



Article

Intelligent and Secure Cloud–Edge Collaborative Industrial Information Encryption Strategy Based on Credibility Assessment

Aiping Tan ¹, Chenglong Dong ¹, Yan Wang ^{1,*}, Chang Wang ¹ and Changqing Xia ^{2,3}

¹ School of Cyber Science and Engineering, Liaoning University, Shenyang 110016, China; aipingtan@lnu.edu.cn (A.T.); 4032232392@smail.lnu.edu.cn (C.D.); 4032232409@smail.lnu.edu.cn (C.W.)
² State Key Laboratory of Robotics, Shenyang 110016, China; xiachangqing@sia.cn
³ Shenyang Institute of Automation, Shenyang 110016, China
* Correspondence: wang_yan@lnu.edu.cn

Abstract: As industries develop and informatization accelerates, enterprise collaboration is increasing. However, current architectures face malicious attacks, data tampering, privacy issues, and security and efficiency problems in information exchange and enterprise credibility. Additionally, the complexity of cyber threats requires integrating intelligent security measures to proactively defend against sophisticated attacks. To address these challenges, this paper introduces an intelligent and secure cloud–edge collaborative industrial information encryption strategy based on credibility assessment. The proposed strategy incorporates adaptive encryption specifically designed for cloud–edge and edge–edge architectures and utilizes attribute encryption to control access to user-downloaded data, ensuring secure information exchange. A mechanism for assessing enterprise credibility over a defined period helps maintain a trusted collaborative environment, crucial for identifying and mitigating risks from potentially malicious or unreliable entities. Furthermore, integrating intelligent threat detection and response systems enhances overall security by continuously monitoring and analyzing network traffic for anomalies. Experimental analysis evaluates the security of communication paths and examines how enterprise integrity influences collaboration outcomes. Simulation results show that this approach enhances enterprise integrity, reduces losses caused by harmful actors, and promotes efficient collaboration without compromising security. This intelligent and secure strategy not only safeguards sensitive data but also ensures the resilience and trustworthiness of the collaborative network.

Keywords: cloud–edge collaboration; information security; attribute encryption; credibility assessment



Citation: Tan, A.; Dong, C.; Wang, Y.; Wang, C.; Xia, C. Intelligent and Secure Cloud–Edge Collaborative Industrial Information Encryption Strategy Based on Credibility Assessment. *Appl. Sci.* **2024**, *14*, 8812. <https://doi.org/10.3390/app14198812>

Academic Editors: Luis Javier Garcia Villalba and Eui-Nam Huh

Received: 16 May 2024

Revised: 8 August 2024

Accepted: 16 September 2024

Published: 30 September 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the continuous development of the industrial Internet, the number of industrial IoT devices is increasing, generating more real-time data. Traditional cloud processing methods lead to resource waste and increased pressure on network, computational, and storage resources. Additionally, device heterogeneity introduces security issues, with edge devices being particularly vulnerable to data leakage and system instability. Utilizing edge information processing capabilities can promote data exchange between edge nodes, reducing overall network burden, and employing dynamically adjustable privacy protection policies can enhance data security and system stability. However, establishing a robust cloud–edge cooperative architecture faces two main challenges: insufficient data exchange between edge nodes, and the security and timeliness of data transmission.

Recent advances in intelligence techniques have significantly enhanced our ability to perceive, understand, and control the physical world, impacting production and lifestyles. Yet, their rapid deployment in critical services raises security and privacy concerns due to vulnerability to malicious attacks. Drawing inspiration from the characteristics of

the natural world, intelligent computing finds widespread application today in problem-solving endeavors. By analyzing and crafting algorithms rooted in natural principles, intelligent computing offers a suite of benefits including self-learning, self-organization, and self-adaptation. Its versatility has led to its integration across various domains. Key methodologies within intelligent computing encompass evolutionary computation, fuzzy set theory, neural network computation, and swarm intelligence computation. Continuously influenced by biological intelligence, intelligent computing tackles challenges of increasing complexity.

In the current research on cloud edge collaboration, how to make the connection between the edges closer and guarantee security while maintaining efficient information exchange is receiving more and more attention from scholars. In different fields, the cloud has more and more applications [1–4]; the cloud can effectively help to reduce the cost of information silos from the original to modern industrial data transformation. There are more and more scholars that are beginning to study Cloud–Edge Collaborative Storage (CECS), allowing the cloud to quickly respond to requests from IoT devices and easily share IoT data with users [5,6]. The cloud has many benefits, but despite the convenience it brings, it also raises many security concerns. Edge endpoints are vulnerable to attacks and counterfeiting, and edge data are susceptible to theft and tampering [7,8], posing new challenges for enhanced edge security [9,10].

To promote a robust Industrial Internet of Things (IIoT) ecosystem, it is crucial to address two main challenges: ensuring secure and timely data exchange, and establishing enterprise credibility. Current encryption frameworks focus on the cloud, where all data are processed before being distributed, but this approach can lead to inefficiencies and high costs. Edge-to-edge interactions, while faster, are prone to security risks, with edge nodes potentially becoming targets for malicious attacks. These vulnerabilities underscore the need for a collaborative architecture that balances security, efficiency, and enterprise credibility.

This paper contributes to the field of industrial information security and cloud–edge collaboration with a focus on architectural innovation. The key contributions are as follows:

- We propose a comprehensive cloud–edge collaborative architecture for industrial cooperation, enabling the seamless interaction between upstream and downstream enterprises while incorporating cloud-based oversight. This structure supports coordinated supervision and collaboration within the Industrial Internet of Things (IIoT) framework.
- To address security and efficiency concerns in data transmission among traditional enterprises, we introduce an adaptive encryption strategy tailored for cloud–edge and edge–edge scenarios. This approach balances secure data transmission with low latency, improving communication efficiency across industrial collaborations.
- Recognizing the importance of enterprise credibility, we propose a mechanism for assessing corporate integrity. This involves periodic collaborative supervision by third-party trusted institutions to ensure quality control and other critical aspects of industrial collaboration.

2. Industrial Cloud–Edge Collaboration

In this section, the relevant research on cloud edge collaboration and security is introduced, describing the rapid development of cloud computing due to its data-intensive processing capabilities but also the challenges faced in terms of low latency and security. At the same time, in real industrial IoT business, it is necessary for edge nodes to establish a good evaluation system, protect the trust relationship between data transactions, and achieve win–win cooperation.

2.1. Related Research

In a study on mobile target defense, Lei et al. [11] propose an optimal strategy selection method for mobile target defense based on Markov game theory. The article first introduces

the information asymmetry of network attackers scanning, collecting, and exploiting vulnerabilities in network system resources, as well as the limitations of existing network defense technologies. The author points out the asymmetry between network attacks and defense, as well as the difficulty of existing defense methods in effectively dealing with complex network intrusions. To address this dilemma, the author proposes the concept of mobile target defense (MTD), which changes the properties of network elements through control, making the network random, dynamic, and heterogeneous, thereby increasing the difficulty for attackers. The author analyzes in detail the process of MTD attack defense confrontation, including non-cooperative, dynamic, and Markov characteristics, constructs an MTD model based on the Markov game, and designs an optimal strategy selection algorithm. In the case study, the author validates the effectiveness of the proposed MG-MTD model and optimal strategy selection algorithm. As mentioned in the article, existing game models in research are often built based on specific MTD scenarios, which limits the universality of the models. This may affect the accuracy and practicality of the proposed optimal strategy in different specific situations. Although the importance of considering defense costs in strategy selection is mentioned, the specific defense costs are not fully considered in the benefit function and standard function. In their 2022 work, Tan et al. [12] focus on the imperfect rationality of both the attack and defense ends; most existing MTD research has focused on strategy design and formulation, neglecting strategy selection and lacking quantitative analysis. They construct the WF-MTD model for mobile target defense strategy evolution based on the Wright–Fisher process. The author abstracts the mobile target defense strategy as a dynamic diversity redundancy transformation of network vulnerabilities, known as the DDR-MTD strategy. By quantifying the reasonable degree of attackers and mobile target defenders to distinguish different participants, it ensures good scalability and is suitable for different attacker behaviors. Finally, a medical information network system is selected as their test case to verify the performance of their proposed model. The article mentions that decision-makers need to have sound memory and computing power, and the dynamic game process will occupy a considerable amount of resources, which may be a challenge for edge devices with scarce computing resources. Our proposed strategy is based on dynamic changes in the environment, requiring only monitoring gateway data and conducting an initial evaluation of transmission tasks to maximize privacy protection.

