Hindawi
Security and Communication Networks
Volume 2023, Article ID 9824580, 1 page
https://doi.org/10.1155/2023/9824580

Retraction

Retracted: Copyright Protection and Data Reliability of AI-Written Literary Creations in Smart City

Security and Communication Networks

Received 17 October 2023; Accepted 17 October 2023; Published 18 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Wei, "Copyright Protection and Data Reliability of AI-Written Literary Creations in Smart City," *Security and Communication Networks*, vol. 2022, Article ID 6498468, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6498468, 13 pages
https://doi.org/10.1155/2022/6498468

Research Article

Copyright Protection and Data Reliability of AI-Written Literary Creations in Smart City

Chenlin Wei

School of Humanities and Social Sciences, Xi'an Jiaotong University, Xi'an 710049, China

Correspondence should be addressed to Chenlin Wei; weichenlin18@xjtu.edu.cn

Received 27 May 2022; Accepted 16 July 2022; Published 9 August 2022

Academic Editor: Mohammad Ayoub Khan

The purpose is to solve copyright disputes over artificial intelligence (AI)-written literary creations and protect copyright by legislation through data reliability research. Accordingly, this work makes a detailed study of the criteria for the copyright protection of AI-written literary creation and the creation process. It constructs the model of swarm intelligence (SI) perception. Then, the Preservation Trustworthiness Incentives Sense (PTISense) scheme is designed based on the encryption algorithm for the SI perception model. The performance of the proposed PTISense scheme is verified and analyzed through experiments. Mainly, it analyzes the impact of PTISense on the accuracy of the reputation model, its robustness against malicious users, and the actual feasibility. The results show that when users complete 50 tasks, the false-positive rate is only 0.1, and the corresponding false-negative rate approximates 0. After each task, the user reputation will be updated, and the data will be evaluated for trust. The trust model of the proposed PTISense scheme based on encryption technology is more accurate. When η (the number of malicious users) is small, the more tasks are performed, the faster the reputation value decreases and tends to zero. The proposed PTISense scheme-based reputation evaluation model can better protect the data submitted by good users. It is robust against malicious users and protects the data and privacy of good users. Further, entities' computing overhead in different SI perception stages is calculated. It is found that the proposed PTISense scheme is feasible for user data privacy protection. Compared with other schemes, it can achieve a safe and reliable SI perception process with a lower computing overhead. It can better ensure the authenticity and reliability of data.

1. Introduction

With the in-depth development of artificial intelligence (AI) technology, urban construction has also entered a new stage. With the continuous influx of Big Data Technology (BDT) and the Internet of Things (IoT), AI-enabled smart city applications have gradually penetrated all aspects of people's life, study, and work [1]. In the cultural field, AI technology has been integrated into literary creation and tends to be common [2]. The copyright of AI-written literary creation has gradually become a hot topic. Whether the Copyright Law can protect the copyright of AI-written literary creation, the amendment of Copyright Law and the solution of AI copyright disputes have gradually been stepped up. Then, many related legal problems need to be further explored [3].

Defining and demonstrating the copyright attributes of AI-written literary creation is the basis for solving the problems of copyright ownership and copyright protection of AI-written literary creation. At present, AI is much more capable of simple automatic behaviors. AI-written literary creation is independent creation through computer deep learning (DL) [4]. AI-written literary creation is a technical means to simulate human brain thinking for data analysis and processing. It also conforms to human language and aesthetic concepts [5]. With the continuous emergence of AI-written literary creations, they are difficult to distinguish from human creations when no clear source is provided. Hyperefficiency is the most revealing advantage of AI-written literary creations [6]. At this stage, the application and research of AI technology are also pervasive. Shen and Ho proposed a hybrid bibliometric method combining direct citation network analysis and text analysis. They aimed to visually check the relevant research articles on higher education retrieved from the science network database [7]. Chen et al. used the DL model to design the smart city's network security system to reduce network security's hidden dangers [8]. Hong and Curran discriminated against AI painting and traditional painting according to AI technology and proposed a new way of AI painting in art creation and a new way of communication [9]. Feng analyzed the process of human artistic creation and outlined the achievements of AI in painting, music, and poetry creation [10]. Lv et al. studied a network physical control system based on the spatiotemporal correlation detection model. They proposed a credible robust intelligent control strategy and credible, intelligent prediction model and made quantitative analysis [11]. The AI-written literary creations under the technical path of data-driven algorithm simulation are essentially the intellectual achievements completed by natural persons using intelligent tools. Defining the intellectual achievement attribute of AI-written literary creations can meet the practical needs of the protection of the interests of multiple subjects. China's legislation has not yet brought AI-written literary creations into the scope of supervision. Whether AI writers can be regarded as the author and creators still needs a huge gap to bridge relevant regulations, interpretations, and laws [12]. Thus, the copyright protection research and data reliability analysis of AI-written literary creations is particularly important.

Firstly, this work expounds on the theory of AI creations and copyright protection and introduces the criteria for the copyright protection of AI-written literary creations and the creation process. Innovatively, it uses an encryption algorithm to study the privacy protection and data reliability of AI-written literary works and constructs a swarm intelligence (SI) perception model for the copyright protection of AI-written literary creations. The Preservation Trustworthiness Incentives Sense (PTISense) scheme based on encryption technology is designed to study data reliability. Its main purpose is to build a PTISense scheme of encryption technology to protect users' privacy to the greatest extent, ensure data reliability, and protect the privacy of participants and data collectors in task allocation and aggregation. It is hoped to promote the research of copyright protection.

2. Copyright Protection Theory and Data Reliability Method

2.1. Smart City. Many foreign organizations or scholars have defined the smart city mainly from three aspects: urban development combines with information technology; the government changes the way of urban governance; and the important role of human and social capital in urban development. Applying "intelligence" to the urban context means the seamless combination of AI and human intelligence with urban development [13]. Chinese scholars put forward the concept of a smart city from the perspective of technology and believe that a smart city should realize urban interconnection based on information technology. Technology, people, and institutions are key parts of smart cities. Specifically, smart cities are composed of eight elements: technology, organization, policy, people and communities, economy, infrastructure, natural environment, and governance structure [14].

2.2. Characteristics of AI-Written Literary Creations. Literary creation is a uniquely human ability but can also be mimicked by an intelligent computer program. In particular, AI-written literary creations lean intensely on the continuous development of computer technology. Nowadays, AI writers can do so much more than simple and repetitive work by carrying out particularly complex creative work and constantly updating the creations more in line with human artistic tastes and aesthetic views [15]. AI writers can independently complete literary creations through program design within the scope of existing laws. The literary achievements have significant value in humanities, social, and other corresponding scientific fields [16].

Compared with traditional literary works, AI-written literary creations are reproducible, an expression in the field of literature, and have unique creativity [17]. From the external expression of the works, AI-written literary creations must meet the formal requirements of literary works. AI writers select the characteristics of relevant information and screen, analyze, and judge the data [18]. The characteristics of AI-written literary creations are shown in Figure 1.

