scientific reports

Check for updates

OPEN

Assessment of cloud service trusted state based on fuzzy entropy and Markov chain

Ming Yang[1,2], Rong Jiang[1,2], Jia Wang[1]✉, Bin Gui[1] & Leijin Long[1,2]

In the era of cloud service popularization, the trustworthiness of service is particularly important. If users cannot prevent the potential trustworthiness problem of the service during long-term use, once the trustworthiness problem occurs, it will cause significant losses. In order to objectively assess the cloud service trustworthiness, and predict its change, this paper establishes a special hierarchical model of cloud service trustworthiness attributes. This paper proposes corresponding management countermeasures around the model, defines the cloud service trustworthiness level, defines the cloud service trusted state based on fuzzy entropy and Markov chain, constructs the membership function of the cloud service trusted state, and realizes the assessment of cloud service trustworthiness and its changes according to the prediction method of Markov chain. Through case analysis and method comparison, it shows that the method proposed in this paper is effective and feasible. This method can provide objective and comprehensive assessment data for the cloud service trustworthiness and its change, makes up the deficiency of fuzzy entropy assessment method. This research has important reference value and significance for the research of cloud service trustworthiness assessment.

Keywords Fuzzy entropy, Markov chain, Cloud service, Trustworthiness, Trustworthiness assessment

According to Canalys' "Cloud Service Analysis Statistics" in November 2022, the global cloud infrastructure service expenditure in the third quarter of 2022 increased by 28% year on year, reaching US $63.1 billion. it is thus clear that global enterprises are using more and more cloud applications, and the range of cloud applications of enterprises is also growing. However, with the popularity of cloud services, cloud service downtime caused by various reasons has become a normal. On October 4, 2021, Facebook, Instagram and WhatsApp, the social media in the United States, experienced a massive outage, which lasted nearly seven hours, and their market value evaporated by 300 billion overnight. On November 16, 2021, Google Cloud, one of the world's largest cloud service providers, went down, causing many large company websites relying on Google Cloud have to interrupt their services. In December 2021, Amazon had three outages in the same month. it is thus clear that even in the era of cloud popularization, cloud service providers cannot promise 100% that the services they provide will not have problems in the use process. Lack of trust in service providers has become the biggest obstacle for users when choosing cloud services[1].

According to the definition of TCG (Trusted Computing Group) [2] a service is considered trustworthy if it always develops towards its expected goals; On the contrary, if a service cannot change towards its predicted goals, then the service is not trustworthy. In order to ensure the trustworthiness of cloud services and meet users' requirements for cloud service trustworthiness, domestic and foreign scholars have conducted research from different perspectives, including analysis of user trustworthiness requirements, research on cloud service assessment methods, research on cloud service recommendation methods, research on service selection methods, or research on cloud computing resource optimization methods. These studies have addressed issues in user trust needs analysis, service recommendation methods, service selection methods, and cloud computing resource optimization methods. However, these methods did not analyze the trustworthiness of cloud services after being selected or used, that is, did not conduct predictive analysis on changes in cloud service trustworthiness during actual long-term use. Due to the lack of prediction of changes in the trustworthiness of cloud services over long-term use, users will be unable to take preventive measures in advance before trustworthiness problems occur. Once the service suddenly fails to operate normally during use, it will cause unpredictable losses. Therefore, it is necessary to predict and assess the trustworthiness and its changes during long-term use, so as to guide the cloud service trustworthiness towards the expected state through decision adjustments before trustworthiness problems occur.

[1]School of Information, Yunnan University of Finance and Economics, Kunming 650221, China. [2]Yunnan Key Laboratory of Service Computing, Kunming 650221, China. ✉email: zz1788@ynufe.edu.cn

In order to guide the trustworthiness of cloud services towards the expected state change. This study aims to quantitatively describe the cloud service trustworthiness and its changes, predict and assess the cloud service trustworthiness and its changes, identify the key factors that affect the cloud service trustworthiness changes based on the assessment results, so as to provide detailed data support for the trustworthiness decision-making.

(1) Established a trusted attribute hierarchy model for cloud services, and proposed the concept of cloud service trusted state based on fuzzy entropy, effectively described the trustworthiness and its changes of cloud services.
(2) Constructed a membership function for the trusted state of cloud services, quantitatively describing the impact of various indicators on the changes in the trusted state of cloud services.
(3) Based on Markov chain, implemented the prediction and assessment of cloud service trustworthiness and its changes, providing comprehensive assessment results for the prevention of trustworthiness problems.

The overall organizational structure of this article is as follows.

In section "Introduction", this chapter describes the necessity of the assessment cloud service trustworthiness and its change, and leads to the research content of this paper;

In section "Related research", this chapter discusses the domestic and foreign research on trustworthiness assessment, describes the characteristics of different methods, and summarizes the main problems of these methods;

In section "Trusted state of cloud service based on fuzzy entropy and Markov chain", this chapter establishes a trusted attribute hierarchy model of cloud service with 16 indicators, and proposes corresponding management countermeasures for each indicator. Then, this chapter defines the trustworthiness level of cloud service according to the risk matrix method, and proposes a method to represent the trusted state of cloud service based on fuzzy entropy and Markov chain theory;

In section "Assessment of cloud service trusted state based on fuzzy entropy and Markov chain", the membership function of cloud service fuzzy entropy is constructed based on the risk matrix, and the calculation method of cloud service trusted state is proposed according to the constructed membership function, thus an effective assessment method of cloud service trusted state is proposed by combining fuzzy entropy and Markov chain;

In section "Case analysis and method comparison", the proposed assessment method of trusted state is applied to a specific case for analysis and comparison with other assessment methods;

In section "Conclusion", this chapter summarizes the research work of the full text, and points out that the methods proposed in this paper need to be improved.