2.2. Cloud–Edge Collaboration

Cloud computing [13,14] is growing rapidly because it can provide flexible services and data-intensive processing power to end users over a wide area network (WAN). Users can use a large amount of computing resources through the cloud without having to build a new computing infrastructure. However, targeting low-latency and high-computational-performance IoT applications [15] such as ultra-high-definition video, augmented reality (AR), and virtual reality (VR), challenges the traditional cloud’s scalable and flexible computing model. Edge servers have relatively low compute and storage capacity but have advantages such as low latency and flexible distribution. However, edge computing also poses complex resource management problems because end devices at the access side are characterized by fast business demands, high mobility, and large data volumes.

For aspects related to the cloud, historically, many companies have grown and expanded from evolving technology and innovation. Cloud computing is seen as a unique solution for delivering applications to businesses [16,17]. It uses different components to deliver services, especially for Internet businesses. However, most studies do not consider the importance of edge services, and the security of data transfer between edges is very understudied. For the automotive industry chain as shown in Figure 1, for the different components of the car, it usually requires multiple enterprises to work together, and these IoT device data can greatly reduce the network and computational pressure if they can directly circulate with each other among enterprises.

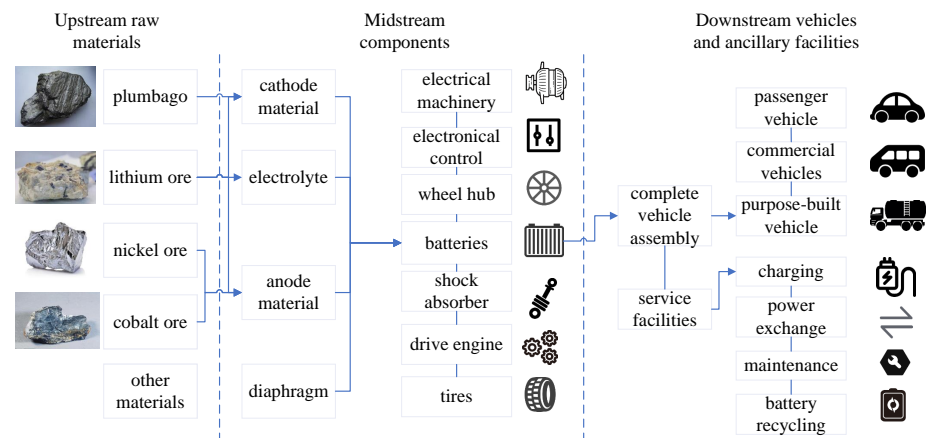


Figure 1. Industrial collaboration architecture diagram under IIoT.

2.3. Cloud–Edge Security

For data storage security in cloud service environment, a series of data privacy management, data transmission encryption, data access control [18], authentication service [19], security audit [20] and other security mechanisms ensure the availability, confidentiality, and non-repudiation of the data in the cloud storage system, thus improving the security of the data. In order to guarantee the data security of edge computing, the network communication encryption technology of computer can be utilized to encrypt the channel and effectively guarantee the security of edge computing data communication.

Currently, some scholars believe that the different computing paradigms from cloud computing to edge computing have formed a unique ecosystem [21]. And for the edge end, Gamage et al. [22] conduct an objective comparison and evaluation using different deep learning models to protect the security well with intrusion detection techniques. Alsaadi [23] proposes a new model of network intrusion detection based on matched filter optimization called Network Intrusion Detection based on Matched Filter Optimization NIDeMFO; the evaluation proves more competitive and effective than the existing detection models compared. Edge data transmission can use data encryption; Wang [24] [H] proposes a hybrid cryptosystem based on state secret algorithms SM2 and SM4 and their system solution for realizing secure communication, which improves the security of information transmission and key sharing. Kounavis [25] proposes a novel low-latency, bit-length parameterizable encryption method to provide the possibility of low-latency communication encryption. In the process of edge computing, if there is a problem in the edge node itself, the impact is quite serious; for example, in the automotive industry chain, if a tire company's products do not meet the standard, then it will lead to quality problems in all the downstream products. At present, for the previous problems, there are many scholars [26–29] researching this, and regulation based on the third-party trustworthy organization is a good strategy to effectively avoid the the previous situation.

With the continuous development of the industrial Internet, the production efficiency is gradually improved, the amount of data is growing, and it is becoming more and more important for the data to be secured. Every node in the industry chain has to face malicious attacks from all angles. In this paper, we use the credibility mechanism to establish a good evaluation system for the edge nodes, and use the adaptive encryption technology to take care of both the efficiency and the security, and ultimately ensure the security of the data.

3. Cloud–Edge Collaborative Intelligent Security Encryption Strategy

In this section, the collaborative architecture of industry is first introduced, and the relevant concepts of the enterprise node layer are proposed and introduced. In this scenario,

CP-ABE is a good choice for data sharing, which can enhance the collaborative relationship between edges and improve the sharing and use of some data.

3.1. Edge Encryption Architecture for the IIoT

The industrial collaboration architecture under IIoT contains four main layers, the industrial device layer, edge computing layer, enterprise node layer, and cloud computing layer as shown in Figure 2.

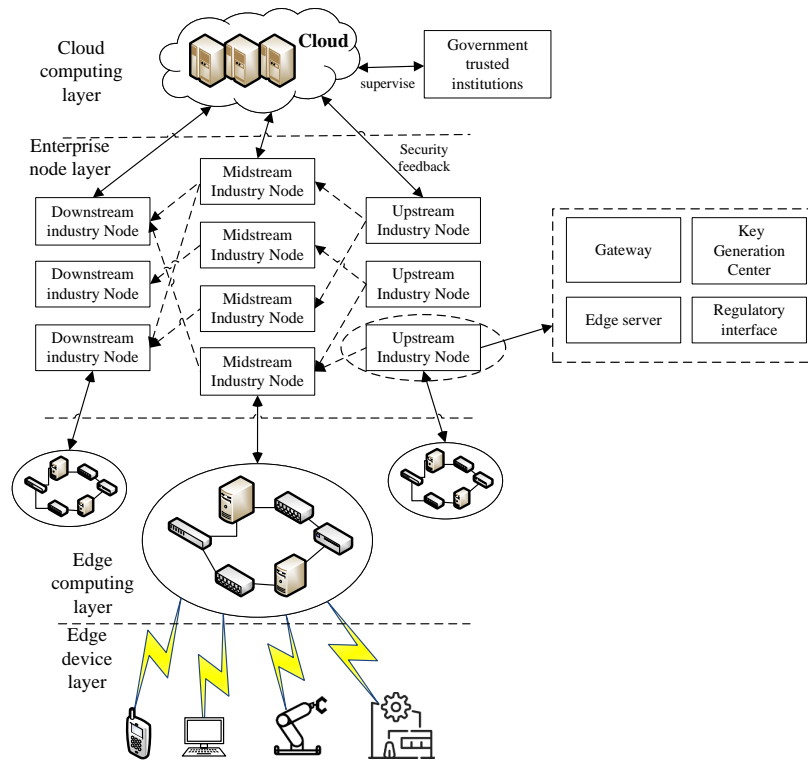


Figure 2. Industrial collaboration architecture diagram under IIoT.

(1) Edge device layer

The edge device layer mainly includes various sensors and IoT devices. Sensors are responsible for monitoring the environment or device status, collecting a large amount of raw data, such as temperature, humidity, images, sound, etc. These data are used as the basis for subsequent processing and analysis. IoT devices mainly include some robotic arms and assembly line devices, which play a role in receiving upper level commands and executing them.

(2) Edge Computing Layer [30]

The edge computing layer comprises numerous edge processing nodes endowed with data processing and storage capabilities. These nodes process data from the industrial equipment layer to a certain extent. When the data volume is excessive or specific tasks surpass the capacity of edge nodes, tasks can be uploaded via the edge gateway for processing by the computational resources of larger cloud computing centers. Subsequently, the results are returned to the industrial equipment. More considerable computing resources within the cloud computing center handle the tasks, after which the computation results are returned to the industrial equipment.

(3) Enterprise Node Layer

The enterprise node layer consists of hardware encryption devices, gateways, regulatory interfaces, and edge servers. Professional devices can perform encryption tasks to

ensure the security and efficiency of these data. Supervision by third-party trusted institutions ensures the accuracy of data. The gateway is responsible for forwarding messages to ensure that data can accurately and accurately reach the destination. We will demonstrate the functionality of these components later.