As shown in Figure 1, AI-written literary creations are difficult to distinguish from human creations regarding content and form of expression. It is also difficult for ordinary people and even professionals to distinguish. Secondly, the creation cost is low. Compared with humans, AI improves work efficiency and accuracy, thus greatly reducing costs. The third is the efficient output rate. Following specific rules, AI can effectively avoid human subjective mistakes and work continuously. The calculation speed and accuracy are unmatched by human beings. Finally, AI has autonomous learning and unique creativity. The program written by AI can simulate the working process of the human brain, and AI machines can think independently and complete autonomous learning tasks like humans.

2.3. Copyright Protection of AI-Written Literary Creations

2.3.1. Copyright Criteria. In theory, adopting the object-independent definition criteria for identifying the copyright of AI-written literary creations is a compromise strategy based on treating AI as the legal authors [19]. According to the technical characteristics of human-computer interaction (HCI), human creative intention, human choice, and other factors may have been integrated into the creative process of AI-written literary creations [20]. The specific logic content is unfolded in Figure 2.

As shown in Figure 2, AI-written literary creations are nothing but a simple automatic content generation. The importance of discovering the personality elements of natural persons behind AI writers must be acknowledged. Firstly, AI-written literary creations are unique in the form

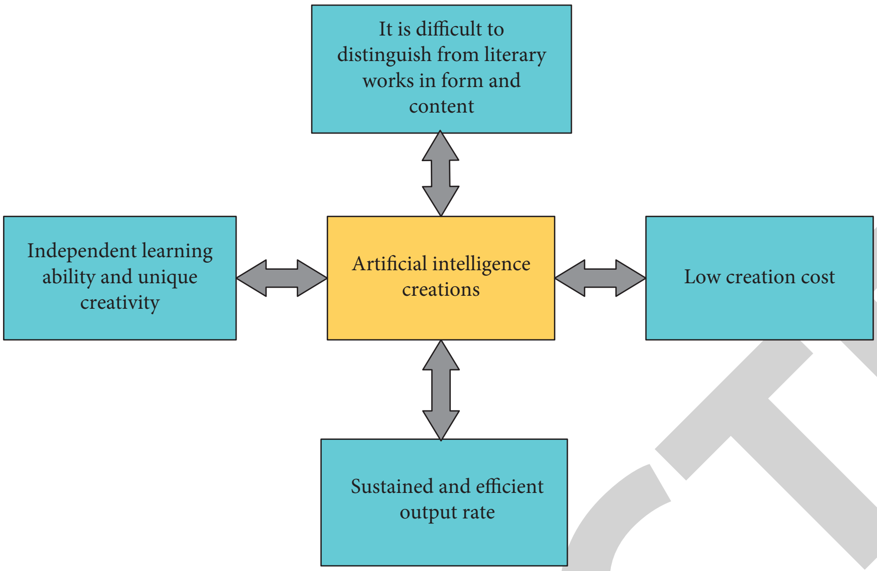

It is difficult to distinguish from literary works in form and content
Independent learning ability and unique creativity
Artificial intelligence creations
Low creation cost
Sustained and efficient output rate

Figure 1: Characteristics of AI-written literary creations.

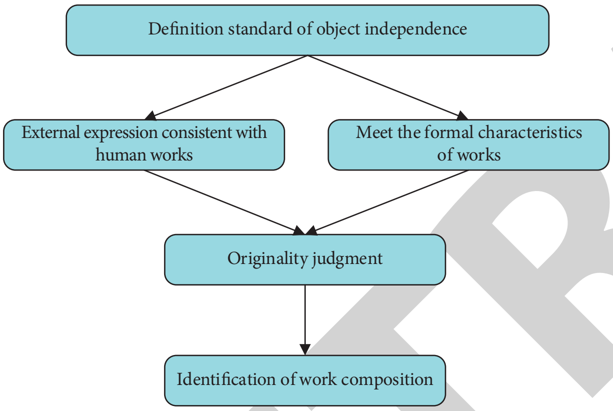

Definition standard of object independence
External expression consistent with human works
Meet the formal characteristics of works
Originality judgment
Identification of work composition

Figure 2: Definition criteria of object independence.

of expression. Secondly, suppose the original creations meet the requirements of the characteristics of the literary creations. In that case, they can be considered original and eligible literary works.

2.3.2. Criteria and Basis for Copyright Protection. From the legal perspective, this work expounds on copyright protection from the evaluation criteria of the subject-object separation. It takes AI-written literary creations as objects and natural persons as subjects. Then, it identifies the object's originality from the creativity of the subject [21]. The specific representation is presented in Figure 3.

As given in Figure 3, originality and the main identity are two independent elements of the copyrightability of works. First, it judges the originality of the external manifestation of AI-written literary creations. It excludes the main identity elements from the identification category of originality. The judgment requirements of originality are consistent with the definition criteria of object independence. If originality is confirmed, it analyzes and judges whether the expression result of originality comes from the creative behavior of natural persons through the AI creation process. If the expression comes from a natural person, copyright protection can be given.

The criteria of subjective and objective unity, also known as copyright recognition, follow the principles of personality and natural law. The specific logical relationship is illustrated in Figure 4.

As shown in Figure 4, the subjective and objective unified standard must be composed of objective forms of expression and the subjective personalized requirements of the author. The external forms of expression must be innovative and different from the works of other authors. In terms of subjective personalization, the creation should reflect the characteristics of a natural person's personalized choice and judgment.

2.4. AI Creation Process. Comparing the AI creation process with ordinary natural person authors unveils their differences. The creative process of the natural person author is specified in Figure 5.

Natural person authors' conception is based on inspiration, and they create following certain thinking logic and creative structure rules. The whole process is also an emotional expression of the subject. The final literary creation reflects the input of human wisdom. The creative process is also called the process of the author's ideological expression.

Compared with natural persons, the creative process of AI writers has both similarities and differences. The specific process is explained in Figure 6.

According to Figure 6, the AI program is started according to the creation intention, and the previous intelligence of the natural person is imported into the system to realize the algorithm simulation creation. Dominated by the previously predetermined goal, the two processes have a causal relationship: controlling vs. being controlled and

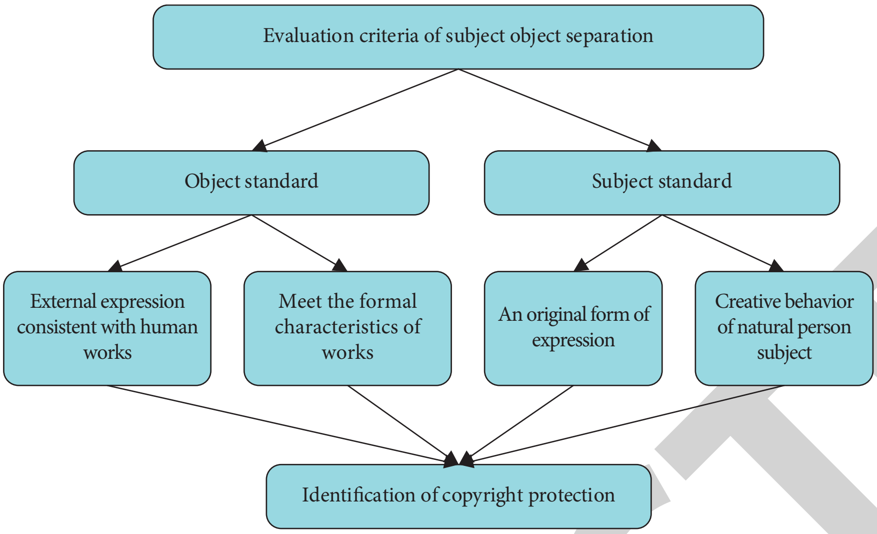

Evaluation criteria of subject object separation
Object standard
Subject standard
External expression consistent with human works
Meet the formal characteristics of works
An original form of expression
Creative behavior of natural person subject
Identification of copyright protection

Figure 3: Evaluation criteria for separation of subject and object.