Related research

Cloud service is not only referring to SaaS (Software as a Service), but also IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). What is closely related to cloud service trustworthiness is service quality, security and reliability. TCG (trusted computing group)[2] points out that an entity is trusted if it always develops towards the expected goal. ISO/IEC[3] defines trustworthiness as the components, operations or processes involved in computing are predictable. In order to comprehensively assess the cloud service trustworthiness, China Communications Standardization Association has proposed the standard YDB 144–2014[4], which points out the key to the trustworthiness assessment, including the cloud service capabilities, the cloud service security, and the operation and maintenance capabilities of service providers. As for how to conduct trustworthiness assessment, Shen et al.[5] pointed out that the following three aspects should be carried out, including the establishment of attribute model, the study of evidence model and the definition of trustworthiness level.

In order to ensure that the services provided can meet the trustworthiness needs of users, Chuan[6] propose to use image blur information to evaluate users' needs and expectations in cloud service trustworthiness, Tang et al.[7] proposes a two-dimensional time aware hybrid cloud service recommendation method based on network similarity and trust enhancement. In order to ensure the stable operation of the service, Tofighy[8], Salimian[9] and Shahidinejad[10] have proposed different solutions from the perspective of optimizing computing resources, aiming to improve the quality of the service by optimizing computing resources. From the perspective of service selection, in response to the problem of difficult optimization of service composition, Arani et al.[11] propose a linear programming approach to web service composition problem which is called 'LP-WSC', for selecting the most efficient service for each request in a geographically distributed cloud environment to improve service quality standards. These methods have solved the problem of user trustworthiness requirement analysis, optimized the computing resources of services, and improved the accuracy of service selection and recommendation. These methods solve the problem of user trustworthiness requirement analysis, optimize the computing resources of services, and improve the accuracy of service selection and recommendation. However, these methods do not provide predictive analysis for potential cloud service trustworthiness problems that may occur in long-time use, nor do they provide quantitative references for users on how to avoid such problems.

In addition to the above research, relevant scholars have also proposed many effective assessment methods for the security or reliability of cloud service. The method based on AHP (analytic hierarchy process)[12–18] provides model support for the trustworthiness assessment of cloud service, and can ensure the objectivity of the assessment results to a certain extent. However, this single model-based assessment lacks the analysis of changes in cloud service trustworthiness. The uncertainty assessment method based on information entropy[19–23] is an effective method to measure the trustworthiness of cloud service. However, the assessment result of this method only describes the uncertainty of risk, and does not give an estimate for the change of service trustworthiness. The assessment method based on D-S evidence theory[24–28] can effectively solve the problem of information conflict in the assessment process, but this method needs to collect a lot of assessment evidence. The assessment method based on risk matrix[29,30] can give an intuitive level for the trustworthiness of cloud service, but it is obviously insufficient in objectivity. The trusted computing method based on trusted chain[31–33] is an integrity detection method, which focuses on detecting system quality problems and does not comprehensively analyze other factors. The prediction and assessment method based on Bayesian network[34–36] can effectively predict the trustworthiness of cloud service under the condition of having sufficient known data. However, how to reduce the gap between the assessment results and the real data is a problem that needs attention in this method. Using the above methods, domestic and foreign scholars have carried out research on cloud service trustworthiness, either based on service QoS parameters[37–39], or based on user feedback[40], or based on third-party monitoring data[41,42]. Among them, the assessment based on QoS assessment only focuses on quality of service; The assessment based on user feedback evaluation has high requirements for the accumulation of historical data; The assessment based on third-party supervision or assessment data, needs to establish a special monitoring mechanism and requires high costs.

Through the above related research, it is thus clear that any single method or single angle analysis will have its defects in the trustworthiness assessment of cloud service, and they are not fully competent for the assessment of cloud service trustworthiness and its change. To achieve an effective assessment of cloud service trustworthiness and its change, only by combining relevant methods and using the advantages of different methods to deal with the corresponding key issues in cloud service trustworthiness assessment research, can the entire assessment research work be carried out smoothly.

Therefore, around the assessment contents and problems mentioned in the related research, this paper will establish the cloud service trustworthiness assessment attribute model, study the cloud service trustworthiness and its change based on the fuzzy entropy theory, propose the concept of trusted state, and combine Markov chain to realize the assessment of the cloud service trusted state and its change.

Trusted state of cloud service based on fuzzy entropy and Markov chain

Using trusted state instead of trustworthiness level to describe cloud service trustworthiness can more objectively describe the actual trustworthiness. When assessing the cloud service trustworthiness, experts cannot directly assess the trustworthiness of the entire cloud service. In order to effectively assess the cloud service trustworthiness, this paper first establishes a trustworthiness attribute model of cloud service, which will help experts to assess the trustworthiness of the entire cloud service from the bottom up.

Trustworthiness attribute model of cloud service

According to the standard YDB144-2014[10] proposed by China Communications Standardization Association, this paper divides the cloud service trustworthiness into three classes β_i, namely, the trustworthiness of service providers' operation and maintenance, the trustworthiness of service data, and the trustworthiness of service quality. Around these 3 trustworthiness classes β_i, this paper further combs out 16 important indicators α_j that affect the cloud service trustworthiness through literature review and expert visits. Finally, the trustworthiness attribute model of cloud service is established. The model is shown in Fig. 1.

The cloud service trustworthiness attribute model proposed in this paper includes 3 classes and 16 indicators. The meaning of each indicator α_j is shown in Table 1.

After establishing the model shown in Fig. 1, this paper will study the cloud service trustworthiness level.

Trustworthiness level of cloud service

According to the definition of TCG[1], a service is trusted if it always develops in the expected direction; On the contrary, if a service cannot continue to run normally due to a trustworthiness problem, the service is not trusted. Therefore, in order to quantitatively describe the service trustworthiness and further describe the service trusted state, this paper will classify the trustworthiness level from the trustworthiness problem frequency and the loss severity. As shown in Table 2, this paper defines the trustworthiness problem frequency level F and the loss severity level L.

