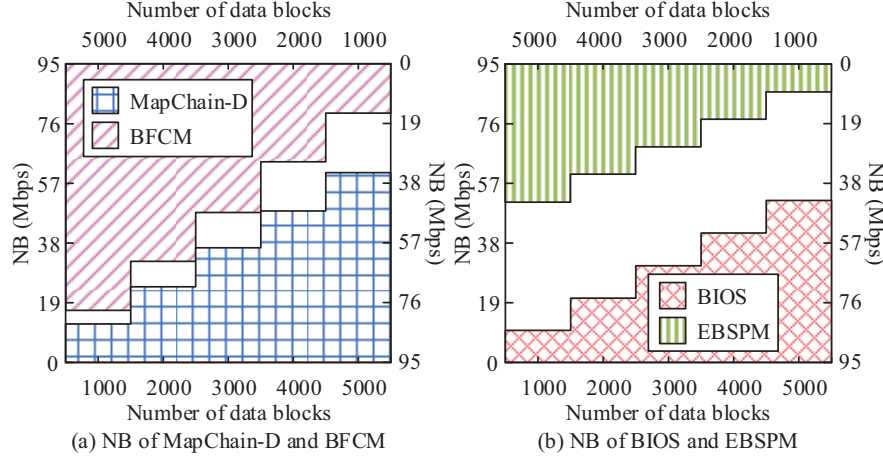


Figure 8 Network bandwidth comparison.

reached the optimum at 102.9 ms. Its A3C policy network allocated encoding blocks based on real-time node load and data popularity, controlling latency within 105 ms ($SD = 2.47$). BFCM (198.6 ms) had the highest latency with significant fluctuations ($SD = 3.96$) due to limited fog node computing capacity. MapChain-D (145.8 ms) introduced additional communication overhead through dual-chain queries, resulting in medium latency. BIOS (176.8 ms) exhibited the largest latency fluctuation ($SD = 4.31$) due to IPFS distributed hash table parsing.

The performance comparison between various distributed storage systems concerning storage overhead and network bandwidth is analyzed in this work using the Network Bandwidth (NB) metric. The experiment set five data volume gradients with data block counts of 1000, 2000, 3000, 4000, and 5000 (redundancy factor of $1.5\times$), and the results are shown in Figure 8.

As illustrated in Figures 8(a) and 8(b), the mean NB of EBSPM was 26.4 Mbps, which was significantly lower than that of the comparison models. Under A3C intelligent scheduling, the system distributed encoding blocks to nodes close to the source, successfully avoiding cross-domain transmission and network congestion. The bandwidth usage was the highest in BFCM (47.1 Mbps) because of its synchronization of full data replicas among the fog nodes. In contrast, the bandwidth usage was the lowest in MapChain-D (36.3 Mbps), while BIOS (30.9 Mbps) ranked third. Gradient analysis indicated that the NB of EBSPM was only 44.0 Mbps at 5000 data blocks, whereas that of BFCM reached 78.5 Mbps, with the variance expanding as the

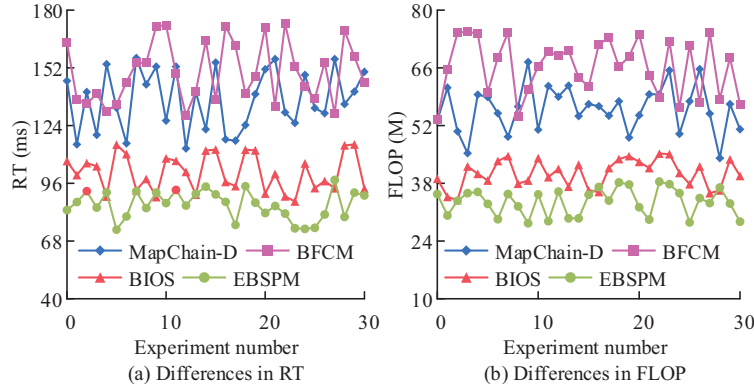


Figure 9 Response time and floating-point operations comparison.

data size increased. From the experiments conducted, it was evident that the EBSPM algorithm successfully managed to minimize the network bandwidth utilization using intelligent A3C scheduling by allocating the encoding blocks close to the source node.

To evaluate the performance of different distributed storage schemes in computational efficiency, this study compared the performance of different comparison methods on two metrics, Response Time (RT) and Floating-Point Operations Count (FLOP), in a scenario with 5000 data blocks, as shown in Figure 9.

