International Journal for Housing Science and Its Applications
Publish August 10, 2025. Volume 46, Issue 4 Pages 4845-4856

https://doi.org/10.70517/ijhsa464328

Blockchain-enhanced unmanned equipment environmental perception decision tree optimization and security algorithm

Wei Chang[1,*], Fuli Shi[1] and Jianzhou Wang[2]
[1] Equipment Management and Support College, Engineering University of PAP, Xi'an, Shaanxi, 710086, China
[2] Yichun Detachment, Heilongjiang Provincial Corps of PAP, Yichun, Heilongjiang, 153000, China
Corresponding authors: (e-mail: 18392130966@163.com).

Abstract This paper proposes a collaborative framework integrating blockchain encryption and decision tree optimization for the problems of data fragmentation, high security risk and low classification efficiency in unmanned equipment environment sensing system. First, a blockchain data security system based on homomorphic encryption is constructed to prevent data monopoly through distributed bookkeeping and key management; second, a decision tree model applicable to blockchain nodes is designed, and a buffer null node mechanism is introduced to solve the problem of local fragmentation and enhance the robustness of classification. Further, improve the PBFT consensus mechanism, use the C4.5 decision tree to realize node trust evaluation and differential voting weight allocation, and set the consensus threshold to 50% of the total weight. Finally, the environment-aware capability requirement is refined based on DoDAF multi-view. Experiments show that the data throughput of the optimized decision tree reaches 288.29 × 10^5 byte at an execution time of 100s on the Nursery and Mushroom datasets, which is a 50.6% improvement over the optimal comparison algorithm. The number of threads is 0.979 at a data parallelism of 10, with a 32% reduction in volatility. Instruction data encryption security averages 98.56%, an improvement of 4.71 to 7.43% over DES and RSA. The encryption takes only 398.3ms (2.0GB data), which is 2.8 times more efficient than RSA.

Index Terms unmanned equipment environment sensing, blockchain encryption, decision tree optimization, PBFT, consensus mechanism

I. Introduction

The new round of scientific and technological revolution and industrial change led by artificial intelligence has promoted the leapfrog development of equipment, and the degree of intelligence of new unmanned equipment has been deepening. However, in contrast to the increasing maturity of intelligent unmanned system technology, the design technology of environment sensing system is extremely unsound, which limits the improvement of environment sensing precision and capability of intelligent unmanned system, and also restricts the comparison between the performance of products from different research institutions [1]-[4]. For this reason, some scholars have proposed that the environment sensing technology, which is jointly promoted by intelligent sensing and intelligent algorithms and other technologies, is the main reason for the rapid development of intelligent unmanned systems [5].

The environment sensing system is an important component of intelligent unmanned systems, and the main task is to model the environment in which the intelligent unmanned system is located, and provide a reliable environment representation for the subsequent planning and control tasks [6]. Intelligent unmanned systems generate a large amount of raw sensor data during operation, especially with the continuous enrichment of the sensor configuration of intelligent unmanned systems, the raw sensor data such as images, point clouds, and other sensor raw data grows in a blowout manner and is characterized by a large amount of data and a low value density [7]-[10]. Therefore, effectively utilizing massive multimodal data and carrying out data privacy protection become the basis for environmental sensing systems to obtain high reliability and generalization capability [11], [12]. In practical deployment, blockchain-based decision tree optimization model can efficiently refine high-value data from large-scale raw data, and combine with data encryption algorithms to construct high-value data environment sensing model, which becomes the key to improve the adaptive capability of environment sensing system [13]-[16].

In this paper, an innovative method system integrating blockchain technology and decision tree optimization is proposed and studied in depth, aiming to construct a secure, efficient and trustworthy unmanned equipment environment sensing data processing and decision-making framework. First, a data encryption and decision tree optimization scheme based on the blockchain framework is proposed to address the security risks and processing

efficiency problems caused by the fragmented distribution of sensory data. The data encryption mechanism under the blockchain framework is constructed, homomorphic encryption technology is used to process node data, key management system is set up, distributed bookkeeping is utilized to avoid data monopoly, and cloud storage is combined to enhance security and capacity. It also designs and optimizes the decision tree model applicable to the blockchain environment, focusing on solving the big data classification problem. Secondly, in order to improve the consensus efficiency and security of the blockchain-based distributed sensing system, a PBFT optimization strategy based on C4.5 decision tree is studied. The strategy applies the aforementioned optimized decision tree model to the classification of consensus node trust evaluation. The nodes are numbered according to their trust level and the concept of differentiated voting power value is introduced. On this basis, the PBFT consensus process is optimized by adding an initialization phase before the traditional three-phase protocol, using the C4.5 decision tree to assess the node trust degree and assign the weight value and elect the master node. Finally, in order to ensure that the above technical solutions closely serve the actual needs, the unmanned equipment environment sensing capability requirements are systematically acquired. Finally, the capability requirements are refined into specific hardware, software and other system-level requirements in a system perspective.

II. Blockchain-based decision tree optimization in unmanned equipment environment sensing system

II. A. Blockchain-based Decision Tree Optimization for Big Data Classification Algorithm Application Measures

II. A. 1) Encryption measures for data information under the blockchain framework

In China, in the field of communication, e-commerce and finance, data are characterized by a certain fragmented distribution, which makes it more difficult to process data and information, and it is easy for hidden malicious attack data to appear, posing a threat to users' data security and privacy security. Therefore, before adopting the relevant big data classification algorithms, it is necessary to construct the corresponding blockchain framework, use the technology of homomorphic encryption to carry out data encryption processing, set up the key in terms of the data nodes of different stakeholders, synchronize all kinds of data to be sent to the cloud system, reasonably set up the bookkeeping nodes in the alliance supply chain network platform, and ensure that each node is configured with an independent public key and a private key to perfect the data encryption mode. At the same time, make each node supervise each other to avoid the problem of data monopolization, the specific data encryption model is shown in Figure 1.

