Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5866570, 14 pages
https://doi.org/10.1155/2022/5866570

Research Article

Cloud Platform Credibility Assessment System Based on D-S Theory and Blockchain Technology

Ming Yang, Li Jia, Tilei Gao, Yuanyuan He, Bin Gui, and Tao Zhang

School of Information, Yunnan University of Finance and Economics, Kunming 650221, China

Correspondence should be addressed to Tilei Gao; gtllei@ynufe.edu.cn

Received 17 May 2022; Revised 1 July 2022; Accepted 7 July 2022; Published 1 August 2022

Academic Editor: Yin Zhang

Even well-known cloud platforms will have sudden credibility problems in the long-term application process. Effectively evaluating the credibility of the cloud platform and providing users with scientific evaluation results can help users reasonably choose a trusted cloud platform. However, there are often conflicting opinions or malicious assessments in the process of assessment. In addition, the personal privacy information of the users participating in the assessment is at risk of being leaked, and the data that the users have evaluated is also easy to be modified. In order to solve the above problems, this paper defines the credibility category and confidence interval of cloud platform, puts forward a quantitative assessment method combined with fuzzy theory, and realizes the fusion of different users' assessment results based on D-S theory. On this basis, this paper further proposes an effective cloud platform credibility assessment system combined with blockchain technology. Finally, through experimental analysis, this paper shows that the credibility assessment system proposed in this paper is feasible and illustrates the characteristics of the system through method comparison. The system solves the problem of conflicting information in the assessment process, can effectively assess the credibility of the cloud platform, and effectively protects user privacy and the security of assessment data with blockchain technology.

1. Introduction

According to "the first quarter 2020 global data center infrastructure revenue data" released by synergy research group, benefiting from the significant growth of cloud computing demand during the epidemic, the revenue of the global cloud computing market in the first quarter increased by 37% year-on-year. According to "2020 cloud status report" published by Flexera [1], 59% of enterprises expect cloud usage to exceed previous plans. The above report shows that the demand for cloud services in the global market is gradually increasing. However, due to the cloud platform characteristics such as improper management, complex network transmission, huge data storage demand, large number of tenants, and diverse services of cloud platform, there are large credibility problems in the cloud platform. According to the report of Amazon which is the largest cloud computing provider, its company's cloud platform and services had 22 sudden failures during 2010-2019. The report shows that even well-known platforms will have credibility problems. Therefore, when choosing a cloud platform, users need to understand the credibility of the platform. The most effective way is to refer to the comments of users who have used it. However, in the absence of effective evaluation methods and tools, the value of the assessment results given by users who do not have professional knowledge will be greatly reduced. In addition, when users participate in the assessment process, there is bound to be the problem of privacy information being leaked, and the users' assessment results will also have the possibility of being tampered with or deleted. Therefore, in order to effectively assess the cloud platform credibility and give scientific assessment results, it is necessary to establish special assessment systems, methods, and tools.

Shen [2] pointed out that credibility includes reliability and safety. Yang [3] pointed out that credibility includes ability credibility, integrity credibility, predictability, correctness, privacy, and loss cost. As a kind of credibility evaluation, the credibility evaluation process of cloud platform is bound to be affected by human subjective factors [4]. In

the process of assessment, due to the influence of human subjective factors, conflict information is bound to appear. In addition, in the process of assessment, it is difficult to give an accurate credibility assessment result due to the influence of users or experts' own complex psychology.

Therefore, how to ensure the objectivity of the assessment, solve the problem of conflicting information in the assessment process, and reduce the scoring difficulty of users are the problems that need to be solved to realize the credibility assessment of cloud platform. In order to ensure the objectivity, relevant studies at home and abroad include the assessment method based on AHP (Analytic Hierarchy Process) [5–11] and the uncertainty assessment method based on information entropy [12–16]. These relevant studies establish an effective credibility assessment system, and realize the quantitative assessment of multi-index system through pairwise comparison, which effectively reduces the impact of human subjective factors on the assessment results. In order to solve the conflict information in the assessment process, scholars at home and abroad have carried out many studies based on D-S evidence theory [17–22]. These related studies point out that using D-S fusion method can effectively solve the problem of conflicting information in the assessment process. In order to ensure the accuracy of the assessment results and reduce the scoring difficulty of users in the assessment process, Wang et al. [23, 24] proposed effective solutions based on fuzzy theory. It can be seen that the comprehensive use of the above methods will effectively solve the problems existing in the cloud platform credibility assessment.

However, in addition to solving the above problems, the cloud platform credibility assessment also faces the problems of privacy security and how to ensure data integrity. It is known that when participating in the assessment, users will leave relevant transaction information and personal information. This leads to the risk that the user's privacy will be stolen or leaked. In order to protect the privacy information of users during evaluation, Shi [25] and Yang [26] both proposed an assessment mechanism based on blockchain, which effectively protects the privacy of users participating in assessment through blockchain technology and can trace the responsibility of malicious users through blockchain traceability technology [27]. In addition, the tamper-proof characteristics of blockchain can also ensure the integrity of assessment data and provide users with continuous and real assessment results in time.

Therefore, in order to realize the effective cloud platform credibility assessment, this paper comprehensively uses the above-mentioned methods to carry out the analysis. Firstly, combined with fuzzy theory, this paper defines the credibility category of cloud platform and its corresponding confidence interval, puts forward the assessment method of cloud platform credibility, and realizes the fusion of different users' assessment results based on D-S theory. On this basis, in order to ensure the privacy of users participating in the evaluation and ensure that the generated evaluation results cannot be tampered with, this paper combines the blockchain technology with the proposed credibility assessment method, proposes an effective assessment block generation method, designs the corresponding consensus mechanism, smart contract and incentive mechanism, and finally proposes a credibility evaluation system based on blockchain technology and D-S theory. The system integrates the characteristics of blockchain technology and D-S theory and provides an effective scheme for the cloud platform credibility assessment.

This paper can be divided into the following parts: in Section 1, this paper introduces the research background and content; in Section 2, the credibility category and confidence interval of cloud platform are defined based on fuzzy theory, and a credibility assessment result fusion method based on D-S theory is proposed to realize the effective evaluation of cloud platform credibility; in Section 3, based on the proposed cloud platform credibility assessment method, this paper further proposes a cloud platform credibility assessment system combined with blockchain technology; in Section 4, in order to verify the effectiveness of the proposed credibility evaluation system, this paper carries out relevant experimental analysis and compares the proposed assessment method with other methods in many aspects; in Section 5, the authors summarize the research work of this paper and point out the future research direction.

2. Cloud Platform Credibility Assessment Method Based on D-S Evidence Theory

Cloud platform generally refers to cloud service platform, which provides users with computing, network, and storage capabilities through distributed processing technology. Because the cloud platform has the characteristics such as large number of tenants, huge data storage demand, complex network transmission, and diverse service functions, its credibility will be affected by many factors in the actual application process, as shown in Figure 1.

These factors include infrastructure credibility, service function credibility, network credibility, service provider management credibility, and platform internal environment credibility. Their meanings and examples are shown in Table 1.

Therefore, to assess the credibility of cloud platform, we need to focus on the credibility category β_i described in Table 1 and carry out comprehensive assessment from multiple aspects.

For example, the infrastructure credibility in Table 1 can be judged by users through the infrastructure information published by the platform. Common information includes number of global acceleration nodes, number of servers, number of data centers, and coverage areas. Users can make basic judgments and give scores through this information. In addition, with the operation of the cloud platform, users who have participated in the assessment can also add scores according to relevant reports or infrastructure failure problems during use. If the platform does not publish the relevant infrastructure information and the user cannot obtain the infrastructure information of the platform, the user can consider the platform's infrastructure credibility as untrusted.

