IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 May 2022, accepted 20 June 2022, date of publication 23 June 2022, date of current version 1 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3185684

RESEARCH ARTICLE

The Assessment of Cloud Service Trustworthiness State Based on D-S Theory and Markov Chain

MING YANG[1], **TILEI GAO**[1], **WANYU XIE**[2], **LI JIA**[1], **AND TAO ZHANG**[1]
[1]School of Information, Yunnan University of Finance and Economics, Kunming 650221, China
[2]Personnel Department, Kunming Metallurgy College, Kunming 650033, China

Corresponding author: Wanyu Xie (396458144qq.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 11861071; and in part by the Yunnan Fundamental Research Projects under Grant 202101AT070211, Grant 202201AT070142, and Grant 202101AT070464.

ABSTRACT The massive cloud service market is full of various services with uneven quality. Even the services that have passed the platform detection will have unknown trustworthiness problems in the actual use process. The risk environment of the cloud service determines that its trustworthiness is random. The static trustworthiness assessment results can only reflect the cloud service trustworthiness at a certain time, not enough to reflect the real trustworthiness of the cloud service. To objectively reflect the trustworthiness of the cloud service, it is necessary to further assess the cloud service trustworthiness state and its changes on the basis of trustworthiness level measurement. To solve this problem, this paper combs the trustworthiness indicators of the cloud service, puts forward an effective assessment method of cloud service trustworthiness level based on D-S theory, and puts forward the representation method of cloud service trustworthiness state and its transition state combined with Markov chain, so as to realize the effective assessment of cloud service trustworthiness state and its changes. Finally, through case analysis, it shows that the method proposed in this paper is feasible, can effectively assess the cloud service trustworthiness state and its changes, and provide users with detailed assessment results, so as to help users make reasonable service selection and trustworthiness management. This research has important significance for ensuring the cloud service trustworthiness and improving the cloud service market security.

INDEX TERMS Cloud service trustworthiness, D-S theory, Markov chain, assessment of cloud service, trustworthiness state.

I. INTRODUCTION

According to the global data center infrastructure revenue data for the first quarter of 2020 published by Synergy Research Group, the revenue of the global cloud computing market in the first quarter was $29 billion, a year-on-year increase of 37%. According to Flexera's 2020 cloud status report [1], 59% of enterprises' demand for cloud services will exceed expectations. It can be seen that the demand for cloud services in the global market is gradually increasing, and more and more institutions begin to choose to use cloud services to expand their applications.

However, cloud services are not completely secure. According to the report of Amazon AWS which is the world's largest cloud computing manufacturer, their company experienced 22 sudden service failures between 2010 and 2019. The most serious server failure lasts up to 4 hours, affecting thousands of online services. In addition to Amazon, other Internet companies such as Google App Engine, apple iCloud and Alipay have also experienced varying degrees of service downtime. On June 8, 2021, according to several international media reports, due to the service failure of Fastly which is an American cloud computing service provider, many global websites such as CNN, the New York Times and the British government were instantly paralyzed. On October 4, 2021, according to the monitoring data of DownDetector, the famous websites such as Twitter, Facebook, photo wall and Amazon all had service failures on the same day, and these servers did not begin to return to normal until six hours later.

It can be seen from the above report that even the cloud services provided by well-known platforms will have sudden trustworthiness problems in long-term use process. Therefore, in order to ensure the use security of services, in addition to platform inspection, it is also necessary to assess the

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

trustworthiness state during their use. On the contrary, if users cannot effectively assess the service trustworthiness and take precautions against the possible risks in use process, once the service fails it will cause unpredictable huge losses. In order to help users reasonably choose trusted cloud services and prevent possible risks in the use of the services, this paper proposes to assess the trustworthiness state of cloud services in the long-term use process. Firstly, this paper combs 8 cloud service trustworthiness indicators, defines 4 intervals of cloud service trustworthiness according to the fuzzy set, and puts forward an effective cloud service trustworthiness level assessment method based on D-S (Dempster-Shafer) theory. Next, based on the proposed trustworthiness level assessment method, combining with the prediction method of Markov chain, this paper further defines the cloud service trustworthiness state and its state transition matrix, then puts forward an effective assessment method of cloud service trustworthiness state in the long-term use process. Finally, through case analysis and method comparison, it shows that the trustworthiness state assessment method proposed in this paper is feasible and has certain advantages.

This paper comprises of seven sections. Section I introduces the research background and content of this paper. Section II discusses the relevant research and points out the problems to be solved in this paper. Section III combs the cloud service trustworthiness indicators, defines the confidence interval of cloud services, and puts forward a trustworthiness level assessment method based on D-S theory. Section IV defines the trustworthiness state of cloud services and its state transition matrix, and proposes a cloud service trustworthiness state assessment method based on Markov chain. In Section V, combining the research in sections III and IV, a cloud service trustworthiness state assessment method based on D-S theory and Markov chain is proposed. In Section VI, this paper carries out case analysis and method comparison, and discusses the feasibility and characteristics of the method proposed in this paper. Section VII summarizes the work of this paper and points out the future research work.

II. RELEVANT RESEARCH

To assess the cloud service trustworthiness state, firstly it needs to clarify what is trustworthiness and sort out the relevant attribute indicators around its definition. For this reason, taking trustworthiness definition and its attribute as the research object, this paper consulted important reports and literatures at home and abroad, and the results are shown in Table 1.

According to the above research on the trustworthiness definition and its attributes, with the research progress the trustworthiness of cloud services has a broader meaning, no longer referring to its security alone, but also includes the significance of reliability, integrity, privacy, accuracy, ease of use, risk prevention, business integrity and other aspects. In addition, according to the report "11 top cloud security threats" [11] published by Cloud Computing Security Alliance(CSA), the responsibility for the security problems in the use of cloud services is no longer entirely directed to the service provider, but more security responsibility are directed to the user enterprise itself. It can be seen that with the development of cloud service applications, the cloud service trustworthiness and its security responsibility have gradually changed. Even the "quality and safety service" guaranteed by service providers will be unreliable in specific user enterprise application scenarios. This is because in specific application scenarios, in addition to the quality factors of the service itself, other factors such as the employee threat of the user's own enterprise, security operation awareness, regulatory compliance, governance management experience, technical vulnerabilities and third-party application attacks will directly affect the credibility of cloud services [12]. Therefore, in order to assess the cloud service trustworthiness state and its changes, it needs to sort out the relevant attribute indicators affecting the cloud service trustworthiness, and analyze the trustworthiness impact of these indicators in practical application scenarios.

As for how to assess the cloud service trustworthiness, Lu *et al.* [13] pointed out that a good assessment model should have the characteristics of scalability, real-time, easy transplantation and low cost. Wang *et al.* [14], [15] pointed out that in the process of cloud service security assessment, it is difficult for experts to give accurate judgment for the assessment object due to their complex psychology. Therefore, in the process of cloud service trustworthiness assessment, if the exact value is used for judgment, it will inevitably lead to inaccurate assessment results. Zhu *et al.* [16] pointed out that "cloud service security assessment separated from user conditions" is not applicable to practice. The security assessment process of cloud services should be carried out in combination with user conditions. Wu *et al.* [17] pointed out that when assessing services, the existing cloud service assessment methods still have the problems of inconsistent assessment standards and unreasonable index weight distribution. Wang *et al.* [18] pointed out that the web service trustworthiness will be in a changing process due to the impact of the open network environment. In order to predict and avoid the service failure in the use of cloud services, Alaei *et al.* [19] proposed an adaptive network-based fuzzy inference system (ANFIS) prediction model to proactively control resource load fluctuation. In order to optimize the service quality during use, Ayoubi *et al.* [20] proposed an autonomous IoT service placement methodology. Through the assessment of available resources and cloud service state during use, this method can formulate a reasonable management of services and resources in the use process. From these studies, it can be seen that improve the security and reliability of cloud services, it needs to assess the cloud service state and predict the possible credibility problems in the use process.

Scholars at home and abroad have also tried different studies on what methods should be used in the assessment process. Representative methods include: assessment

TABLE 1. Research on the definition of trustworthiness and its attribute indicators.

Reference source	The definition and attribute of trustworthiness	Year
Trusted computing organization (TCG) [2]	It is pointed out that an entity is trustworthiness if it always develops towards the expected goal	2001
Microsoft [3]	From the perspective of products, it is believed that trustworthiness should include security, privacy, reliability and business integrity	2002
Academician Chen [4]	He defined trustworthiness as reliability, risk prevention, safety, survivability, fault tolerance and real-time	2003
ISO / IEC [5]	It defined trustworthiness as: the components, operations or processes involved in computing are predictable and can resist a certain degree of interference	2005
Academician Wang [6]	He divided trustworthiness into three dimensions: identity credibility, ability credibility and behavior credibility	2006
Academician Wang [7]	He pointed out that credibility includes two aspects: one is the user's "subjective credibility" of software quality, and the other is the objective quality of software	2010
Gu et al. [8]	They pointed out that the concept of credibility should include correctness, reliability, security, availability, efficiency and so on	2011
Academician Shen [9]	put forward the concept of " Trustworthiness 3.0", which is different from " Trustworthiness 1.0" which only considers software reliability, and also different from " Trustworthiness 2.0" which only considers the credibility of service providers. "Trustworthiness 3.0" points out that the credibility of a service should fully consider the trusted factors from multiple parties in the application environment.	2018
Yang et al. [10]	They defined trustworthiness as generalized reliability, generalized security, identity trustworthiness, basic standard trustworthiness and capability trustworthiness	2019

method based on analytic hierarchy process(AHP) [21]–[27], uncertainty assessment method based on information entropy [28]–[32], assessment method based on fuzzy theory [33]–[35], assessment method based on D-S evidence theory [36]–[39], assessment method based on risk matrix [40], [41], etc. Although these single methods can effectively realize the quantitative assessment of trustworthiness, they lack the assessment of cloud service trustworthiness and its changes in long-time use process. The trusted computing method based on trusted chain [42]–[44] can judge whether the system is damaged by detecting the integrity of the system. However, this method mainly tests the quality problems of the service itself, and does not conduct a comprehensive assessment specifically for the management risk, application environment risk and other relevant factors of the service provider, and the consumption cost of this method is high. The prediction and assessment method based on Bayesian network [45]–[48] can effectively predict the reliability of cloud services, but using this method requires a large number of priori data.