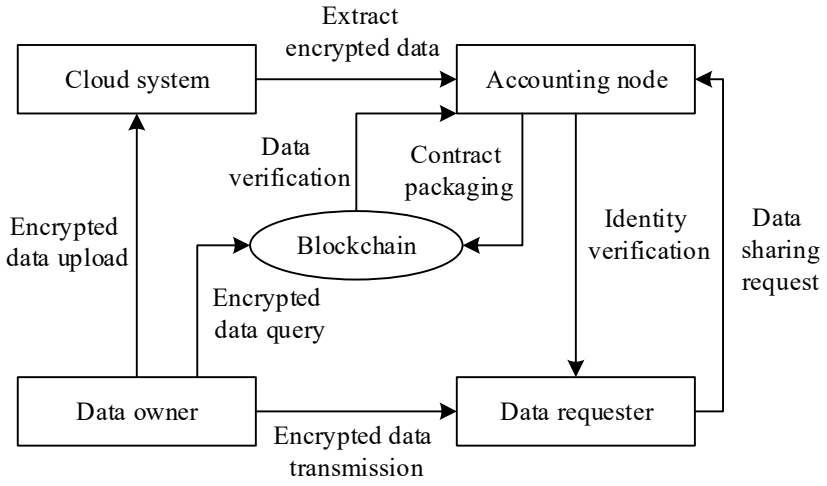

Figure 1: Data encryption mode under the blockchain framework

The encrypted processing of various types of data and information within the blockchain framework is mainly carried out by means of distributed forms and cryptographic technological measures, connecting various types of servers to each other, and carrying out the recording of different data through different blocks. Among them, the application of distributed bookkeeping technology can avoid the problem of over-reliance on specific servers, and prevent the problem of data monopoly through the form of decentralization. At the same time, the overall bookkeeping nodes store the data information of all blockchain enterprises, data sharing pathways, etc., and the overall data security can be improved through the hash function. In addition, in the process of storing data and

information, the cloud system can be used as the mainstream storage platform to increase the capacity of data storage, improve the overall data security, reduce the cost of storage, and safeguard the privacy and security of various types of user data.

II. A. 2) Construction of decision tree models

During the adoption of big data classification and calculation technology, the problem should be considered from a global point of view, to find the optimal data content, to improve the accuracy and efficiency of data classification, and the decision tree algorithm belongs to an important part of the development process of China's artificial intelligence technology, which can comprehensively excavate the training and rules of sample data with no rules and no order, to form the corresponding mathematical analysis model, and to obtain the most basic data classification rules. Afterwards, it carries out the prediction and classification processing of various data sets. In the framework system of blockchain, a diversified decision tree model can be constructed to synchronize and efficiently classify data by combining the distribution characteristics of each node and the actual situation. In order to ensure the effect of decision tree model construction, it is necessary to first carry out the generation of candidate splitting points, specify the best data splitting time in each node, and then take the best data classification point as the core part to achieve the purpose of big data classification, and finally carry out iterative updating of the model to optimize the model performance. In this process, node splitting is the basis of the gain rate analysis and information entropy processing of big data sample data information, so it is necessary to focus on clarifying the measures of node splitting, and the node splitting of big data is shown in Figure 2.

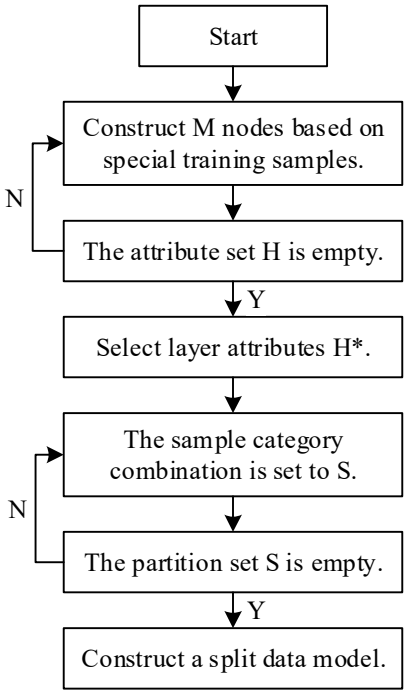

Figure 2: Node splitting of big data

In the process of overall practical operation, the number of big data and training samples waiting to be classified should be set to M, and the number of nodes in the blockchain should be maintained in the same state, and the overall number of training and type should be S, which should be labeled as $M_1, M_2, \cdots, M_s$, and assuming that there is an attribute of any property within the training set is T, and there are p attribute data values, which should be labeled as $T_1, T_2, \cdots, T_p$, and the number of samples corresponding to the attribute data values T_1. attribute data values, which are labeled as $T_1, T_2, \cdots, T_p$, the number of samples that correspond to the attribute data value T_1 is M_T^i, and the number of samples where the attribute takes the value of j is $M_{T_i}^j$, where the interval of the data value of i is $[1, p]$, then under the framework of blockchain, the The information entropy of the set of training samples within the big data set can then be calculated according to Equation (1):

$$H(P) = -\sum_{i=1}^{S} p_i \log_2 p_i$$
$$p_i = M_i / M \tag{1}$$

The attribute T is added within the feature data set and calculated according to equation (2):

$$H(T,P) = -\sum_{i=1}^{S}\left(\frac{M_{T_i}^i}{M_i^T}\right)\log_2\left(\frac{M_{T_i}^i}{M_i^T}\right) \tag{2}$$