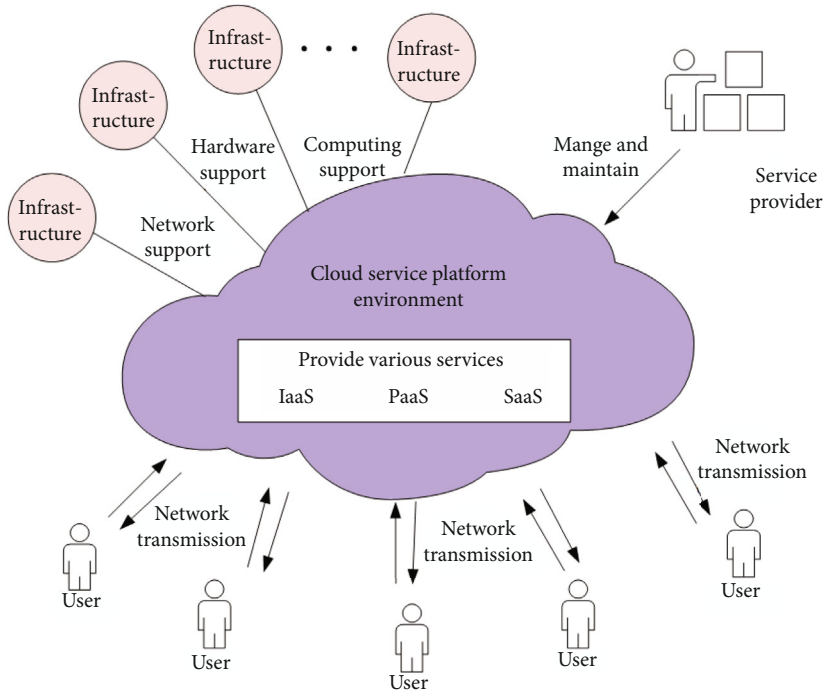

Figure 1: Multiple factors affecting the credibility of cloud platform.

Table 1: Cloud platform trustworthiness category.

β_i	Credibility category	Meaning	Example of credibility problems
β_1	Infrastructure credibility	It refers to the credibility of the platform physical infrastructure.	Such as dilapidated infrastructure, damaged infrastructure, and data center disaster
β_2	Service function credibility	It refers to the credibility of the platform service in terms of function.	Such as lack of function, poor usability, and difficulty in function expansion
β_3	Network credibility	It refers to the credibility of the platform in terms of network transmission.	Such as unstable network transmission, lack of effective network defense support, and vulnerable to DDoS attack or CC attack
β_4	Service provider management credibility	It refers to the credibility of the platform provider in the management of platform environment, services, infrastructure, network, etc.	Such as untimely maintenance and updating and no clear responsibility attribution agreement
β_5	Platform internal environment credibility	It refers to the credibility of the platform internal environment.	Such as the mandatory function of the platform and the attack of other cloud tenants in the same platform

Next, this paper will focus on these 5 credibility categories β_i and put forward effective assessment methods from the perspective of users.

2.1. Confidence Interval of Cloud Platform and Its Assessment Method. It is known that for users who do not have professional knowledge, it is difficult to give an accurate assessment when evaluating the credibility of cloud platform. They can only give a general assessment according to their own use experience, that is, ordinary users can only give a vague assessment. Therefore, this paper will assess the credibility of cloud platform based on fuzzy theory.

Fuzzy theory [28] is based on Fuzzy Set, and its research goal is to deal with uncertain things with fuzzy concepts. Fuzzy Set refers to the set with uncertain boundaries. Since the cloud platform credibility is also a fuzzy concept that is difficult to describe, its credibility can be described by Fuzzy Set.

Firstly, according to the fuzzy theory, this paper sets 5 fuzzy confidence intervals of cloud platform, which are defined as shown in Table 2.

According to the division of Table 2, users can give a fuzzy assessment result according to their use experience. There are 5 possible arbitrary sets of the result, namely, $\{1, 2, 3\}$, $\{3, 4, 5\}$, $\{4, 5, 6, 7\}$, $\{6, 7, 8\}$, $\{8, 9, 10\}$. Among them, $A_3 = \{4, 5, 6, 7\}$ indicates that the credibility level of the cloud platform is between 4 and 7. The greater the credibility level, the more credible the cloud platform is.

As mentioned above, when judging the credibility of the cloud platform, users do not need to give an accurate value,

Table 2: The 5 fuzzy confidence intervals of cloud platform.

Confidence interval	Meaning	The arbitrary sets of credibility level
A_1 completely credible	The platform has few credibility problems and can be fully trusted.	$A_1 = \{8910\}$
A_2 more credible	During the use of the platform service, the credibility problem occasionally occurs.	$A_2 = \{678\}$
A_3 basically credible	The platform has potential credibility problems and belongs to a general trusted platform.	$A_3 = \{4567\}$
A_4 basically untrusted	The platform has obvious credibility problems and is basically untrusted.	$A_4 = \{345\}$
A_5 completely untrusted	The platform is completely untrusted.	$A_5 = \{123\}$

but only need to select one of the confidence intervals. Using the above methods can reduce the difficulty of scoring and obtain the effective assessment results given by users.

2.2. Assessment Result Fusion Method Based on D-S Theory. Next, after collecting the assessment results given by multiple users, these assessment results can be fused with the fusion rules of D-S theory, so as to obtain a more accurate credibility assessment result.

D-S evidence theory [21] is an uncertain reasoning method, which is often used for multi-information fusion. It can effectively deal with the problem of conflict information in the fusion process and fuse the relevant information through calculation.

Suppose that the assessment results given by user 1 and user 2 for a certain platform are shown in Table 3, and the fusion process is as follows.

Step 1: the trust degree $m(A_j)$ of cloud platform confidence interval.

Assessment 1 and Assessment 2 in Table 3 represent the assessment results of the two users, respectively. $m_i(A_j)$ represents the trust degree of A_j given by user i. The greater the value of $m(A_j)$, the greater the possibility that the credibility level of the cloud platform belongs to A_j. The calculation formula of $m(A_j)$ is as follows.

$$m(A_j) = \sum_{\forall \mathrm{lev}(\beta_i) \in A_j} W(\beta_i). \tag{1}$$

In formula (1), $\mathrm{lev}(\beta_i)$ indicates the confidence interval of β_j, and $\mathrm{lev}(\beta_j) \in A_i$ indicates that the user assesses the confidence interval of β_j as A_i.

$W(\beta_j)$ represents the assessment weight of the credibility category β_j, $\sum_{j=1}^{5} W(\beta_j) = 1$. The greater the value of $W(\beta_j)$, the greater the influence weight of credibility category β_j on the credibility of the whole cloud platform. In order to ensure the effectiveness of the assessment, this paper proposes to use the entropy weight method to update the weight value of each credibility category in real time. According to the entropy weight method [29], for a credibility category β_j, the greater the difference between the assessment results, the higher the value of $W(\beta_j)$. Conversely, the lower the value of $W(\beta_j)$. With the increase of user assessment data, the weight value $W(\beta_j)$ of each credibility category will gradually change.

Table 3: Assessment results given by two users.