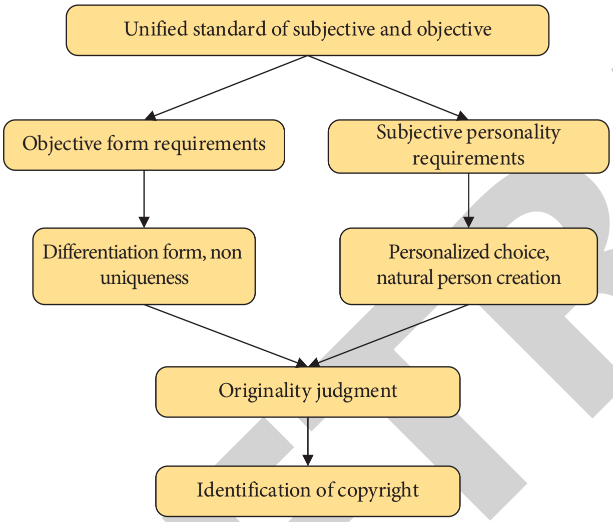

Unified standard of subjective and objective
Objective form requirements
Subjective personality requirements
Differentiation form, non uniqueness
Personalized choice, natural person creation
Originality judgment
Identification of copyright

Figure 4: Unified criteria of subjectivity and objectivity.

making the decision vs. implementing the decision. The AI creation process is divided into three stages: data input, machine learning, and algorithm generation. First, establish the database, further input the data, build the algorithm model of creation after the autonomous learning of the machine, and then generate the algorithm. It is determined based on the technical path characteristics of HCI under Cybernetics and the essential attribute of AI as a tool. The AI creation process is the whole process of automatic generation of algorithms based on people's previous intellectual investment process.

2.5. Privacy Protection and Data Reliability of AI-Written Literary Creations. Data privacy protection methods are mainly divided into data slicing technology, data scrambling technology, and data encryption technology [22]. Data encryption technology is identity-based encryption (IBE), preventing attackers from directly obtaining user-perceived data content [23]. In this work, the Paillier encryption algorithm is used to realize the application's demand for data protection [24]. The specific algorithm process is as follows.

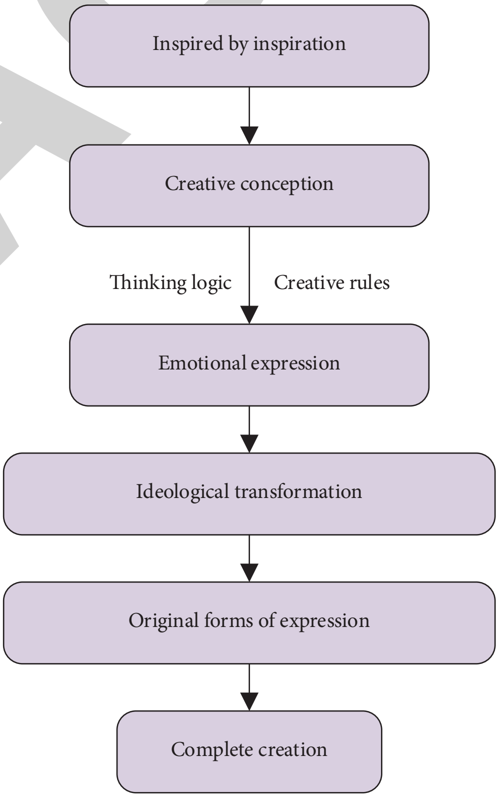


Figure 5: The creative process of natural person authors.

Key generation: the system sets security parameters for input and randomly generates two large prime numbers p and q. The length of these two prime numbers must satisfy the following:

$$\gcd(pq, (p-1)(q-1)) = 1. \tag{1}$$

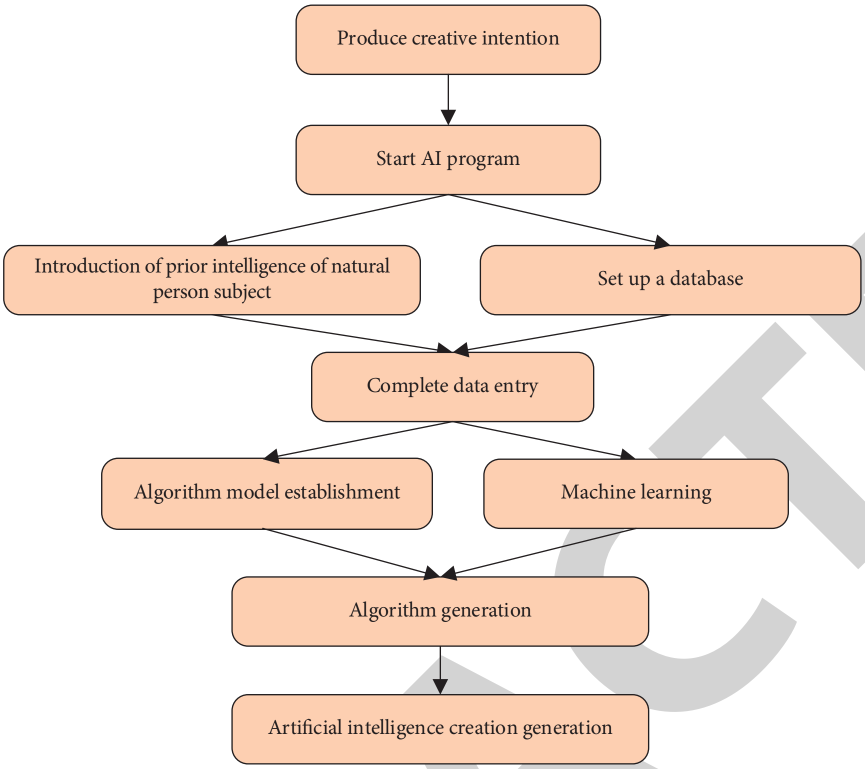

Produce creative intention
Start AI program
Introduction of prior intelligence of natural person subject
Set up a database
Complete data entry
Algorithm model establishment
Machine learning
Algorithm generation
Artificial intelligence creation generation

Figure 6: The creative process of AI.