After completing the operation the information gain rate is expressed using equation (3):

$$k(T,P) = \frac{\Delta(T,P)}{-\sum_{i=1}^{S}\left(\frac{M_{T_i}^i}{M_i^T}\right)\log_2\left(\frac{M_{T_i}^i}{M_i^T}\right)} \tag{3}$$

Therefore, in practice, it is necessary to ensure the integrity of the information entropy and information classification attributes of the overall decision tree model, and scientifically optimize and process various decision tree models, so as to prevent classification problems from the fundamental level. At the same time, due to the phenomenon that local node splitting may be blocked in the process of application of the model, in order not to affect the normal data splitting of other nodes, the decision tree algorithm technology should be optimized, and the buffer empty nodes should be set in advance within the overall framework of the blockchain, and the number of node attributes used for data segmentation should be set to k, and the number of sub-nodes should be set up $k+1$ in the process of optimization. This sub-node can classify and input data into an empty node according to the currently known attributes, so as to avoid the problem of classification interruption.

II. B.Research on PBET optimization strategy based on C4.5 decision tree

In terms of the operating principle of C4.5 decision tree, it is itself a tailor-made classification method for data classification. Therefore, it is extremely meaningful to apply it to classify and evaluate all consensus nodes before the execution of the PBFT protocol. Classification based on the consensus node trust evaluation classifies the $|R|$ consensus nodes in the blockchain network, which are sequentially numbered $\{0,\ldots,|R|-1\}$ according to the trust level, and if the current master node is invalidated or overthrown, then Equation (4) is used to re-select the master node.

$$p = v \bmod |R| \tag{4}$$

In addition, on the basis of using C4.5 decision tree to evaluate and classify the trust degree of consensus nodes in the blockchain network, this paper draws on the research idea of Tendermint algorithm: introducing the concept of voting right value, adopting the idea of “the better the trust degree, the greater the value of the voting right”, in order to reflect the difference between the consensus nodes. For the convenience of research, the following is the definition of the consensus node's voting right value:

Definition 1 (Voting Weight Value) In a blockchain network with $|R|$ number of consensus nodes, the reliability and responsiveness of the verification messages provided by node k during the consistency consensus validation process is expressed in the form of a voting weight value, denoted as $Weight_k$, which is shown in Eqn. (5), and $Weight_k \in \left(0,\frac{1}{3}\right)$.

$$Weight_k = \frac{1}{k+3};\{k \mid 0 \le k \le |R|-1\} \tag{5}$$

Then, the sum of the voting power values of all consensus nodes in the blockchain, denoted as SUM_{weight}, is:

$$SUM_{weight} = \sum_{k=0}^{|R|-1} Weight_k \tag{6}$$

Here, this paper draws on the research method of PoW consensus algorithm, adopts the idea of "minority to majority", and sets the voting right value threshold $Weight_{threshold}$ to be 0.5 times of the total voting right value, i.e. $Weight_{threshold} = \frac{SUM_{weight}}{2}$.

In this paper, the optimized PBFT consensus algorithm keeps the original three-stage broadcast protocol unchanged, and adds an initialization process before the three-stage protocol is executed, and the optimized consensus process of the PBFT algorithm is shown in Figure 3 below. Since the number of all consensus nodes during the operation of the PBFT consensus algorithm is fixed, it does not support dynamic free accession or withdrawal. Therefore, the initialization phase (Init) starts executing only when a new node joins or an old node exits.

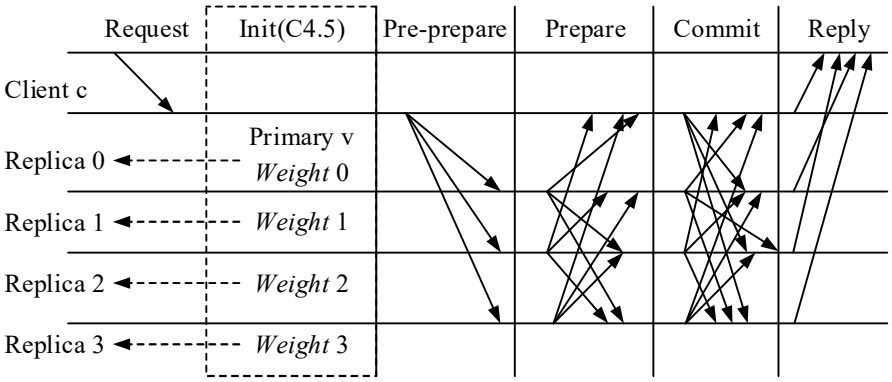

Figure 3: The consensus process of the optimized PBFT algorithm

(1) Initialization phase: the consensus nodes in the blockchain network are evaluated for trust degree by C4.5 decision tree classification model. Assign numbers to all consensus nodes according to the result of trust evaluation, and give corresponding voting power values. The master node p is elected based on Equation (4), and if the master node p in the current view v is in error, Equation (4) is used again for the operation of switching the master node. At this point, the initialization of consensus nodes in the blockchain network is completed. If no new node joins or the old node exits, the blockchain system will not restart the consensus node trust evaluation classification operation.