The arbitrary set A_i	Assessment 1	Assessment 2
$A_5 = \{8910\}$	$m_1(A_5)$	$m_2(A_5)$
$A_4 = \{678\}$	$m_1(A_4)$	$m_2(A_4)$
$A_3 = \{4567\}$	$m_1(A_3)$	$m_2(A_3)$
$A_2 = \{345\}$	$m_1(A_2)$	$m_2(A_2)$
$A_1 = \{123\}$	$m_1(A_1)$	$m_2(A_1)$

Table 4: The 5 credibility category assessments given by user 1 and user 2.

Credibility category β_j	User 1's assessment of $\mathrm{lev}(\beta_j)$	User 2's assessment of $\mathrm{lev}(\beta_j)$
β_1	A_5	A_4
β_2	A_4	A_4
β_3	A_4	A_4
β_4	A_4	A_3
β_5	A_3	A_3

As shown in the following example, assume that the assessment weights of the 5 credibility categories of a cloud platform are equal, $W(\beta_j) = 0.200$, $j = 1, 2, \cdots, 5$. The 5 credibility category assessments given by user 1 and user 2 are shown in Table 4.

By substituting the user assessment data of Table 4 into formula (1) for calculation, the trust degree $m_i(A_j)$ of the cloud platform's confidence interval can be obtained. The results are as follows.

$$m_1(A_5) = W(\beta_1) = 0.200, m_2(A_5) = 0.000, \tag{2}$$

$$m_1(A_4) = \sum_{j=2}^{4} W\left(\beta_j\right) = 0.600, m_2(A_4) = \sum_{j=1}^{3} W\left(\beta_j\right) = 0.600, \tag{3}$$

$$m_1(A_3) = W(\beta_5) = 0.200, m_2(A_3) = \sum_{j=4}^{5} W\left(\beta_j\right) = 0.400, \tag{4}$$

$$m_1(A_2) = 0.000, m_2(A_2) = 0.000, \tag{5}$$

$$m_1(A_1) = 0.000, m_2(A_1) = 0.000. \tag{6}$$

The above results represent the trust degree of the cloud platform's confidence interval, $m_1(A_j)$ represents the assessment result given by user 1, $m_2(A_j)$ represents the assessment result given by user 2, and the two users give different assessment results, respectively. Next, in order to integrate the views of the two users, this paper will fuse the assessment results of the two users combined with the fusion rules of D-S theory.

Step 2: fuse different assessment results based on D-S fusion rules.

Taking the data of Table 3 as an example, in order to reduce the complexity of calculation before fusion, set A_j and its trust $m_i(A_j)$ can be simplified according to Bayes approximation method [30], and the calculation method is shown in

$$m_i(\underline{A}) = \frac{\sum_{\underline{A} \subseteq A} m_i(A)}{\sum_{A \subseteq \Theta} m_i(A) * N}. \tag{7}$$

In formula (7), $\underline{A}$ is the simplified set of A, Θ Represents the complete set, and N is the total number of factors contained in A. As described above, the data in Table 3 can be substituted into formula (2) for calculation, and its calculation process is as follows.

$$\begin{aligned}
\sum_{A \subseteq \Theta} m_i(A) * N &= 3m_i(A_1) + 3m_i(A_2) + 4m_i(A_3) \\
&\quad + 3m_i(A_4) + 3m_i(A_5), \\
m_i(\underline{1}) = m_i(\underline{2}) &= \frac{m_i(A_1)}{\sum_{A \subseteq \Theta} m_i(A) * N}, \\
m_i(\underline{3}) &= \frac{m_i(A_1) + m_i(A_2)}{\sum_{A \subseteq \Theta} m_i(A) * N}, \\
m_i(\underline{4}) = m_i(\underline{5}) &= \frac{m_i(A_2) + m_i(A_3)}{\sum_{A \subseteq \Theta} m_i(A) * N}, \\
m_i(\underline{6}) = m_i(\underline{7}) &= \frac{m_i(A_3) + m_i(A_4)}{\sum_{A \subseteq \Theta} m_i(A) * N}, \\
m_i(\underline{8}) &= \frac{m_i(A_4) + m_i(A_5)}{\sum_{A \subseteq \Theta} m_i(A) * N}, \\
m_i(\underline{9}) = m_i(\underline{10}) &= \frac{m_i(A_5)}{\sum_{A \subseteq \Theta} m_i(A) * N}.
\end{aligned} \tag{8}$$

Through the above calculation method, the simplified $\underline{A}$ and its trust degree $m_i(\underline{A})$ can be obtained. Among them, $\underline{A}$ is the simplified set of A. $\underline{A}$ is different from set A, it contains only one element. $\underline{A} = \{\underline{A}_1, \underline{A}_2, \cdots, \underline{A}_{10}\} = \{\underline{1}, \underline{2}, \cdots, \underline{10}\}$.

As mentioned above, after simplifying the assessment results of two users in Table 3, $m_1(\underline{A}_j)$ and $m_2(\underline{A}_j)$ can be obtained, $j = 1, 2, 10$. Next, by substituting them into the fusion formula of D-S theory shown in formula (9), the final fusion result can be obtained.

$$m(\underline{A}) = (m_1 \oplus m_2)(\underline{A}) = \frac{1}{k} \sum_{A_i \cap A_j = A} m_1(\underline{A}_i) m_2\left(\underline{A}_j\right). \tag{9}$$

In formula (9), K is the normalization factor, and its calculation method is shown in

$$k = \sum_{A_i \cap A_j \neq \varnothing} m_1(\underline{A}_i) m_2\left(\underline{A}_j\right). \tag{10}$$

The final fusion results are shown in Table 5.

In Table 5, $m(\underline{6}) = m(\underline{7}) = 0.377$, and the values of $m(6)$ and $m(7)$ are the largest, indicating that the cloud platform credibility level is most likely to be 6 and 7.

2.3. Method Improvement. Through the above method, the two results can be fused to update the current credibility assessment results of the cloud platform. However, this method of pairwise integration has defects in the actual assessment process. As shown in Table 5, in the process of fusion, if the value of $m_j(\underline{A}_1)$ given by user j is equal to 0, the value of the fusion result $m(\underline{A}_1)$ will always be equal to 0 in all subsequent fusion processes. This situation is not consistent with the actual assessment. Therefore, this paper will improve the above method. The improved method is as follows.

Step 1: add the complete set U on the basis of Table 2.

U is the complete set of cloud platform credibility level, $U = \{1, 2, \cdots, 10\}$. It contains all possible values of cloud platform credibility level. In order to solve the problem mentioned at the beginning of this section, this paper sets the value of $m_j(U)$to the average value, that is, $m_j(U) = 0.1$.

Step 2: recalculate $m_j(\underline{A}_i)$ according to formula (7).

When the complete set U is added, according to the method of D-S theory, the value of $m_j(\underline{A}_i)$ needs to be recalculated before fusion. Taking the data of Table 2 as an example, when the complete set U is introduced, $m_j(\underline{A}_i)$ is recalculated according to formula (7). The results are shown in Table 6.

Step 3: refuse users' assessment results according to formula (9).

After obtaining the assessment result $m_1(\underline{A}_i)$ and $m_2(\underline{A}_i)$ of the two users according to step 2, fuse them according to formula (9), and the obtained results are shown in Table 6.

As shown in Table 6, the results of the improved method are consistent with those before the improvement. $m(\underline{6})$ and $m(\underline{7})$ are still the largest, indicating that the cloud platform credibility level is most likely to be 6 and 7. On the premise of ensuring the correctness of the results, this method retains all possibilities of the cloud platform credibility level, so as to

Table 5: The fusion results of two assessment results in Table 3.