In Table 2, F indicates the trustworthiness problems frequency level in the long-term operation of cloud service. The higher the value of F, the higher the frequency of cloud service trustworthiness problems. Similarly, $F(\beta_i)$ represents the trustworthiness problems frequency level of class β_i, $F(\alpha_j)$ represents the trustworthiness problems frequency level of α_j.

L indicates the cloud service loss severity level during long-term operation. The higher the value of L, the greater the damage caused by the cloud service trustworthiness problem. Similarly, $L(\beta_i)$ represents the loss severity level of class β_i, $L(\alpha_j)$ represents the loss severity level of α_j.

After defining the trustworthiness level of cloud service, this paper will continue to study the trusted state representation method of cloud service.

The trusted state representation method of cloud service

It is known that the cloud service trustworthiness is a concept which is difficult to define, and it always changes randomly in the long-term use process. It is not objective to describe the cloud service trustworthiness only with a fixed trustworthiness level. In order to more accurately describe the cloud service trustworthiness, this paper divides the cloud service trustworthiness into 4 states according to the trustworthiness level from high to low. The 4 states are extremely trusted state A_1,basic trusted state A_2,critical trusted state A_3 and untrusted A_4.

- Extremely trusted state A_1:it means that the service is extremely trusted. The frequency level F is extremely low, and the loss severity level L is extremely low;
- Basic trusted state A_2:this indicates that the service is basically trusted, and the frequency level F and the loss severity level L are both general;

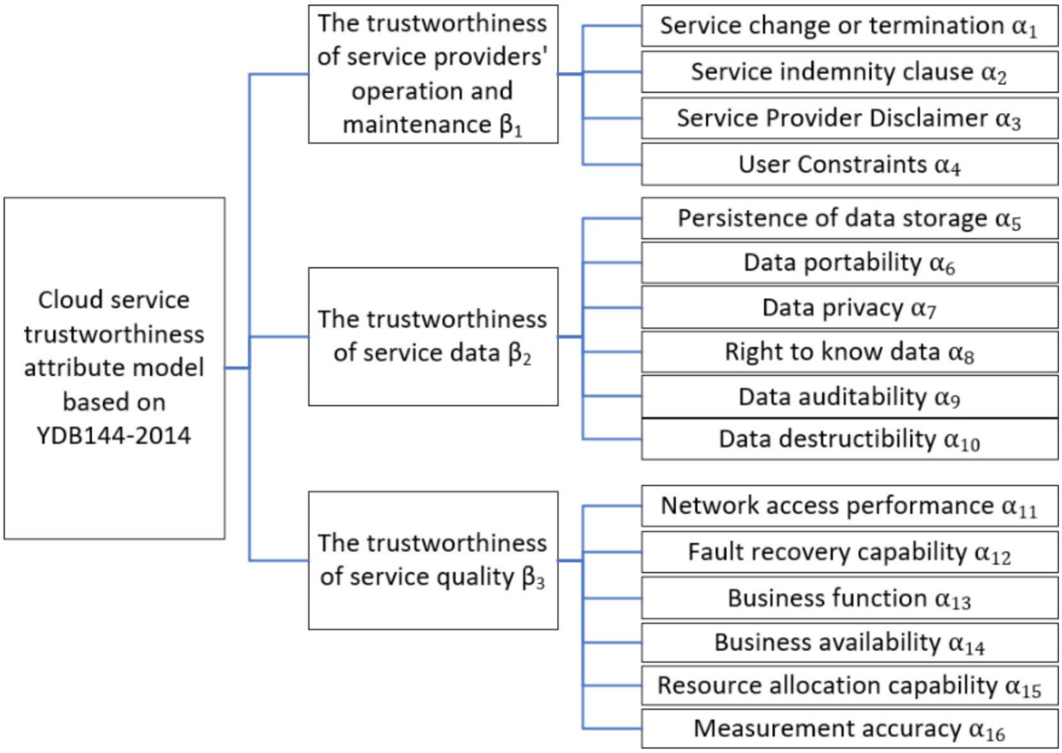


Fig. 1. The trustworthiness attribute model of cloud service.

- Critical trusted state A_3:this indicates that the service is at the edge of trusted state. The frequency level F and the loss severity level L are higher than normal;
- Untrusted A_4:it means that the service is untrusted. The frequency level F is extremely high, and the loss severity level L is extremely high.

Substitute the above 4 trusted states into the risk matrix, as shown in Table 3.

In Table 3, $\{A_1, A_2, A_3, A_4\}$ respectively represent the 4 trusted states. However, in the actual use of cloud service, due to various factors, the trustworthiness of cloud service always changes randomly, that is, it always switches between different trusted states. In order to effectively describe the randomness of cloud service trustworthiness, this paper, based on Markov chain principle[43], treats the change of cloud service trustworthiness as a random process, and proposes the concept of trusted state matrix, as shown in the following matrix.

$$TM = \left| \begin{array}{cccc} P\left(A_{1\to 1}\right) & P\left(A_{1\to 2}\right) & P\left(A_{1\to 3}\right) & P\left(A_{1\to 4}\right) \\ P\left(A_{2\to 1}\right) & P\left(A_{2\to 2}\right) & P\left(A_{2\to 3}\right) & P\left(A_{2\to 4}\right) \\ P\left(A_{3\to 1}\right) & P\left(A_{3\to 2}\right) & P\left(A_{3\to 3}\right) & P\left(A_{3\to 4}\right) \\ P\left(A_{4\to 1}\right) & P\left(A_{4\to 2}\right) & P\left(A_{4\to 3}\right) & P\left(A_{4\to 4}\right) \end{array} \right|$$

TM refers to the trusted state matrix of cloud service. The element $P\left(A_{n\to m}\right)$ in the matrix represents the probability of cloud service trustworthiness transferring from trusted state n to trusted state m ,$\sum_{m=1}^{4} P\left(A_{n\to m}\right) = 1$. This matrix effectively describes the change of the cloud services trusted state in the process of long-term use in a mathematical way. Compared with the fixed trustworthiness level representation method, this matrix can more accurately reflect the actual cloud service trustworthiness and its change.