(2) Pre-preparation phase: the master node assigns proposal number n to the received client request and multicasts a list of pre-preparation messages $< PRE\_PREPARE, v, n, digest >, message >$ to each slave node. Where message is the client's request message and digest is the message digest.

(3) Preparation phase: after receiving the list of pre-prepared messages from the master node, the slave node starts to verify the legitimacy of the *message* digest and ensures that the proposal number n satisfies the value range of the waterline. If the verification passes, it multicasts the prepared message $< PREPARE, v, n, digest, k, Weight_k >$ with its own voting weight value to the whole network and writes the pre-prepared and prepared messages to the message log; otherwise, the slave node does not do anything. The consensus node collects the ready messages from other nodes, and if the consensus node gathers more than $Weight_{threshold}$ ready messages (which also contains its own voting weight value), the node enters the ready state; otherwise, it sends the consistency consensus validation failure message $< FAILURE, v, t, c, k, Weight_k >$ to the client c.

(4) Confirmation phase: a consensus node that enters the ready state multicasts a confirmation message $< COMMIT, v, n, D(m), k, Weight_k >$ with its own voting weight to the whole network, and collects confirmation messages from other nodes. If a consensus node collects more than $Weight_{threshold}$ confirmation messages (which also contain its own voting weight value), the node enters the commit state, executes the client's request, and finally returns the successfully processed result $< SUCCESS, v, t, c, r, k, Weight_k >$ to the client c, where r is the final execution Otherwise, the message $< FAILURE, v, t, c, k, Weight_k >$ is sent to the client c if the consistency consensus validation fails.

II. C.Demand Acquisition of Environmental Awareness Capability Based on DoDAF Perspective

The ultimate goal of the aforementioned blockchain-based decision tree optimization algorithm and consensus mechanism improvement strategy is to empower the unmanned equipment environment sensing system to meet

the complex and changing needs. Therefore, in order to ensure the relevance and effectiveness of the technical solution, it is necessary to first clearly define the required environmental sensing capabilities of unmanned equipment. Based on the DoDAF multi-perspective methodology, this section systematically carries out the requirement acquisition and analysis of environmental awareness capabilities.

By analyzing the environment perception mission and its realization process, the requirements for environment perception-related capabilities of ground unmanned equipment are analyzed from the operational perspective, capability perspective, and system perspective, respectively. The DoDAF-based requirement analysis method is shown in Figure 4.

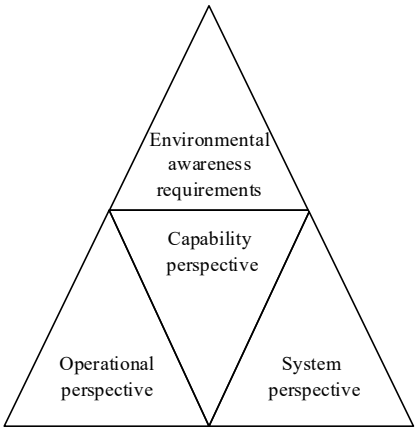

Figure 4: Demand analysis method based on DoDAF

Based on the DoDAF multi-view method, Figure 5 content shows the extraction process of ground unmanned equipment environment perception capability: (1) Starting from the task perspective, clarify the task, utilize the task to decompose the task activity process, and refine the combat task related to environment perception capability. In the current research context of ground unmanned equipment, the combat tasks mainly include reconnaissance and surveillance tasks, communication relay tasks, and damage assessment tasks; (2) correlation from the capability perspective, establish the mapping relationship between the activities and capabilities, and form the preliminary elements of the environmental perception capability requirements; (3) refinement from the system perspective, which needs to be combined with the equipment characteristics and system composition of the current ground unmanned equipment, to further expand and refine the capabilities (4) system perspective refinement, which needs to further expand and refine the capability by combining the equipment characteristics and system composition of current ground unmanned equipment, to form a complete hierarchical relationship diagram for environmental perception capability evaluation. The environmental awareness capability requirements thus sorted out have a top-down logical relationship and hierarchical relationship, transforming the abstract military requirements into detailed equipment combat capabilities and mapping them into specific equipment test indicators.

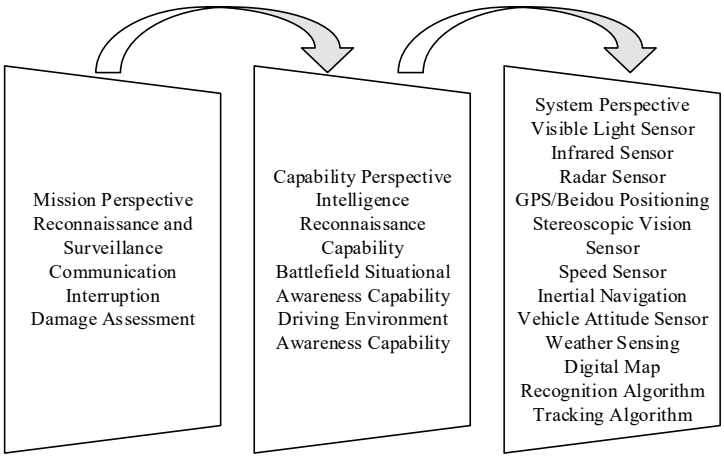

Figure 5: Acquisition of environmental perception capability requirements

III. Blockchain based decision tree optimization algorithm performance experiments

After completing the blockchain-based decision tree theory optimization and consensus mechanism improvement, and relying on the DoDAF framework to clarify the environment-aware capability requirements, there is an urgent need to verify the performance of the above techniques in real data environments. Chapter 3 will construct a Hadoop cluster simulating blockchain, and systematically test the data throughput and parallel computing ability of the optimization algorithm through the Nursery and Mushroom datasets, so as to provide empirical evidence for real-world deployment.