Through the above research, it can be seen that any single method or analysis from a single angle will have its defects in the assessment of cloud services, and cannot be fully competent for the assessment of cloud service trustworthiness and its changes. If the cloud service trustworthiness and its changes cannot be effectively assessed, the effectiveness of the assessment results will be greatly reduced, resulting in the services have trustworthiness problems in practical applications. In order to solve this problem, firstly this paper sorts out the cloud service trustworthiness indicators, defines the trustworthiness level and its trust degree according to fuzzy theory, and proposes an effective cloud service trustworthiness level assessment method based on D-S theory; Secondly this paper further studies the cloud service trustworthiness state and its changes combined with the prediction method of Markov chain; Finally, an effective assessment method of trustworthiness state is proposed to provide a basis for users' service selection and use.

III. ASSESSMENT OF CLOUD SERVICE TRUSTWORTHINESS LEVEL

According to the previous discussion, in order to assess the cloud service trustworthiness, it first need to sort out its trustworthiness indicators, measure its trustworthiness, and propose an effective trustworthiness level assessment method. Therefore, this paper has carried out the following research in turn.

A. CLOUD SERVICE TRUSTWORTHINESS INDICATORS AND THEIR DEFINITION

Cloud service trustworthiness indicators can provide a basis for the trustworthiness assessment. On the other hand, it can be used as an important reference for users to choose services. Combined with the application interaction environment of cloud services, focusing on the security problems pointed out in the report "11 top cloud security threats" [49], this paper combs the relevant trustworthiness indicators through literature reference and investigation, as shown in Table 2.

TABLE 2. The definitions of cloud service trustworthiness indicators.

	Indicators	Definitions	Examples
C_1	Terminal trustworthiness	It refers to the trustworthiness of the service in the terminal application environment	Due to application vulnerabilities, service is attacked by a third-party application on the terminal device
C_2	Physical security trustworthiness	It refers to the trustworthiness of computer room environment, storage devices, servers, network communication equipment and other hardware facilities	The server is damaged; The data backup is lost
C_3	Trustworthiness of laws and regulations	It refers to the trustworthiness of cloud services in terms of legal liability attribution, review support, restrictions of laws and regulations, etc	Mandatory removal from shelves by laws and regulations; Disputes over attribution responsibility
C_4	Trustworthiness of service provider operation	It refers to the trustworthiness of service providers in their own enterprise capital operation and platform service operation.	Business failure; Service off the shelf
C_5	Functional trustworthiness	It refers to the trustworthiness of cloud services in using functions.	Loss of function; Difficult to use

C_6	Network trustworthiness	It refers to the trustworthiness of network stability and defense of cloud services	Network blocking;
			DDoS attack;
			CC attack

C_7	Trustworthiness of service provider management	It refers to the trustworthiness of service providers in staff management, service renewal and maintenance	Internal employee threats Service stop update; No response after sales
C_8	Trustworthiness of encryption and authority management	It refers to the trustworthiness of service providers in data isolation, identity access control, key management and storage	Data leakage; The loss of theft of keys; Illegal invasion

TABLE 3. The definition of risk occurrence frequency level and risk loss level.

Level	Risk occurrence frequency	Risk loss	Privacy information involved
1	This risk hardly occurs	The risk will not affect the normal operation of the service	User's basic account information
2	This risk occurs occasionally	The risk will affect the normal operation of some functions of the service. The problems caused by this risk can be repaired quickly	User's location information,preferences, contact information, etc
3	This risk often occurs	When risks occur, the service will be shut down for a short time, requiring a period of maintenance	User's real identity information, health information, etc
4	This risk is inevitable	Risk will lead to service stop or shutdown, and the service is difficult to return to normal	User's financial information, key information, etc

TABLE 4. Cloud service risk level matrix.

		Risk Lose Level			
		1	2	3	4
Risk Frequency Level	4	$4/II$	$8/III$	$12/IV$	$16/IV$
	3	$3/I$	$6/II$	$9/III$	$12/IV$
	2	$2/I$	$4/I$	$6/II$	$8/III$
	1	$1/I$	$2/I$	$3/I$	$4/II$

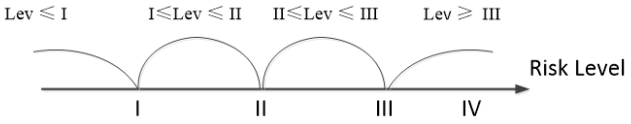

FIGURE 1. Four intervals of cloud service trustworthiness.

B. CLOUD SERVICE TRUSTWORTHINESS FUZZY SET

According to the viewpoint of "trustworthines ≈ reliability + security" [9], this paper proposes to use "uncertainty of risk" to measure the trustworthiness of services. As shown in Table 3, this paper divides the risk levels from two aspects: risk occurrence frequency and risk loss.

Next, according to the risk matrix method [50], substitute the risk occurrence frequency level and risk loss level into the matrix shown in Table 4, the cloud service risk level can be obtained, $Risk\ Level = \{I, II, III, IV\}$.

As shown in Table 4, the higher the risk level of cloud service, the higher the risk occurrence frequency and the greater the risk loss, that is, the lower the reliability and security of the service. Therefore, according to the definition of "trustworthiness ≈ reliability + security," the risk level I, II, III, IV can be used to describe the cloud service trustworthiness level.

However, in the actual assessment process, due to the insufficient judgment reasons of experts, it is difficult to give an accurate level for the trustworthiness, that is, it is impossible to directly apply the above method to express the trustworthiness level with an accurate value [14], [15]. In order to solve this problem, based on the risk matrix shown in table 4, this paper divides the cloud service trustworthiness into four different intervals, as shown in Figure 1.

Figure 1 shows the 4 intervals of cloud service trustworthiness, and their meanings are as follows.

TABLE 5. Different expert assessment results of indicator C_i.

	Assessment 1	Assessment 2	Assessment 3
Arbitrary set A	$m_1(A_1, C_i)$	$m_2(A_2, C_i)$	$m_3(A_3, C_i)$
I	0.00	0.00	0.10
I, II	0.10	0.15	0.15
II, III	0.50	0.55	0.40
III, IV	0.40	0.30	0.35

1) Fully trusted, $lev \leq I$. It indicates that the trustworthiness level of cloud services is relatively clear, that is, it contains only one possible level I.
2) Basically trusted, $I \leq lev \leq II$. It indicates that there are two possible levels I, II for the trustworthiness level of cloud services.
3) Basically untrusted, $II \leq lev \leq III$. It indicates that there are two possible levels II, III for the trustworthiness level of cloud services.
4) Fully untrusted, $lev \geq III$. It indicates that there are two possible levels III, IV for the trustworthiness level of cloud services.

Based on the above definition of trustworthiness interval, this paper proposes to describe the cloud service trustworthiness level combined with fuzzy theory.

Fuzzy theory [51] is based on Fuzzy Set, and its research goal is to deal with uncertain things with fuzzy concepts. Fuzzy Set refer to the set with uncertain boundaries. Since the cloud service trustworthiness is also a fuzzy concept that is difficult to describe, its trustworthiness can be described by setting its corresponding trustworthiness level fuzzy set.

Assuming that A represents the fuzzy set of the cloud service trustworthiness level and $m(A)$ represents its trust degree, $A \in \{\{I\}, \{I, II\}, \{II, III\}, \{III, IV\}\}$. According to fuzzy theory, the greater the value of trust degree $m(A)$, the higher the possibility that the cloud service trustworthiness level belongs to A, $\sum m(A) = 1$. Compared with the accurate assessment method, this method describes the trustworthiness level of cloud services through Fuzzy Set, which can reduce the difficulty of experts' scoring and ensure the accuracy of assessment results.

C. ASSESSMENT OF CLOUD SERVICE TRUSTWORTHINESS LEVEL BASED ON D-S THEORY

It is known that in the assessment process of cloud service trustworthiness, different experts may give different assessment results to the same object. As shown in Table 5, for the same trustworthiness indicator C_i. According to the method proposed III-B, different experts may give different assessment results.