The following equation calculates the parameter n of the public key pair (n, g):

$$n = p * q. \tag{2}$$

The parameter λ of the private key pair (λ, μ) is calculated as follows:

$$\lambda = lcm(p-1)(q-1). \tag{3}$$

The parameter μ of the private key pair (λ, μ) is calculated as follows:

$$\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1}. \tag{4}$$

Data encryption: set the encrypted plaintext as m and the public key parameter as g. The system randomly selects $r \in Z_{n^2}^*$, and $0 < r < 1$. The following equation uses the public key pair (n, g) to encrypt the plaintext to obtain the ciphertext:

$$c = g^m r^n \bmod n^2. \tag{5}$$

Data decryption: the private key pair (λ, μ) is used to decrypt ciphertext c, as demonstrated in

$$m = L\left(c^{\lambda} \bmod n^2\right) * \mu \bmod n. \tag{6}$$

In encrypting two plaintexts m_1 and m_2, the public key (n, g) is used to generate ciphertext c_1 and c_2. The expression of c_1 and c_2 reads

$$\begin{aligned} c_1 &= g^{m_1} r_1^n \bmod n^2, \\ c_2 &= g^{m_2} r_2^n \bmod n^2. \end{aligned} \tag{7}$$

Multiplying Eq. (7) and (8) obtains

$$c_1 * c_2 = g^{m_1} g^{m_2} r_1^n r_2^n \bmod n^2 = g^{m_1+m_2} * \left(r_1 \cdot r_2\right)^n \bmod n^2. \tag{8}$$

Set $r_1 * r_2 \in Z_{n^2}^*$, which is equivalent to $r^n \in Z_{n^2}^*$. Here, $c_1 * c_2$ is the ciphertext of $m_1 + m_2$. The private key (λ, μ) is used directly to generate decipher $c_{1*} c_2$ to get the results of $m_1 + m_2$. The specific expression reads

$$m_1 + m_2 = L\left(\left(c_{1*} c_2\right)^{\lambda} \bmod n^2\right) * \mu \bmod n. \tag{9}$$

After decrypting the private key once in the whole process, different encrypted plaintext can be obtained. The obtained plaintext is consistent with the plaintext before encryption.

2.6. Experimental Scheme Design and Experimental Environment Setting

2.6.1. SI Perception Mechanism for User Privacy and Data Reliability. This section establishes a SI perception mechanism for user privacy and data reliability. The SI perception system has three key factors: user privacy, data reliability, and incentive mechanism [25]. The relationship between them is laid out in Figure 7.

As shown in Figure 7, the three factors relate to and influence each other. Some malicious users may abuse user

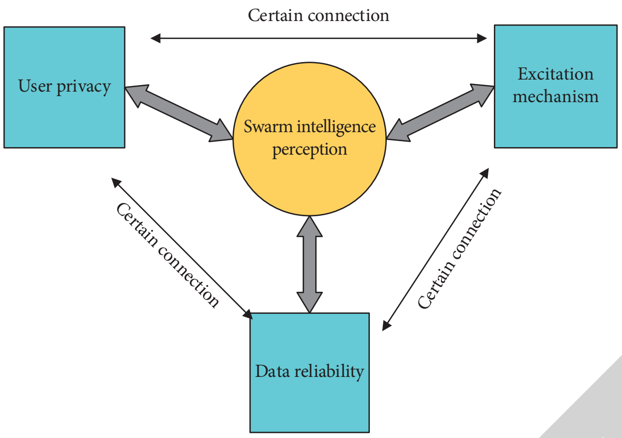


Figure 7: Internal relationship of SI perception factors.

privacy anonymously to submit false data, tamper with data, or steal other user information to obtain remuneration. Therefore, the system should encourage users to submit more reliable data.

2.6.2. SI Perception System Model. The SI perception system, also known as the perception platform (Server), is composed of four parts: Group Manager (GM), Pseudonym Authority (PA), Data Collectors (DCs), and participants [26]. The specific model is shown in Figure 8.

As shown in Figure 8, the sensing platform is a third-party service that provides data sensing services for DCs. The platform evaluates the participants' perception data. The platform feedbacks the reputation information to the participants and is used to update the reputation of later participants. GM is responsible for user registration, user task request Token, and managing the user reputation database. The PA can issue pseudonyms to participants. Participants submit data anonymously under a pseudonym, and the certificate is the submission voucher. Participants are composed of mobile users using smart devices. After registering with GM, participants can request tasks and submit perception data anonymously to the platform through Fifth Generation (5G) mobile communication network.

2.6.3. Scheme Design of PTISense Based on Encryption Technology. PTISense specifically refers to implementing Privacy Preservation, Data Trustworthiness, and Fair incentives in SI perception [27]. It can protect users' privacy and prevent malicious users from abusing privacy [28]. The specific scheme design is described in Figure 9.

According to Figure 9, the whole design is divided into seven steps. Users with a reputation lower than the minimum criteria will be deleted. Similarly, suppose the trust of a task data report is lower than the minimum requirement. All other data submitted by the corresponding user for the same task will be detected and determined as invalid data together.

In user registration, to perform perception task T_j, the first user P_i must send some private information to GM and get the task request Token. Then, blind signature technology is used to protect the task privacy of participants, and the requested task number T_j is blinded [29]. P_i selects a random number b as the blind factor, and b is coprime with the common modulus Q of GM. Further, P_i calculates the blinded task BT_j that is used together with real identity P_i as a Task Token Request (TTR) message. The TTR is sent to GM. BT_j is calculated as follows:

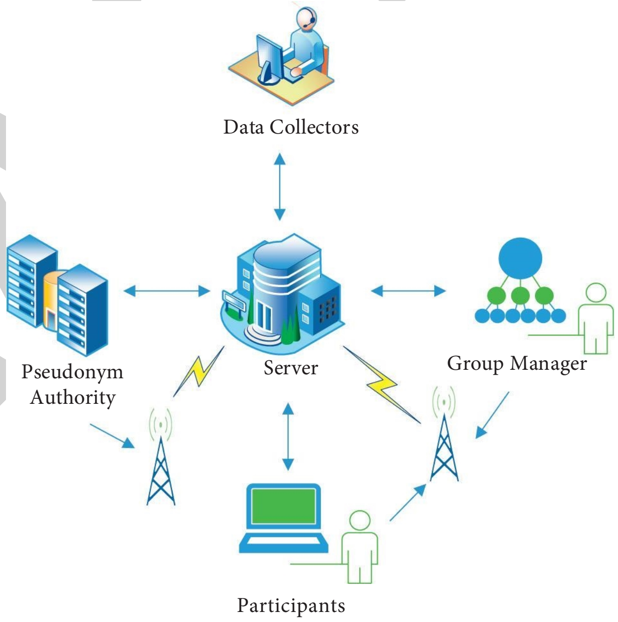


Figure 8: SI perception system model.

$$BT_j = T_j \cdot b^{pk_{GM}} \mathrm{mod} Q. \tag{10}$$

The user reputation level $L(P_i)$ is included in the Token. GM calculates two hash values h_i^1 and h_i^2, as shown in (11) and (12).

$$h_i^1 = H\left(P_i|R(P_i)|BT_j\right), \tag{11}$$

$$h_i^2 = H\left(P_i \mid BT_j\right). \tag{12}$$

Next, partial information of h_i^2 is bound. H is a single hash function. GM signs a signature on BT_j. Then,