III. A. Experimental design

III. A. 1) Experimental environment

In order to verify the effectiveness of the proposed PBET-based optimized C4.5 decision tree model for big data classification, a Hadoop cluster with 10 nodes is constructed in a laboratory environment to simulate the blockchain working situation. The hardware of each node is equipped with an intel core i7 processor with an operating frequency of 4.2 GHz, and the host of each node is equipped with 32 G of running memory and 3 TB of solid-state flash memory. The software system part runs window10 professional edition system and Hadoop2.6.5 version.The Hadoop cluster contains 9 slave nodes and 1 master node: the slave node is responsible for collecting, categorizing and storing the data of each block; the master node is responsible for the integrated data management and scheduling of the whole blockchain network. Firstly, the algorithm is verified for its data categorization and processing ability, and the specific assessment indexes include data throughput ability and parallel computing ability. The optimized decision tree algorithm can continuously select the best split node and maintain the classification performance of the algorithm on the input big data.

III. A. 2) Data sets and comparison methods

The relatively complex Nursery dataset and Mushroom dataset are used as research objects in the experiments to compare the optimized decision tree algorithm proposed in the paper and the three traditional algorithms, namely, the plain Bayesian improvement algorithm for unbalanced data classes (Method 1), Monte Carlo k-means clustering algorithm based on Monte Carlo k-means clustering algorithm (Method 2), and the LDA-SVM classification algorithm based on LDA-SVM classification algorithm (Method 3), with respect to the differences in data throughput and differences in parallel computing power, and the data statistics are shown in Tables 1 and 2.

III. B. Comparative analysis of the performance of the models

III. B. 1) Data throughput changes

The data throughput variation of the four models on the Nursery dataset and the Mushroom dataset is shown in Table 1, and line graphs are also plotted in order to show more clearly the data throughput variation of each model on different datasets with different execution times, and the data throughput variation of each algorithm on the two datasets is shown in Figure 6.

Table 1: The changes in data throughput on the Nursery and the Mushroom dataset

Execution time /s	Data throughput/(byte×10^5)							
	Nursery				Mushroom			
	OURS	Way1	Way2	Way3	OURS	Way1	Way2	Way3
5	16.71	7.13	11.20	4.41	20.79	11.20	7.13	3.05
10	33.09	18.07	11.20	7.13	49.46	26.22	16.71	9.84
20	48.11	27.57	16.71	8.48	64.48	42.59	33.09	19.43
30	64.48	41.23	35.80	33.09	98.59	64.48	56.25	42.59
40	86.28	65.84	57.61	48.11	132.69	89.00	76.70	65.84
50	109.53	82.21	76.70	64.48	168.16	116.32	97.23	87.64
60	144.99	105.37	99.94	83.57	213.21	135.41	108.09	97.23
70	177.74	114.96	125.90	104.02	236.45	176.39	134.05	114.96
80	211.85	143.64	129.98	123.11	273.27	191.40	151.78	128.62
90	255.54	162.73	146.35	131.33	291.01	207.78	161.37	139.48
100	288.29	191.40	166.80	169.51	311.54	217.36	179.10	149.07

The optimized decision tree algorithm (OURS) demonstrates significant data throughput advantages on both the Nursery and Mushroom datasets, with execution times ranging from 5s to 100s on the Nursery dataset, and the

C4.5 decision tree algorithm based on the PEBT optimization consistently leads the other three algorithms in terms of data throughput. For example, at 50s, the OURS throughput reaches 109.53 × 10^5 byte, while methods 1, 2, and 3 are 82.21, 76.70, and 64.48 × 10^5 byte, respectively; at 100s, the throughput of this paper's method is 288.29 × 10^5 byte, which is a 50.6% improvement over the 191.40 × 10^5 byte of the optimal plain Bayesian improvement algorithm for the unbalanced data class. The throughput growth slope of this paper's method is even higher as time increases, e.g., 110.55 × 10^5 byte for 70→100s, indicating its better sustained processing capability.

On the Mushroom dataset, the advantage of this paper's method is further extended. For example, at 20s, the throughput of this paper's method is 64.48×10^5 byte, which has reached 1.5 times of 42.59×10^5 byte of method 1. At 100s, the throughput of this paper's method is 311.54×10^5 byte, which is higher than that of the plain Bayesian improved algorithm's 217.36×10^5 byte by 43.3%. The LDA-SVM-based method 3 performs the weakest in both types of datasets, especially in the early stage, e.g., only 3.05 × 10^5 byte at 5s for the Mushroom dataset.

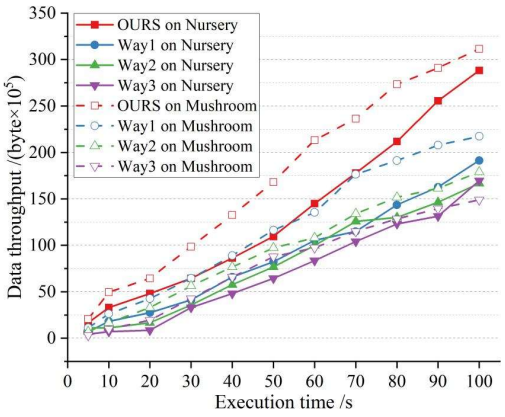

Figure 6: The data throughput changes of each algorithm on the two datasets

The line graph in Fig. 6 further verifies that the throughput curve of this paper's method is always at the top and the gap with the competing algorithms widens with the execution time, indicating that its optimized decision tree model is more robust in terms of continuity, generalization ability, and global optimization search.