In Table 5, $m_1(A_1, C_i)$ represents the trust degree given by the expert 1 for the trustworthiness level fuzzy set of indicator C_i. Table 5 contains the assessment results of 3 experts. The assessment results of each expert are valid, but there is a big conflict between these assessment results. Therefore, in order to correctly judge the trustworthiness of indicator C_i, it also need to comprehensively consider the assessment opinions of each expert and effectively solve the conflict. To solve the conflict, this paper proposes to use D-S theory to fuse the assessment results of different experts.

D-S evidence theory [52] is an uncertain reasoning method, which is often used in the field of information fusion. It can effectively deal with the problem of conflict information in the fusion process and fuse the relevant information through calculation. Its fusion process is described below.

Firstly, according to D-S theory, the fuzzy set A in Table 5 can be simplified by Bayes approximation [53]. After simplification, each fuzzy set A only contains one element and can more directly describe the cloud service trustworthiness. The calculation process is shown in formula (1) below.

$$m(\underline{A}) = \frac{\sum_{\underline{A}\subseteq A} m(A)}{\sum_{A\subseteq\Theta} m(A) * N} \tag{1}$$

In formula (1), Θ represents the complete set, and N is the total number of elements contained in A. $\underline{A}$ is the simplified set of A. Taking the data in Table 5 as an example, its simplification process is as follows.

$$m(\underline{I}) = \frac{m(I) + m(I, II)}{m(I) + m(I, II) * 2 + m(II, III) * 2 + m(III, IV) * 2}$$

$$m(\underline{II}) = \frac{m(I, II) + m(II, III)}{m(I) + m(I, II) * 2 + m(II, III) * 2 + m(III, IV) * 2}$$

$$m(\underline{III}) = \frac{m(II, III) + m(III, IV)}{m(I) + m(I, II) * 2 + m(II, III) * 2 + m(III, IV) * 2}$$

$$m(\underline{IV}) = \frac{m(III, IV)}{m(I) + m(I, II) * 2 + m(II, III) * 2 + m(III, IV) * 2}$$

After simplification, each arbitrary set $\underline{A}$ contains only one element, such as $\{I\}, \{II\}, \{III\}, \{IV\}$. Next, according to the fusion rules of D-S, substituting $\underline{A}$ into formula (2) for calculation, the trust degree $m(\underline{A}, C_i)$ of each trustworthiness level I, II, III, IV after fusion can be obtained, as shown in Table 6.

$$m(\underline{A}) = \frac{1}{k} \sum_{\underline{A_1}\cap\underline{A_2}\cap\ldots\cap\underline{A_n}=\underline{A}} m_1(\underline{A_1}) m_2(\underline{A_2}) \cdots m_n(\underline{A_n}) \tag{2}$$

In formula (2), k is the normalization factor, and its calculation method is shown in formula (3).

$$k = \sum_{\underline{A_1}\cap\underline{A_2}\cap\ldots\cap\underline{A_n}\neq\emptyset} m_1(\underline{A_1}) m_2(\underline{A_2}) \cdots m_n(\underline{A_n}) \tag{3}$$

As shown in Table 6, the simplified assessment results can more directly and effectively describe the cloud service trustworthiness level. $m(I, C_i)$, $m(II, C_i)$, $m(III, C_i)$ and $m(IV, C_i)$ respectively represent the trust degree of indicator C_i belonging to different trustworthiness levels. The higher

TABLE 6. Simplified fuzzy set $\underline{A}$ and its fusion result.

	Assessment 1	Assessment 2	Assessment 3	
Arbitrary set $\underline{A}$	$m_1(\underline{A}, C_i)$	$m_2(\underline{A}, C_i)$	$m_n(\underline{A}, C_i)$	$m(\underline{A}, C_i)$
I	0.050	0.075	0.132	0.004
II	0.300	0.350	0.289	0.272
III	0.450	0.425	0.395	0.675
IV	0.200	0.150	0.184	0.049

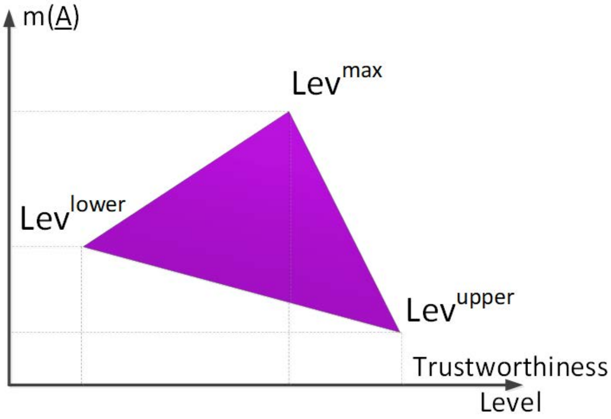

FIGURE 2. Four intervals of cloud service trustworthiness.

the value of $m(\underline{A}, C_i)$, the greater the possibility that the indicator C_i belongs to $\underline{A}$. In Table 6, the result after fusion is $m(III, C_i) > m(II, C_i) > m(IV, C_i) > m(I, C_i)$, it indicates that the trustworthiness level of the indicator is most likely III. The upper limit of its trustworthiness level is IV and the lower limit is I. Therefore, in order to provide users with more intuitive assessment results and provide support for subsequent trustworthiness state assessment research, the trustworthiness level of the above indicators can be expressed as a fuzzy triangular value, as shown in Figure 2.

In Figure 2, the horizontal axis represents the cloud service trustworthiness level, and the vertical axis represents the trust degree $m(\underline{A})$. The triangle consists of three points.

1) lev^{upper} indicates the upper limit of the trustworthiness level. The necessary condition is that $m(\underline{A}) > 0$. The upper limit lev^{upper} can serve as a warning to let users know the possible maximum hazard level and the possible maximum damage. The higher the trust degree $m(\underline{A})$, and the smaller the gap between the trust degree and the maximum trust degree, the more attention needs to be paid to it.
2) lev^{lower} represents the lower limit of the trustworthiness level. The necessary condition is that $m(\underline{A}) > 0$. The lower limit lev^{lower} indicates the minimum level that the trustworthiness can be controlled. The higher the lower limit, the lower its trustworthiness.
3) lev^{max} indicates the maximum possible trustworthiness level, that is, the possibility degree $m(\underline{A})$ that the trustworthiness level belongs to lev^{max} is the highest. lev^{max} represents the maximum possible trustworthiness level of cloud services in the actual environment of long-term operation. Compared with the upper limit lev^{upper} and the lower limit lev^{lower}, this value of lev^{max} can better reflect the actual cloud service trustworthiness state.

As mentioned above, this paper substitutes fuzzy theory and D-S theory into the assessment process of cloud service trustworthiness level, and puts forward an effective trustworthiness level assessment method. On this basis, focusing on the research goal, this paper will assess the cloud service trustworthiness state and its changes in the next chapter combined with Markov chain.

IV. ASSESSMENT OF CLOUD SERVICE TRUSTWORTHINESS STATE BASED ON MARKOV CHAIN

The trustworthiness level and its trust degree can only describe the cloud service trustworthiness at a certain time or in a specific state. To reflect the trustworthiness of the service in the actual use process, it needs to further assess the service trustworthiness state and its changes on the basis of its level assessment. Since there are many possibilities for the trust degree $m(\underline{A})$ of cloud service trustworthiness level, $\underline{A} \in \{I, II, III, IV\}$, thus the cloud service trustworthiness is bound to have multiple random trustworthiness states. Therefore, the change of cloud service trustworthiness state can be regarded as a random process, and it can be assessed combined with Markov chain.

Markov chain [54] is a process with discrete set and random state space. It is suitable for analyzing things with random process. According to the method of Markov chain, in order to assess the random process of cloud service trustworthiness state, this paper studies the trustworthiness state matrix of the cloud service and its state transition matrix respectively.

A. THE TRUSTWORTHINESS STATE MATRIX OF CLOUD SERVICE

1) DESCRIPTION OF CLOUD SERVICE TRUSTWORTHINESS STATE

Use S_t represents the cloud service trustworthiness state at time t. according to the definition of cloud service trustworthiness level in this paper, the representation method of cloud service trustworthiness state matrix S_t is as follows.

$$S_t = |m(I), m(II), m(III), m(IV)|$$

S_t consists of $m(I), m(II), m(III)\, and m(IV)$, which respectively represent the trust degree of the 4 trustworthiness levels. With the change of the trust degree of the 4 trustworthiness levels, cloud service will produce multiple random trustworthiness states, which together constitute the random trustworthiness state interval. As shown in Figure 3.

2) CALCULATION OF TRUSTWORTHINESS STATE MATRIX

In Figure 3, there are 8 indicators that affect the cloud service trustworthiness state, and $m(\underline{A}, C_i)$ is used to represent the

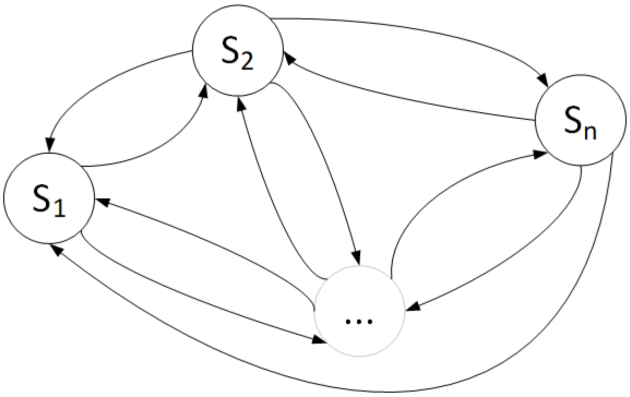

FIGURE 3. **Random trustworthiness state interval of cloud service.**

trust degree of the indicator C_i belongs to $\underline{A}$, $m\left(\underline{A}, C_i\right) = \{m(I, C_i), m(II, C_i), m(III, C_i), m(IV, C_i)\}$. $W(C_i)$ represents the trustworthiness influence weight of indicator C_i, which can be obtained by FAHP (fuzzy analytical hierarchy process). FAHP is a mature and effective weight assignment method, which has been widely recognized. According to establish the fuzzy consistency matrix of the above 8 indicators by FAHP method [50], the assessment weight $W(C_i)$ of each indicator can be obtained by comparing the weights of each indicator. The greater the value of $W(C_i)$, the greater the impact of this indicator on the cloud service trustworthiness state.