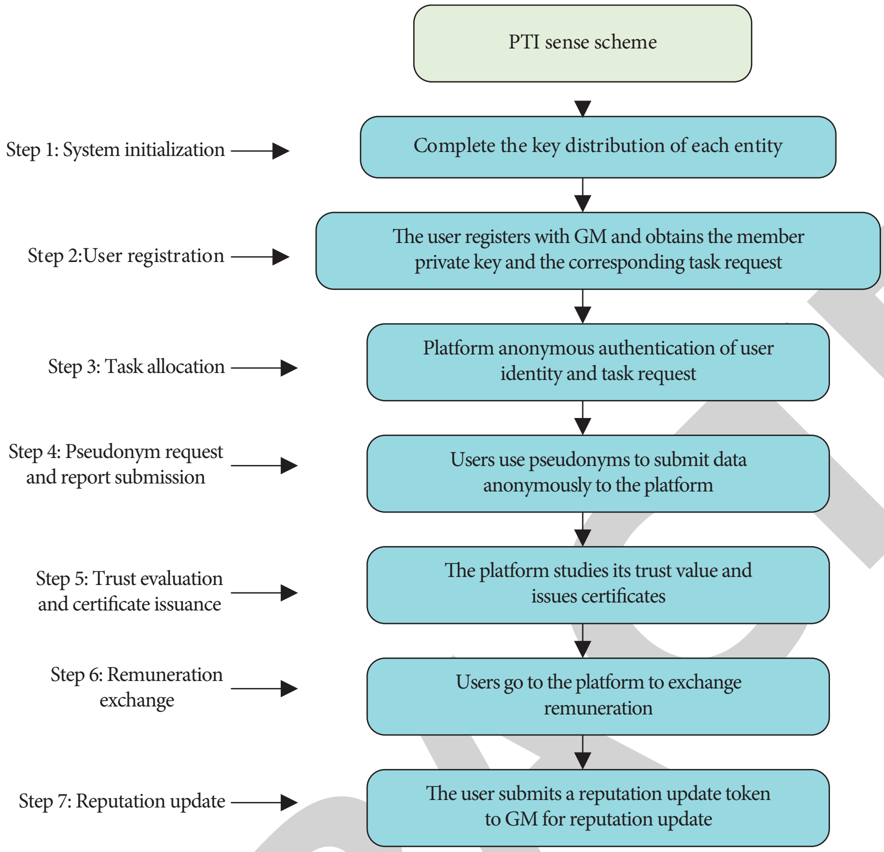

PTI sense scheme
Step 1: System initialization
Complete the key distribution of each entity
Step 2:User registration
The user registers with GM and obtains the member private key and the corresponding task request
Step 3: Task allocation
Platform anonymous authentication of user identity and task request
Step 4: Pseudonym request and report submission
Users use pseudonyms to submit data anonymously to the platform
Step 5: Trust evaluation and certificate issuance
The platform studies its trust value and issues certificates
Step 6: Remuneration exchange
Users go to the platform to exchange remuneration
Step 7: Reputation update
The user submits a reputation update token to GM for reputation update

Figure 9: PTISense scheme design process.

Table 1: Experimental parameter setting.

Names	Setting
Participant	100
Malicious participant η	10
Reputation threshold setting	0.2–0.8
Number of tasks M	0–40
Number of malicious nodes	0–50
Number of data reports n	5–25
Client equipment	Mobile phone Snapdragon 830
Client CPU	2.0 GHz
Physical end equipment	AMD Athlon M320
Entity end CPU	2.1 GHz

calculating τ_i^j constructs the request for P_i on task T_j. The specific calculation of τ_i^j reads

$$\tau_i^j = \left\{h_i^1, h_i^2, \left\{BT_j\right\}_{sk_{GM}}, L\left(P_i\right)\right\}_{sk_{GM}}. \tag{13}$$

This section evaluates the performance of the PTISense scheme design based on encryption technology. The main performance indicators include the accuracy of the reputation/trust evaluation model, the robustness against malicious users, and the computing overhead at each end.

2.6.4. Experimental Environment. According to Wang et al., combined with the text theory, the simulation experiment parameters are designed [30], as shown in Table 1.

3. Experimental Results and Analysis

3.1. Performance Analysis of PTISense Scheme Based on Encryption Technology

3.1.1. Influence of Design Scheme on the Accuracy of Reputation Model. Under different trustworthiness thresholds ε, the false-positive (FP) and false-negative (FN) rates are analyzed in Figure 10.

As shown in Figure 10, FP means that some credible reports are calculated to have a trust value lower than ε. In an FN case, an actually credible report is calculated to have a trust value higher than ε. There is a great difference between the FN rate and the FP rate, and the FN rate tends to be zero as a whole. FP and FN rates are meager, given a tiny ε. As ε further increases, the FP rate increases while the FN rate becomes 0. This phenomenon is reasonable. Due to a large threshold of ε, the probability that the trustworthiness of a real trusted report is lower than ε is high. The probability that the trustworthiness of a real untrusted report is higher than ε is basically 0. When users perform more tasks, the FP and FN rates decrease to varying degrees. This is because the user reputation will be updated after each task. Therefore, the accuracy of data trustworthiness evaluation based on the updated user reputation is higher. When $\varepsilon = 0.5$, after the user completes 50 tasks, the FP rate is only 0.1, and the

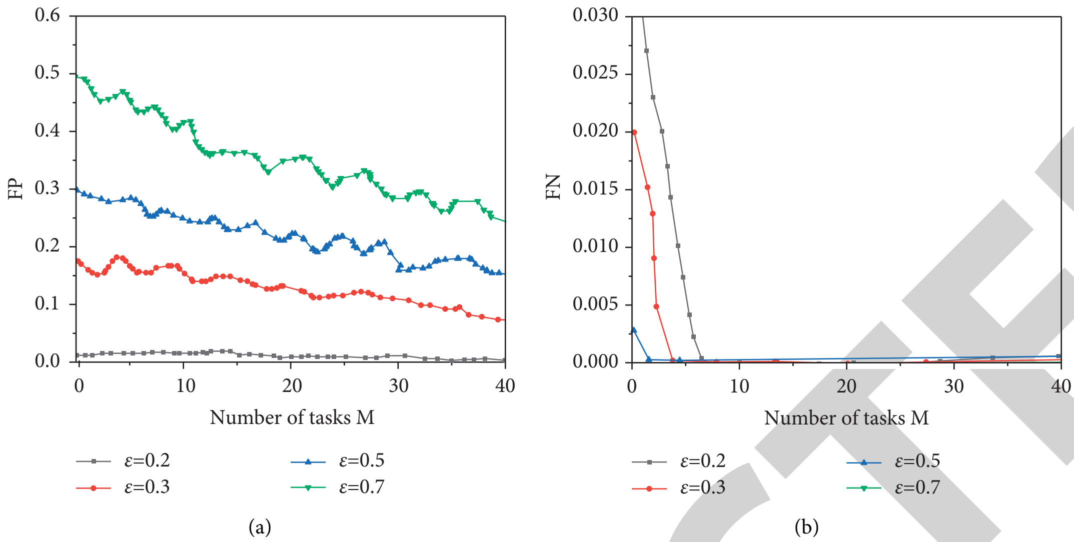


Figure 10: Changes in trustworthiness evaluation models with different trustworthiness thresholds. (a) FP rate; (b) FN rate.

corresponding FN rate is 0. Thus, the trustworthiness model of the PTISense scheme based on encryption technology has high accuracy.

3.1.2. Robustness Analysis of Design Scheme against Malicious Users.

Under different numbers of malicious users η, the change of reputation of a malicious user with the number of tasks is analyzed in Figure 11.