$\underline{A}$	$m_1(\underline{A}_i)$	$m_1(\underline{A}_i)$	$m(\underline{A})$
{10}	0.063	0.000	0.000
{9}	0.063	0.000	0.000
{8}	0.250	0.176	0.214
{7}	0.250	0.294	0.357
{6}	0.250	0.294	0.357
{5}	0.063	0.118	0.036
{4}	0.063	0.118	0.036
{3}	0.000	0.000	0.000
{2}	0.000	0.000	0.000
{1}	0.000	0.000	0.000

Table 6: The fusion results calculated by the improved method.

$\underline{A}$	$m_1(\underline{A}_i)$	$m_1(\underline{A}_i)$	$m(\underline{A})$
{10}	0.071	0.023	0.010
{9}	0.071	0.023	0.010
{8}	0.214	0.159	0.210
{7}	0.214	0.250	0.330
{6}	0.214	0.250	0.330
{5}	0.071	0.114	0.050
{4}	0.071	0.114	0.050
{3}	0.024	0.023	0.003
{2}	0.024	0.023	0.003
{1}	0.024	0.023	0.003

effectively solve the problems mentioned at the beginning of Section 2.3.

So far, based on D-S theory, this paper puts forward an effective assessment method for the credibility of cloud platform. This method has low requirements for users' professionalism and can effectively integrate the assessment results of different users, so as to solve the conflict information between different users in the assessment process. Although this method reduces the scoring difficulty of users and solves the problem of conflicting information in the evaluation process, this method still has many defects, such as the risk of user's privacy information exposure, the risk of the assessment results be changed, malicious users, and the low user assessment enthusiasm. In order to solve these problems, this paper will make further study combined with blockchain technology and integrate blockchain technology and D-S theory to improve the assessment method.

3. Design of Cloud Platform Credibility Assessment System Based on Blockchain Technology

In order to realize the system, based on the architecture of Ethereum, this paper will combine the blockchain technology with the assessment method proposed in Section 2 to establish a cloud platform credibility assessment system.

It is known that there are 6 layers in Ethereum structure. The 6 layers from bottom to top are data layer, network layer, consensus layer, actuator layer, contract layer, and application layer, as shown in Figure 2.

Among them, the application layer refers to the application scenario of blockchain technology. In this paper, it refers to the assessment of the cloud platform credibility. Like most blockchains, the network layer of the system to be established in this paper adopts a typical P2P network, including data dissemination and verification. Therefore, in order to integrate blockchain technology into the research process of this paper, in addition to the above application layer and network layer, it is also necessary to clarify the meaning of the other 4 layers and put forward effective construction schemes for these 4 layers.

3.1. Data Layer. The data layer refers to the data structure in the blockchain, that is, the "block + chain" structure. In order to ensure the privacy security of users participating in the assessment and ensure the assessment results cannot be modified, this paper intends to encrypt the corresponding assessment data with the encryption technology of blockchain, so as to generate the corresponding block, as shown in Figure 3.

The block header includes the hash value "PreHash" of the previous block, the Merkle root generated by the assessment data contained in this block after layer-by-layer encryption, timestamp, and the random parameter "Nonce" of workload proof. The block body stores the detailed data of this block. In this study, it refers to the assessment data of the cloud platform credibility. The assessment data is composed of the unique address of the user, the trust degree $m(\underline{A})$ of the cloud platform credibility level, and the assessment weight $W(\beta_i)$ of the 5 credibility categories of the cloud platform.

Example: a user's address is 0x6c19a33efc41a1beddc91133a8422e89f041b7, the assessment weight $W(\beta_i) = \{0.200,0.200,0.200,0.200,0.200\}$, and the trust degree of the cloud platform credibility level obtained by the assessment method proposed in Section 2 is $m(\underline{A}) = \{0.000,0.000,0.176,0.294,0.294,0.118,0.000,0.000,0.000,0.000\}$. According to the encryption method of blockchain, this series of values can be spliced together into a string, which is recorded as Assessment Data1. Next, encrypt the Assessment Data1, we can get the encrypted value, namely, Hash1. Similarly, we can get another encrypted value Hash2 generated by another user's assessment data. Then, the Merkle root can be obtained by encrypting Hash1 and Hash2. The Merkle root can be used to verify the data contained in the block and ensure that the block data cannot be modified.

According to the privacy protection technology of Ethereum blockchain, the nonpublic data of the block can only be viewed by the data owner. Therefore, compared with the scoring method proposed in Section 2, the combination of blockchain technology can further effectively protect the user's hidden information.

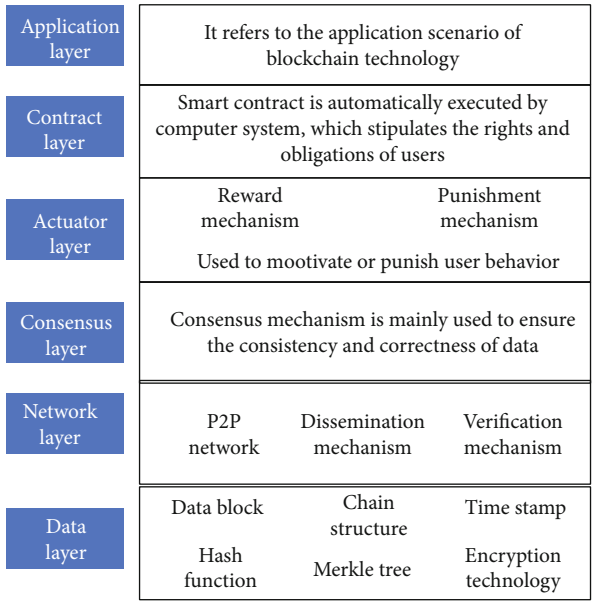

Figure 2: The 6 layers of blockchain.

3.2. Consensus Layer. Consensus mechanism is mainly to solve the problem of data consistency and correctness in unreliable networks. If there is no consensus mechanism, whoever calculates the block can be regarded as an effective block, and the consistency of data cannot be guaranteed. Therefore, only the blocks that meet the requirements can be regarded as effective blocks, and then be added to the chain as new blocks.

At present, the consensus mechanism of Ethereum is a workload proof algorithm based on Ethash (consensus engine) [25]. The algorithm will set the target hash value in the block header. Only when the hash value of the new block is less than or equal to the target hash value, the block can be regarded as a valid block and added to the blockchain. The schematic diagram is shown in Figure 4.

If the hash value of the new block does not meet the conditions, the random number Nonce needs to be changed continuously until the hash value of the new block meets the conditions. For example, when calculating the hash value of a new block, we can return the value of Nonce to zero. When the calculated hash value does not meet the conditions, the value of Nonce can be incremented by 1 until the new block's hash value is less than or equal to the target hash value. The greater the value of Nonce, the greater the difficulty of calculation. Therefore, the workload can be proved according to the value of Nonce.

The cloud platform credibility evaluation system proposed in this paper is based on Ethereum architecture. According to the current Ethereum workload proof algorithm diff = 2^{256}/difficulty, the block is valid only when the hash value of the new block is less than diff. The greater the number of difficulty, the more difficult the calculation is and the slower the block output speed is. On the contrary, the smaller the value of difficulty, the lower the calculation difficulty and the faster the block output speed. Therefore, in order to ensure the calculation speed of the whole assessment system, the value of difficulty needs to be set to a smaller value in Genesis block.

3.3. Actuator Layer. In order to improve the enthusiasm of users and punish malicious users, the system will set up a special mechanism which includes reward mechanism and punishment mechanism. As described below, in order to support this mechanism, the system will set a certain number of initial reputation points for authenticated users, which can be used for scoring and query.