Therefore, when $m\left(\underline{A}, C_i\right)$ and $W(C_i)$ are obtained through assessment, the 4 trustworthiness levels $m(I)$, $m(II)$, $m(III)$ and $m(IV)$ of cloud service can be obtained, then the trustworthiness state matrix S_t of cloud service can be obtained. The calculation is shown in formula (4).

$$\begin{cases} m(I) = \left\{\sum_1^8 m(I, C_i) * W(C_i)\right\} \\ m(II) = \left\{\sum_1^8 m(II, C_i) * W(C_i)\right\} \\ m(III) = \left\{\sum_1^8 m(III, C_i) * W(C_i)\right\} \\ m(IV) = \left\{\sum_1^8 m(IV, C_i) * W(C_i)\right\} \end{cases} \tag{4}$$

In formula (4), the 4 cloud service trustworthiness levels are normalized, which together constitute the trustworthiness state matrix of cloud service, $m(I) + m(II) + m(III) + m(IV) = 1$.

B. TRUSTWORTHINESS STATE TRANSITION MATRIX OF CLOUD SERVICES

According to the method of Markov chain, when the trustworthiness state matrix S_t of cloud service is established, to assess the changes of the cloud service trustworthiness state, it is necessary to further calculate the trustworthiness state transition matrix STM of cloud service. The matrix is shown below.

$$STM = \begin{vmatrix} P_{I,I} & P_{I,II} & P_{I,III} & P_{I,IV} \\ P_{II,I} & P_{II,II} & P_{II,III} & P_{II,IV} \\ P_{III,I} & P_{III,II} & P_{III,III} & P_{III,IV} \\ P_{IV,I} & P_{IV,II} & P_{IV,III} & P_{IV,IV} \end{vmatrix}$$

In the matrix STM, $P_{i,j}$ represents the transition probability of cloud service trustworthiness from level i to level j, $i, j = I, II, III, IV$. In order to obtain the transition probability $P_{i,j}$ between each level, this paper makes the following analysis based on the trust degree of each indicator trustworthiness level.

Suppose that when the trustworthiness level of indicator C_i is $m(I, C_i) > 0$, it indicates that the trustworthiness level of indicator C_i has the probability of belonging to I. Assuming that the trustworthiness level of indicator C_i is I at this time, thus $m(II, C_i)$ represents the probability that indicator C_i will be transferred from level I to level II. Similarly, $m(III, C_i)$ indicates the probability that indicator C_i will be transferred from level I to level III. $m(IV, C_i)$ indicates the probability that indicator C_i will be transferred from level I to level IV.

It is known that the cloud service trustworthiness level is affected by the trustworthiness of each indicator. Therefore, the transfer probabilities of all indicators can be summarized, and then the transfer probabilities between the trustworthiness levels of the whole cloud service can be calculated, as shown in formula (5).

$$\begin{cases} P_{I,\underline{A}} = \dfrac{\hat{P}_{I,\underline{A}}}{\hat{P}_{I,I} + \hat{P}_{I,II} + \hat{P}_{I,III} + \hat{P}_{I,IV}} \\ \hat{P}_{I,\underline{A}} = \sum_{\forall m(I,C_i)>0} m\left(\underline{A}, C_i\right) \\ P_{II,\underline{A}} = \dfrac{\hat{P}_{II,\underline{A}}}{\hat{P}_{I,I} + \hat{P}_{I,II} + \hat{P}_{I,III} + \hat{P}_{I,IV}} \\ \hat{P}_{II,\underline{A}} = \sum_{\forall m(II,C_i)>0} m\left(\underline{A}, C_i\right) \\ P_{III,\underline{A}} = \dfrac{\hat{P}_{III,\underline{A}}}{\hat{P}_{I,I} + \hat{P}_{I,II} + \hat{P}_{I,III} + \hat{P}_{I,IV}} \\ \hat{P}_{III,\underline{A}} = \sum_{\forall m(III,C_i)>0} m\left(\underline{A}, C_i\right) \\ P_{IV,\underline{A}} = \dfrac{\hat{P}_{IV,\underline{A}}}{\hat{P}_{I,I} + \hat{P}_{I,II} + \hat{P}_{I,III} + \hat{P}_{I,IV}} \\ \hat{P}_{IV,\underline{A}} = \sum_{\forall m(IV,C_i)>0} m\left(\underline{A}, C_i\right) \end{cases} \tag{5}$$

In formula (5), $\hat{P}_{I,\underline{A}}$ is equal to the sum of the transition probabilities $m\left(\underline{A}, C_i\right)$ of all indicators whose conditions satisfy $m(I, C_i) > 0$. When $\hat{P}_{I,\underline{A}}$ is calculated, $P_{I,\underline{A}}$ can be obtained by normalizing $\hat{P}_{I,\underline{A}}$. $P_{I,\underline{A}}$ represents the probability of cloud service trustworthiness level from I to $\underline{A}$, that is, the first-row element in the transfer matrix STM. $P_{II,\underline{A}}$, $P_{III,\underline{A}}$ and $P_{IV,\underline{A}}$ respectively represent the elements of the remaining rows in the matrix STM.

C. ASSESSMENT OF TRUSTWORTHINESS STATE

So far, this paper has proposed a cloud service trustworthiness state matrix S_t and its transition matrix STM based on Markov

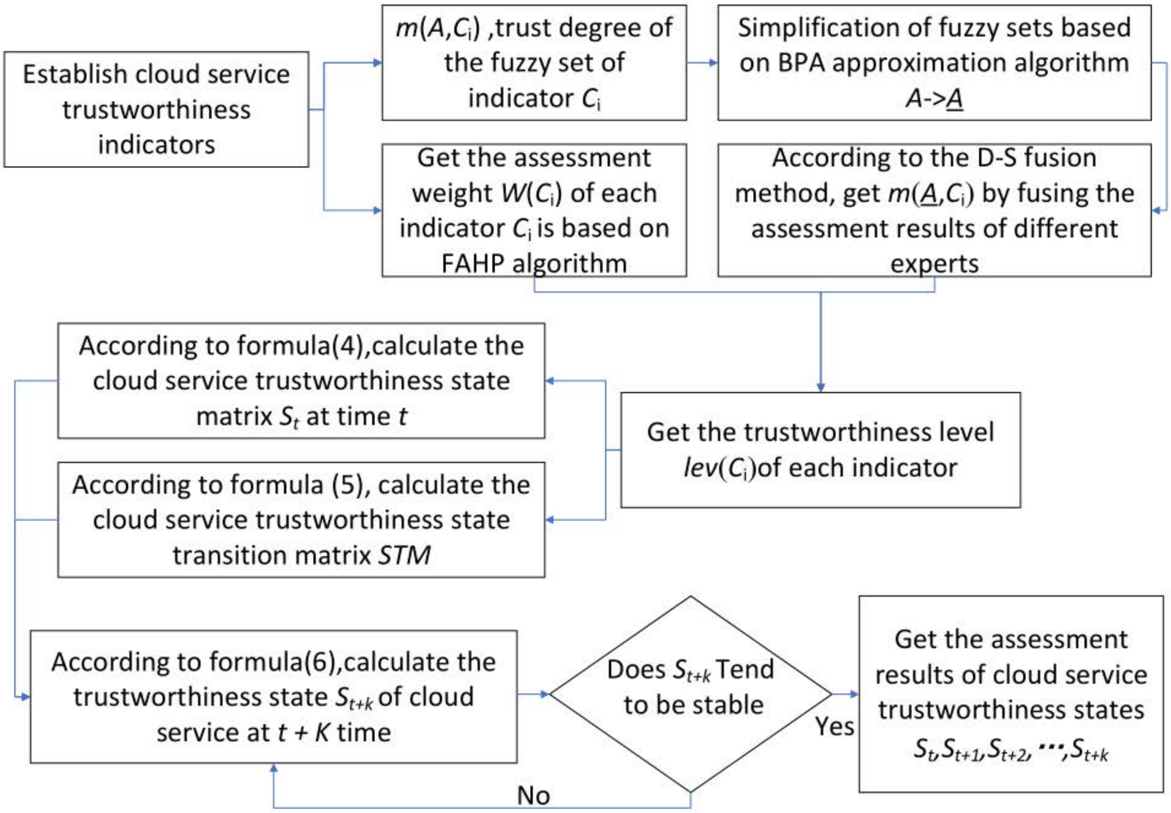
Establish cloud service trustworthiness indicators
$m(A,C_i)$,trust degree of the fuzzy set of indicator C_i
Simplification of fuzzy sets based on BPA approximation algorithm A->$\underline{A}$
Get the assessment weight $W(C_i)$ of each indicator C_i is based on FAHP algorithm
According to the D-S fusion method, get $m(\underline{A},C_i)$ by fusing the assessment results of different experts
According to formula(4),calculate the cloud service trustworthiness state matrix S_t at time t
Get the trustworthiness level $lev(C_i)$of each indicator
According to formula (5), calculate the cloud service trustworthiness state transition matrix STM
According to formula(6),calculate the trustworthiness state S_{t+k} of cloud service at $t + K$ time
Does S_{t+k} Tend to be stable
Yes
No
Get the assessment results of cloud service trustworthiness states $S_t, S_{t+1}, S_{t+2}, \cdots, S_{t+k}$

FIGURE 4. Computing process of cloud service trustworthiness state assessment model.