According to Figure 11, under a small number of malicious users η, the more tasks are performed, the faster user reputation decreases and gradually tends to zero. When malicious users gradually increase, the decline rate of reputation slows down with a downward trend. Finally, with the increase in tasks, the reputation tends to zero. The malicious user data are contrary to those of Users with Good Reputations (credible users). The data trustworthiness is low, and the negative trustworthiness feedback level is high. When η increases, the untrusted data report increases, the negative trustworthiness feedback level decreases, and the reputation decline rate value slows down. When the system has more than 50% malicious users, untrusted data dominate. This results in the malicious user data being mistaken for trusted and maintaining a high reputation level. Therefore, as long as the credible users outnumber malicious users, the reputation and trustworthiness evaluation model of the PTISense scheme can accurately identify low-quality data and malicious nodes with low reputations. It can identify malicious users with low reputations, protect the credible users' data, and protect the data and privacy of credible users.

3.1.3. Practical Feasibility Evaluation and Analysis of the Proposed PTISense Scheme.

To measure the computation overhead of each entity, the running time of the basic cryptographic element operation is given in milliseconds. The specific results are presented in Figure 12.

Figure 12 shows the overhead of different entities in each stage of SI perception ($n = 10$). “Participants” refers to the participants in the SI perception system, “Server” is the perception platform, and “GM” is the group administrator. “PA” is the pseudonym center. Apparently, computing overhead is concentrated on the perception platform, and the credential generation phase takes up the most time. The client overhead is concentrated in the voucher generation stage. It can be observed from Figure 12 that it takes about 430 ms to submit ten reports, which is relatively low for the whole SI perception-based privacy protection system. The lower the overhead is, the more feasible the scheme is.

3.2. Comparative Analysis of Proposed PTISense Scheme and Other Schemes

3.2.1. Comparison of Client Computation Overhead of Different Schemes in Different Stages.

The proposed PTISense scheme is compared with other schemes. As a result, other schemes do not involve encryption technology. Further, Figure 13 analyzes the client overheads in different stages.

According to Figure 13, in the task allocation stage, the computing overhead of users and perception platforms in the proposed PTISense scheme remains stable within 170 ms. The other scheme's corresponding computing overhead increases with the number of reports n. When $n = 25$, the computing overhead approximates 600 ms. In the voucher generation stage, the difference between the two schemes is not large, but the value of the proposed PTISense scheme is lower. In the compensation exchange stage, Figure 13(c) highlights the advantages of the proposed PTISense scheme, with a lower computational overhead, almost zero. Overall, the proposed PTISense scheme can achieve a safe and reliable SI perception with lower computing overhead and has more prominent advantages for users with limited energy. The security and reliability of data are guaranteed.

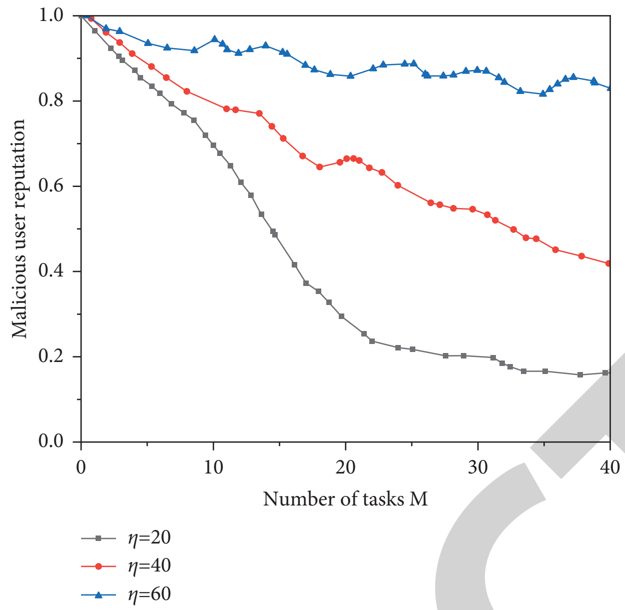


Figure 11: Changes in malicious user reputation with the number of tasks.

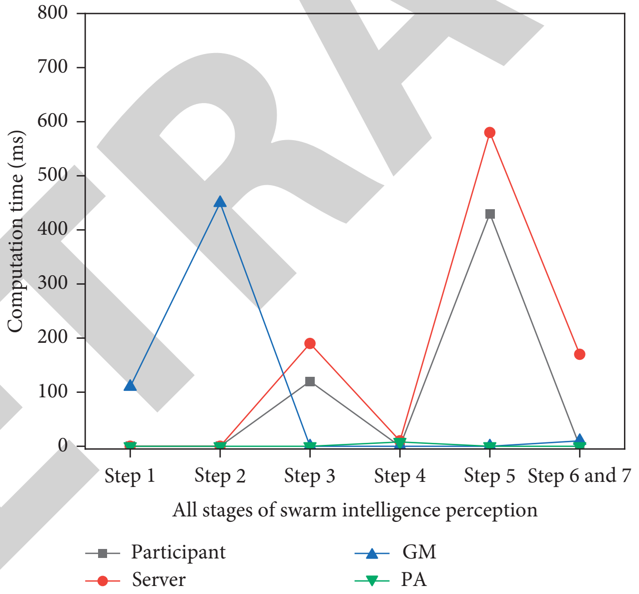
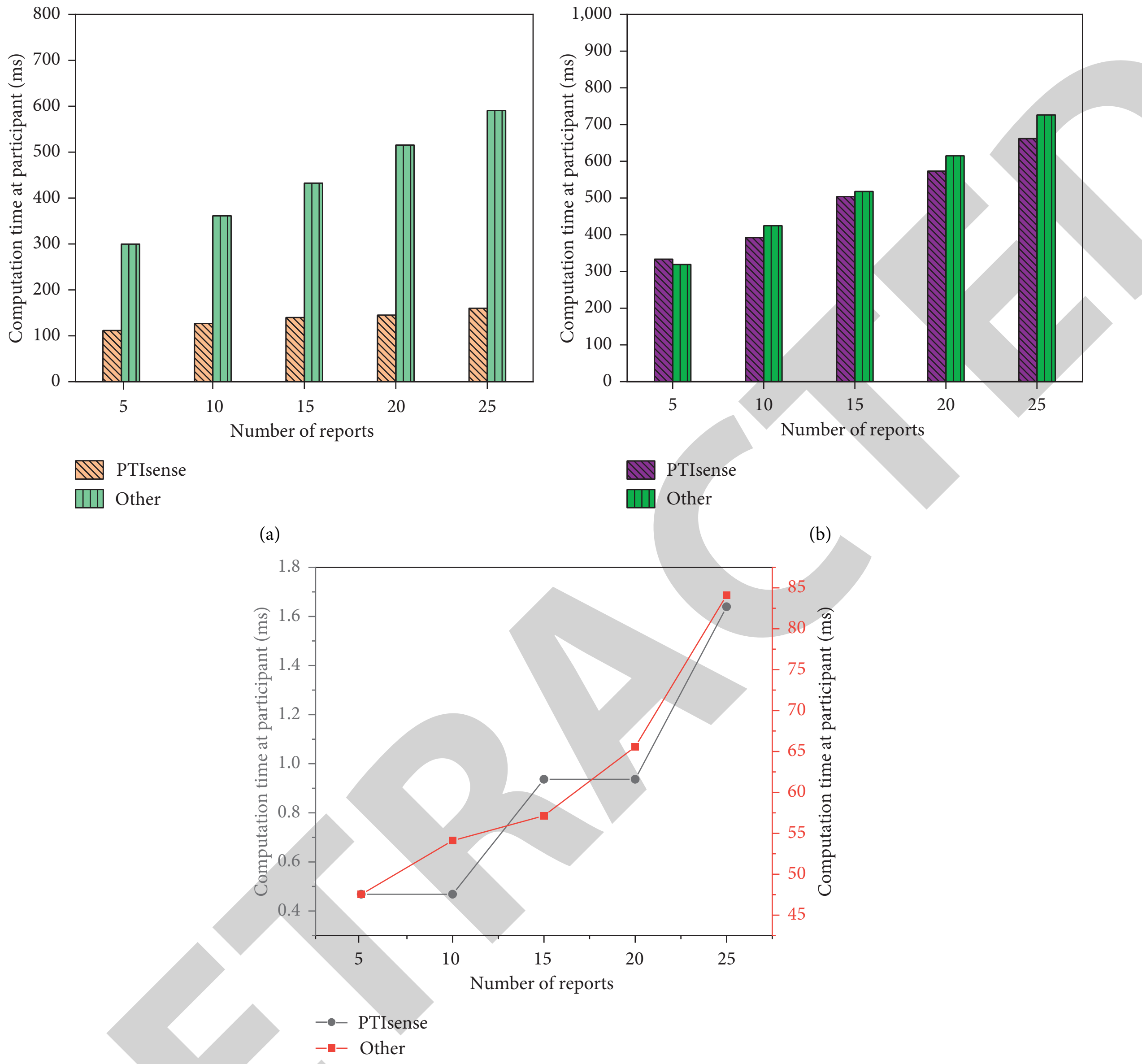