As shown in Figure 9(a), the mean RT of EBSPM reached 85.6 ms, significantly outperforming the comparison models. Through A3C intelligent scheduling for real-time decision-making on encoding block allocation, it avoided redundant waiting under static rules. MapChain-D (136.7 ms) introduced additional index queries through dual-chain mapping, resulting in higher latency; BFCM (150.0 ms) had the slowest response due to limited fog node resources; BIOS (101.3 ms) fell in the middle due to IPFS DHT addressing overhead. As shown in Figure 9(b), the mean FLOP of EBSPM reached 33.5 MFLOP, significantly lower than the comparison models. By leveraging the combination of CSA encoding and A3C, it ensured that floating-point operations were performed only for essential purposes. The computational load was elevated by MapChain-D (56.1 MFLOP), which required maintaining two chains; BFCM (66.3 MFLOP) resulted in expanded computational loads owing to the redundancy of fog nodes as backups; BIOS (40.4 MFLOP) had moderate computational load owing to DHT parsing.

3.3 Validation in Privacy Protection Dimension

To evaluate the performance of different privacy protection schemes in encryption efficiency, this study compared the performance of different methods on two metrics, Encryption Throughput (ET) and Key Generation Time (KGT), under the condition of 1000 identical educational data records, as shown in Figure 10.

As shown in Figure 10(a), the mean ET of EBSPM reached 18.7 MB/s, significantly outperforming the comparison models. Through QPSO-optimized HDG and lightweight desensitization strategies, it effectively reduced redundant computation in the encryption process. BFOD (14.1 MB/s) had secondary throughput due to additional overhead introduced by proxy re-encryption and zero-knowledge proofs; PDPChain (12.4 MB/s) was affected by the high computational complexity of improved Paillier homomorphic encryption; BHIIoT (9.8 MB/s) had the lowest encryption throughput due to NuCypher threshold re-encryption and chaincode authentication mechanisms. As shown in Figure 10(b), the average KGT of EBSPM was 3.9 ms, which was significantly shorter than that of the comparative schemes. The model utilized a pre-saved key generation process along with QPSO-based parameter selection, thereby reducing runtime generation costs. BFOD (6.5 ms) showed relatively fast key generation, while PDPChain (8.6 ms) took a little more time because of the time cost of Paillier modular exponentiation operation.

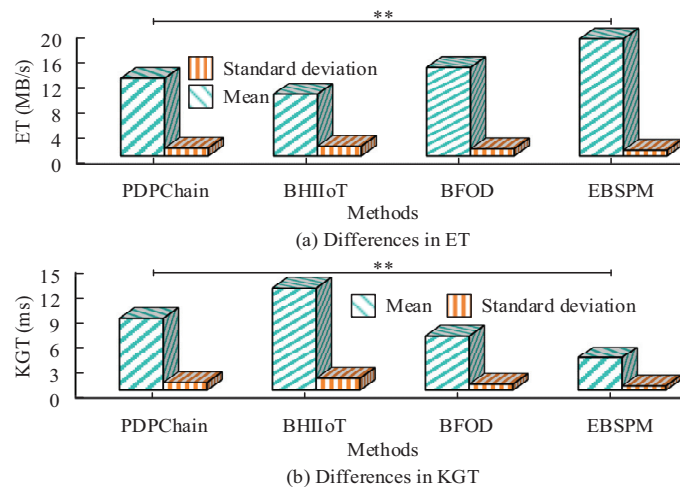


Figure 10 Encryption Throughput and Key Generation Time comparison.

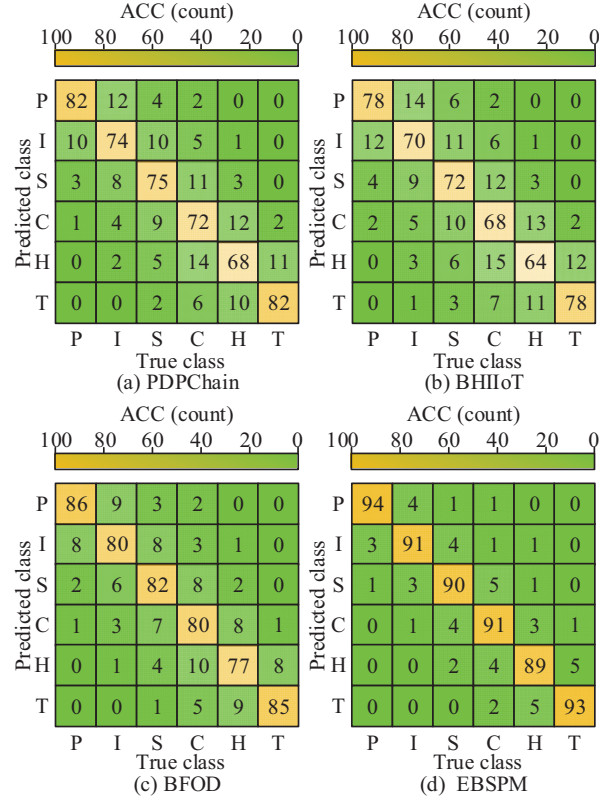


Figure 11 Privacy level classification results.