(4) Cloud Computing Layer [31,32]

The cloud computing layer houses extensive computing and storage resources. Its primary function involves storing and processing large volumes of data with non-real-time requirements and extracting potential value from massive datasets. Furthermore, the cloud computing layer oversees the security supervision of the enterprise node layer, engaging in dynamic management to uphold system security and stability.

In the industrial cloud, key technologies include but are not limited to the cloud computing platform, industrial Internet of Things (IIoT), big data analysis, artificial intelligence (AI), edge computing, and 5G communication. These technologies work together to support the following core capabilities: unified data management, service oriented and platformized, intelligent analysis and optimization, security and privacy protection, and flexible expansion and upgrading.

3.2. Granularity Upload and Download

In terms of data sharing, in order for the data to be better utilized, the state encourages that enterprises open part of the data, but enterprises do not want their data to be seen by their competitors, so attribute encryption can satisfy this demand very well. Non-competing enterprises can choose whether they need to download this part of the data according to their own needs, and enterprises sharing this part of the data need them to be encrypted only once. Sensitive information in the traditional CP-ABE method may be leaked; the scheme proposed by Han et al. [33] applies a hidden strategy to make attribute encryption efficient and promising. Chen et al. [34] propose a ciphertext strategy for shared decryption, where the authorized users can decrypt the message independently and the semi-authorized users can work collaboratively to decrypt the message, which is very efficient in terms of computational overhead and storage cost. Sangjukta Das et al. [35] propose an ECC-based CP-ABE technique for fine-grained access control to data or resources to reduce the overhead of decryption resources. By sharing industrial data with upstream and downstream companies, they can improve their products. Then, the data uploaded to the cloud need to be encrypted in order to reduce the encryption overhead; attribute encryption can be very good at the task, with a given time for encryption, to meet the decryption required. Through one encryption, the enterprise or organization that meets the required attributes for decryption and needs to decrypt their data can decrypt the data by themselves, while those that do not meet the attribute conditions, such as those of competitors, cannot be encrypted. At present, there are many scholars to carry out research on this, and there are many mature programs [36]. The flow chart is shown in Figure 3. The specific algorithm flow is as follows:

1. The user enterprise shows its attributes and relevant evidence to the third-party trusted organization.
2. The third-party trusted organization audits the user's attributes and returns a blind token with a signature to the user.
3. When the user needs to obtain its attribute key, it submits the blind token to the Key Generation Center (KGC).
4. The KGC cannot obtain any information about the user's attributes. It can only confirm that the user does have the relevant attribute.
5. The Key Generation Center (KGC) first checks the legitimacy of the token and aborts if the signature is illegal; otherwise, it runs the key generation algorithm and outputs the blind key.
6. The user receives the blind key from the KGC and extracts the private key.
7. The user decrypts the data from the cloud and performs computation on the data.
8. The cloud computing center returns the computation results.

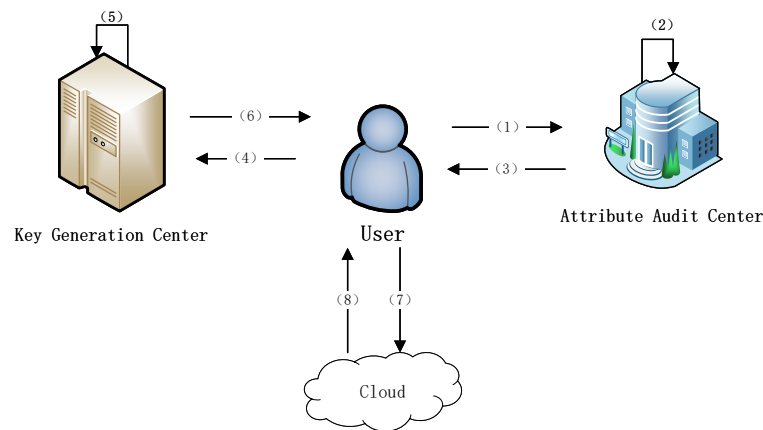


Figure 3. User granularity download process.

3.3. Industry Synergy Process Analysis

Based on the cloud–edge collaboration IoT architecture, which comprehensively considers data interaction within the enterprise, between enterprises, and between the enterprise and the cloud, along with low-latency task requirements and data transmission security, the industry collaboration architecture offers the following advantages compared to a single cloud-based factory:

- (1) Facilitation of swift processing for time-sensitive tasks between enterprises enhances collaboration and communication across industries.
- (2) Utilizing cloud computing resources enables the dynamic regulation of safety, efficiency, and product quality. This ensures secure and efficient data communication between enterprises while also identifying non-compliant operations to safeguard the interests of legitimate enterprises.
- (3) Leveraging third-party credible supervision enables timely feedback on enterprise collaboration information, ensuring regulated product quality. This proactive approach aligns with the national initiatives, allowing enterprises to realize the potential value of industrial data sharing while ensuring good data management and appropriate data-sharing practices.

The enterprise node layer establishes a dynamic encryption system to ensure data security during industrial collaboration. A security feedback mechanism to the cloud enables the dynamic adjustment of enterprise communication security levels, ensuring both security and efficiency throughout the communication process as shown in Figure 4.

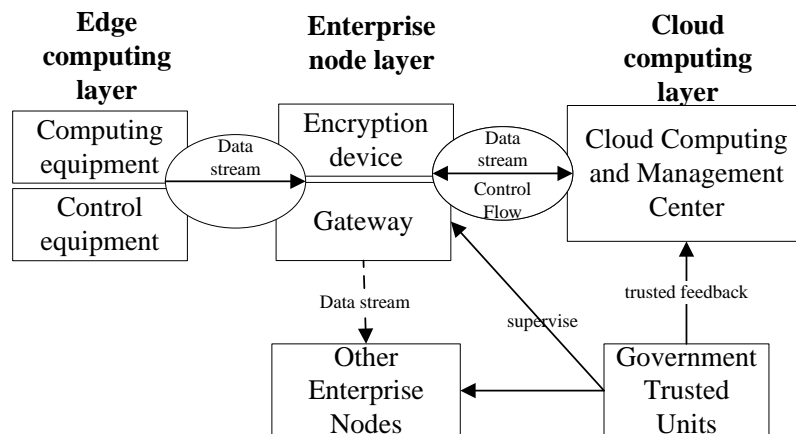


Figure 4. Data flow and control information.

4. Steps and Analysis of Cloud–Edge Collaborative Intelligent Security Encryption Strategy

In this section, a formal definition and description of security scenarios are provided, followed by the addition of a credible component to the security model to detect malicious nodes. Finally, appropriate encryption methods are adopted based on the importance of the task and analysis of the current transmission environment.

4.1. Security Model

We provide Table 1, and these variables are used in the instructions that follow. From Figure 4, it can be seen that the task of data transmission between edges may need to be secured and of low latency, and in the case of data theft may lead to property damage, so encryption measures are needed for the transmitted data. The strength of encryption will result in transmission delay, so it is especially important to adopt low-delay encryption measures in secure transmission paths and the dynamic adaptation of encryption algorithms with good encryption in insecure transmission paths. First of all, we usually use symmetric encryption algorithms when transmitting data, the common ones being DES, AES, RC5, etc., which have different effective key lengths with each other, such as 128, 192, 256 bits, etc. We define the problem as follows.

Table 1. Variables of interest.

Parameter	Definition
c	Coded text
p	Explicit message
X_s	Key security level
K_s	Number of valid key bits
Em	Number of rounds of encryption algorithm execution
$Cost$	The cost to the user of completing the task
M_i	Importance of the task
r	Pearson correlation coefficient
N_i	The the number of attacks of category i in a period of time
U	Key update cycle
Sec_i	The severity of the attack of category i
t	Attack severity factor [37]

Definition 1. There is a symmetric encryption algorithm X , the encryption function is EN , the plaintext is p , the key is k , the encrypted ciphertext is c , and then $c = EN(p, k)$. In the same set, the decryption function is DE , the function to recover plaintext data is $p = DE(c, k)$, and the use of k is the same.