As mentioned above, this paper proposes an effective trusted state representation method. To calculate the matrix, it needs to calculate the value of $P\left(A_{i\to j}\right)$ of each element in the matrix. In this regard, then this paper will propose an effective calculation method of cloud service trusted state matrix based on fuzzy entropy theory, and further realize the assessment of cloud service trusted state.

Assessment of cloud service trusted state based on fuzzy entropy and Markov chain

In order to carry out the assessment of cloud service trustworthiness based on fuzzy entropy, this paper defines the domain of discourse, fuzzy sets, fuzzy variables, membership and fuzzy entropy of cloud service trustworthiness in turn according to the fuzzy entropy theory, as described below.

Fuzzy entropy of cloud service trusted state

According to the fuzzy entropy theory, this paper regards the trustworthiness environment of cloud service as the research domain U, and puts forward 4 trusted states $A_n = \{A_1, A_2, A_3, A_4\}$ are regarded as four 4 sets

α_j	Meaning	Countermeasure
α_1	The service change and termination terms formulated by the service provider, which are used to regulate the conditions and procedures for changing and terminating the relationship between the service provider and cloud users.	Before providing or using cloud services, the notification method shall be agreed in advance to ensure that both parties can notify each other as soon as possible.
α_2	Indemnity clause formulated by service providers. The more detailed the indemnity clause, the higher the trustworthiness of the service.	Before providing or using cloud services, compensation terms should be clearly defined, including indemnity matters, indemnity methods, indemnity amounts, etc.
α_3	The exemption clauses formulated by the service provider, such as the interpretation of force majeure factors and exemption scenarios.	Users shall ensure that they can accept the exemption clauses of the service provider.
α_4	Service providers' constraints on user permissions and application scenarios. The smaller the constraint on users, the higher the service trustworthiness.	Users should check whether the relevant constraints will limit their subsequent application extensions.
α_5	The probability that data will not be lost during the service contract period. The smaller the probability of data loss, the higher the trustworthiness.	Users should make their own database backups every day and back up data to different devices.
α_6	Refers to the portability of data. If the data can be fully migrated, then the credibility is highest.	Users should minimize the dependence of application data on the server system environment.
α_7	The effectiveness of data encryption or isolation processing by service providers. The higher the encryption level of data, the higher the credibility.	Users should detect their own application vulnerabilities and require the service provider to provide an encrypted transmission mechanism.
α_8	Refers to the user's right to know, about the location of data storage and the usage of service provider data. The greater the user's legitimate right to know, the higher the trustworthiness.	Users need to clarify the authority of the service provider and prevent data leakage caused by malicious employees inside the service provider.
α_9	When the user needs to review the data, the service provider can provide the data to the user. The more detailed the data that can support the review, the higher the trustworthiness.	Users need to agree with the service provider on the audit data they can provide, and make their own log records for key operations.
α_{10}	The extent to which data can be destroyed. If the data can be completely destroyed, the trustworthiness is high.	The user needs to agree with the service provider which data must be deleted and the deadline for deletion.
α_{11}	The actual network bandwidth that the service can reach. The greater the network bandwidth, the higher the service trustworthiness.	Service providers need to clearly explain the cost of increasing network bandwidth and the minimum number of online users that bandwidth can support.
α_{12}	The capability of service failure recovery. The faster the failure recovery, the higher the service trustworthiness.	Users shall set up alternative servers for possible service failures to ensure the operation of basic functions.
α_{13}	The functions of the service. The more complete the function, the higher the service trustworthiness.	Before purchase or use, users should judge whether the service function can meet the current and subsequent business needs.
α_{14}	The time when the service can operate normally. The longer the service can operate normally during use, the higher the trustworthiness.	The user shall make clear whether there is regular maintenance or overhaul time for the service.
α_{15}	The deployment capability of calculates resource. The higher the feasibility of expanding or reducing computing resources, the higher the service trustworthiness.	Users should investigate whether the service has the ability to expand or reduce computing resources, and determine the time required.
α_{16}	Measurement of the computing resources. The more accurate the measurement, the higher the service trustworthiness.	For some special metering services, such as SMS verification and message push, users should make their own statistics. Service providers should provide measurement details for their services.

Table 1. Meaning of cloud service trustworthiness assessment indicators.

Frequency Level F	Meaning	Loss Severity Level L	Meaning
5	Ineluctable	5	Catastrophic loss
4	Frequent	4	Very serious loss
3	Occasional	3	Serious loss
2	Rarer	2	Losses to be considered
1	Almost impossible	1	Negligible loss

Table 2. Frequency level and loss severity level.

	$L=1$	$L=2$	$L=3$	$L=4$	$L=5$
$F=5$	5(A_2)	10(A_3)	15(A_4)	20(A_4)	25(A_4)
$F=4$	4(A_2)	8(A_2)	12(A_3)	16(A_4)	20(A_4)
$F=3$	3(A_1)	6(A_2)	9(A_2)	12(A_3)	15(A_4)
$F=2$	2(A_1)	4(A_1)	6(A_2)	8(A_2)	10(A_3)
$F=1$	1(A_1)	2(A_1)	3(A_1)	4(A_2)	5(A_2)

Table 3. Division of the cloud service trusted state regions based on risk matrix.

of cloud service trustworthiness. U contains 16 fuzzy variables, $U = \{a_1, a_2, \ldots, a_{16}\}$, which are respectively the 16 trustworthiness indicators shown in Table 1. $\mu_{A_n}(a_j)$ is the membership of the trusted state fuzzy set of cloud service, which indicates the degree of possibility that a_j belongs to the fuzzy set A_n, and its interval is [0,1] .The greater the value of $\mu_{A_n}(a_j)$, the higher the possibility that indicator a_j belongs to A_n.Substitute $\mu_{A_n}(a_j)$ into the fuzzy entropy calculation formula to calculate, the trusted state fuzzy entropy of β_i can be obtained, as shown in Eq. (1).