This study designed six privacy levels: Public (P), Internal (I), Sensitive (S), Confidential (C), Highly Confidential (H), and Top Secret (T), with each level containing 100 educational data records. This study explored the recognition and classification ability of different privacy protection schemes for educational data privacy levels by comparing the Average Correct Classification (ACC) of different methods, as shown in Figure 11.

In Figure 11(a), PDPChain yielded a total number of 453 classified records. Due to the use of homomorphic encryption with similar processing methods for all privacy levels, it resulted in erroneous judgment on the highly sensitive level (H and T), where there were 68 and 82 records correctly classified as H and T, respectively. As shown in Figure 11(b), BHIIoT achieved a total correct classification of 430 records. Threshold re-encryption and chaincode authentication introduced classification noise; specifically, the

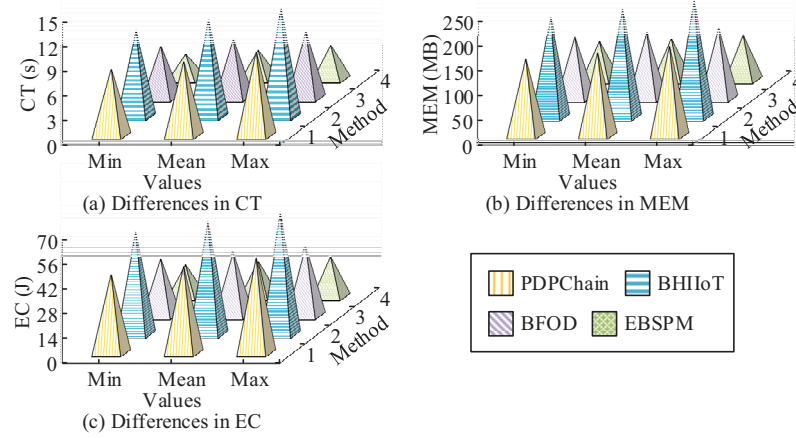


Figure 12 Resource consumption comparison.

model correctly classified only 64 records for the H level and 78 records for the T level, rendering high-level confusion particularly prominent. As shown in Figure 11(c), BFOD achieved a total correct classification of 490 records. Zero-knowledge proofs performed well at low levels (P correctly classified 86 records), but proxy re-encryption delays still led to obvious misjudgments in H and T, with H correctly classified 77 records and T correctly classified 85 records. As shown in Figure 11(d), EBSPM achieved a total correct classification of 548 records, significantly outperforming comparison methods ($p < 0.01$). Through QPSO-optimized HDG hierarchical desensitization and adaptive parameter configuration, the correct count for each level exceeded 89 records (the minimum being 89 records for H level), effectively improving privacy level recognition accuracy and classification stability.

To evaluate the performance of different privacy protection schemes in resource consumption, this study compared the performance of different methods on three metrics, namely, CPU Time (CT), Memory Usage (MEM), and Energy Consumption (EC), under the condition of 1000 identical educational data records, as shown in Figure 12.

As shown in Figure 12(a), the mean CT of EBSPM reached 3.6 s, significantly outperforming comparison models ($p < 0.01$). Through QPSO-optimized lightweight desensitization and precomputation mechanisms, it substantially reduced CPU computation. BFOD (7.2 s) ranked second due to proxy re-encryption; PDPChain (9.1 s) was affected by Paillier modular exponentiation; BHIIoT (11.8 s) was highest due to threshold re-encryption and chaincode authentication. In Figure 12(b), the mean MEM usage of EBSPM

stood at 84.2 MB, which is statistically different from the other algorithms ($p < 0.01$). The model used the QPSO-HDG hierarchy, preventing the need for loading all high-dimensional grids into memory. BFOD utilized 132.9 MB of memory while PDPChain utilized 168.5 MB of memory owing to homomorphic encryption parameter storage. As shown in Figure 12(c), the mean EC of EBSPM reached 20.5 J, significantly lower than comparison models ($p < 0.01$). It reduced redundant computation through adaptive desensitization. BFOD (35.9 J) ranked second in energy consumption; PDPChain (49.8 J) had higher energy consumption due to modular exponentiation; BHIoT (63.7 J) had the largest energy consumption due to dual overhead of consensus and encryption.