(i) Reward mechanism: when a new score is generated, all users in the system can participate in the calculation of new blocks. The system will reward the first user who successfully calculates the effective block and give the user a certain reputation point

(ii) Punishment mechanism: on the contrary, if the user has malicious behavior and is identified as a malicious user, the system will find the user and deduct a certain reputation point of the user according to the traceability method of the blockchain. When users' reputation point is insufficient, they will no longer be able to participate in the assessment.

The above incentive mechanism and punishment mechanism will be written into the smart contract and automatically executed by the system.

3.4. Contract Layer. Combined with the assessment method proposed in Section 2, this paper will set the smart contract of the system according to the reward mechanism and punishment mechanism. The execution process of the whole system is shown in Figure 5.

Several important smart contract functions are involved in the system, as shown below.

(1) Initial.sol: this function is mainly used to grant users the initial reputation point. When the user becomes a contract user and obtains the account address, the system will automatically perform the contract and remit a certain initial reputation point to the account address

(2) ScorePayment.sol: this function is mainly used to deduct a certain number of users' reputation points before scoring, and the deducted reputation points will be used as collateral. When the system judges that the user's reputation score is insufficient, according to the contract, the user will not be able to participate in the scoring. When the new effective block is be calculated, the user's mortgaged reputation points will be returned

(3) PayAndGetInfo.sol: this function is mainly used to deduct the user's query fee and return the queried block information to the user

(4) Reward.sol: this function is mainly used to reward users who successfully calculate new blocks. When

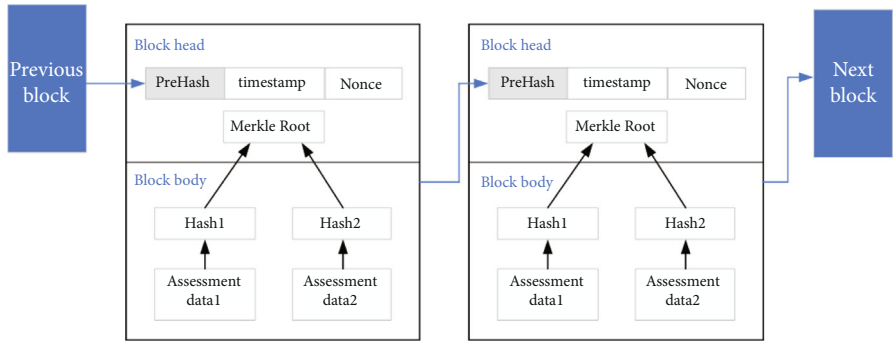

Figure 3: The blocks of the system proposed in this paper.

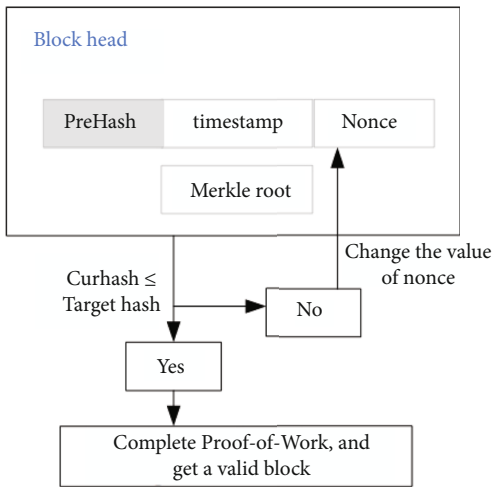

Figure 4: The schematic diagram of blockchain workload proof algorithm.

the user calculates a new effective block, the system will give the user a certain reputation point as a reward according to the reward mechanism

(5) Punish.sol: this function is mainly used to punish malicious users. When a user is identified as a malicious user, the system will trace back to the user through the traceability method of blockchain and deduct the user's reputation points according to the punishment mechanism

As mentioned above, this paper proposes a cloud platform credibility assessment system based on blockchain technology and D-S theory. The blockchain node of the system performs scoring operation through the smart contract and uses the privacy protection technology in blockchain technology to realize the anonymity of scoring process and protect the user's personal privacy.

At the same time, in order to prevent users from scoring maliciously on the platform, the system will deduct a certain number of users' reputation points as collateral before scoring according to the contract. When a new effective block is generated, the system will automatically return the users' mortgaged reputation points. In addition, with the help of blockchain traceability technology, the system can also find users or organizations with malicious behavior and punish them accordingly.

The consensus algorithm in the assessment system ensures the reliability of the blockchain system. After the blockchain nodes reach a consensus, the system will fuse the user's assessment results according to the credibility assessment method based on D-S theory proposed in Section 2, so as to update and record the credibility assessment results of the cloud platform. The result will be uploaded to the blockchain for users to access and query. The results include the current block address, the previous block address, the address of the user who participating in the assessment, the assessment date, the trust degree $m(\underline{A})$of the cloud platform credibility level, the assessment weight $W(\beta_i)$ of the 5 credibility categories of the cloud platform, and the random parameter Nonce of workload proof, as shown in Table 7.

4. Experimental Design and Analysis

4.1. Experimental Analysis of D-S Fusion Method in This Paper. Before the experimental analysis of the credibility assessment system, this paper first verifies the effectiveness of the proposed fusion method. Suppose that for a cloud platform, the assessments given by 3 different users is shown in Table 8.

As shown in Table 8, there is a big conflict between Assessment 2 and other assessments. In this case, the results obtained by traditional D-S fusion method and the results obtained by the improved D-S fusion method proposed in this paper are shown in Table 9.

It can be seen from the results in Table 9, when there are occasional conflicts or malicious assessments in the assessment process, the assessment results obtained by the traditional D-S fusion method will be greatly affected. However, the fusion results obtained by this paper method will not be greatly affected and can still reflect the views of most effective assessments. The above experiments show that the proposed fusion method is effective and feasible.

4.2. Experimental Analysis of the Credibility Assessment System. After verifying the effectiveness of the proposed fusion method, this paper will verify the effectiveness of the proposed assessment system.

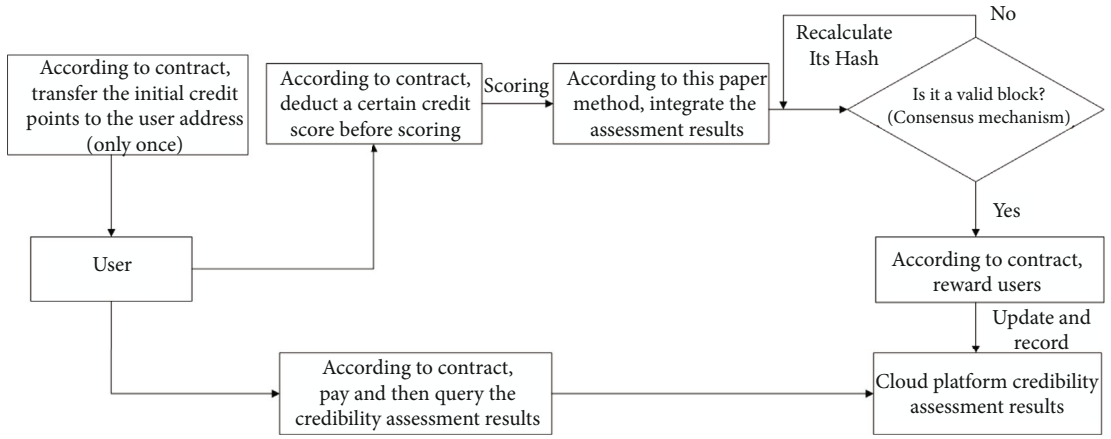

Figure 5: The process of cloud platform credibility assessment system proposed in this paper.