Definition 2. The algorithmic security X_s and time of X are related to the number of bits (K_s) of the encryption key, and the encryption rounds (Em). For a particular encryption algorithm X , we can use the multivariate Pearson correlation coefficients to express the correlation $r_{X_s, K_s, Em} = \frac{\sum_{i=1}^n (X_{s_i} - \bar{X}_s)(K_{s_i} - \bar{K}_s)(Em_i - \bar{Em})}{\sqrt{\sum_{i=1}^n (X_{s_i} - \bar{X}_s)^2 \sum_{i=1}^n (K_{s_i} - \bar{K}_s)^2 \sum_{i=1}^n (Em_i - \bar{Em})^2}}$, where X_{s_i} , K_{s_i} , and Em_i are the observations in the X -encrypted sample data; \bar{X}_s , \bar{K}_s , and \bar{Em} are the mean values of X_s , K_s , and Em , respectively; and n is the number of X -encrypted samples. And $r_{X_s, K_s, Em} > 0$ means that the security of encryption algorithm X is positively correlated with K_s and Em , and on the contrary, $r_{X_s, K_s, Em} < 0$ means that the encryption time of encryption algorithm X is negatively correlated with K_s and Em .

Definition 3. As the effective key length K_s of the encryption algorithm X and the encryption round Em become more complex, the sender’s cost of sending and hardware cost increase accordingly, and there will be a non-linear relationship between these three: $Cost = K_s^2 + Em^2 + K_s \cdot Em$.

Definition 4. For a certain data transmission process, the type of attack uses the UNSW-NB15 dataset [38], which contains 10 network data types as shown in Table 2, 1 normal sample and 9

attack samples, respectively, and the consequences of the attack occurrence are described by the following formula: $Sec_i = N_i \cdot e^t$.

Definition 5. In transmitting tasks, each one has a different level of importance, denoted by M_i .

Definition 6. For this symmetric encryption algorithm X , the use of the periodic updating of the key will counteract the attack to a certain extent by using U -cycle updating of the key, where the shorter the updating period, the higher the security X_s of the encryption algorithm X .

Then, the objective BF (benefit function) can be expressed as

$$\begin{aligned}
 BF &= f_1(U) + f_2(Ks, Em) - f_3(Cost) - f_4(Mi) - \sum_{i=1}^{10} Sec_i \\
 &= f_1(U) + f_2(Ks, Em) - f_3(Ks^2 + Em^2 + Ks \cdot Em) - f_4(Mi) - \sum_{i=1}^{10} N_i \cdot e^t
 \end{aligned}
 \tag{1}$$

The “−” part of the previous equation is the factor that is unfavorable to the user, and the “+” part is the factor that is favorable to the user. From Equation (1), it can be seen that the worthwhile size of BF depends greatly on Ks and Em , so it is necessary and practical to grade the key. In the experiment, this paper uses three encryption strategies with different security levels, compares the three encryption strategies, and repeats the experiment to ensure the accuracy of the experiment.

Table 2. Network data types.

Type of Attack	Descriptions	Attack Severity Factor
Normal	Normal Transaction Data	0.275
Fuzzers	Sending random data to suspend programs or networks	0.473
Analysis	Port scanning, spam and html file infiltration	0.560
Backdoors	Access to computers bypassing system firewalls	0.473
DoS	Malicious attempts to disable a user’s access to a server	0.400
Exploits	Exploiting security holes in operating system software	0.300
Generic	Applying grouped passwords without regard to their structure	0.250
Reconnaissance	Simulated information-gathering attacks	0.500
Shellcode	Through a small piece of code in the vulnerability payload	0.770
Worms	Spreads to other computers by copying itself	0.450

4.2. Credibility Model

4.2.1. Node Relationship Input

As shown in Figure 5, in the context of the industrial collaboration chain, there are enterprise nodes $E = \{E_1, E_2, E_3, \dots, E_m\}$; enterprise nodes E_1, E_2, E_3 compete with each other, and E_2, E_4 cooperate with each other, resulting in a relationship where it is assumed that the E_3 to E_5 partnership situation can be used to indicate the credible value of 0–1. A value closer to 1 indicates that the E_3 to the E_5 nodes provide more compliance with the requirements of the product situation, while a value closer to 0 indicates that the E_3 to E_5 products meet the requirements for greater non-compliance. Connections are used to describe the cooperation at the node level of the enterprise, which can be a more intuitive way to see the flow of data and serve as the basis for calculating the trustworthiness value of the data in the later section.

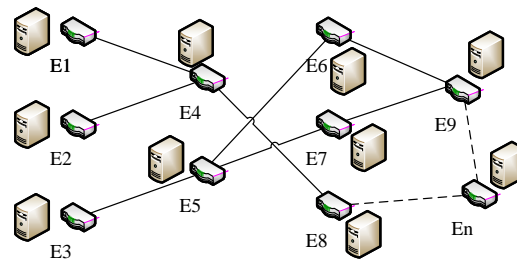


Figure 5. Industrial relationship map.

4.2.2. Introduction to Credibility Model

Cyclical supervision of a service-providing enterprise through a third-party government trusted unit comprises reviewing the national product quality qualification standard $S = (S_1, S_2, \dots, S_m)$, and standardizing the quality of the services provided around the previous rules. The credible value is used to measure the integrity of the enterprise’s breach of contract and whether the product quality meets the standards required by the downstream enterprise. Specific credible value calculation can be comprehensively considered from n perspectives in this paper, from the product quality situation and time delivery situation to the calculation. P_e is the number of qualified products, and P_a is the number of all products. The product quality situation can be calculated by the following Formula (2):

$$Q = \frac{P_e}{P_a} \tag{2}$$

Regarding the time delivery situation, certain companies may prefer that the upstream companies supplying their products deliver as early as possible so that they have sufficient time to prepare their production capacity, so it is calculated based on 80% (this is denoted by w in (3)) of the delivery time of the contract, with earlier than that being preferred, and later than that starting to decrease. T_f is the completion time of the actual task, T_s is the start time of the task, and T_e is the deadline of the task. This is calculated using the following Formula (3):

$$S = \begin{cases} 1, & \frac{T_f - T_s}{T_e - T_s} \leq w \\ w \cdot \sqrt{\frac{T_f - T_s}{T_e - T_s}}, & \frac{T_f - T_s}{T_e - T_s} > w \end{cases} \tag{3}$$

By using Formula (3), the direct trust level T_{ij} calculated by node i and node j based on the direct interaction behavior information during the time period is

$$T_{ij} = \sqrt{Q_{ij} \cdot S_{ij}} \tag{4}$$

where n , W_{ij} is the set of nodes that have a cooperative relationship with node i and their weights; the weights are generally averaged, and when some business interactions are more important, the weights can also be distributed unevenly. Weighting the feedback information of node i with all the other cooperating nodes of node i during the time period gives the direct credibility of node i T_i :

$$T_i = \sum_{j=1}^n \sqrt{Q_{ij} \cdot S_{ij}} \cdot W_{ij} \tag{5}$$

Considering that the historical information of node i has some degree of information reflecting the business status of the enterprise, the historical credible value can occupy a part of the weights, and then the integrated credible value calculated with the direct credible value can reflect the enterprise integrity and collaboration:

$$T_{new} = w \cdot \sum_{j=1}^n \sqrt{Q_{ij} \cdot S_{ij}} \cdot W_{ij} + (1 - w) * T_{old} \tag{6}$$

From (6), it is evident that the credibility of an enterprise fluctuates with its level of collaboration. A higher credibility value suggests that the enterprise’s products adhere more closely to national standards. Engaging with third-party government-certified entities for supervision can effectively identify untrustworthy enterprises, mitigating losses and preventing credible enterprises from collaborating.

4.3. Strategy

The use of traditional single encryption techniques does not take into account the cost and security issues that may arise when the volume of data is large, and the security assessment of the transmission task is carried out at the time of each data transmission, with high-security encryption being used for high-security tasks, and low-security encryption for low-security tasks, and the security assessment strategy is carried out in the following ways:

1. Strategy based on historical experience: based on the information that has been evaluated historically, its data value is categorized, and at each new task, the priority is to go through the existing data attributes to be evaluated. The following rules can be used when there are no matching data attributes:
 - (a) Adoption has maximum matching. Assume that the matching strategies are A_1, A_2, \dots, A_n , the attributes of each class are $H(A)$, and the attributes of this transmission data matching each strategy are $M(A)$, then the strategy A_i that maximizes the value of $\frac{H(A)}{M(A)}$ is selected, and the matching rate is set to be greater than a certain threshold.
 - (b) If none of the strategies satisfy in the previous strategies, a default strategy approach is given using customized data values.
2. Learning-based strategy: a hierarchical strategy function is formed by giving samples and examples, and machine learning and neural networks are used to extract features and mine the attributes of the data, which leads to a strategy that matches the value of the specific data.