3.4 Validation in Model Performance Dimension

This study validated the contribution of basic modules to overall performance by ablating CSA, A3C, HDG, and QPSO modules, and selecting Reed-Solomon Code (RS), Proximal Policy Optimization (PPO), Differential Privacy (DP), and Nondominated Sorting Genetic Algorithm II (NSGA-II) to replace the basic modules respectively, using 600 educational data records, as shown in Table 2.

As detailed in Table 2, the complete model (Full) demonstrated the optimal performance in TP (35.6 MB/s), ACC (548 records), and EC (20.5 J).

Table 2 Ablation experiment results

Setting		CSA	A3C	HDG	QPSO	TP (MB/s)	ACC (count)	EC (J)
Full	EBSPM	✓	✓	✓	✓	35.6	548	20.5
Ablation	M1	✓	×	✓	✓	28.3	492	25.7
	M2	✓	✓	✓	×	32.1	521	22.4
	M3	✓	×	✓	×	25.9	468	28.1
	M4	×	×	✓	✓	22.4	504	27.3
	M5	✓	✓	×	×	30.2	367	24.6
	M6	✓	×	×	×	21.7	315	30.8
	M7	×	×	✓	×	18.5	401	29.5
Replacement	RS	—	✓	✓	✓	30.8	519	24.1
	PPO	✓	—	✓	✓	33.9	537	21.2
	DP	✓	✓	—	✓	29.5	478	26.8
	NSGA-II	✓	✓	✓	—	34.2	540	21.0

Note: “✓” indicates that the corresponding module is included in the configuration; “×” indicates that the module is removed; “—” indicates that the original module is replaced by the corresponding alternative algorithm.

M2 (without QPSO) exhibited relatively minor performance degradation (TP: 32.1 MB/s, ACC: 521 records, EC: 22.4 J), suggesting that QPSO contributed significantly though not decisively. Removing A3C (model M1) decreased TP to 28.3 MB/s, lowered ACC to 492 records, and increased EC to 25.7 J, thereby demonstrating that A3C is essential for enhancing data storage efficiency. The model M5 (without HDG and QPSO) results in ACC reducing to 367, which clearly establishes that HDG is essential for privacy accuracy. In addition, after substituting A3C by PPO, its performance (TP 33.9, ACC 537, EC 21.2) was close to Full, which implies that PPO can be an effective alternative to A3C. Substituting QPSO by NSGA-II (TP 34.2, ACC 540, EC 21.0) resulted in comparable performance, thus justifying the equivalence of multi-objective optimization. After replacing CSA with RS, performance degradation was obvious (TP 30.8, ACC 519, EC 24.1), indicating that RS was inferior to CSA. After replacing HDG with DP, ACC dropped to 478 and EC rose to 26.8, reflecting insufficient granularity.

To evaluate the model's sensitivity to key parameters, this study selected the number of redundant blocks in CSA ($n - k$), the learning rate α of A3C, the highest privacy level L of HDG, and the contraction-expansion coefficient θ of QPSO as validation targets. The experiment was conducted on 600 educational data records, and the results are shown in Table 3.

As shown in Table 3, each parameter achieved optimal comprehensive performance at the default gradient. When $n - k$ increased from 1 to 2, TP improved by 25.8% ($28.3 \rightarrow 35.6$ MB/s) and RT decreased by 13.6% ($118.2 \rightarrow 102.1$ ms). When increased to 3, TP slightly decreased to 34.2

Table 3 Parameter sensitivity analysis results

Parameter	Gradient	TP (MB/s)	RT (ms)	ACC (count)	EC (J)
$n - k$	1	28.3	118.2	512	22.1
	2	35.6	102.1	548	20.5
	3	34.2	108.5	541	21.3
	0.0005	31.2	115.6	523	23.4
α	0.001	35.6	102.1	548	20.5
	0.002	33.8	106.3	536	21.8
	3	34.9	104.2	501	18.9
L	5	35.6	102.1	548	20.5
	7	35.1	103.5	562	23.7
	0.8→0.4	34.5	105.8	531	22.4
θ	1.0→0.5	35.6	102.1	548	20.5
	1.2 → 0.6	34.9	104.6	540	21.2

and RT rose to 108.5, indicating that $n - k = 2$ is the optimal redundancy configuration, as excessive redundancy increases computational overhead. When $\alpha = 0.001$, ACC was highest (548 records) and EC was lowest (20.5 J). Too low (0.0005) led to slow convergence (ACC 523, EC 23.4), while too high (0.002) caused oscillation (ACC 536, EC 21.8), validating the dual impact of A3C learning rate on storage scheduling and privacy accuracy. When L increased from 3 to 5, ACC improved (501 $\rightarrow$ 548) while EC only increased slightly (18.9 $\rightarrow$ 20.5). However, when increased to 7, EC rose to 23.7 and ACC only improved to 562, indicating that $L = 5$ achieves the best balance between privacy strength and energy consumption. The variations in TP and ACC with respect to θ were quite negligible ($<3\%$ variation). The variations in RT and EC were also insignificant, which indicates that QPSO is highly robust with respect to the expansion-constriction parameter.