TABLE 7. The input, intermediate results and output results of the model proposed in this paper.

Input data	The assessment weight $W\left(C_i\right)$ of each indicator C_i, and the trust degree of the trustworthiness level fuzzy set $m(A, C_i)$
Intermediate results	The trustworthiness level, $lev = lev^{lower}, lev^{max}, lev^{upper}$, and its trust degree $m(\underline{A}, C_i)$
output results	The assessment result of the cloud service trustworthiness state,$S_t, S_{t+1}, ..., S_{t+k}$

chain. Next, according to the prediction method of Markov chain, substitute the trustworthiness state matrix S_t and state transition matrix *STM* into the calculation formula of Markov chain, the change of the trustworthiness state of cloud service can be predicted, as shown in formula (6).

$$S_{t+k} = S_t * STM^k \tag{6}$$

In formula (6), k is an integer indicating the number of state transitions, $k \geq 1$. According to the Markov chain principle, when the value of k is large enough, that is, after a certain number of transformations, the cloud service trustworthiness state will eventually become stable, reach a stable trustworthiness state and will not change. This state is called the stable trustworthiness state, which means the final stable state of a cloud service in the long-term use process. Different from the meaning of the trustworthiness state at time t, this stable trustworthiness state reflects the mutual transformation possibility of cloud service among various trustworthiness levels. By observing the trustworthiness state and its change trend, users can reasonably carry out risk management and prevention.

V. CLOUD SERVICE TRUSTWORTHINESS STATE ASSESSMENT MODEL BASED ON D-S THEORY AND MARKOV CHAIN

Through the research in section III and section IV, this paper establishes the trustworthiness attribute model of cloud services, puts forward the assessment method of the cloud service trustworthiness level combined with D-S theory, and proposes the trustworthiness state matrix and its state transition matrix combined with Markov chain. As shown in Figure 4, based on the research results in section III and section IV, this paper finally puts forward a cloud service trustworthiness state assessment model, realizes the assessment of the cloud service trustworthiness state.

The input, intermediate results and output results of the model are shown in Table 7.

TABLE 8. The characteristics of the assessment object.

Some aspect	Characteristic
Service provider operation	The service provider has been operating stably for more than 10 years and has multiple data centers around the world.
Server configuration	2G memory, 4-core and 2M bandwidth
Management authority of service provider	The service provider has all administrative rights to the server.
Data backup	Service providers can recover and restore server data in time.
Users' access rights	The access rights, user roles and keys of the server are managed by users themselves, including public IP and Intranet IP. During use,it can be accessed by other IP of the intranet.
System update	The server can change the operating system at any time.
Function expansion	Users can pay to expand the new functions they need.
Network defense	The service provider platform only provides basic network defense strategies for the server, and does not provide special DDoS and CC defense support.
Responsibility attribution	The service provider has a clear responsibility attribution agreement. The service provider is only responsible for managing the security of the platform, and the users are responsible for managing the security of their own server.

TABLE 9. The trust degree of the trustworthiness level fuzzy set *m(A, C$_i$)*.

	$m(A, C_1)$			$m(A, C_2)$		
A	Assessment1	Assessment2	Assessment3	Assessment1	Assessment2	Assessment3
I	0	0	0	0.5	0.6	0.5
I, II	0.2	0.2	0.1	0.3	0.3	0.4
II, III	0.5	0.4	0.7	0.2	0.1	0.1
III, IV	0.3	0.4	0.2	0	0	0
	$m(A, C_3)$			$m(A, C_4)$		
A	Assessment1	Assessment2	Assessment3	Assessment1	Assessment2	Assessment3
I	0.4	0.6	0.5	0.5	0.6	0.8
I, II	0.3	0.2	0.3	0.4	0.4	0.2
II, III	0.2	0.1	0.1	0.1	0	0
III, IV	0.1	0.1	0.1	0	0	0
	$m(A, C_5)$			$m(A, C_6)$		
A	Assessment1	Assessment2	Assessment3	Assessment1	Assessment2	Assessment3
I	0.3	0.3	0.2	0	0	0
I, II	0.5	0.5	0.4	0.1	0.2	0.2
II, III	0.1	0.2	0.3	0.6	0.6	0.5
III, IV	0.1	0	0.1	0.3	0.2	0.3
	$m(A, C_7)$			$m(A, C_8)$		
A	Assessment1	Assessment2	Assessment3	Assessment1	Assessment2	Assessment3
I	0	0	0	0	0	0
I, II	0.6	0.3	0.4	0.4	0.4	0.3
II, III	0.2	0.4	0.4	0.4	0.4	0.4
III, IV	0.2	0.3	0.2	0.2	0.2	0.1

As shown in Figure 4 and table 7, using the assessment model proposed in this paper, it only needs to assess the weight of each indicator at the bottom, and assess the trustworthiness level fuzzy set of each indicator according to the method proposed in Section III-C, thus the corresponding intermediate results and output results can be obtained. These corresponding intermediate results and output results can provide users with detailed reference basis, help users reasonably choose trust services, and help users effectively carry out risk management and prevention.

VI. CASE ANALYSIS AND METHOD COMPARISON

In order to verify the feasibility of the proposed model, this paper convened 3 experts in cloud computing security research to assess the cloud services provided by a service provider combined with the proposed model. The object of this assessment is a cloud server called ECS (Elastic Compute service) provided by the above service provider. This cloud server belongs to IaaS (infrastructure as a service) level cloud computing service. The characteristics of the cloud service are shown in Table 8.

A. CASE ANALYSIS

Around to the characteristics of the above cloud service, according to the process shown in Figure 4, after the initial assessment, this paper obtains the input data shown in Table 9 and Table 10.

In Table 9, A represents the fuzzy set of the cloud service trustworthiness level, $A \in \{\{I\}, \{I, II\}, \{II, III\}, \{III, IV\}\}$. $m(A, C_i)$ represent the trust degree of the indicator C_i belongs to A. Assessment1, Assessment2 and Assessment3

TABLE 10. Fuzzy consistency matrix based on FAHP and assessment weight $W(C_i)$ of each indicator.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	$W(C_i)$
C_1	0.5	0.85	0.95	0.65	0.55	0.35	0.4	0.3	0.137
C_2	0.15	0.5	0.75	0.3	0.25	0.25	0.2	0.15	0.097
C_3	0.05	0.25	0.5	0.25	0.15	0.3	0.2	0.2	0.078
C_4	0.35	0.7	0.75	0.5	0.55	0.45	0.6	0.8	0.139
C_5	0.45	0.75	0.85	0.45	0.5	0.45	0.2	0.4	0.129
C_6	0.65	0.75	0.7	0.55	0.55	0.5	0.3	0.4	0.135
C_7	0.6	0.8	0.8	0.4	0.8	0.7	0.5	0.85	0.149
C_8	0.7	0.85	0.8	0.2	0.6	0.6	0.15	0.5	0.135

TABLE 11. The trust degree of the simplified trustworthiness level fuzzy sets $m(\underline{A}, C_i)$.

$\underline{A}$	C_1	C_2	C_3	C_4
I	0.050	0.600	0.533	0.833
II	0.400	0.333	0.267	0.167
III	0.450	0.067	0.133	0.000
IV	0.100	0.000	0.067	0.000
$\underline{A}$	C_5	C_6	C_7	C_8
I	0.333	0.100	0.200	0.150
II	0.389	0.350	0.400	0.350
III	0.222	0.400	0.300	0.350
IV	0.056	0.150	0.100	0.150

respectively represent the assessment of $m(A, C_i)$ given by 3 experts.

In Table 10, the element in row C_i and column C_j represents the weight ratio of indicator C_i relative to C_j. The larger the value of the weight ratio, the greater the influence weight of C_i relative to C_j on the whole cloud service trustworthiness. According to FAHP, the weight ratios between the each indicator constitute their fuzzy consistent matrix. According to the weight calculation method of FAHP[55], the assessment weight $W(C_i)$ of each indicator can be obtained by solving the matrix.

After obtaining $m(A, C_i)$, according to the process shown in Figure 4, the data shown in Table 11 can be obtained by substituting $m(A, C_i)$ into formulas (1) and (2) for calculation

In Table 11, $\underline{A}$ is the simplified set of A in Table 9, $\underline{A} \in \{I, II, III, IV\}$. It is the set of the 4 cloud service trustworthiness levels propose in Section III-B, and its calculation method is shown in formula (1). $m(\underline{A}, C_i)$ represents the trust degree of the indicator C_i belongs to $\underline{A}$, that is, the possibility that indicator C_i belongs to different trustworthiness levels.