The previous strategy determines that $f(m_i)$; in order to facilitate the calculation, we only focus on the encryption rounds when considering the security level, without considering the weighting problem and ignoring the influence brought by the key update cycle, using B for gain and D for loss, then the previous benefit formula can be expressed as

$$BF = B - D = f_1(Em) - f_2(M_i) - \sum_{i=1}^{10} N_i \cdot e^t \tag{7}$$

For a task with a constant security level, we only need to make the benefit function (BF) slightly greater than 0; because $f_1(Em)$ does not keep increasing, it receives a constraint from cost, so we can use a suitable security policy to categorize the transmission of different security tasks to ensure security while saving cost. For the RC5 encryption method, it has three variable parameters: group size, key size, and number of encryption rounds. It is characterized by high flexibility, fast encryption speed, and high security. We fix the group size to 128 bits. The steps are as follows to calculate the encryption rounds.

The following steps should be referred to when selecting the security key to be used according to the security level of the task:

1. Select a suitable security evaluation strategy, and then output its security level and calculate the security value M_i .
2. Calculate $f_1(Ks) - f_2(M_i) - \sum_{i=1}^{10} N_i \cdot e^t = 0$, and the calculated Ks will be chosen as the appropriate number of encryption bits for the encryption method for this task.

- Send the situation of this task to the key management center, encrypt the data using the corresponding key to get the ciphertext c , and then start sending.

For the three different security level tasks in the previous algorithm design, key grading technology is used to categorize different security tasks, reduce costs, and increase security. In the actual industrial production, there will be m encryption levels and n levels of security tasks. The use of the previous algorithms can greatly reduce the cost of data transmission, reduce the pressure on the host computer, and, at the same time, protect security. The algorithm process is shown in Figure 6.

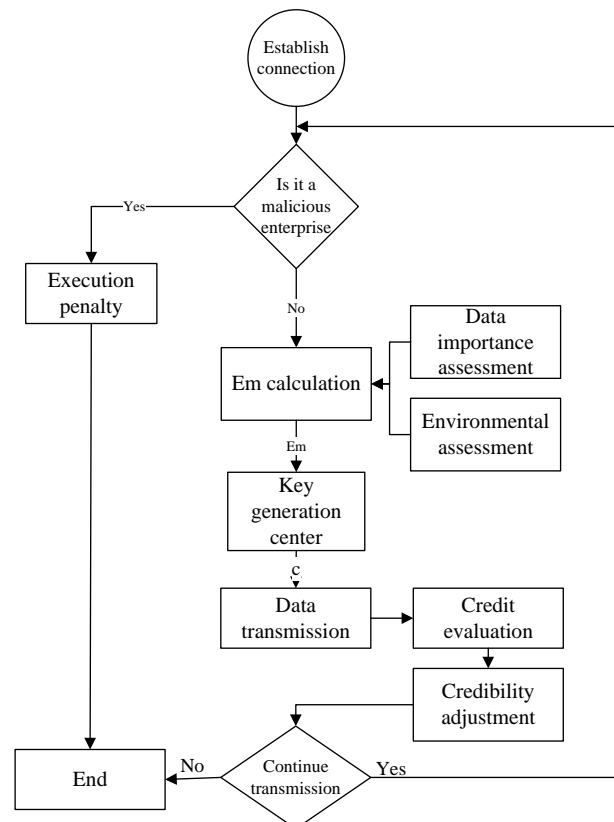


Figure 6. Algorithm operation flow chart.

5. Experimental Results and Analysis

In this section, simulation experiments are conducted on both secure and credibility scenarios, and the relevant parameters of the experimental process and analysis of the experimental results are listed. In the analysis, it is demonstrated that adopting adaptive encryption can balance security and efficiency, which should be particularly advantageous in industrial scenarios that require the transmission of large amounts of data.

5.1. Security Analysis

To assess the performance disparity between the industrial collaborative architecture proposed in this paper and traditional information transfer methods, this section conducts algorithm simulations. Experimental cases are randomly generated based on the initial parameters, encompassing node and path information. The experiments are iterated 100 times for credibility. Table 3 outlines the characteristic parameters. The experimental environment is shown in Figure 7: Win10 i7-8750H and Win11 i7-12650H; the software used is Idea and Pycharm; and the development languages used are Java(17) and Python(3.9).

The interval parameter in the table indicates that it will be generated randomly within the interval in the simulation, and the rate of change of intrusion refers to the fact that after

the first number of path intrusions is determined, subsequent path intrusions are generated at a random rate of change of intrusion. The experimental process is shown in Figure 8.

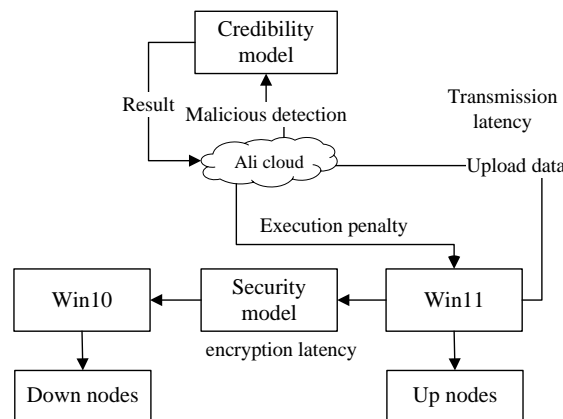


Figure 7. Experimental topology diagram.

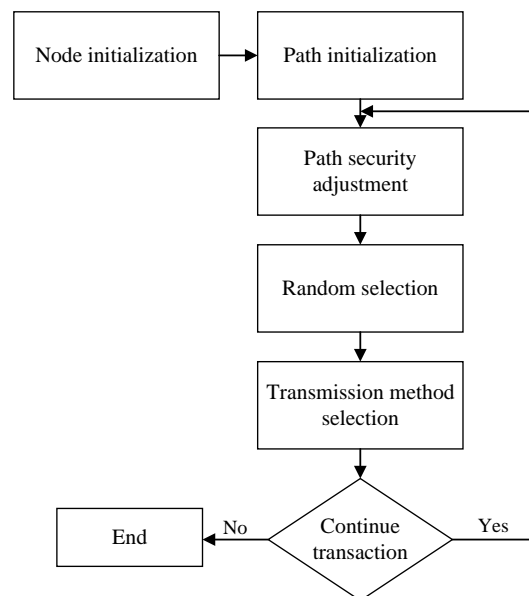


Figure 8. Safety experiment flow chart.

Table 3. Simulation node parameter generation table.

Parameter	Value
Number of downstream nodes	100
Number of upstream nodes	110
Unit node production	4
Unit node demand	3
Industry standard value	(0.1–0.2)
Number of path intrusions	(0–20)
Rate of change of intrusion	(0.7–1.3)
Number of rounds of cooperative maintenance	(3–5)
Historical safety weights	0.4
Maximum number of iterations	100

The simulation first initializes the corresponding upstream and downstream nodes. Each downstream node will randomly select four upstream nodes for collaboration. When

the number of collaboration of upstream nodes reaches the output, the collaboration will be rejected. The initial upstream enterprise set is $E_d = \{E_{d1}, E_{d2}, E_{d3}, \dots, E_{d110}\}$, and the initial set of downstream firms is $E_u = \{E_{u1}, E_{u2}, E_{u3}, \dots, E_{u100}\}$. We set the initial security degree to 0.7. In the next downstream enterprises, we pick the upstream enterprises to produce the collaboration, establish virtual connection, produce the path $R_{E_{du}}$ and prepare to send the data. Each path has the probability of being compromised by others after intruding, and the Formula (8) for the probability of compromised leakage after being cracked (CLSP) is

$$CLSP = 1 - (1 - S)^{NR} \tag{8}$$

where N is the number of intrusions, R is the intruded path, and S is the leakage probability of the adopted encryption method.

The results of the security degree assessment are shown in the following Figure 9; we can observe that the number of leaks between enterprises through the edge direct transmission is higher, while the number of leaks based on the cloud-edge supervised collaborative transmission and cloud transmission are both significantly lower than the edge transmission. At the initial stage, when there are fewer enterprises cooperating, the gap between the number of leaks of the three is not obvious, and with the increase in the number of enterprises joining, the number of enterprises' collaboration increases, and the gap between the security of the edge transmission and cloud transmission, cloud-edge collaborative transmission, gradually becomes obvious. It tends to be stabilized when the number of enterprises seeking to cooperate reaches 360, which indicates that at this time, due to the limitations in the production of the upstream, the number of enterprises cooperating in each round reaches saturation.