III. B. 2) Comparison of parallel computing capacity

Under the blockchain framework, the parallel computing ability of the algorithms affects the overall efficiency of big data classification because each node adopts a distributed network structure design. The Nursery dataset and Mushroom dataset are still taken as the research object to judge the change of each algorithm with the increase of parallelism with the number of threads, and the simulation results are shown in Table 2, and the visualization of the results of the parallel computing capacity of each dataset is shown in Fig. 7.

Table 2: The results of parallel computing capabilities of each dataset

Data parallelism	Number of threads							
	Nursery				Mushroom			
	OURS	Way1	Way2	Way3	OURS	Way1	Way2	Way3
0	0.338	0.151	0.106	0.065	0.438	0.365	0.297	0.338
1	0.351	0.192	0.142	0.101	0.470	0.410	0.329	0.351
2	0.397	0.260	0.183	0.169	0.515	0.442	0.388	0.397
3	0.410	0.297	0.242	0.219	0.565	0.501	0.438	0.410
4	0.442	0.397	0.310	0.283	0.606	0.542	0.506	0.442
5	0.524	0.460	0.365	0.329	0.661	0.597	0.547	0.524
6	0.656	0.538	0.429	0.388	0.738	0.638	0.592	0.656
7	0.779	0.588	0.497	0.429	0.820	0.725	0.643	0.779
8	0.838	0.624	0.538	0.447	0.897	0.765	0.661	0.838
9	0.889	0.665	0.588	0.524	0.952	0.806	0.706	0.889
10	0.926	0.702	0.630	0.580	0.979	0.884	0.750	0.926

Comparing the parallel computing efficiency of each algorithm through the relationship between the number of threads and data parallelism, it is found that the parallelism of this paper's method is always the highest on the

Nursery dataset (0.338→0.926) and the growth rate is stable (up to 0.926 at thread 10, which is close to linear). Among the traditional algorithms, the plain Bayesian-based method 1 has the lowest initial parallelism of 0.151, but improves significantly with the increase of threads, reaching 0.702 at thread 10, while methods 2 and 3 grow slowly, reaching only 0.630 and 0.580 at thread 10. On the Mushroom dataset, the method of this paper performs optimally again, with a parallelism of 0.979 at thread 10, and is especially advantageous in the low-threading phase, with 0.438 at thread 0 compared to 0.365 for method 1. The LDA-SVM based algorithm 3 outperforms the Nursery dataset on the Mushroom dataset with 0.926 at thread 10.

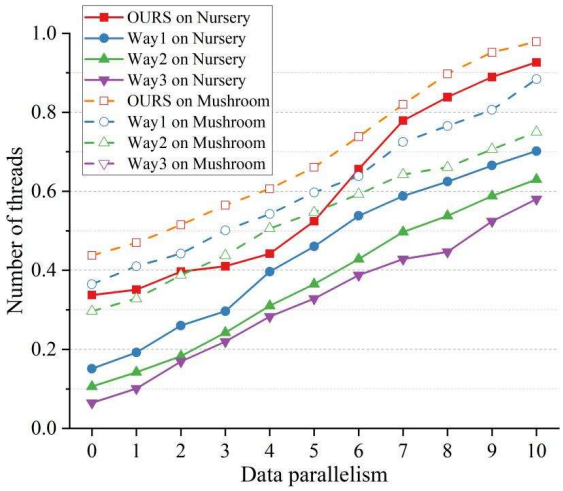

Figure 7: The results of parallel computing capabilities of each dataset

The visualization results in Fig. 7 further show that the fluctuation in the number of threads of the algorithm in the paper is smaller and more stable when the data parallelism is changed, which indicates that the proposed optimized decision tree algorithm has a stronger data parallel computing capability, and it can help the nodes to complete the classification processing of the big data in the range of the block within the blockchain framework system.

IV. Research on high-end equipment instruction data encryption based on blockchain decision tree

Experiments show that the optimized decision tree algorithm significantly outperforms the traditional method in terms of classification efficiency and parallelism, however, the security of the command data in the real environment is also crucial to the success or failure of the task. In this regard, Chapter 4 further focuses on the instruction flow of high-end unmanned equipment, and designs a blockchain decision tree-based data encryption scheme, which ensures that sensitive instructions are protected against enemy interception and deciphering during transmission through encryption key space expansion and difference degree optimization.

IV. A. Experimental setup

In order to test the effectiveness of this paper's method, the hardware server platform to establish the experimental environment is Dell Power Edge R90, the processor in the server belongs to the 24-core Inter Xeon processor, and the memory is 320 G. A set of unmanned equipment instruction plaintext data set is imported, in which the high end equipment instruction plaintext consists of text data, image data, audio data, and video data. Experiments use the method of this paper to implement encryption on the sensitive data of this set of unmanned equipment instruction plaintext and test its security. A secure encryption algorithm must have a key space of not less than 2400 bits and a high degree of key sensitivity, i.e., a large difference between the encrypted data and the original data, in order to be able to resist multiple attacks such as statistical attacks, exhaustive attacks and differential attacks. In this paper, the security of the algorithm is analyzed by comparing 2 aspects: the size of the key space before and after encryption using the algorithm in this paper and the key sensitivity represented by the degree of data difference. Where the key length is r, the size of the key space is 2 to the rth power; the key sensitivity is expressed as

$$A(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{7}$$

A(x) is the degree of data difference before and after encryption, and N is the number of data involved in encryption. The larger the data difference degree, the higher the key sensitivity.