Table 7: Data uploaded to blockchain.

Data	Example
User address	0x6c19a33EF2cc41a1bedDC91133a8422e89f041B7
$m(\underline{A})$	0.001,0.001,0.162,0.389,0.389,0.027,0.027,0.0002,0.00006,0.00006
$W(\beta_i)$	0.180,0.223,0.107,0.242,0, 248
BlockNumber	101
The previous block address	0xa13782ab4bcb6e9670d315fb341ebbc95d45a2bdb0ea5034ef432b74f30b1b4f
The current block address	0x78dacc2af60900d2e4cae90b71e27446e6e883df36c53f21cbc9e071f7a586f4
Assessment date	20220407
Nonce	4

Table 8: The assessments of 3 different users.

	Assessment 1	Assessment 2	Assessment 3
$A_5 = \{8910\}$	0.500	0.000	0.600
$A_4 = \{678\}$	0.300	0.000	0.200
$A_3 = \{4567\}$	0.200	0.000	0.200
$A_2 = \{345\}$	0.000	0.400	0.000
$A_1 = \{123\}$	0.000	0.600	0.000

4.2.1. Experimental Design. The consensus mechanism of this experiment adopts the workload proof algorithm based on Ethash. The test framework is Remix provided by Ethereum, the experimental server is configured with CPU 5.0ghz and Ram 32g. After setting up the environment required for the experiment, the initial weight of the 5 credibility categories of the platform is set to 0.200, namely, $W(\beta_j) = 0.200$, $j = 1, 2, \cdots, 5$. Then, this experiment convened 10 experts to score a cloud platform and generated the initial block data according to the method proposed in this paper. Next, this paper has visited and consulted users who have used the platform and asked them to assess the platform in the form of questionnaire. Finally, this experiment substitutes the assessment data of all users into the system and obtains the data of more than 300 blocks.

Table 9: The assessments of 3 different users.

	Results obtained by traditional D-S fusion method	Results obtained by the improved D-S fusion method proposed in this paper
{10}	0.00000	0.12353
{9}	0.00000	0.12353
{8}	0.00000	0.23824
{7}	0.00000	0.08824
{6}	0.00000	0.08824
{5}	0.50000	0.13235
{4}	0.50000	0.13235
{3}	0.00000	0.03235
{2}	0.00000	0.02059
{1}	0.00000	0.02059

Through the system, the user can obtain the block information returned by the system after paying according to the contract. According to the address of the block, the user will be able to further query the weight $W(\beta_i)$ of the 5 credibility categories of the cloud platform and can also query the trust degree $m(\underline{A})$ of the cloud platform credibility level.

4.2.2. Experimental Result Analysis. Using the expert account to query, the following results can be obtained.

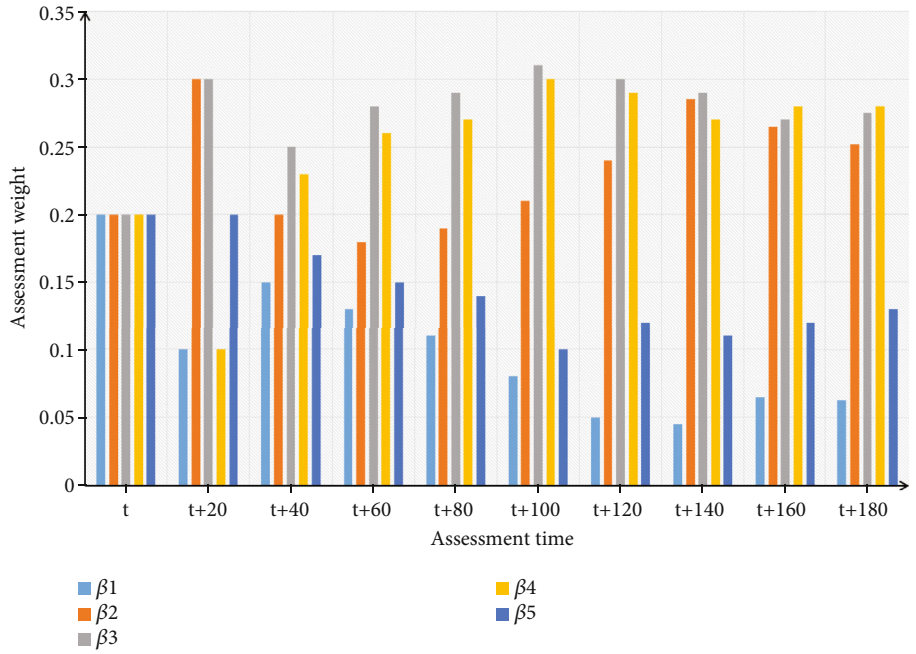

Figure 6: Changes in the assessment weight $W(\beta_i)$.

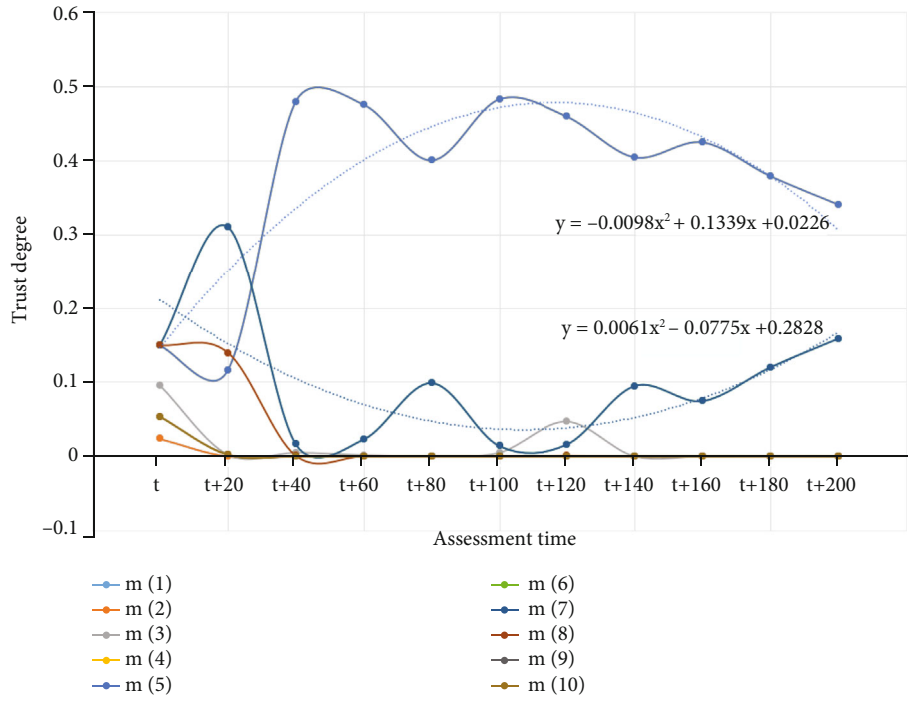

Figure 7: The change of $m(\underline{A})$.

(1) Changes in the Assessment Weight $W(\beta_i)$ of the 5 Credibility Categories. In Figure 6, t represents the generation time of the first block, that is, the time of the first assessment. As can be seen from Figure 6, in the initial stage, the assessment weight $W(\beta_i)$ of each credibility category changes greatly. However, with the increase of the number of user assessments, the assessment weight $W(\beta_i)$ of the 5 credibility categories will gradually stabilize. Finally, the assessment weight sorting result is $W(\beta_4) > W(\beta_3) > W(\beta_2) > W(\beta_5) > W(\beta_1)$. According to the entropy weight method, the sorting results show that β_4 has the greatest impact on the credibility of the whole platform, and users have the greatest difference in the assessment of "service provider management credibility β_4"; on the contrary, the value of $W(\beta_1)$ is the lowest, indicating that β_1 has the lowest impact on the credibility of the whole platform, and users have the

Table 10: Cost comparison and comprehensive comparison.