$$E_{A_n}(\beta_i) = -k\sum_{j=1}^{m}\left[\mu_{A_n}(a_j)\log_2\mu_{A_n}(a_j) + (1-\mu_{A_n}(a_j))\log_2(1-\mu_{A_n}(a_j))\right] \tag{1}$$

In Eq. (1), m represents the total number of trustworthiness indicators $a_j$included in β_i, k is a constant, $k \geq 0$. In order to normalize the assessment results, this paper sets the value of k as $1/m$. $E_{A_n}(\beta_i)$ is the fuzzy entropy of β_i, which indicates the degree of fuzziness that β_i belongs to A_n, $0 \leq E_{A_n}(\beta_i) \leq 1$.In addition to Eq. (1), according to the definition of fuzzy entropy, fuzzy entropy $E_{A_n}(\beta_i)$ can also be calculated by Eq. (2).

$$E_{A_n}(\beta_i) = -\mu_{A_n}(\beta_i)\log_2\mu_{A_n}(\beta_i) - \bar{\mu}_{A_n}(\beta_i)\log_2\bar{\mu}_{A_n}(\beta_i) \tag{2}$$

In Eq. (2), $\mu_{A_n}(\beta_i)$ represents the probability that β_i belongs to state A_n, and $\bar{\mu}_{A_n}(\beta_i)$ represents the probability that β_i does not belong to state A_n.When $E_{A_n}(\beta_i) = 0$, whether β_i belongs to A_n is clearly defined, indicating that β_i clearly belongs to A_n or does not belong to A_n, that is, $\mu_{A_n}(\beta_i) = 1$ or $\mu_{A_n}(\beta_i) = 0$.On the contrary, the greater the value of $E_{A_n}(\beta_i)$, the greater the fuzzy degree that β_i belongs to A_n, that is, the closer the values of $\mu_{A_n}(\beta_i)$ and $\bar{\mu}_{A_n}(\beta_i)$ are.After calculating the value of $E_{A_n}(\beta_i)$, the fuzzy degree ranking of β_i can be obtained, as shown in the following example.

Suppose that the ranking of $E_{A_n}(\beta_i)$ is $E_{A_2}(\beta_i) > E_{A_1}(\beta_i) > E_{A_3}(\beta_i) > E_{A_4}(\beta_i)$. This ranking indicates that the fuzzy degree that β_i belongs to A_2 is the greatest, that is, the closer the values of $\mu_{A_2}(\beta_i)$ and $\bar{\mu}_{A_2}(\beta_i)$ are. On the contrary, the fuzzy degree that β_i belongs to A_4 is the lowest, which means that the difference between $\mu_{A_4}(\beta_i)$ and $\bar{\mu}_{A_4}(\beta_i)$ is large.

Membership function of cloud service trusted state fuzzy set

According to Eq. (1), to calculate the fuzzy entropy $E_{A_n}(\beta_i)$ of the trusted state of cloud service, it is necessary to calculate $\mu_{A_n}(a_j)$, that is, to construct the membership function of the trusted state fuzzy set.In this regard, according to the division of trusted states in Table 3, combined with the fuzzy entropy theory, this paper constructs the membership function of the cloud service trusted state fuzzy set, as shown in Eq. (3).

$$\mu_{A_n}(a_j) = \frac{Square(a_j) \cap Square(A_n)}{Square(a_j)} \tag{3}$$

In Eq. (3), $Square(A_n)$ represents the geometric area of trusted state A_n, and, $Square(a_j)$ represents the geometric area of a_j. The geometric meaning of Eq. (3) is shown in Fig. 2. As shown in Fig. 2, $Square(a_j)$ is composed of intervals$[F_{min}(a_j), F_{max}(a_j)]$ and $[L_{min}(a_j), L_{max}(a_j)]$ of indicator a_j. Among them, $F_{min}(a_j)$and $F_{max}(a_j)$ respectively refer to the minimum and maximum trustworthiness problems frequency levels of indicator a_j, while $L_{min}(a_j)$ and $L_{max}(a_j)$ respectively refer to the minimum and maximum trustworthiness problems loss severity levels of indicator a_j. Their values can be obtained by experts' assessment according to the definition in Table 2.

- In Fig. 2, $F_{max}(a_j)$ represents the maximum trustworthiness problem occurrence frequency level of a_j, and $F_{min}(a_j)$ represents the minimum trustworthiness problem occurrence frequency level of a_j. $L_{max}(a_j)$ represents the maximum loss severity level of a_j, and $L_{min}(a_j)$ represents the minimum loss severity level of a_j;
- In Fig. 2, the intersection of $Square(a_j)$ and $Square(A_n)$ means the possibility that a_j belongs to A_n, and the value of $\mu_{A_n}(a_j)$ is equal to the intersection of $Square(a_j)$ and $Square(A_n)$ divided by the geometric area of $Square(a_j)$;
- If $Square(a_j) \cap Square(A_n) = 0$, it means that the possibility of a_j belonging to A_n is 0.

As mentioned above, this paper proposes the concepts of maximum level and minimum level. With this method, experts do not need to give an exact value for $F(a_j)$ or $L(a_j)$ during the assessment of indicator a_j at the third layer in Fig. 1.As long as the interval $[F_{min}(a_j), F_{max}(a_j)]$ and $[L_{min}(a_j), L_{max}(a_j)]$ of each indicator are given according to the definition of Table 2, the value of $\mu_{A_n}(a_j)$ can be calculated according to Eq. (3). Next, substitute $\mu_{A_n}(a_j)$ into Eq. (2), $E_{A_n}(\beta_i)$ of each trustworthiness class β_i at the second layer can be calculated.The above method reduces the difficulty of expert assessment, and realizes the bottom-up cloud service trustworthiness assessment.