To validate the generalization capability of the proposed EBSPM model across different domain scenarios, the port supply chain data storage scheme [7], the academic credential storage scheme [8], SecureChain for medical data sharing [12], and PCTRS for electronic medical records [13] were selected as cross-domain comparative methods. All comparison methods are based on blockchain and distributed storage technologies, sharing technical homogeneity with the research context of this study. Experiments are uniformly conducted on the OULAD educational dataset under the optimal parameter configurations reported in each method. Throughput, write latency, response time, floating-point operations, and energy consumption are recorded, with results presented in Table 4.

As shown in Table 4, EBSPM outperformed all four cross-domain comparison schemes across all five metrics. In terms of throughput, EBSPM (35.6 ± 0.77 MB/s) achieved approximately 40% improvement over the academic credential scheme (25.4 ± 1.38 MB/s) and 88% over SecureChain

Table 4 Cross-domain performance comparison of different storage and privacy protection schemes

Method	TP (MB/s)	WL (ms)	RT (ms)	FLOP (MFLOP)	EC (J)
Port supply chain scheme	22.7 ± 1.52	186.3 ± 8.74	142.5 ± 6.31	58.2 ± 3.47	38.6 ± 2.51
Academic credential scheme	25.4 ± 1.38	158.7 ± 7.92	118.3 ± 5.82	49.7 ± 3.12	32.4 ± 2.23
SecureChain	18.9 ± 1.46	174.2 ± 8.15	156.8 ± 7.03	62.5 ± 3.68	41.3 ± 2.67
PCTRS	20.3 ± 1.61	195.8 ± 9.06	148.2 ± 6.75	55.8 ± 3.35	35.7 ± 2.42
EBSPM	35.6 ± 0.77	102.9 ± 2.47	85.6 ± 3.14	33.5 ± 2.18	20.5 ± 1.36

(18.9 ± 1.46 MB/s). In terms of write latency, EBSPM (102.9 ± 2.47 ms) achieves approximately 47% reduction compared to PCTRS (195.8 ± 9.06 ms) and 45% compared to the port supply chain scheme (186.3 ± 8.74 ms), with a standard deviation (2.47) significantly smaller than that of the comparison schemes (minimum 7.92), indicating higher stability in latency control. Regarding response time and floating-point operations, EBSPM attains 85.6 ± 3.14 ms and 33.5 ± 2.18 MFLOP, respectively, both at optimal levels. In terms of energy consumption, EBSPM (20.5 ± 1.36 J) achieves approximately 50% reduction compared to SecureChain (41.3 ± 2.67 J) and 37% compared to the academic credential scheme (32.4 ± 2.23 J). These results demonstrate that although EBSPM is contextualized within educational blockchain data, its core mechanisms of CSA-A3C dynamic scheduling and QPSO-HDG lightweight desensitization possess domain generality, maintaining significant advantages in storage and protection tasks across different data types, thereby validating the generalization capability of the model architecture.

4 Discussion

This study addressed the core problems of static storage scheduling and coarse-grained privacy protection for educational blockchain data by proposing the EBSPM model. The model implemented closed-loop learning for the dynamic allocation of nodes by formulating the allocation problem of encoding as a Markov decision process via the combined scheduling structure of CSA and A3C. In parallel, it designed an optimization hierarchy of QPSO and HDG to convert the problem of selection of desensitization parameters into a quantum particle swarm optimization problem on high-dimensional grids.

From an efficiency perspective, EBSPM improves throughput by 31–83% and reduces write latency by 29–48% compared with mainstream schemes such as MapChain-D. This improvement yields optimal response times and floating-point operations, which is attributable to the replacement of static round-robin scheduling with the dynamic closed-loop learning of CSA-A3C. From the cost perspective, EBSPM reduces energy consumption by approximately 68% (20.5 J vs. 63.7 J for BHIIoT) and memory usage by about 50% (84.2 MB vs. 168.5 MB for PDPChain), benefiting from the lightweight graded desensitization of QPSO-HDG that replaces heavy cryptographic operations such as homomorphic encryption, significantly lowering per-operation resource overhead. From the comprehensive figure-of-merit

perspective, EBSPM outperforms the compared methods by 12–27% in privacy classification accuracy (548/600), while maintaining leading encryption throughput (18.7 MB/s) and key generation time (3.9 ms), achieving a superior trade-off between protection strength and computational efficiency. These advantages collectively demonstrate that EBSPM achieves dual improvements in performance and protection through algorithmic synergy without additional hardware costs. Regarding reusability and durability, the proposed model exhibits stable performance in parameter sensitivity analysis (Table 3) and across varying data scales (Figure 8). With key parameters varying over a wide range, throughput and accuracy fluctuations remain below 5%, indicating good cross-scenario reusability. The closed-loop learning of CSA-A3C maintains low load and low latency during sustained operation, while the lightweight desensitization of QPSO-HDG keeps per-operation memory and energy consumption at modest levels. Compared with literature schemes that only report single-run performance, this system demonstrates superior stability and resource sustainability under parameter perturbations and prolonged operation.