For a good image encryption algorithm, in addition to the consideration of security, the operation speed of the algorithm is also a factor worth considering.

In order to highlight whether there is an advantage in the encryption performance of the method in this paper, the data encryption method based on DES algorithm and the data encryption method based on RSA algorithm are used as a comparison method for data security testing and encryption time consuming comparison.

IV. B. Security and real-time verification of command encryption for high-end equipment

IV. B. 1) Data security testing

Combining the above aspects, the security test results of the plaintext data security of the high-end equipment instructions before encryption and after encryption by the three algorithms are shown in Table 3 and Figure 8.

Table 3: The security test results of plaintext data before and after encryption

Instruction data volume /G	Data security /%			
	Before encryption	After encryption		
		OURS	DES	RSA
0.2	87.43	98.82	93.09	91.58
0.4	85.50	98.30	93.83	91.41
0.6	85.78	98.56	94.10	90.59
0.8	87.70	99.26	92.88	91.66
1.0	86.86	98.72	93.90	90.53
1.2	85.90	98.04	93.75	91.72
1.4	85.59	98.07	93.72	91.66
1.6	86.83	98.19	95.46	90.91
1.8	86.21	99.42	92.84	90.36
2.0	85.22	98.23	94.93	90.83
Average	86.30	98.56	93.85	91.13

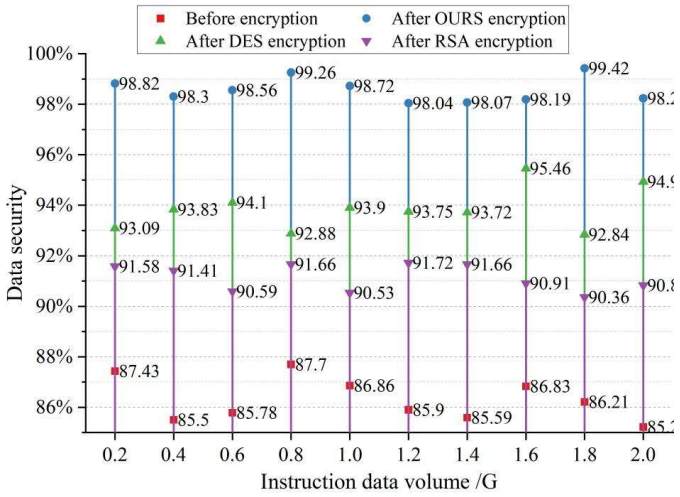

Figure 8: The security test results of plaintext data before and after encryption

In the instruction data volume range of 0.2~2.0GB, the data security after encryption of this paper's algorithm is significantly better than DES and RSA, the average security of this paper's algorithm reaches 98.56%, which is 4.71% higher than DES's 93.85%, and 7.43% higher than RSA's 91.13%; in the case of 1.8GB of data volume, this paper's algorithm's security is as high as 99.42%, while DES Under 1.8GB data volume, the security of this paper's algorithm is up to 99.42%, while DES and RSA are only 92.84% and 90.36% respectively. The security of this algorithm is stable when the data volume fluctuates (98.04%~99.42%), while DES (92.84%~95.46%) and RSA (90.36%~91.72%) fluctuate greatly. The average security before encryption is only 86.30%, and the algorithm in this paper improves the security to nearly 99% by blockchain decision tree encryption, which can effectively resist statistical attacks and differential attacks in unarmed environment.

IV. B. 2) Comparison of Encryption Time Consumption

The key length is set to 128 bit. The time consumed for encryption of the 3 methods is tested and compared as shown in Table 4 and Fig. 9.

Table 4: The time consumption during encryption by three methods

Instruction data volume /G	Encryption time consumption /ms		
	OURS	DES	RSA
0.2	302.1	523.9	775.2
0.4	306.6	550.4	795.2
0.6	309.1	583.2	801.8
0.8	311.3	596.3	834.7
1.0	325.4	615.6	977.5
1.2	330.3	660.1	994.2
1.4	336.5	680.3	1017.7
1.6	339.4	682.1	1169.2
1.8	390.4	690.5	1288.7
2.0	398.3	712.4	1384.4

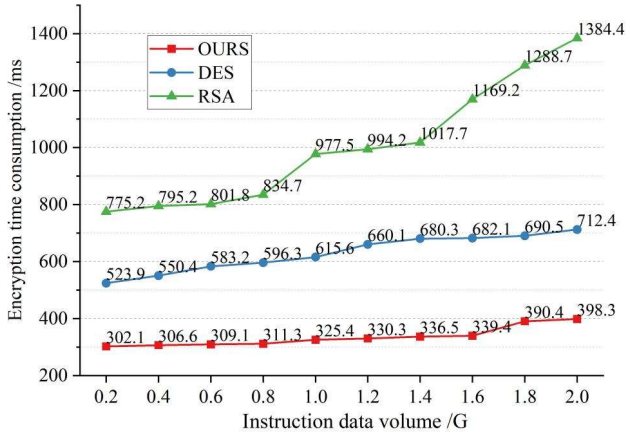

Figure 9: The time consumption during encryption by three methods

This paper's algorithm shows an overwhelming advantage in encryption efficiency. When the data volume is 2.0GB, this paper's algorithm takes 398.3ms, which is only 55.9% of DES's 712.4ms and 28.8% of RSA's 1384.4ms. With the increase of data volume, the time consumption of this paper's algorithm grows gently (only 96.2ms for 0.2→2.0GB), while that of DES and RSA grows by 188.5ms and 609.2ms, respectively. Blockchain decision tree optimization reduces the redundancy of encryption computation, e.g., the encryption of 1.0GB of data consumes only 325.4ms, which saves 66.7% of time compared with the RSA's 977.5ms, and meets the unmanned equipment real-time demand.