As shown in Fig. 2, assuming the expert assesses and gives the $[F_{min}(a_j), F_{max}(a_j)]$ and $[L_{min}(a_j), L_{max}(a_j)]$ of indicator a_j as [2,4] and [2,4], respectively. The area composed of $[F_{min}(a_j), F_{max}(a_j)]$ and $[L_{min}(a_j), L_{max}(a_j)]$ is $Square(a_j)$, occupying a total of 9 squares. Through

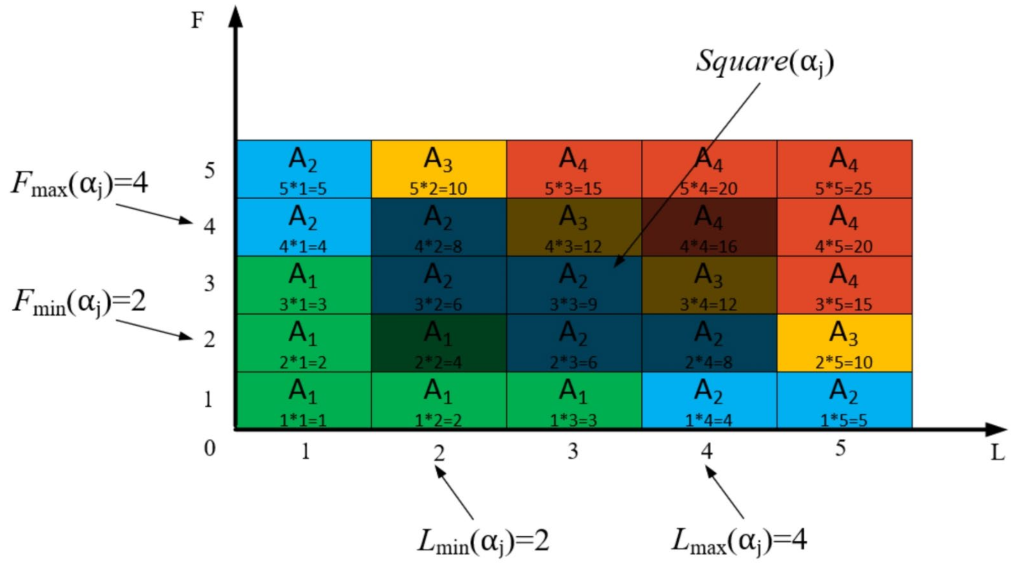


Fig. 2. Geometric meaning of membership function of trusted state fuzzy set.

observation, it can be seen that this trustworthiness indicator may belong to 4 random states: A_1, A_2, A_3, and A_4, where $\mu_{A_1}(a_j) = 1/9$, $\mu_{A_2}(a_j) = 4/9$, $\mu_{A_3}(a_j) = 2/9$, $\mu_{A_4}(a_j) = 1/9$.

Computing method of cloud service trusted state

Although the fuzzy entropy $E_{A_n}(\beta_i)$ can be calculated through the membership function proposed in section "Membership function of cloud service trusted state fuzzy set", $E_{A_n}(\beta_i)$ can only describe the fuzzy degree that β_i belongs to A_n, which is not enough to objectively describe the cloud service trustworthiness and its change in the actual operation process. Therefore, this paper will further study the calculation method of cloud service trusted state based on the proposed fuzzy membership function, so as to realize the assessment of cloud service trustworthiness and its change by combining the trusted state matrix and fuzzy entropy.

It is known that during the use of cloud service, the trustworthiness of β_i will change between different states due to the impact of the indicator a_j it contains. In addition, it is known that $\mu_{A_n}(a_j)$ represents the probability that indicator a_j belongs to trusted state A_n.

$\mu_{A_n}(a_j) > 0$, it indicates that a_j may belong to A_n.Therefore, the trusted state matrix $TM(\beta_i)$ of trustworthiness class β_i can be calculated by comprehensively calculating $\mu_{A_n}(a_j)$ of each indicator a_j, as shown in Eq. (4).

$$\widehat{P}(A_{n\to m}, \beta_i) = \sum_{j=1}^{total} \mu_{A_m}(a_j), \forall \mu_{A_n}(a_j) > 0 \tag{4}$$

In Eq. (4), $\widehat{P}(A_{n\to m}, \beta_i)$ represents the probability that trusted state of β_i transferring from A_n to A_m due to the influence of $\mu_{A_m}(a_j)$, $n = 1,2,3,4$, $m = 1,2,3,4$. $total$ represents the total number of indicators a_j contained in β_i.The calculation of $\mu_{A_n}(a_j)$ and $\mu_{A_m}(a_j)$ are shown in Eq. (3), which represents the possibility of the indicator a_j belonging to trusted state A_n and A_m.

For example, when $n = 1$ and $\mu_{A_1}(a_j) > 0$, take $m = 1, 2, 3$, and 4 respectively, then the values of $\widehat{P}(A_{1\to 1}, \beta_i)$, $\widehat{P}(A_{1\to 2}, \beta_i)$, $\widehat{P}(A_{1\to 3}, \beta_i)$ and $\widehat{P}(A_{1\to 4}, \beta_i)$ can be calculated according to Eq. (4).