Figure 12: The computing cost of each entity in different stages of SI perception.

3.2.2. Comparison of SI Perception Platform Computation Overhead of Different Schemes in Different Stages. The calculation results of the SI perception platform overhead of different schemes in the stages of task allocation, voucher generation, and compensation exchange are compared in Figure 14.

According to Figure 14, in the task allocation phase, the computing overhead of the user and the perception platform in



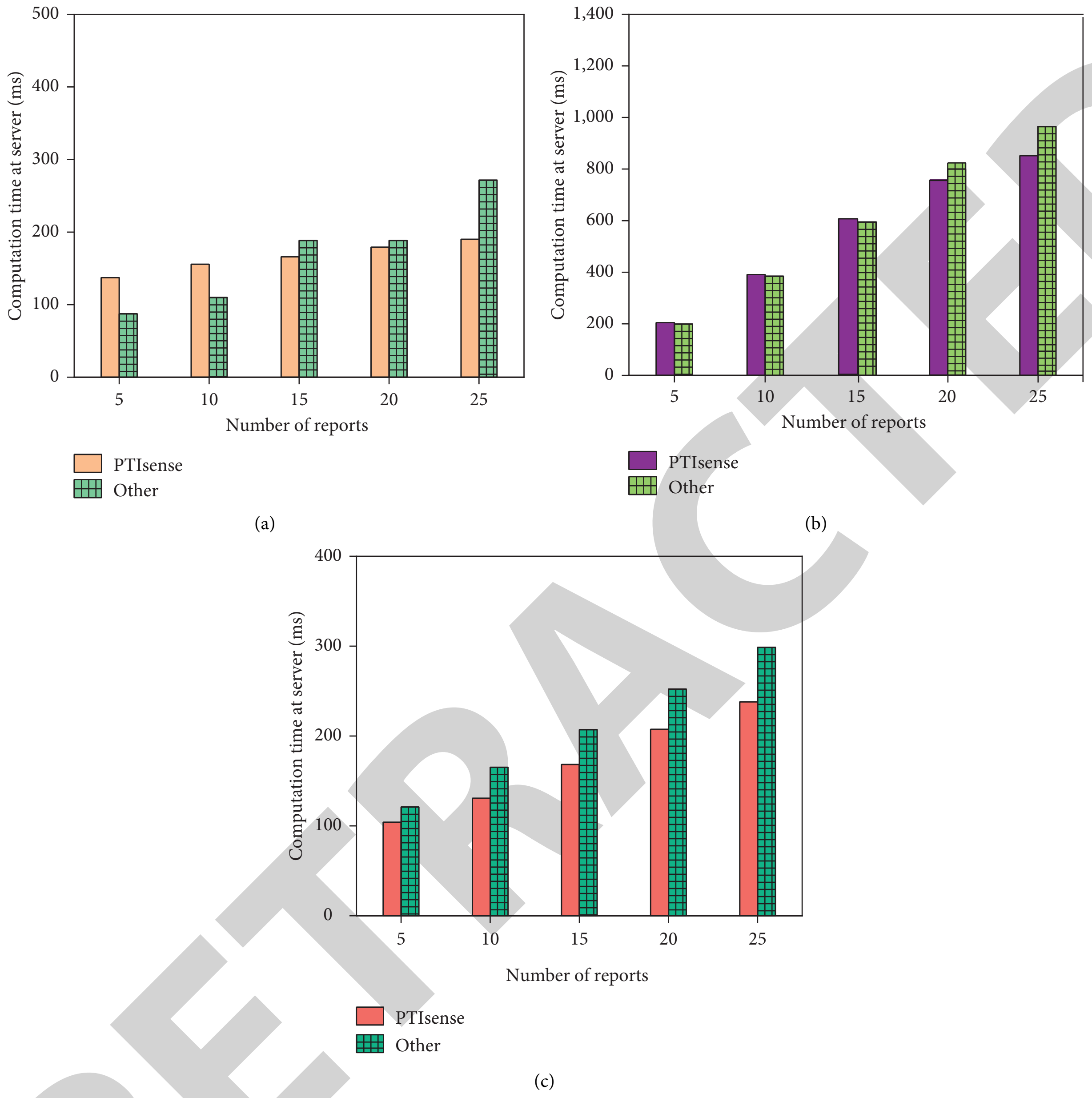
(a)

(b)

(c)

Figure 13: Comparison of client computation overhead in different stages. (a) Task allocation stage; (b) voucher generation stage; (c) compensation exchange stage.

the proposed PTISense scheme remains stable within 200 ms. The computational overhead of the other scheme increases with the number of reports n. When $n = 25$, the computational overhead approximates 280 ms. The perception platform encrypts each trust feedback value in the voucher generation stage. The computational overhead of the proposed PTISense scheme's perception platform is smaller than the other scheme. In the compensation exchange stage, when $n = 25$, the overhead of the proposed PTISense and the other schemes approximates 240 ms and 300 ms, respectively. The above analysis shows that



(a)

(b)

(c)

Figure 14: Comparison of platform computation overhead in different stages. (a) Task allocation stage; (b) voucher generation stage; (c) compensation exchange stage.

PTISense can realize a safe and reliable SI perception with a lower computing overhead. It presents stronger data protection and can better ensure the authenticity and reliability of data.