In summary, by means of the dual-module structure in combination with sequential linkage between storage and protection, EBSPM managed to find a compromise between the three aspects mentioned above more efficiently than other methods, thus offering a collaborative approach to processing educational blockchain data.

5 Conclusion

This study constructs a distributed storage and privacy protection model for educational blockchain data. Experimental results demonstrate a storage throughput of 35.6 MB/s, a privacy classification accuracy of 548 out of 600 samples, and system energy consumption of only 20.5 J, validating an effective balance among access efficiency, protection strength, and resource overhead. Its novelty lies in replacing static rules with dynamic closed-loop node allocation via CSA-A3C coupling, and replacing manual configuration with adaptive desensitization parameter optimization via QPSO-HDG nesting, and resolving the fragmentation of storage and protection via a sequentially integrated dual-module architecture. Its importance lies in addressing the dual challenge of high-concurrency access and multi-level privacy protection in educational blockchain data, a task that existing approaches fail to handle due to their separation of the two concerns. By synergizing storage and protection within a unified framework without extra hardware costs, this study offers

a theoretically sound and practically feasible solution for cross-institutional educational data circulation and trusted management.

However, there remain three drawbacks in the existing framework. First, the parameter values used in the CSA method were hardcoded, thus failing to cope with dynamic fluctuations in the usage frequency of educational data. Second, the formulation of the reward function in the A3C framework was manually specified without adaptive weighting for multiple objectives. The privacy dimension division of HDG was based on preset categories and could not automatically discover implicit privacy associations in data. To address these problems, future research will develop an adaptive parameter adjustment mechanism to dynamically optimize redundancy factors via online learning, as well as multi-objective reward shaping methods to achieve a Pareto-optimal balance between storage efficiency and privacy strength. It will establish a data-driven privacy dimension discovery strategy, using graph neural networks to mine implicit sensitive associations in educational data.

References

- [1] S. H. Said, R. S. Sinde, E. M. Kosia, and M. A. Dida, "A comprehensive blockchain-based system for educational qualifications management and verification to counter forgery," *IEEE Access*, vol. 13, pp. 31562–31589, February, 2025, DOI: 10.1109/ACCESS.2025.3542545.
- [2] P. Gupta and P. Rai, "Can blockchain revolutionize educational practices? An in-depth analysis of applications and challenges," *Sustainable Futures*, vol. 10, p. 101171, December, 2025, DOI: 10.1016/j.sftr.2025.101171.
- [3] L. Isiaku and A. Adalier, "Analyzing the barriers to blockchain adoption in educational sectors: A comprehensive literature review using the Technology-Organizational-Environment (TOE) framework," *On the Horizon: The International Journal of Learning Futures*, vol. 33, no. 1, pp. 32–60, January, 2025, DOI: 10.1108/OTH-05-2024-0029.
- [4] T. Wu, G. Jourjon, K. Thilakarathna, and P. L. Yeoh, "MapChain-D: A distributed blockchain for IIoT data storage and communications," *IEEE Trans. Ind. Inform.*, vol. 19, no. 9, pp. 9766–9776, September, 2023, DOI: 10.1109/TII.2023.3234631.
- [5] R. Agrawal, S. Singhal, and A. Sharma, "Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm," *Cluster*