	Cost	Comprehensiveness
This paper method	The cost required includes the following: (1) Assessment weight $W(\beta_i)$of each credibility category given by users (2) Confidence interval lev(β_i) of each credibility category given by users (3) D-S fusion method is required in the assessment process, and its average time complexity is $O(n^2)$ (4) In addition, this method also needs to build a blockchain system	The output assessment results include the following: (1) The change of $W(\beta_i)$ (2) Cloud platform credibility level and its trust degree $m(\underline{A})$ (3) The change of $m(\underline{A})$
Method based on AHP	The cost required includes the following: (1) Weight judgment matrix of credibility categories (2) Asymptotic normalization coefficient (ANC) is required in the assessment process, and its average time complexity is $O(n^2)$	The output assessment results include the following: (1) Assessment weight $W(\beta_i)$ of each credibility category calculated by ANC
Method based on entropy	The required input data include the following: (1) Risk frequency of each credible category (2) Risk loss severity of each credible category (3) Entropy weight method is required in the assessment process, and its average time complexity is $O(n^2)$	The output assessment results include the following: (1) Entropy weight of each credibility categories, namely, the assessment weight $W(\beta_i)$ (2) The uncertainty degree of cloud platform risk, namely, cloud platform credibility level
Method based on D-S theory	The required input data include the following: (1) The confidence interval and trust degree of each credibility category (2) D-S fusion method is required in the assessment process, and its average time complexity is $O(n^2)$	The output assessment results include the following: (1) Cloud platform credibility level and its trust degree $m(\underline{A})$
Method based on fuzzy theory	The required input data include the following: (1) The confidence interval and trust degree of each credibility category (2) Directly assess the cloud platform credibility level and its trust degree according to Fuzzy Sets. The average time complexity is $O(1)$	The output assessment results include the following: (1) Cloud platform credibility level and its trust degree $m(\underline{A})$

smallest difference in the assessment of "infrastructure credibility β_1".

(2) Changes in the Trust Degree $m(\underline{A})$ of the Cloud Platform Credibility Level. Through query, the change of $m(\underline{A})$ is shown in Figure 7.

Starting from the initial assessment records, the query is conducted every 20 blocks. A total of 11 assessment records are queried in this experiment.

In Figure 7, t represents the generation time of the first block, that is, the time of the first assessment. As can be seen from Figure 7, the platform credibility level is 6 and 7, followed by 4 and 5. However, from the change trend, the values of $m(\underline{6})$ and $m(\underline{7})$ show a downward trend, while the values of $m(\underline{4})$ and $m(\underline{5})$ show an upward trend, indicating that the credibility level of the platform shows a downward trend with the increase of the number of user assessments.

In addition, on the whole, the possibility of the platform credibility level belonging to other levels is low, indicating that the platform is relatively stable. The values of $m(\underline{10})$ and $m(\underline{1})$ are close to 0, indicating that the platform is neither a highly trusted platform nor a low trusted platform and is always in a generally trusted state.

4.3. Method Comparison. The above experiments show that the assessment method proposed in this paper is effective and feasible. Next, this paper compares the proposed method with other similar methods.

The methods proposed in this paper are mainly aimed at assessing the credibility of cloud platforms. In order to illustrate the advantages of the methods proposed in this paper, it is necessary to compare it with other similar assessment methods, such as method based on AHP, method based on entropy, method based on D-S theory, and method based on fuzzy theory.

Suppose a cloud platform contains n credibility categories, and the above methods are used to assess the platform. The comparative analysis of each method is shown in Tables 10 and 11.

Summarizing the above comparison, the results are shown in Table 12.

In Tables 10–12, cost represents the cost required for assessment when using this method; comprehensiveness

Table 11: Comparison of privacy security, data stability, and objectivity.

	Privacy security	Data stability	Objectivity
This paper method	Adopt blockchain technology for privacy protection	The assessment result cannot be tampered with	D-S fusion method can effectively solve the conflict information in the assessment process and ensure the objectivity of the assessment results.
Method based on AHP	No privacy protection	The assessment result is easy to be tampered with	In weight assessment, the method of pairwise comparison can effectively reduce the impact of human subjective factors.
Method based on entropy	No privacy protection	The assessment result is easy to be tampered with	Describing the credibility level by the risk uncertainty can effectively reduce the impact of human subjective factors on the assessment results.
Method based on D-S theory	No privacy protection	Because the assessment result is the fusion of different users' assessment results, the result is not easy to be tampered with	D-S fusion method can effectively solve the conflict information in the assessment process and ensure the objectivity of the assessment results.
Method based on fuzzy theory	No privacy protection	The assessment result is easy to be tampered with	The assessment results are obtained by human subjective assessment. There is no effective method to improve the objectivity of the assessment results in the assessment process. Compared with other methods, its objectivity is low.

Table 12: Comparison between this paper method and other methods.

	Cost	Comprehensiveness	Privacy security	Data stability	Objectivity
This paper method	High	High	High	High	Medium
Method based on AHP [5–11]	Medium	Low	Low	Low	Medium
Method based on entropy [12–16]	Medium	Medium	Low	Low	Medium
Method based on D-S theory [17–22]	Medium	Medium	Low	Medium	Medium
Method based on fuzzy theory [31–33]	Low	Medium	Low	Low	Low

means the comprehensiveness of the evaluation results. The more assessment results this method can provide to users, the more comprehensiveness this method; privacy security refers to the security degree of the method in user privacy protection; data stability indicates the stability of the evaluation results. The higher the stability, the less likely the assessment results will be modified by malicious users; objectivity means the objectivity of the assessment results. The higher the objectivity, the lower the impact of human subjective factors on the assessment results.

5. Conclusion

This paper integrates blockchain technology and D-S theory and carries out a series of research on the credibility assessment of cloud platforms. Firstly, based on D-S theory and fuzzy theory, this paper proposes an effective cloud platform credibility assessment method, which solves the conflict problem in the assessment process by integrating the user's assessments and reduces the difficulty of user scoring. On this basis, combined with blockchain technology, this paper regards the fused assessment results as effective blocks on the blockchain, proposes an effective block generation method, and designs the corresponding consensus mechanism, smart contract, and incentive mechanism. As mentioned above, combined with D-S theory and blockchain technology, this paper designs and proposes an effective cloud platform credibility assessment system. Through the encryption technology and traceability technology of blockchain, the system makes up for the defects of the assessment method based on D-S theory, effectively protects the privacy of users participating in the assessment process, ensures the assessment results cannot be tampered with, and improves the assessment enthusiasm of users. Finally, the experimental analysis results show that the assessment system proposed in this paper is effective and feasible.

However, as an assessment system, the assessment results that the system can provide to users are not comprehensive enough. In the follow-up research, we also need to sort out the specific impact indicators based on the cloud platform credibility categories divided in this paper and carry out the assessment combined with the specific credibility evidence, so as to improve the objectivity of the assessment results.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (no. 11861071), the Yunnan Fundamental Research Projects (nos. 202101AT070211, 202201AT070142, and 202201AT070166), and the Talent Introduction Projects of Yunnan University of Finance and Economics (no. 2021D16).

References

[1] Flexera, *Flexera 2020 State of the Cloud Report*, Flexera, America, 2020.