After obtaining the data of Table 11, combined with the assessment weight $W(C_i)$ in Table 10, the cloud service trustworthiness state matrix S_t and its transition matrix STM can be obtained by successively calculating according to formulas (4) and (5). The results are as follows.

$$S_t = |0.367, 0.289, 0.300, 0.043|$$

$$STM = \begin{vmatrix} 0.473 & 0.304 & 0.215 & 0.007 \\ 0.414 & 0.279 & 0.270 & 0.037 \\ 0.337 & 0.313 & 0.308 & 0.042 \\ 0.188 & 0.326 & 0.427 & 0.059 \end{vmatrix}$$

TABLE 12. Assessment results of cloud service trustworthiness state.

	$m(I)$	$m(II)$	$m(III)$	$m(IV)$
t	0.3667	0.2894	0.3005	0.0434
$t+1$	0.4027	0.3003	0.2683	0.0287
$t+2$	0.4107	0.2994	0.2628	0.0271
$t+3$	0.412	0.2993	0.2619	0.0268
$t+4$	0.4122	0.2993	0.2618	0.0267
$t+5$	0.4122	0.2993	0.2617	0.0267
$t+6$	0.4122	0.2993	0.2617	0.0267

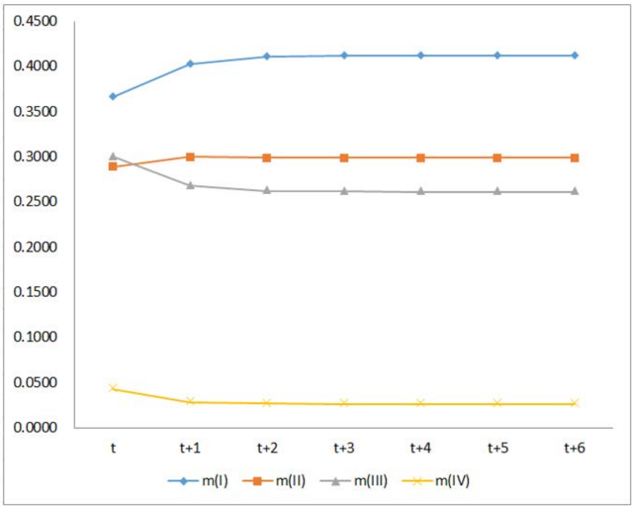

FIGURE 5. Change trend of cloud service trustworthiness state.

Finally, by substituting the above S_t and STM into formula (6), the change trend of the cloud service trustworthiness can be assessed, and the results are shown in Table 12.

Table 12 records assessment results of the cloud service trustworthiness state from time t to time $t + 6$. The elements $m(I)$, $m(II)$, $m(III)$ and $m(IV)$ in row t, respectively represent the trust degrees of cloud service trustworthiness belongs to different levels at time t. They constitute the trustworthiness state matrix S_t.

In order to visually observe the changes of cloud service trustworthiness state, the data of Table 12 is converted into a line chart, as shown in Figure 5.

The following conclusions can be drawn from the results of Table 12 and Figure 5.

1) When the service reaches a stable state, $m(I) > m(II) > m(III) \gg m(IV)$. It shows that the overall trustworthiness of the service is high, the possibility of its trustworthiness level belonging to I is the greatest, and the possibility of its trustworthiness level belonging to IV is very low.
2) It can be seen from the change trend of the trustworthiness state, $m(I)\, andm\, (II)$ gradually increase, but $m(III)$ and $m(IV)$ gradually decrease, and finally $m(II) > m(III)$. This conclusion shows that in the long-term use process, the trustworthiness state of the service will show a good change trend.

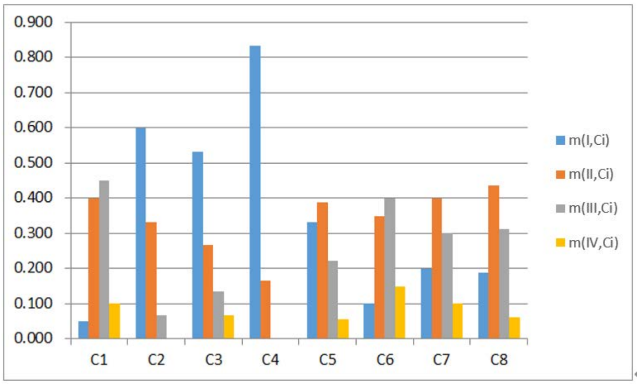

FIGURE 6. ***m*(*A*, *C*$_i$) comparison of each trustworthiness indicator.**

3) In addition, it can be seen from the range of change, that the service has a large trustworthiness change only when it is first put into use, but its trustworthiness will gradually stabilize with the passage of time.

Then convert the data shown in Table 9 into a histogram, as shown in Figure 6.

Through the comparison of Figure 6, combined with the meaning of the triangular fuzzy value of trustworthiness level proposed in Figure 2, the following conclusions can be obtained.

1) The lev^{max} of C_4, C_2 and C_3 indicators are equal to I, indicating that "the trustworthiness of service provider operation," "the physical security trustworthiness" and "the trustworthiness of laws and regulations" of the service belong to the "Fully trusted" level.
2) The lev^{max} of C_1 and C_6 indicators are equal to III, indicating that the trustworthiness of "terminal trustworthiness" and "network trustworthiness" of the service is low, belonging to the "Basically untrusted" level.
3) The lev^{max} of other indicators are equal to II, indicating that other indicators are at the "Basically trusted" level.

B. METHOD COMPARISON

From the above case analysis, it can be seen that the model proposed in this paper is suitable for the trustworthiness assessment of cloud services. It can provide users with the cloud service trustworthiness state and its change trend, and provide users with the trustworthiness level of relevant indicators, so as to help users reasonably select and use trusted cloud services. As a trustworthiness assessment method, this method belongs to the category of safety assessment and risk assessment. In order to explain its characteristics, it should be compared with other common risk assessment methods. Therefore, this paper compares the proposed methods with other common security assessment methods. These methods include risk uncertainty assessment method based on information entropy [28], [30]–[32], risk weight method based on FAHP [24], [25], [56], risk level assessment method based on risk matrix [40], [41], and trust assessment method based on trust chain [42]–[44].

In order to explain its characteristics, it should be compared with other common risk assessment methods. Therefore, this paper compares the proposed methods with other common security assessment methods. These methods include risk uncertainty assessment method based on information entropy [28]–[30], risk weight method based on FAHP [22], [23], [51], risk level assessment method based on risk matrix [38], [39], and trust assessment method based on trust chain [40]–[42]. In order to reasonably compare the characteristics of different methods, this paper makes a comparative analysis from the following 5 aspects around input, output and assessment process of each method.

1) Assessment costs. It refers to the cost of using this method for assessment, including early model establishment, input data collection, expert assessment workload, etc.
2) Decision support of output results. The more trustworthiness assessment results can be output, and the more detailed reference data can be provided to users, the greater the help for users in risk management.
3) Method scalability. When the needs of the assessment change, the less adjustments need to be made, the higher the scalability of this method.
4) Objectivity of assessment results. It refers to the objectivity of the assessment results obtained by this method. The higher the objectivity, the more reliable the result can reflect the actual cloud service.
5) Applicability of the method. The wider the scope of this method, the higher its applicability.

1) COST COMPARISON

Use $\{1, 2, 3\}$ to express the level of assessment cost, 3 expresses high, 2 expresses moderate, and 1 expresses easy. To assess the cloud service trustworthiness, the cost comparison of each method is shown in Table 13.

2) COMPARISON ON THE DEGREE OF DECISION SUPPORT

Use $\{1, 2, 3\}$ to express the degree of decision support, 3 expresses high, 2 expresses moderate, and 1 expresses easy. Applying these methods to assess the cloud service, the comparison on the degree of decision support is shown in Table 14.

3) SCALABILITY COMPARISON

Use $\{1, 2, 3\}$ to express the level of scalability, 3 expresses high, 2 expresses moderate, and 1 expresses easy. The scalability comparison of different methods is shown in Table 15.

4) OBJECTIVITY COMPARISON

Use $\{1, 2, 3\}$ to express the level of objectivity, 3 expresses high, 2 expresses moderate, and 1 expresses easy. The comparison of the objectivity of the results is shown in Table 16.

TABLE 13. Comparison of assessment cost of each method.

Method	Assessment cost of each method	Cost
Method based on FAHP [25]	It is necessary to establish a hierarchical model of cloud service trustworthiness, including target layer, indicator layer and scheme layer. The cost of this method is low.	1
Method based on Risk Matrix [40]	It is necessary to sort out the trustworthiness indicators of cloud services and establish a risk matrix for risk level judgment. Like FAHP method, both of them only need to establish a simple model before assessment, and the cost is low.	1
Method based on Information Entropy [28]	It is necessary to sort out the risk dimensions and its related influencing factors. Similarly, the cost is low.	1
Method of this paper	It is necessary to sort out the trustworthiness indicators of cloud services, and assess the risk level and weight of each indicator. The assessment of risk level and weight of this method is based on risk matrix and FAHP respectively,and its trustworthiness cost is moderate.	2
Method based on Trust Chain [42]	It is necessary to establish corresponding trust nodes and build a trust chain. Compared with other methods, it is more difficult to establish the trust chain, which needs the support of relevant monitoring systems and nodes, and the cost is higher.	3

TABLE 14. Comparison on the degree of decision support.