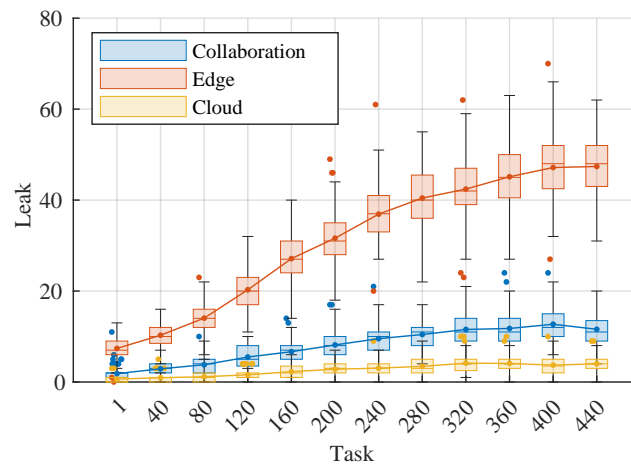


Figure 9. Relationship between transmission mode and security.

The efficiency situation is shown in Figure 10; we can observe that because the edge transmission does not consider the security degree of the transmission path, adopts the same encryption method, does not have a unified key replacement mechanism, does not have a rotation mechanism for different encryptions, and is more likely to be exploited by others, it can easily lead to the leakage of the data. And the cloud, although it adopts the dedicated single line transmission, which can guarantee the security of the data, because the cloud is usually located farther away from the edge nodes, the transmission delay brought about by a long transmission distance is higher. Although the cloud adopts a dedicated single-line transmission, which can guarantee data security, because the cloud is usually located far away from the edge nodes, the transmission distance is far, which brings high transmission delay and cannot guarantee that the low-latency tasks can be effectively executed. The transmission architecture based on cloud-edge collaboration has periodic key update and cloud security supervision, which can look at the collaboration path problem between enterprises from the historical perspective and ensure that the data

of the enterprise collaboration are not leaked. Multiple key encryption mechanisms can take into account the efficiency under the circumstance of maximizing the security.

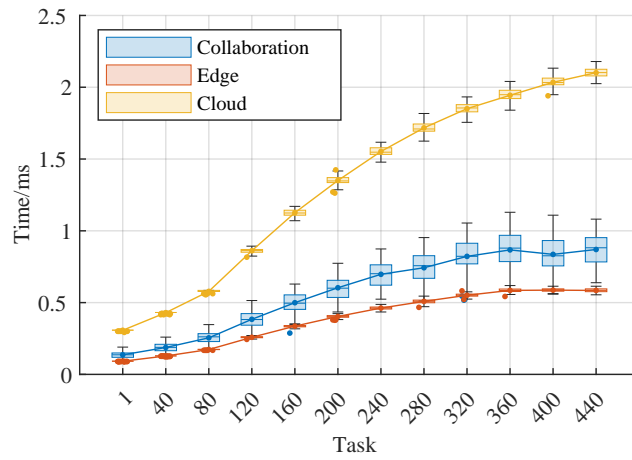


Figure 10. Relationship between transmission mode and time (ms).

The different encryption algorithms used are shown in Figure 11. When the number of encryption rounds is 12, it takes about 2000 ms to encrypt the data of a 256 MB file, and when the number of encryption rounds is 24, it takes 5000 ms to encrypt a file of the same size, so the security grading of files with different security levels can effectively reduce the latency brought by encryption.

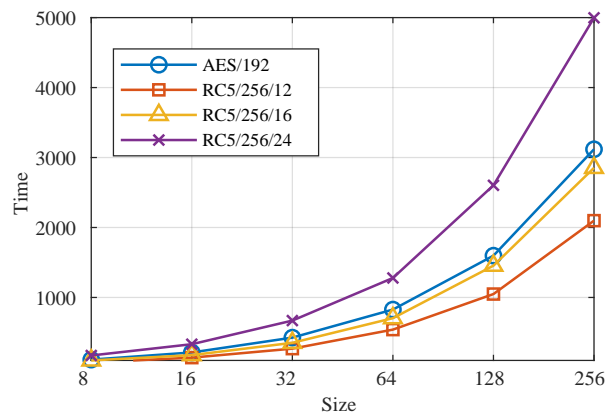


Figure 11. The relationship between time (ms) and size (MB) under different encryption methods.

In this paper, from the perspective of security and transmission delay, we propose the secure transmission score (ST), which is calculated as follows (9):

$$ST = \alpha_T e^{-\frac{mean(T)}{max(T)}} + \alpha_L e^{-\frac{mean(L)}{max(L)}} \tag{9}$$

where $max(T)$ is the maximum data throughput, which is unchanged in a certain system or architecture, and is determined by the performance of the enterprise equipment, data volume, etc. T is the time required for data transmission, L is the number of leaks caused by intrusion during data transmission, and $max(L)$ is the maximum number of leaks. α_T and α_L are the weights corresponding to the data throughput and the number of leaks. When T is larger, it means that the system data size is large, ST decreases, and the security transmission score will be reduced; when L is larger, it means that the system as a whole has a high number of leaks, ST decreases, and the security transmission score will be reduced as well. Bringing the experimental data into the formula yields the secure transmission score of the three transmission modes under different data sizes as shown in Figure 12.

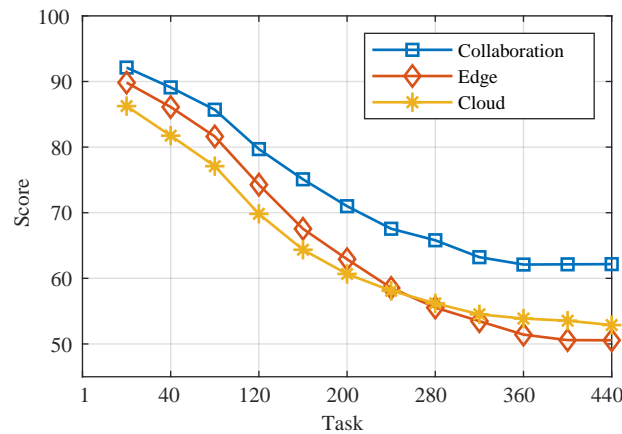


Figure 12. Secure transmission score in each mode.

As seen from Figure 12, the transmission effect of cloud–edge collaboration is higher than that of cloud transmission and edge transmission at different collaboration numbers. The new architecture of industrial collaboration can synthesize the two advantages of the traditions, consider security and efficiency, ensure low-latency tasks, and solve the most common security and efficiency problems in industrial data transmission for enterprises.

5.2. Credibility Analysis

In order to explore the impact of good or bad corporate integrity on the success of collaboration, whether the proposed method can improve the probability of successful corporate collaboration, and whether it can detect malicious enterprises in time to provide a good collaboration environment for other enterprises, this subsection simulates the credibility experiment to explore the existence of malicious enterprises. This architecture, from the perspective of the product qualification rate, detects the malicious enterprises and expels them. The relevant parameters involved are shown in Table 4:

Table 4. Simulation node parameter generation table.

Parameter	Value
Number of downstream nodes	60
Number of upstream nodes	80
Unit node production	3
Unit node demand	4
Number of upstream malicious nodes	20
Industry credibility	0.7
Normal node product pass rate	(0.68–1)
Malignant Node Product Qualification Rate	(0.52–0.8)
Malicious node yield	(0–0.2)
Historical safety weights	0.4
Maximum number of iterations	100

The experimental process is shown in Figure 13.

In addition, the enterprise selects the collaboration object using the roulette wheel; the higher the enterprise credibility, the higher the probability that the enterprise is selected, in line with real-life enterprises with good integrity being easily favored by others. The cloud monitors the number of marks used to screen malicious enterprises in accordance with the following methods: 1. Take the rating of 0.7 for each transaction as the malicious cut-off point, and mark the enterprises producing products with a qualification rate of 0.7 or less once; if the enterprise’s product qualification rate is marked three times in a row at (0.6, 0.7), the enterprise is judged to be a malicious enterprise, and the next time a normal enterprise cooperates with it, the normal enterprise will be notified; if the enterprise’s product qualification rate is at (0.55, 0.6), it is marked twice consecutively, then it is judged

as a malicious enterprise; and if the enterprise's product qualification rate is at $(0.5, 0.55)$, then it is judged as a malicious enterprise directly. 2. Considering the enterprise's last five product situations, the average of these five product situations will be averaged, and if the average value is less than 0.7, then it is judged as a malicious enterprise. This paper adopts the first scheme to judge whether the enterprise is a malicious enterprise or not.