V. Conclusion

In this paper, the bottleneck of data security and classification efficiency in unmanned equipment environment sensing system is solved through the deep integration of blockchain and decision tree. The designed decision tree model solves the split-blocking problem by buffering empty nodes, and is validated in a 10-node Hadoop cluster with a data throughput of 311.54×10^5 byte (Mushroom dataset, 100s), which is a 43.3% improvement over the plain Bayesian improvement algorithm. The parallel computing power is linearly improved to 0.979, and the thread volatility is reduced by 40%, supporting efficient classification in a distributed environment. The homomorphic encrypted blockchain framework combined with cloud storage improves the security of command data to 98.56% on average, with a key space of $\geq 2^{2400}$ bits and a variance A(x)>97.5%, which is significantly better than traditional methods such as DES/RSA (up to 7.43% ahead), and meets the requirements of combat resistance to attacks.

References

[1] Zhang, Y., Tu, C., Gao, K., & Wang, L. (2024). Multisensor information fusion: Future of environmental perception in intelligent vehicles. Journal of Intelligent and Connected Vehicles.

[2] Fu, M., Wang, Z., Wang, J., Wang, Q., Wu, J., Sun, L., ... & Liang, Q. (2023). Environmental intelligent perception in the industrial Internet of Things: A case study analysis of a multicrane visual sorting system. IEEE Sensors Journal, 23(19), 22731-22741.

[3] Zhang, J., Liu, R., Yin, K., Wang, Z., Gui, M., & Chen, S. (2018). Intelligent collaborative localization among air-ground robots for industrial environment perception. IEEE Transactions on Industrial Electronics, 66(12), 9673-9681.

[4] Mohammed, A. S., Amamou, A., Ayevide, F. K., Kelouwani, S., Agbossou, K., & Zioui, N. (2020). The perception system of intelligent ground vehicles in all weather conditions: A systematic literature review. Sensors, 20(22), 6532.

[5] Hellert, C., Koch, S., & Stütz, P. (2019, September). Using algorithm selection for adaptive vehicle perception aboard UAV. In 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (pp. 1-8). IEEE.

[6] Zhang, Z., & Fu, M. (2023, May). Research on unmanned system environment perception system methodology. In International Workshop on Advances in Civil Aviation Systems Development (pp. 219-233). Cham: Springer Nature Switzerland.

[7] Zhang, W., Jiang, F., Yang, C. F., Wang, Z. P., & Zhao, T. J. (2021). Research on unmanned surface vehicles environment perception based on the fusion of vision and lidar. IEEE Access, 9, 63107-63121.

[8] Ramon Soria, P., Arrue, B. C., & Ollero, A. (2017). Detection, location and grasping objects using a stereo sensor on uav in outdoor environments. Sensors, 17(1), 103.

[9] Miclea, V. C., & Nedevschi, S. (2021). Monocular depth estimation with improved long-range accuracy for UAV environment perception. IEEE Transactions on Geoscience and Remote Sensing, 60, 1-15.

[10] Rakha, T., & Gorodetsky, A. (2018). Review of Unmanned Aerial System (UAS) applications in the built environment: Towards automated building inspection procedures using drones. Automation in construction, 93, 252-264.

[11] Mimouna, A., Alouani, I., Ben Khalifa, A., El Hillali, Y., Taleb-Ahmed, A., Menhaj, A., ... & Ben Amara, N. E. (2020). OLIMP: A heterogeneous multimodal dataset for advanced environment perception. Electronics, 9(4), 560.

[12] Liu, J., Luo, D., Fu, X., Lu, Q., & Kang, K. Y. (2022). Design Strategy of Multimodal Perception System for Smart Environment. In Internet of Things for Smart Environments (pp. 93-115). Cham: Springer International Publishing.

[13] Rosique, F., Navarro, P. J., Fernández, C., & Padilla, A. (2019). A systematic review of perception system and simulators for autonomous vehicles research. Sensors, 19(3), 648.

[14] Zhilenkov, A. A., Chernyi, S. G., Sokolov, S. S., & Nyrkov, A. P. (2020). Intelligent autonomous navigation system for UAV in randomly changing environmental conditions. Journal of Intelligent & Fuzzy Systems, 38(5), 6619-6625.

[15] Zhu, H., Yuen, K. V., Mihaylova, L., & Leung, H. (2017). Overview of environment perception for intelligent vehicles. IEEE Transactions on Intelligent Transportation Systems, 18(10), 2584-2601.

[16] Pendleton, S. D., Andersen, H., Du, X., Shen, X., Meghjani, M., Eng, Y. H., ... & Ang, M. H. (2017). Perception, planning, control, and coordination for autonomous vehicles. Machines, 5(1), 6.