Method	The degree of decision support of each method	the degree of decision support
Method based on FAHP [25]	Through the established FAHP model, this method can judge the influence weight of different indicators on cloud service trustworthiness, and can give the decision-making scheme with high weight through calculation.	2
Method based on Risk Matrix [40]	Through the established risk matrix, this method can effectively assess the risk level of relevant indicators affecting the trustworthiness of cloud services, so as to help users understand the risk level of the service.	1
Method based on Information Entropy [28]	This method can provide users with uncertainty assessment results of different dimensions, and help users understand the trustworthiness of the service in different dimensions.	2
Method of this paper	This method inherits the advantages of FAHP and risk matrix, and can provide assessment results, including indicator weight, indicator trustworthiness level, cloud service trustworthiness state and its change trend. It can provide detailed reference for users make reasonable service selection and use.	3
Method based on Trust Chain [42]	Through the established trust chain, this method can effectively judge whether the integrity of the system is damaged and detect the defects of the system.	3

TABLE 15. The scalability comparison of each method.

Method	When the needs of the assessment change, the adjustments need to be made	Scalability
Method based on FAHP [25]	When the assessment demand changes, due to the change of indicators, the method needs to re-establish the weight judgment matrix of each indicator. Compared withthe risk matrix method,the scalability of this method is moderate.	2
Method based on Risk Matrix [40]	When assessing the change of demand, this method only needs to increase or decrease the corresponding indicators according to the demand, and there is little need to make adjustment.	1
Method based on Information Entropy [28]	When the assessment demand changes, it is necessary to re-divide the dimensions of risks and their influencing factors. Its scalability is moderate.	2
Method of this paper	Due to the change of indicators, this method also needs to re-evaluate the weight of each indicator based on FAHP. Its scalability is moderate.	2
Method based on Trust Chain [42]	Because the trust chain is not easy to change,the scalability of this method is lower than other methods.	1

TABLE 16. The comparison of the objectivity of the results.

Method	Analysis of objectivity	objectivity
Method based on FAHP [25]	This method adopts the pairwise comparison method when judging theweight, which can reduce the influence of human subjective factors on the assessment results to a certain extent.	2
Method based on Risk Matrix [40]	In the assessment process, this method usually directly gives thelevel of risk, its assessment process is vulnerable to human subjective factors, and the objectivity of its assessment results is low.	1
Method based on Information Entropy [28]	The evaluation method based on information entropy can effectivelyassess the uncertainty of risk. Its assessment results are expressed in the form of entropy,which has a certain objectivity, but it is difficult to clearly explain the impact of different indicators on the trustworthiness of cloud services	2
Method of this paper	This method adopts the pairwise comparison method of FAHP when assessing the indicator weight, which ensures the objectivity of the assessment weight. In addition, this method introduces the concept of trust degree in the assessment of trustworthiness level,and combines the assessment results of multiple experts with D-Sfusion method, so the objectivity of the results is relatively high. Finally, based on Markov chain, this paper assesses the trustworthiness state of cloud services and its change, and the results can better reflect the real trustworthiness of cloud services.	3
Method based on Trust Chain [42]	As long as the integrity of the system is detected to be destroyed,this method can effectively reflect some defects of the system, and there is almost no artificial evaluation. Therefore, this method has high objectivity.	3

5) APPLICABILITY COMPARISON

Use {1, 2, 3} to express the level of applicability, 3 expresses high, 2 expresses moderate, and 1 expresses easy. The applicability comparison of different methods is shown in Table 17.

By summarizing the above comparison results, the results shown in Figure 7 can be obtained.

To sum up, the method proposed in this paper inherits the advantages of other basic methods. The comparison shows that this method has high applicability and scalability, can effectively assess the trustworthiness of cloud services, and can provide users with detailed assessment results. These assessment results include: the weight of the cloud service trustworthiness indicators, the trustworthiness level of each indicator, the cloud service trustworthiness state and its change trend. Compared with other assessment methods mentioned in this section, the assessment results of this paper method have higher objectivity and can better reflect the trustworthiness and its changes in the long-term use process. Compared with the assessment method based on trust chain, the cost of this paper method is lower. The method based on trust chain focuses on assessing the integrity of the system,

TABLE 17. The applicability comparison of each method.

Method	Applicability description of the method	Applicability
Method based on FAHP [25]	This method can be used to judge the influence weight of each indicator on cloud service security,and can also judge the weight of different risk management schemes.	2
Method based on Risk Matrix [40]	This method is only applicable to the quantitative assessment of the risk level.	1
Method based on Information Entropy [28]	This method is suitable for the uncertainty analysis of cloud service security, such as the uncertainty of risk occurrence frequency, the uncertainty of risk loss.	3
Method of this paper	This method can assess the changes of cloud service trustworthiness, as well as trustworthiness level of each indicator and its impact weight	3
Method based on Trust Chain [42]	This method is mainly suitable for assessing the integrity of the system, but it is not suitable forthe comprehensive assessment of the trustworthinessof cloud services in the actual interactive environment.	2

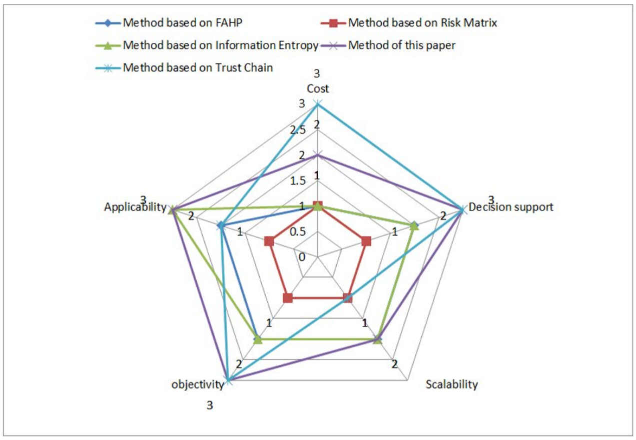

FIGURE 7. Characteristics comparison of each method.

and the method proposed in this paper comprehensively considers many factors in the process of cloud service interaction, so it is more applicable.

VII. CONCLUSION

This paper combs the trustworthiness indicators of cloud services, divides the trustworthiness interval of cloud services, and defines the cloud service trustworthiness state, finally proposes a cloud service trustworthiness state assessment method based on D-S evidence theory and Markov chain. This method reduces the experts' scoring difficulty and solves the conflicting problem in the assessment process. Different from the general trustworthiness assessment method, the general assessment method can only give a static assessment result which is not enough to represent the trustworthiness in practical application scenarios. The method proposed in this paper realizes the effective assessment of the cloud service trustworthiness state and its changes in the long-term use process. The assessment results obtained by this method can more objectively reflect the real cloud service trustworthiness, and help users understand the cloud service trustworthiness and its changes in the long-term use process, so as to help users make reasonable service selection and use. Through the method comparison, it shows that the method proposed in this paper is simple and feasible, and it is of great significance to ensure the security of cloud services.

However, when the trustworthiness indicators affecting cloud services increase, the difference of each indicator's trustworthiness assessment results obtained by this method will become little. Although such results will become more comprehensive due to the increase of indicators, their reference value will be greatly reduced. Therefore, in the follow-up research, with the development of cloud services and the increase of the assessment indicators, while improving the comprehensiveness of the assessment method, it is also necessary to ensure the identification of each indicator's trustworthiness assessment results.

AUTHOR CONTRIBUTIONS

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Tilei Gao, Wanyu Xie, Li Jia, and Tao Zhang. The first draft of the manuscript was written by Ming Yang and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

FUTURE WORKS

For the trustworthiness assessment of cloud services, this study only proposes 8 cloud service trustworthiness indicators and their corresponding rating standards. In the future research, in order to improve the comprehensiveness and accuracy of the assessment results, it is necessary to further sort out its sub indicators on the basis of the trustworthiness indicators proposed in this study, then establish a multi-level assessment indicator system and its corresponding objective trustworthiness evidence. Combining with trustworthiness evidence, experts will be able to give a more objective and accurate assessment of each trustworthiness indicator. Therefore, establishing a multi-level assessment indicator system and establishing its corresponding objective trustworthiness evidence will be the future research work.

REFERENCES

[1] *Flexera 2020 State of the Cloud Report*, Flexera, Itasca, IL, USA, 2020.

[2] (2001). T. C. Group, *Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b*. [Online]. Available: http://www. trustedcomputinggroup.org

[3] M. Howard and D. E. Leblanc, *Writing Secure Code*. Redmond, WA, USA: Microsoft Press, 2001.

[4] C. Huo-wang, W. Ji, and D. Wei, "High confidence software engineering technologies," *Acta Electronica Sinica*, vol. 31, no. S1, pp. 1933–1938, 2003.

[5] *Information Technolog —Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model*, Standard 15408-1:2005, ISO/IEC, 2005.

[6] W. Huai-Min, T. Yang-Bin, Y. Gang, and L. Lei, "Trusted mechanism of internet software," *Sci. China Inf. Sci.*, vol. 36, no. 10, pp. 1156–1169, 2006.