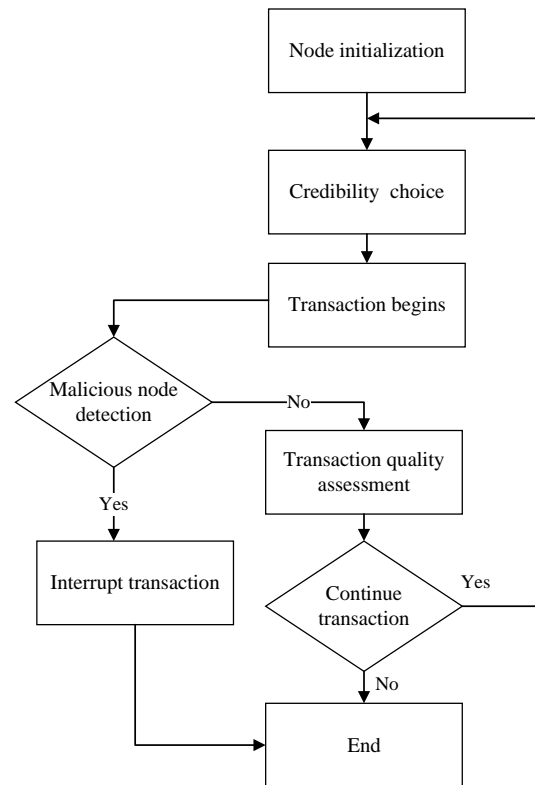


Figure 13. Credibility experiment flow chart.

Under the experimental simulation, the number of discovered malicious nodes is shown in the following Figure 14, and we can observe that with the collaboration between enterprises, the credibility is constantly updated, and some malicious enterprises are gradually exposed; 20 malicious nodes are basically all exposed after 40 rounds, which avoids the interference of malicious nodes and protects the interests of the honest enterprises in the normal nodes' collaboration with each other. As shown in the following Figure 15, we can observe that with the stability of the credibility, the malicious enterprises are gradually discovered, and the number of collaboration successes rises significantly, from 217 successes in the first round of experiments to a stable 236 successes later. After the discovery of the malicious enterprises, the honest enterprises will ask the collaboration object whether it is a malicious enterprise or not in every transaction, and give up the collaboration if it is a malicious enterprise, and they can re-select an enterprise for collaboration. The number of successful collaboration remains stable around 235.

At different numbers of malicious nodes, the possibility of collaboration failure is relatively low when the ratio of malicious nodes to normal nodes is 12.5%, and the number of failures in the first round of experiments is about 13 times. The possibility of collaboration failure is high when the ratio of malicious nodes to normal nodes is 50%, and the number of failures in the first round of experiments is about 35 times. After 50 rounds of collaboration, the collaboration is stable, and the number of failures in collaboration is around 3 times. The higher the number of malicious nodes, the higher the possibility of enterprise collaboration failure, and the more serious the actual loss brought about, so it is important to discover malicious nodes and mark them in time. Under the timely discovery of the system, the final

number of collaboration tends to stabilize, reaching the threshold of industrial collaboration. The specific results of the experiment are shown in the following Figure 16.

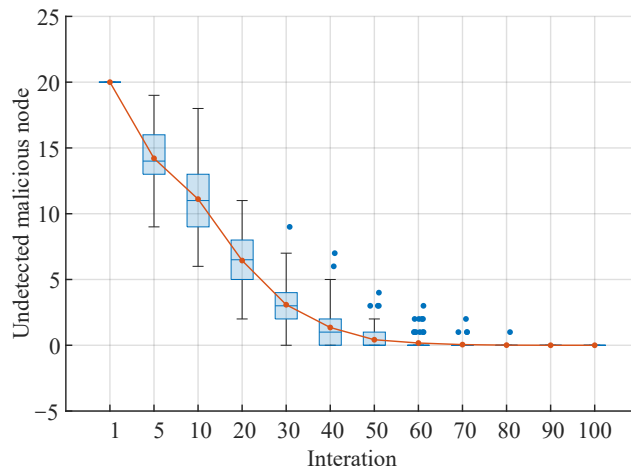


Figure 14. Trend chart of malicious node changes.

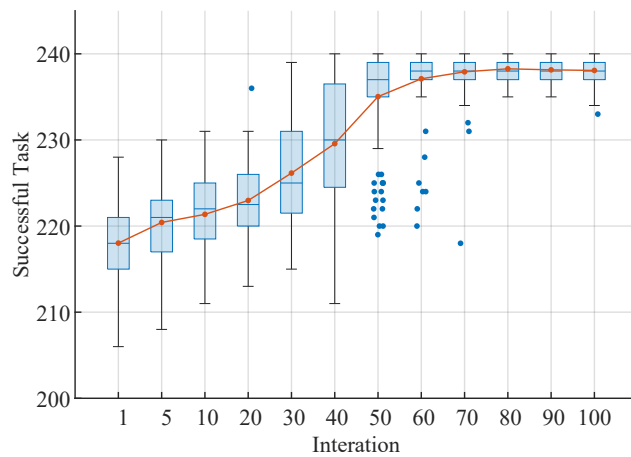


Figure 15. Trends in the number of successful collaborations.

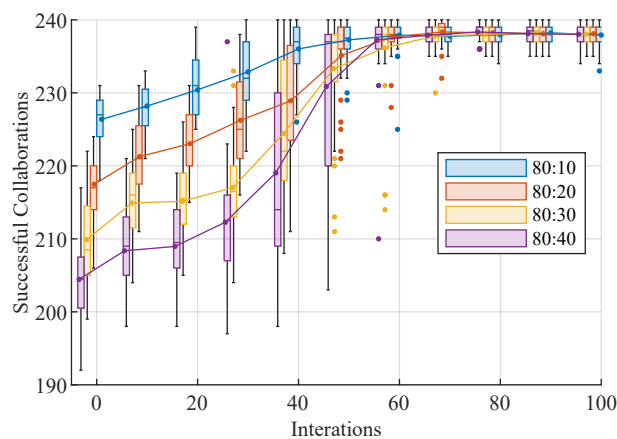


Figure 16. Impact of varying number of malicious nodes as a percentage.

In this experiment, the industrial collaboration architecture can well protect the interests of honest enterprises, detect malicious nodes in time, and reduce the loss of legitimate nodes. At the same time, because of the principle of roulette when selecting enterprises, enterprises with high credibility have a greater enterprise selection rate than those with low credibility, encouraging enterprises to cooperate in good faith and improve product quality,

which to a certain extent can motivate enterprises to improve the qualification rate of their products, actively participate in collaboration in good faith, and safeguard the sustainable development of the industrial chain.

5.3. Strategy Discussion

This article mainly proposes a method to adjust the encryption level based on the current environment. By scientifically detecting the gateway environment and quantifying the security at this time, the purpose of dynamically adjusting the encryption level is achieved. When the environment of the gateway changes and the importance of tasks varies, the encryption level should also be correspondingly increased. In secure environments, fast encryption methods should be used, and in high-risk environments, more secure encryption methods should be used to improve time efficiency. The environmental security we are considering has better universality compared to the MG-MTD strategy. We only need to establish traffic monitoring at the gateway, and our defense strategy is not complex to implement, achieved by designing the number of encryption rounds for the key. The DDR-MTD strategy can have good defense effects by quantifying attackers and mobile target defenders, but it poses a challenge to edge devices with scarce computing resources. Our solution incorporates lightweight encryption methods for computing resources, effectively reducing encryption latency. In this experiment, there are still some shortcomings, as too few encryption methods were used; mainly AES and RC5 with different encryption rounds were used, without considering the impact of key updates. In subsequent work, different encryption methods can be considered based on the characteristics of different data formats to study the impact of different encryption algorithms on encryption efficiency during data fusion.

6. Conclusions

In this article, we investigated the issues of insufficient security and single encryption strategy in traditional edge or cloud-centric network architectures. The timely detection of malicious nodes at the edge through credibility evaluation reduces internal attacks. Use task importance assessment and environmental assessment are used to generate appropriate security keys. At the same time, simulation results show that the new architecture of credibility evaluation can, in a timely manner, detect malicious nodes, protect other normal nodes, and reduce encryption latency at the transmission end. Although many efforts have been made, more experiments are needed to develop more accurate and reasonable defense strategies. In the next step of work, how to improve the accuracy of gateway traffic detection is a crucial issue, possibly using deep learning to accurately classify different attack methods and adopt appropriate defense strategies. We still need to further study how to combine it with other network defense methods to find more comprehensive defense strategies.