4. Conclusion

With the in-depth development of AI technology, AI-written literary creations' copyright disputes are not uncommon. There is an urgency to protect the copyright of AI, where data reliability is the focus of research. This work uses an encryption algorithm to study the privacy protection and data reliability of AI-written literary creations. It designs a SI perception model and PTISense scheme based on encryption technology. Through experimental tests, the performance of the PTISense scheme based on encryption technology is analyzed and compared with other schemes. It mainly analyzes the PTISense scheme's impact on the reputation model's accuracy and its robustness against malicious users. Its feasibility is further evaluated. The test results are as follows. (1) Under different trustworthiness thresholds ε, the trustworthiness model of the proposed PTISense scheme based on encryption technology has high accuracy. (2) The proposed PTISense scheme's reputation and trustworthiness evaluation model can accurately identify low-quality data and malicious nodes with low reputation. It can protect the data credible users' data and resist malicious users to protect the data and privacy of credible users. (3) By measuring the computation overhead of each entity in different stages of SI perception, it is concluded that this design scheme is feasible for the SI perception of privacy protection. (4) Compared with other schemes, the proposed PTISense scheme can realize a safe and reliable SI sensing process with lower computation overhead, has stronger data protection, and ensures data authenticity and reliability. The deficiency of this work is that the performance research needs to be expanded. There is less research on practical application. Studying more performance and detailed comparison with other schemes are also the direction of future work.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] G. Rong, A. Mendez, and E. B. Assi, "Artificial intelligence in healthcare: review and prediction case studies," *Engineering*, vol. 6, no. 3, pp. 291–301, 2020.

[2] C. Zhang and Y. Lu, "Study on artificial intelligence: the state of the art and future prospects," *Journal of Industrial Information Integration*, vol. 23, Article ID 100224, 2021.

[3] S. Bag, S. Gupta, A. Kumar, and U. Sivarajah, "An integrated artificial intelligence framework for knowledge creation and B2B marketing rational decision making for improving firm performance," *Industrial Marketing Management*, vol. 92, pp. 178–189, 2021.

[4] G. Spindler, "Copyright law and artificial intelligence," *IIC-International Review of Intellectual Property and Competition Law*, vol. 50, no. 9, pp. 1049–1051, 2019.

[5] Z. Naqvi, "Artificial intelligence, copyright, and copyright infringement," *Marquette Intellectual Property Law Review*, vol. 24, p. 15, 2020.

[6] N. Selvadurai and R. Matulionyte, "Reconsidering creativity: copyright protection for works generated using artificial intelligence," *Journal of Intellectual Property Law & Practice*, vol. 15, no. 7, pp. 536–543, 2020.

[7] C. w Shen and J. t Ho, "Technology-enhanced learning in higher education: a bibliometric analysis with latent semantic approach," *Computers in Human Behavior*, vol. 104, Article ID 106177, 2020.

[8] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: a review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol. 66, Article ID 102655, 2021.

[9] J. W. Hong and N. M. Curran, "Artificial intelligence, artists, and art: attitudes toward artwork produced by humans vs. artificial intelligence," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 15, no. 2s, pp. 1–16, 2019.

[10] S. Feng, "The application of artificial intelligence technology in the field of artistic creation," in *Proceedings of the International Conference on Cognitive Based Information Processing and Applications (CIPA 2021)*, pp. 537–543, Springer, Singapore, September 2022.

[11] Z. Lv, Y. Han, A. K. Singh, G. Manogaran, and H. Lv, "Trustworthiness in industrial IoT systems based on artificial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1496–1504, 2021.

[12] J. X. Wang, "Meta-learning in natural and artificial intelligence," *Current Opinion in Behavioral Sciences*, vol. 38, pp. 90–95, 2021.

[13] G. Boeing, M. Besbris, A. Schachter, and J. Kuk, "Housing search in the age of big data: smarter cities or the same old blind spots?" *Housing Policy Debate*, vol. 31, no. 1, pp. 112–126, 2021.

[14] Z. Shan, Y. Zhang, Y. Zhang, S. Tang, and W. Wang, "A review of recent progress and developments in China smart cities," *IET Smart Cities*, vol. 3, no. 4, pp. 189–200, 2021.

[15] H. Yarong, "A study of xu dishan's literary creation from the perspective of southeast asia," *Art and Performance Letters*, vol. 2, no. 1, pp. 71–77, 2021.

[16] C. Wang, T. S. H. Teo, and M. Janssen, "Public and private value creation using artificial intelligence: an empirical study of AI voice robot users in Chinese public sector," *International Journal of Information Management*, vol. 61, Article ID 102401, 2021.

[17] A. N. Bakhtiyari, Z. Wang, L. Wang, and H. Zheng, "A review on applications of artificial intelligence in modeling and optimization of laser beam machining," *Optics & Laser Technology*, vol. 135, Article ID 106721, 2021.

[18] H. Sun, "Redesigning copyright protection in the era of artificial intelligence," *Iowa Law Review*, vol. 107, no. 3, pp. 1213–1251, 2022.

[19] J. M. N. Zatarain, "The role of automated technology in the creation of copyright works: the challenges of artificial intelligence," *International Review of Law, Computers & Technology*, vol. 31, no. 1, pp. 91–104, 2017.

[20] Y. Sun, C. Xu, G. Li et al., "Intelligent human computer interaction based on non redundant EMG signal," *Alexandria Engineering Journal*, vol. 59, no. 3, pp. 1149–1157, 2020.

[21] Z. Navruz-zoda, "Evaluation of holy places of the regions for the development of pilgrimage tourism," *Indonesian Journal of Law and Economics Review*, vol. 6, 2020.

[22] Y. Duan, Z. Lu, Z. Zhou, X. Sun, and J. Wu, "Data privacy protection for edge computing of smart city in a DIKW architecture," *Engineering Applications of Artificial Intelligence*, vol. 81, pp. 323–335, 2019.

[23] I. Indu, P. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: mechanisms and challenges," *Engineering science and technology, an international journal*, vol. 21, no. 4, pp. 574–588, 2018.

[24] W. Fang, M. Zamani, and Z. Chen, "Secure and privacy preserving consensus for second-order systems based on paillier encryption," *Systems & Control Letters*, vol. 148, Article ID 104869, 2021.

[25] M. Hasal, J. Nowaková, K. Ahmed Saghair, H. Abdulla, V. Snasel, and L. Ogiela, "Chatbots: security, privacy, data protection, and social aspects," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 19, 2021.

[26] Y. Luo, S. Li, and D. Li, "Intelligent perception system of robot visual servo for complex industrial environment," *Sensors*, vol. 20, no. 24, p. 7121, 2020.

[27] H. Wu, L. Wang, G. Xue, J. Tang, and D. Yang, "Enabling data trustworthiness and user privacy in mobile crowdsensing," *IEEE/ACM Transactions on Networking*, vol. 27, no. 6, pp. 2294–2307, 2019.

[28] P. Lu, H. Yang, H. Li, M. Li, and Z. Zhang, "Swarm intelligence, social force and multi-agent modeling of heroic

altruism behaviors under collective risks," *Knowledge-Based Systems*, vol. 214, Article ID 106725, 2021.

[29] H. Xiao and Z. Zhang, "Swarm intelligence approaches to power allocation for downlink base station cooperative system in dense cellular networks," *Science China Information Sciences*, vol. 63, no. 6, Article ID 169302, 2020.

[30] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Enabling reputation and trust in privacy-preserving mobile sensing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2777–2790, 2014.