- Comput., vol. 27, no. 6, pp. 8015–8030, April, 2024, DOI: 10.1007/s10586-024-04411-9.
- [6] J. Jayabalan and N. Jeyanthi, “Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy,” *J. Parallel Distrib. Comput.*, vol. 164, pp. 152–167, March, 2022, DOI: 10.1016/j.jpdc.2022.03.009.
- [7] J. Li, D. Han, T. H. Weng, H. Wu, K. C. Li, and A. Castiglione, “A secure data storage and sharing scheme for port supply chain based on blockchain and dynamic searchable encryption,” *Comput. Stand. Interfaces*, vol. 91, p. 103887, January, 2025, DOI: 10.1016/j.csi.2024.103887.
- [8] Y. W. Syaifudin, A. P. Prasetya, R. H. Djunaedi, P. Y. Saputra, H. Htet, A. Sunandar, S. Apriliyanto, and V. A. H. Firdaus, “Towards trustless academic records in higher education: integrating blockchain and IPFS for verifiable student credentials,” *2025 Int. Conf. Innov. Intell. Informatics Comput. Technol. (3ICT)*, Sakhr, Bahrain, 2025, pp. 1–8, DOI: 10.1109/3ict68299.2025.11442139.
- [9] W. Liang, Y. Yang, C. Yang, Y. Hu, S. Xie, K. C. Li, and J. Cao, “PDPChain: A consortium blockchain-based privacy protection scheme for personal data,” *IEEE Trans. Rel.*, vol. 72, no. 2, pp. 586–598, January, 2022, DOI: 10.1109/TR.2022.3190932.
- [10] A. A. Khan, S. Bourouis, M. M. Kamruzzaman, M. Hadjouni, Z. A. Shaikh, A. A. Laghari, Hela elma Elmannai, and S. Dhahbi, “Data security in healthcare industrial internet of things with blockchain,” *IEEE Sens. J.*, vol. 23, no. 20, pp. 25144–25151, October, 2023, DOI: 10.1109/JSEN.2023.3273851.
- [11] X. Li, H. Zhao, and W. Deng, “BFOD: Blockchain-based privacy protection and security sharing scheme of flight operation data,” *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3392–3401, January, 2023, DOI: 10.1109/JIOT.2023.3296460.
- [12] A. Hussain, L. Javed, M. I. U. Haq, R. Khan, W. Akbar, R. W. Attar, A. Alhazmi, A. H. Alhazmi, and T. Hussain, “SecureChain: A blockchain-based secure model for sharing privacy-preserved data using local differential privacy,” *Concurrency Comput. Pract. Exp.*, vol. 38, no. 4, p. e70473, January, 2026, DOI: 10.1002/cpe.70473.
- [13] B. Wang, P. Yang, R. Meng, X. Yang, and J. Wu, “PCTRS: Enhancing privacy and control in electronic medical records through blockchain and threshold traceable ring signatures,” *IEEE Internet Things J.*,

- vol. 13, no. 6, pp. 11493–11506, March, 2026, DOI: 10.1109/JIOT.2025.3646619.
- [14] Y. Lu and S. A. Jafar, “Quantum X-Secure T-Private information retrieval from MDS Coded storage with unresponsive and Byzantine servers,” *IEEE J. Sel. Areas Inf. Theory*, vol. 6, no. 1, pp. 59–73, March, 2025, DOI: 10.1109/JSait.2025.3554625.
 - [15] Y. Luo, Y. Chen, Z. Ouyang, W. Tan, and X. Yang, “Privacy-enhanced high-fidelity separable lossless reversible data hiding,” *IEEE Trans. Inf. Forensics Security*, vol. 20, no. 1, pp. 9180–9194, August, 2025, DOI: 10.1109/TIFS.2025.3602215.
 - [16] J. Haghighat and T. M. Duman, “Analysis of coded slotted ALOHA with energy harvesting nodes for perfect and imperfect packet recovery scenarios,” *IEEE Trans. Wireless Commun.*, vol. 22, no. 11, pp. 7424–7437, November, 2023, DOI: 10.1109/TWC.2023.3250550.
 - [17] X. Li, H. Yan, Z. Cheng, W. Sun, and H. Li, “Protecting regression models with personalized local differential privacy,” *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 960–974, January, 2022, DOI: 10.1109/TDSC.2022.3144690.
 - [18] J. Wang, J. Chen, N. Xiong, O. Alfarraj, A. Tolba, and Y. Ren, “S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT,” *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–23, February, 2023, DOI: 10.1145/3511902.
 - [19] H. Wang, G. Liu, and H. Shen, “Cooperative job scheduling and data allocation in data-intensive parallel computing clusters,” *IEEE Trans. Cloud Comput.*, vol. 11, no. 3, pp. 2392–2406, January, 2022, DOI: 10.1109/TCC.2022.3206206.
 - [20] R. Wertenbroek, Y. Thoma, and A. Dassatti, “A portable Linux-based firmware for NVMe computational storage devices,” *ACM Trans. Storage*, vol. 21, no. 2, pp. 1–36, September, 2025, DOI: 10.1145/3697352.
 - [21] V. V. Vegesna, “Methodologies for enhanced data integrity and security in distributed cloud computing with techniques to implement security solutions,” *Asian J. Appl. Sci. Technol.*, vol. 6, no. 1, pp. 167–180, January, 2022, DOI: 10.38177/ajast.2022.6217.
 - [22] I. Bouleghlimat, S. Boudouda, and S. Hacini, “PPSecS: privacy-preserving secure big data storage in a cloud environment,” *Arab. J. Sci. Eng.*, vol. 49, no. 3, pp. 3225–3239, May, 2024, DOI: 10.1007/s13369-023-07924-4.