[2] S. Chang-xiang, "Scientific concept of network security and trusted computing 3.0," in *China Software Industry Annual Conference*, Beijing, 2018.

[3] Y. Xi, L. Ping, and G. Jabeen, "The concept model of software trustworthiness based on trust-theory of sociology," *Acta Electronica Sinica*, vol. 47, no. 11, pp. 2344–2353, 2019.

[4] T. Zhang, K. Zhao, M. Yang, T. Gao, and W. Xie, "Research on privacy security risk assessment method of mobile commerce based on information entropy and Markov," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8888296, 11 pages, 2020.

[5] K. A. Alam, R. Ahmed, F. S. Butt, S. G. Kim, and K. M. Ko, "An uncertainty-aware integrated fuzzy AHP-WASPAS model to evaluate public cloud computing services," *Procedia Computer Science*, vol. 130, pp. 504–509, 2018.

[6] C. Li, S. Wang, L. Kang, L. Guo, and Y. Cao, "Trust evaluation model of cloud manufacturing service platform," *International Journal of Advanced Manufacturing Technology*, vol. 75, no. 1-4, pp. 489–501, 2014.

[7] P. Lou, L. Yuan, J. Hu, J. Yan, and J. Fu, "A comprehensive assessment approach to evaluate the trustworthiness of manufacturing services in cloud manufacturing environment," *IEEE Access*, vol. 6, pp. 30819–30828, 2018.

[8] R. Fattahi and M. Khalilzadeh, "Risk evaluation using a novel hybrid method based on FMEA, extended MULTIMOORA, and AHP methods under fuzzy environment," *Safety Science*, vol. 102, pp. 290–300, 2018.

[9] M. Fagundes, T. C. Keler, E. O. Teles, S. Melo, and F. Freires, "Multicriteria decision-making system for supplier selection considering risk: a computational fuzzy AHP-based approach," *IEEE Latin America Transactions*, vol. 19, no. 9, pp. 1564–1572, 2021.

[10] Z. Li and R. Jie, "Cloud service trust evaluation algorithm optimization based on multi-level structure model," *Journal of Nanjing University of Science And Technology*, vol. 44, no. 1, p. 6, 2020.

[11] C. Ze-Qian, S. Xiao-Tong, Z. Na-Jing, and Y. Shuo, "Construction and application of evaluation index of public cultural cloud service," *Library and Information Knowledge*, vol. 2020, no. 6, pp. 54–66, 2020.

[12] T. Tilei, L. Tong, Y. Ming, and J. Rong, "Research on a trustworthiness measurement method of cloud service construction processes based on information entropy," *Entropy*, vol. 21, no. 5, p. 462, 2019.

[13] T. Gao, T. Li, R. Jiang, M. Yang, and R. Zhu, "Research on cloud service security measurement based on information entropy," *International Journal of Network Security*, vol. 21, no. 6, pp. 1003–1013, 2019.

[14] H. Guesmi, A. Kalghoum, C. Ghazel, and L. A. Saidane, "FFED: a novel strategy based on fast entropy to detect attacks against trust computing in cloud," *Cluster Computing*, vol. 24, no. 3, pp. 1945–1954, 2021.

[15] A. Sharma, P. Munjal, and H. Banati, "Entropy-based classification of trust factors for cloud computing," *International Journal of Grid and Utility Computing*, vol. 11, no. 6, pp. 747–754, 2020.

[16] S. Nie, "A novel trust model of dynamic optimization based on entropy method in wireless sensor networks," *Cluster Computing*, vol. 22, no. S5, pp. 11153–11162, 2019.

[17] L. Wei, Z. Lu-Kun, B. A. Yuan-Jie, L. I. Guang-Li, and Z. Zhi-Gang, "A relevance aware cloud service trust model based on convex evidence theory," *Computer Engineering & Science*, vol. 41, no. 1, pp. 47–55, 2019.

[18] L. Zuan-shi and G. Xiu-li, "Trusted cloud service evaluation method research based on D-S theory," *Computer Engineering and Applications*, vol. 53, no. 17, pp. 70–76, 2017.

[19] D. X. Wang and Q. Wang, "Trustworthiness evidence supporting evaluation of software process trustworthiness," *Journal of Software*, vol. 29, no. 11, pp. 3412–3434, 2018.

[20] W. Xu, W. Yang, and Y. Yao, "Multi-dimensional trust evaluation method based on D-S evidence theory," *Computer and Digital Engineering*, vol. 47, no. 2, p. 7, 2019.

[21] M. Yang, T. Gao, R. Jiang, L. Jia, and D. Yang, "Comprehensive assessment of mobile service privacy security based on FAHP and D-S theory," *Wireless Communications and Mobile Computing*, vol. 2, 20 pages, 2022.

[22] M. Yang, T. Gao, W. Xie, L. Jia, and T. Zhang, "The assessment of cloud service trustworthiness state based on D-S theory and Markov chain," *IEEE Access*, vol. 10, pp. 68618–68632, 2022.

[23] W. Tiedan, Z. Yang, and P. Dinghong, "Research on cloud service safety evaluation based on improved IVHF-TODIM method," *Computer Engineering and Applications*, vol. 54, no. 4, pp. 84–89, 2018.

[24] W. Tie-dan, T. Miao, and P. Ding-hong, "Hesitant fuzzy Taguchi multi-attribute decision making method for cloud service quality evaluation," *Fuzzy Systems and Mathematics*, vol. 33, no. 3, p. 16, 2019.

[25] S. Huiyang, L. Peng, and W. He, "Threat intelligence evaluation based on blockchain and a neural network," *Journal of Tianjin University(Science and Technology)*, vol. 55, pp. 527–534, 2022.

[26] Y. Ming, H. Xuexian, Z. Qihui, W. Jianghong, and L. Wenfen, "Federated learning scheme for mobile network based on reputation evaluation mechanism and blockchain," *Chinese Journal of Network and Information Security*, vol. 7, no. 6, pp. 99–112, 2021.

[27] L. Haiou, H. Xutao, L. Kai, and G. Yue, "A literature review of blockchain traceability mechanism," *Journal of Intelligence*, vol. 2022, no. 4, pp. 1–7, 2022.

[28] T. Aiguo and H. Chunhua, "Application of fuzzy theory in software project risk assessment," *Journal of Central South University (Science and Technology)*, vol. 48, no. 2, pp. 411–417, 2017.

[29] D. Li, J. Chen, and M. Qiu, "The evaluation and analysis of the entropy weight method and the fractional grey model study on the development level of modern agriculture in Huizhou," *Mathematical Problems in Engineering*, vol. 2021, 8 pages, 2021.

[30] F. Voorbraak, "A computationally efficient approximation of Dempster-Shafer theory," *International Journal of Man-Machine Studies*, vol. 30, no. 5, pp. 525–536, 1989.

[31] X. Hu, R. Jiang, M. Shi, and J. Shang, "A privacy protection model for health care big data based on trust evaluation access control in cloud service environment," *Journal of Intelligent and Fuzzy Systems*, vol. 38, no. 3, pp. 3167–3178, 2020.

[32] A. Mohsenzadeh, H. Motameni, and J. E. Meng, "Retraction note to: a new trust evaluation algorithm between cloud entities based on fuzzy mathematics," *International Journal of Fuzzy Systems*, vol. 21, no. 6, p. 1988, 2019.

[33] R. Pei-Zhi, L. Wei, B. Ran, and M. Ping, "A simulation credibility assessment method based on improved fuzzy comprehensive evaluation," *Journal of System Simulation*, vol. 32, no. 12, pp. 185–190, 2020.