Author Contributions: Conceptualization, A.T. and C.D.; methodology, A.T. and C.D.; software, C.D. and C.W.; validation, C.D., Y.W. and C.X.; formal analysis, A.T. and C.D.; resources, Y.W.; writing—original draft preparation, C.D. and C.W.; writing—review and editing, Y.W. and C.X.; project administration, Y.W.; funding acquisition, Y.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Key Research and Development Program of China, 2023YFC3304904.

Institutional Review Board Statement: Not applicable for studies not involving humans or animals.

Informed Consent Statement: Not applicable for studies not involving humans or animals.

Data Availability Statement: No data was used for the research described in the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Sun, M.; Zhang, J. Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. *Comput. Commun.* **2020**, *149*, 332–342. [\[CrossRef\]](#)
2. Ghosh, S.; Hughes, M.; Hodgkinson, I.; Hughes, P. Digital transformation of industrial businesses: A dynamic capability approach. *Technovation* **2022**, *113*, 102414. [\[CrossRef\]](#)
3. Papulová, Z.; Gažová, A.; Šufliarský, L. Implementation of automation technologies of industry 4.0 in automotive manufacturing companies. *Procedia Comput. Sci.* **2022**, *200*, 1488–1497. [\[CrossRef\]](#)
4. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. *IEEE Access* **2018**, *6*, 6900–6919. [\[CrossRef\]](#)
5. Tao, Y.; Xu, P.; Jin, H. Secure data sharing and search for cloud-edge-collaborative storage. *IEEE Access* **2019**, *8*, 15963–15972. [\[CrossRef\]](#)
6. Mollah, M.B.; Azad, M.A.K.; Vasilakos, A. Secure data sharing and searching at the edge of cloud-assisted internet of things. *IEEE Cloud Comput.* **2017**, *4*, 34–42. [\[CrossRef\]](#)
7. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [\[CrossRef\]](#)
8. Ranaweera, P.; Jurcut, A.D.; Liyanage, M. Survey on multi-access edge computing security and privacy. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1078–1124. [\[CrossRef\]](#)
9. Jia, Y.; Gu, Z.; Du, L.; Long, Y.; Wang, Y.; Li, J.; Zhang, Y. Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model. *Knowl.-Based Syst.* **2023**, *276*, 110781. [\[CrossRef\]](#)
10. Kumar, R.; Kumar, P.; Jolfaei, A.; Islam, A.N. An Integrated Framework for Enhancing Security and Privacy in IoT-Based Business Intelligence Applications. In Proceedings of the 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 6–8 January 2023; pp. 1–6.
11. Lei, C.; Ma, D.H.; Zhang, H.Q. Optimal Strategy Selection for Moving Target Defense Based on Markov Game. *IEEE Access* **2017**, *5*, 156–169. [\[CrossRef\]](#)
12. Tan, J.; Jin, H.; Hu, H.; Hu, R.; Zhang, H.; Zhang, H. WF-MTD: Evolutionary decision method for moving target defense based on wright-fisher process. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 4719–4732. [\[CrossRef\]](#)
13. Cinar, B.; Bharadiya, J.P. Cloud computing forensics; challenges and future perspectives: A review. *Asian J. Res. Comput. Sci.* **2023**, *16*, 1–14. [\[CrossRef\]](#)
14. Li, J.; Qiu, J.J.; Zhou, Y.; Wen, S.; Dou, K.Q.; Li, Q. Study on the reference architecture and assessment framework of industrial internet platform. *IEEE Access* **2020**, *8*, 164950–164971. [\[CrossRef\]](#)
15. Bandyopadhyay, D.; Sen, J. Internet of things: Applications and challenges in technology and standardization. *Wirel. Pers. Commun.* **2011**, *58*, 49–69. [\[CrossRef\]](#)
16. Yang, H.; Li, L.; Liu, Y. The effect of manufacturing intelligence on green innovation performance in China. *Technol. Forecast. Soc. Chang.* **2022**, *178*, 121569. [\[CrossRef\]](#)
17. Zhu, X. Research on Countermeasures of Intelligent Manufacturing Training Base Serving Local Industry Collaborative “Three Chains” Innovation. *J. Phys.* **2021**, *1748*, 042035. [\[CrossRef\]](#)
18. Han, D.; Zhu, Y.; Li, D.; Liang, W.; Souri, A.; Li, K.C. A blockchain-based auditable access control system for private data in service-centric IoT environments. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3530–3540. [\[CrossRef\]](#)
19. Rocha, R.; Carneiro, D.; Novais, P. Continuous authentication with a focus on explainability. *Neurocomputing* **2021**, *423*, 697–702. [\[CrossRef\]](#)
20. Rosati, P.; Gogolin, F.; Lynn, T. Cyber-security incidents and audit quality. *Eur. Account. Rev.* **2022**, *31*, 701–728. [\[CrossRef\]](#)
21. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A survey of security in cloud, edge, and fog computing. *Sensors* **2022**, *22*, 927. [\[CrossRef\]](#)
22. Gamage, S.; Samarabandu, J. Deep learning methods in network intrusion detection: A survey and an objective comparison. *J. Netw. Comput. Appl.* **2020**, *169*, 102767. [\[CrossRef\]](#)
23. Alsaadi, H.S.; Hedjam, R.; Touzene, A.; Abdessalem, A. Fast binary network intrusion detection based on matched filter optimization. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 195–199.
24. Wang, Z.; Dong, H.; Chi, Y.; Zhang, J.; Yang, T.; Liu, Q. Research and Implementation of Hybrid Encryption System Based on SM2 and SM4 Algorithm. In Proceedings of the 9th International Conference on Computer Engineering and Networks, Singapore, 16–18 July 2021; pp. 695–702.
25. Kounavis, M.; Deutsch, S.; Ghosh, S.; Durham, D. K-Cipher: A Low Latency, Bit Length Parameterizable Cipher. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–7. [\[CrossRef\]](#)
26. Liu, Z.; Qian, Q.; Hu, B.; Shang, W.L.; Li, L.; Zhao, Y.; Zhao, Z.; Han, C. Government regulation to promote coordinated emission reduction among enterprises in the green supply chain based on evolutionary game analysis. *Resour. Conserv. Recycl.* **2022**, *182*, 106290. [\[CrossRef\]](#)
27. Palanski, M.E.; Kahai, S.S.; Yammarino, F.J. Team virtues and performance: An examination of transparency, behavioral integrity, and trust. *J. Bus. Ethics* **2011**, *99*, 201–216. [\[CrossRef\]](#)

28. Alzoubi, H.M.; Ghazal, T.M.; El Khatib, M.; Alshurideh, M.T.; Alami, R.; Al Masaeid, T. Creation of indicator system for quality estimation of safety management of personnel and it's psychological impact on industrial enterprises. *J. Reatt. Ther. Dev. Divers.* **2022**, *5*, 143–151.
29. Shehada, D.; Gawanmeh, A.; Yeun, C.Y.; Jamal Zemerly, M. Fog-based distributed trust and reputation management system for internet of things. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 8637–8646. [[CrossRef](#)]
30. Xhafa, F.; Kilic, B.; Krause, P. Evaluation of IoT stream processing at edge computing layer for semantic data enrichment. *Future Gener. Comput. Syst.* **2020**, *105*, 730–736. [[CrossRef](#)]
31. Alouffi, B.; Hasnain, M.; Alharbi, A.; Alosaimi, W.; Alyami, H.; Ayaz, M. A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access* **2021**, *9*, 57792–57807. [[CrossRef](#)]
32. Sunyaev, A.; Sunyaev, A. Cloud computing. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*; Springer: London, UK, 2020; pp. 195–236.
33. Han, D.; Pan, N.; Li, K.C. A Traceable and Revocable Ciphertext-Policy Attribute-based Encryption Scheme Based on Privacy Protection. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 316–327. [[CrossRef](#)]
34. Chen, N.; Li, J.; Zhang, Y.; Guo, Y. Efficient CP-ABE scheme with shared decryption in cloud storage. *IEEE Trans. Comput.* **2020**, *71*, 175–184. [[CrossRef](#)]
35. Das, S.; Namasudra, S. Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure. *IEEE Trans. Ind. Inform.* **2023**, *19*, 821–829. [[CrossRef](#)]
36. Song, Y.; Wang, H.; Wei, X.; Wu, L.; et al. Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud. *Secur. Commun. Netw.* **2019**, *2019*. [[CrossRef](#)]
37. Zhang, H.; Kang, C.; Xiao, Y. Research on network security situation awareness based on the LSTM-DT model. *Sensors* **2021**, *21*, 4788. [[CrossRef](#)]
38. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.