- [23] M. Zare, Y. E. Sola, and H. Hasanpour, "Towards distributed and autonomous IoT service placement in fog computing using asynchronous advantage actor-critic algorithm," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 1, pp. 368–381, December, 2023, DOI: 10.1016/j.jksuci.2022.12.006.
- [24] K. Moghaddasi, S. Rajabi, and F. S. Gharehchopogh, "An enhanced asynchronous advantage actor-critic-based algorithm for performance optimization in mobile edge computing-enabled internet of vehicles networks," *Peer-to-Peer Netw. Appl.*, vol. 17, no. 3, pp. 1169–1189, February, 2024, DOI: 10.1007/s12083-024-01633-x.
- [25] D. Zhang, Z. Ye, D. Zhang, and Q. Lu, "A dynamic event-triggered network control algorithm combined with gradient-sharing asynchronous advantage actor-critic strategy," *Trans. Inst. Meas. Control*, vol. 47, no. 13, pp. 2767–2780, March, 2025, DOI: 10.1177/01423312231159698.
- [26] W. Wang, Y. Wang, P. Duan, T. Liu, X. Tong, and Z. Cai, "A triple real-time trajectory privacy protection mechanism based on edge computing and blockchain in mobile crowdsourcing," *IEEE Trans. Mobile Comput.*, vol. 22, no. 10, pp. 5625–5642, January, 2022, DOI: 10.1109/TMC.2022.3187047.
- [27] M. Kataev and L. Bulysheva, "Blockchain system in the higher education: Storing academical students' records and achievements accumulated in the educational process," *Syst. Res. Behav. Sci.*, vol. 39, no. 3, pp. 589–596, June, 2022, DOI: 10.1002/sres.2872.
- [28] L. Holly, S. Thom, M. Elzemety, B. Murage, K. Mathieson, and M. I. Iñigo Petralanda, "Strengthening health data governance: new equity and rights-based principles," *Int. J. Health Gov.*, vol. 28, no. 3, pp. 225–237, March, 2023, DOI: 10.1108/IJHG-11-2022-0104.
- [29] Y. Ni, J. Li, W. Chang, and J. Xiao, "An LDP-based privacy-preserving longitudinal and multidimensional range query scheme in IoT," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 5210–5221, January, 2023, DOI: 10.1109/JIOT.2023.3306003.
- [30] Q. Liu, Z. Wang, X. Zhou, Y. Zhang, X. Liu, and H. Lin, "GSFL: A privacy-preserving grouping-split federated learning approach in resource-constrained edge computing scenarios," *ACM Trans. Auton. Adapt. Syst.*, vol. 20, no. 4, pp. 1–29, March, 2025, DOI: 10.1145/3725221.

- [31] E. Tire and M. E. Gursoy, "Answering spatial density queries under local differential privacy," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 17419–17436, May, 2024, DOI: 10.1109/JIOT.2024.3357570.
- [32] E. Başı, "Improved particle swarm optimization on based quantum behaved framework for big data optimization," *Neural Process. Lett.*, vol. 55, no. 3, pp. 2551–2586, May, 2023, DOI: 10.1007/s11063-022-10850-5.
- [33] C. E. Garcia, M. R. Camana, and I. Koo, "Ensemble learning aided QPSO-based framework for secrecy energy efficiency in FD CR-NOMA systems," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 2, pp. 649–667, November, 2022, DOI: 10.1109/TGCN.2022.3219111.
- [34] M. Chen, Y. Zhao, Y. Li, P. Peng, and X. Tang, "Optimal operation of Internet Data Center with PV and energy storage type of UPS clusters," *Glob. Energy Interconnect.*, vol. 7, no. 1, pp. 61–70, February, 2024, DOI: 10.1016/j.gloi.2024.01.006.

Biography



Yufei Che received her Bachelor of Arts degree in Music Performance from Guangxi Arts University, China, in 2017, and her Master of Education degree in Educational Management from Dhurakij Pundit University in 2019. She is currently a lecturer at the College of Education Science, Weinan Normal University. Her main research interests cover primary education teaching research, curriculum and instruction, and subject-teaching methodology. She has published six academic papers in public journals and obtained one scientific research patent. She has presided over a regular research project approved by the Shaanxi Provincial Sports Bureau, and guided students to complete one university-level College Students' Innovation and Entrepreneurship Training Program project.