Therefore, the following matrix can be obtained according to Eq. (4).

$$\begin{vmatrix} \widehat{P}(A_{1\to 1}, \beta_i) & \widehat{P}(A_{1\to 2}, \beta_i) & \widehat{P}(A_{1\to 3}, \beta_i) & \widehat{P}(A_{1\to 4}, \beta_i) \\ \widehat{P}(A_{2\to 1}, \beta_i) & \widehat{P}(A_{2\to 2}, \beta_i) & \widehat{P}(A_{2\to 3}, \beta_i) & \widehat{P}(A_{2\to 4}, \beta_i) \\ \widehat{P}(A_{3\to 1}, \beta_i) & \widehat{P}(A_{3\to 2}, \beta_i) & \widehat{P}(A_{3\to 3}, \beta_i) & \widehat{P}(A_{3\to 4}, \beta_i) \\ \widehat{P}(A_{4\to 1}, \beta_i) & \widehat{P}(A_{4\to 2}, \beta_i) & \widehat{P}(A_{4\to 3}, \beta_i) & \widehat{P}(A_{4\to 4}, \beta_i) \end{vmatrix}$$

Next, normalize the elements in each row of the above matrix, the trusted state matrix $TM(\beta_i)$of β_i can be obtained, as shown below.

$$TM(\beta_i) = \begin{vmatrix} P(A_{1\to 1}, \beta_i) & P(A_{1\to 2}, \beta_i) & P(A_{1\to 3}, \beta_i) & P(A_{1\to 4}, \beta_i) \\ P(A_{2\to 1}, \beta_i) & P(A_{2\to 2}, \beta_i) & P(A_{2\to 3}, \beta_i) & P(A_{2\to 4}, \beta_i) \\ P(A_{3\to 1}, \beta_i) & P(A_{3\to 2}, \beta_i) & P(A_{3\to 3}, \beta_i) & P(A_{3\to 4}, \beta_i) \\ P(A_{4\to 1}, \beta_i) & P(A_{4\to 2}, \beta_i) & P(A_{4\to 3}, \beta_i) & P(A_{4\to 4}, \beta_i) \end{vmatrix}$$

$TM\left(\beta_i\right)$ represents the trusted state matrix of β_i. The element $P(A_{\mathrm{n}\to\mathrm{m}},\beta_i)$ represents the probability that β_i transferring from state A_n to A_m. The sum of elements in each row $\sum_{m=1}^{4} P\left(A_{n\to m}\right)=1$.After the matrix $TM\left(\beta_i\right)$ is obtained, combined with the fuzzy entropy $E_{A_n}\left(\beta_i\right)$, the trusted state assessment of β_i can be realized.

According to Eq. (2), $E_{A_n}\left(\beta_i\right)$ describes the fuzzy degree that $\beta_i$belongs to A_n. The greater the value of $E_{A_n}\left(\beta_i\right)$, the closer the values of $\mu_{A_n}\left(\beta_i\right)$ and $\bar{\mu}_{A_n}\left(\beta_i\right)$ are, indicating that trusted state A_n is more difficult to control. Therefore, in the assessment process, it is necessary to focus on the two cases that β_i belongs to A_n or does not belong to A_n. In view of these two cases, the trusted state change trend of β_i can be assessed in combination with matrix $TM\left(\beta_i\right)$. As described in the following example.

For example, if the value of a cloud service $E_{A_2}\left(\beta_i\right)$ is the highest, it means that β_i have the highest possibility belonging to A_2 or not. Therefore, in order to further effectively assess β_i's trustworthiness and its change, it is necessary to focus on the two cases of β_i belonging to A_2 or not.

- When β_i belongs to A_2, the trusted state change trend of β_i can be assessed according to the 2nd row elements in matrix $TM\left(\beta_i\right)$;
- When β_i does not belong to A_2, the trusted state change trend of β_i can be assessed according to other row elements in matrix $TM\left(\beta_i\right)$.

In addition, after getting $TM\left(\beta_i\right)$, the trusted state of cloud service can be regarded as a random change process according to the Markov chain[38], and $TM\left(\beta_i\right)$ can be regarded as the random state transition matrix of cloud service. Assume that the probability that β_i belongs to different trusted states at time t is $\mu_{A_1}^t\left(\beta_i\right),\mu_{A_2}^t\left(\beta_i\right),\mu_{A_3}^t\left(\beta_i\right)$ and $\mu_{A_4}^t\left(\beta_i\right)$ respectively, $\sum_{n=1}^{4}\mu_{A_n}^t\left(\beta_i\right)$.According to the prediction method of Markov chain, the change of trusted state β_i at the next time can be predicted, as shown in Eq. (5).

$$\begin{aligned}&\left|\mu_{A_1}^{t+1}\left(\beta_i\right),\mu_{A_2}^{t+1}\left(\beta_i\right),\mu_{A_3}^{t+1}\left(\beta_i\right),\mu_{A_4}^{t+1}\left(\beta_i\right)\right|\\&=\left|\mu_{A_1}^{t}\left(\beta_i\right),\mu_{A_2}^{t}\left(\beta_i\right),\mu_{A_3}^{t}\left(\beta_i\right),\mu_{A_4}^{t}\left(\beta_i\right)\right|\cdot TM\left(\beta_i\right)\end{aligned} \tag{5}$$

According to the Markov chain principle, after a long enough time, that is, after a sufficient number of transfers as shown in Eq. (5), the trusted state of β_i will eventually become stable. Therefore, according to Eq. (5), the trusted state change of β_i can be effectively predicted, and the cloud service trustworthiness can be further assessed by combining fuzzy entropy $E_{A_n}\left(\beta_i\right)$ and matrix $TM\left(\beta_i\right)$.

Assessment process of cloud service trusted state

According to the above analysis, when the trusted state matrix $TM\left(\beta_i\right)$ of cloud service is calculated, combined with fuzzy entropy $E_{A_n}\left(\beta_i\right)$, the trusted state of each trustworthiness class can be assessed. The whole assessment process is shown in Fig. 3.

As shown in Fig. 3, this paper proposes a cloud service trusted state assessment method based on fuzzy entropy and Markov chain. The steps of the whole process are shown below.

Step 1. Assess the indicators of the bottom layer according to the definition shown in Table 2, and calculate the occurrence frequency level interval $\left[F_{min}\left(a_j\right),F_{max}\left(a_j\right)\right]$ and loss severity level interval $\left[L_{min}\left(a_j\right),L_{max}\left(a_j\right)\right]$ of a_j. The calculation time complexity of the steps will increase linearly with the increase of the number of trustworthiness indicators a_j, so its time complexity is $O\left(n\right)$.