[7] W. Huai-Min and Y. Gang, "Evolution of software trustworthiness in the network age," *Commun. China Comput. Fed.*, vol. 6, no. 2, pp. 28–34, 2010.

[8] G. Xin, X. Zheng-Quan, and L. Jin, "Review of cloud based trust model," *J. Commun.*, vol. 32, no. 7, pp. 176–181, 2011.

[9] S. Chang-Xiang, "Scientific concept of network security and trusted computing 3.0," in *Proc. China Softw. Ind. Annu. Conf.*, Beijing, China, 2018, pp. 1–3.

[10] 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.

[11] Y. Liang, "11 threats of cloud services," *Comput. Netw.*, vol. 46, no. 19, p. 53, 2020.

[12] J. Rong, M. Zi-Fei, T. Sheng-Hu, and Y. Ming, *Measurement and Evaluation of Trusted Cloud Services*. Beijing, China: Science Press, 2021.

[13] L. Yue-Ming and Z. Zhi-Hui, "Research on metrics models for cloud services information security evaluation," *Chin. J. Netw. Inf. Secur.*, vol. 2, no. 7, pp. 18–25, 2016.

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

[15] W. Tie-Dan, T. Miao, and P. Ding-Hong, "Hesitant fuzzy Taguchi multi-attribute decision making method for cloud service quality evaluation," *Fuzzy Syst. Math.*, vol. 33, no. 3, p. 16, 2019.

[16] Z. Xuan, P. Ping, and M. Xin-Yue, "Security risk assessment of cloud service," *Commun. Technol.*, vol. 49, no. 12, p. 7, 2016.

[17] W. Xu, Y. Yao, and W. Yang, "A model for QoS-aware cloud service selection based on FAHP," *Comput. Digit. Eng.*, vol. 47, no. 9, p. 9, 2019.

[18] W. Peng and L. Ke-Wen, "Dynamic trustworthy evaluation model for web service," *Comput. Syst. Appl.*, vol. 28, no. 3, pp. 185–190, 2019.

[19] M. Alaei, R. Khorsand, and M. Ramezanpour, "An adaptive fault detector strategy for scientific workflow scheduling based on improved differential evolution algorithm in cloud," *Appl. Soft Comput.*, vol. 99, Feb. 2021, Art. no. 106895.

[20] M. Ayoubi, M. Ramezanpour, and R. Khorsand, "An autonomous IoT service placement methodology in fog computing," *Softw., Pract. Exper.*, vol. 51, no. 5, pp. 1097–1120, May 2021.

[21] 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," *Proc. Comput. Sci.*, vol. 130, pp. 504–509, Jan. 2018.

[22] C. Li, S. Wang, L. Kang, L. Guo, and Y. Cao, "Trust evaluation model of cloud manufacturing service platform," *Int. J. Adv. Manuf. Technol.*, vol. 75, nos. 1–4, pp. 489–501, Oct. 2014.

[23] 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.

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

[25] M. V. C. Fagundes, A. C. Keler, E. O. Teles, S. A. B. V. de Melo, and F. G. M. Freires, "Multicriteria decision-making system for supplier selection considering risk: A computational fuzzy AHP-based approach," *IEEE Latin Amer. Trans.*, vol. 19, no. 9, pp. 1564–1572, Sep. 2021.

[26] Z. Li and R. Jie, "Cloud service trust evaluation algorithm optimization based on multi-level structure model," *J. Nanjing Univ. Sci. Technol.*, vol. 44, no. 1, p. 6, 2020.

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

[28] G. 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, May 2019.

[29] T. Gao, T. Li, R. Jiang, M. Yang, and R. Zhu, "Research on cloud service security measurement based on information entropy," *IJ Netw. Secur.*, vol. 21, pp. 1003–1013, 2019.

[30] 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 Comput.*, vol. 24, pp. 1–10, Sep. 2021.

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

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

[33] 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," *J. Intell. Fuzzy Syst.*, vol. 38, no. 5, pp. 1–12, 2020.

[34] A. Mohsenzadeh, H. Motameni, and M. J. Er, "Retraction note to: A new trust evaluation algorithm between cloud entities based on fuzzy mathematics," *Int. J. Fuzzy Syst.*, vol. 21, no. 6, p. 1988, Sep. 2019.

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

[36] 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," *Comput. Eng. Sci.*, vol. 41, no. 1, pp. 47–55, 2019.

[37] L. Zuan-Shi and G. Xiu-Li, "Trusted cloud service evaluation method research based on D-S theory," *Comput. Eng. Appl.*, vol. 53, no. 17, pp. 70–76, 2017.

[38] D. X. Wang and Q. Wang, "Trustworthiness evidence supporting evaluation of software process trustworthiness," *J. Softw.*, vol. 29, no. 11, pp. 178–200, 2018.

[39] W. Xu, W. Yang, and Y. Yao, "Multi-dimensional trust evaluation method based on D-S evidence theory," *Comput. Digit. Eng.*, vol. 47, no. 2, p. 7, 2019.

[40] R. M. C. Ratnayake and K. Antosz, "Development of a risk matrix and extending the risk-based maintenance analysis with fuzzy logic," *Proc. Eng.*, vol. 182, pp. 602–610, Jan. 2017.

[41] S. Albery, D. Borys, and S. Tepe, "Advantages for risk assessment: Evaluating learnings from question sets inspired by the FRAM and the risk matrix in a manufacturing environment," *Saf. Sci.*, vol. 89, pp. 180–189, Nov. 2016.

[42] W. Shang and X. Xing, "ICS software trust measurement method based on dynamic length trust chain," *Sci. Program.*, vol. 2021, pp. 1–11, Apr. 2021.

[43] Y. Zheng, Y. Chunlin, F. Zhengyun, and Z. Na, "Trust chain model and credibility analysis in software systems," in *Proc. 5th Int. Conf. Comput. Commun. Syst. (ICCCS)*, May 2020, pp. 153–156.

[44] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "TrustChain: A privacy preserving blockchain with edge computing," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–17, Jul. 2019.

[45] D. Wang, T. Zhou, Y. Wu, and W.-B. Zhao, "Risk assessment model for trusted platform control module based on Bayesian network," *J. Comput. Appl.*, vol. 31, no. 3, pp. 767–770, May 2011.

[46] Y. Song, Y. Wang, and D. Jin, "A Bayesian approach based on Bayes minimum risk decision for reliability assessment of web service composition," *Future Internet*, vol. 12, no. 12, p. 221, Dec. 2020.

[47] C. Ping, W. Xinjian, and D. Depeng, "Construction of model based on Petri net and reliability analysis based on Bayes net of web service transaction," *J. Commun.*, vol. 39, no. S1, pp. 99–104, 2018.

[48] Q. Shuangyang, C. Zhe, and L. Yuanxu, "Cloud service reliability prediction method based on improved Bayes," *Comput. Appl. Softw.*, vol. 34, no. 11, p. 6, 2017.

[49] *Top 11 Cloud Computing Threats Report*, Cloud Secur. Alliance, Beijing, China, 2020.

[50] Q. Zhu, X. Kuang, and Y. Shen, "Risk matrix method and its application in the field of technical project risk management," *Eng. Sci.*, vol. 5, no. 1, pp. 89–94, 2003.

[51] T. Aiguo and H. Chunhua, "Application of fuzzy theory in software project risk assessment," *J. Central South Univ. Sci. Technol.*, vol. 48, no. 2, pp. 411–417, 2017.

[52] 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 Commun. Mobile Comput.*, vol. 2022, pp. 1–20, Feb. 2022.

[53] H. Robbins, *An Empirical Bayes Approach to Statistics*. Berkeley, CA, USA: Univ. California Press, 2020.

[54] 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 Commun. Mobile Comput.*, vol. 2020, pp. 1–11, Jul. 2020.

[55] F. Meng and X. Chen, "A new method for triangular fuzzy compare wise judgment matrix process based on consistency analysis," *Int. J. Fuzzy Syst.*, vol. 19, no. 1, pp. 27–46, Feb. 2017.

[56] Q. Wang, H. Wang, and Z. Qi, "An application of nonlinear fuzzy analytic hierarchy process in safety evaluation of coal mine," *Saf. Sci.*, vol. 86, pp. 78–87, Jul. 2016.

MING YANG received the Ph.D. degree in system analysis and integration from the School of Software, Yunnan University. He is currently an Associate Professor with the School of Information, Yunnan University of Finance and Economics, China. His research interests include information management and data mining.

TILEI GAO is currently pursuing the Ph.D. degree in system analysis and integration with the School of Software, Yunnan University. He is also an Associate Professor with the School of Information, Yunnan University of Finance and Economics. His research interests include software engineering and information management.

WANYU XIE received the master's degree in computer science and technology from the School of Information Science and Engineering, Yunnan University. She is currently a Lecturer with the Kunming Metallurgy College. Her research interest includes information management.

LI JIA is currently an Associate Professor with the School of Information, Yunnan University of Finance and Economics, China. His research interests include network communication, security control, and data mining technology.

TAO ZHANG received the Ph.D. degree from the Yunnan University of Finance and Economics. He is currently a Lecturer with the School of Information, Yunnan University of Finance and Economics. His research interests include information management and privacy security.