Step 2. Substitute $\left[F_{min}\left(a_j\right),F_{max}\left(a_j\right)\right]$ and $\left[L_{min}\left(a_j\right),L_{max}\left(a_j\right)\right]$ into Eq. (3), and calculate the membership degree $\mu_{A_n}\left(a_j\right)$. The calculation time complexity is $O\left(1\right)$.

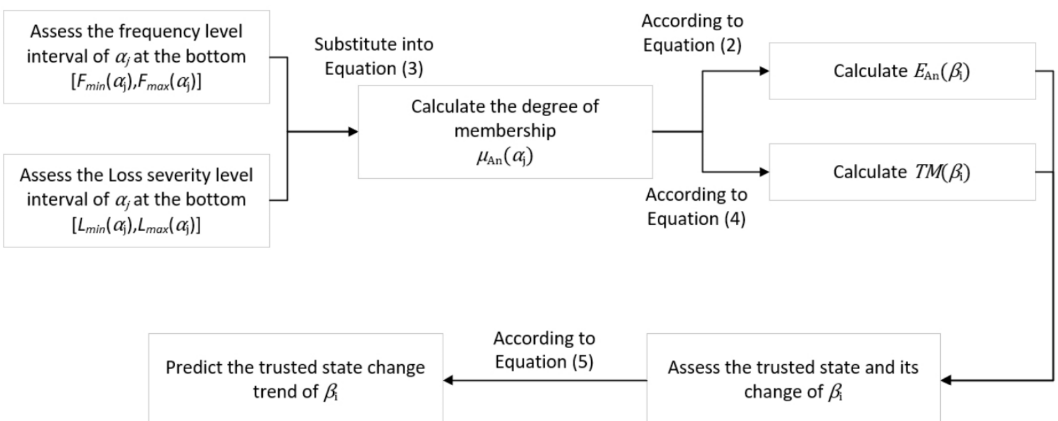


Fig. 3. Assessment process of cloud service trusted state.

Step 3. Substitute $\mu_{A_n}(a_j)$ into Eq. (2) for calculation to obtain $E_{A_n}(\beta_i)$. The calculation time complexity of the steps also will increase linearly with the increase of the number of indicators, so its time complexity is $O(n)$.

Step 4. Substitute $\mu_{A_n}(a_j)$ into Eq. (4) for calculation to obtain $TM(\beta_i)$. In Eq. (4), $\widehat{P}(A_{n\to m},\beta_i)$ represents the sum of probabilities that trusted state of β_i transferring from A_n to A_m. As mentioned in the previous Sections, this paper proposes a total of 16 trustworthiness assessment indicators and 4 trusted states. According to Eq. (4), to calculate $TM(\beta_i)$, it is necessary to comprehensively consider the impact of these 16 trusted indicators on the mutual transition of each trusted state. When there are n states, this step requires $n \bullet n$ calculations, so the computational time complexity of this step is $O\left(n^2\right)$.

Step 5. Assess the trusted state of β_i and its change in combination with $E_{A_n}(\beta_i)$ and $TM(\beta_i)$.

Step 6. According to Eq. (5), predict the trusted state change trend of each trustworthiness class β_i. The calculation time complexity of this step will not be affected by changes in the number of trustworthiness indicators a_j, its calculation time complexity is $O(1)$.

In the whole process, only the bottom indicators need to be assessed, and then the trusted state of β_i and its change can be assessed step by step. The input and output of this method are shown below.

- **Input Data**: $[F_{min}(a_j), F_{max}(a_j)]$ and $[L_{min}(a_j), L_{max}(a_j)]$。
- **Intermediate output Data**: $TM(\beta_i), E_{A_n}(\beta_i)$
- **Output Data**: $\{\mu^t_{A_1}(\beta_i), \mu^t_{A_2}(\beta_i), \mu^t_{A_3}(\beta_i), \mu^t_{A_4}(\beta_i)\}$

As mentioned above, this paper defines 4 random trusted states of cloud services based on fuzzy entropy, constructs membership functions $\mu_{A_n}(a_j)$for each trustworthiness indicator a_j belonging to different trusted states A_n, quantitatively describes the impact of each trustworthiness indicator a_j on the changes in the cloud service trusted state A_n. Throughout the assessment process, experts only need to provide $[F_{min}(a_j), F_{max}(a_j)]$ and$[L_{min}(a_j), L_{max}(a_j)]$ for each trustworthiness indicator to calculate the trusted state transition matrix $TM(\beta_i)$and fuzzy entropy of cloud services $E_{A_n}(\beta_i)$, and achieve effective assessment of cloud service trustworthiness and its changes, that is, $\{\mu^t_{A_1}(\beta_i), \mu^t_{A_2}(\beta_i), \mu^t_{A_3}(\beta_i), \mu^t_{A_4}(\beta_i)\}$.

Case analysis and method comparison

Next, in order to verify the feasibility of the proposed method, this paper will put the proposed method into a specific case for analysis.

Case analysis

This paper selects an ECS (Elastic Compute Service) provided by a well-known platform with 2G memory, 4 CPU cores and 2 M network bandwidth. The service provider has been in stable operation for more than 10 years. This paper has investigated the service based on the proposed trustworthiness indicators, and sorted out the indicator information of the service, as shown in Table 4.

According to the steps shown in Fig. 3, this paper first convened 5 experts to assess the trusted indicators a_j of the service, and obtained the data shown in Table 5.

Next, substitute the data in Table 5 into Eq. (3) to obtain the membership $\mu_{A_n}(a_j)$ of each indicator a_j, as shown in Table 6.

Next, substitute the data of Table 6 into Eq. (2) and Eq. (4), $E_{A_n}(\beta_i)$ and $TM(\beta_i)$ can be obtained. The results are shown below.

Indicators	Reference information
Service Agreement termination clauses and exemption clauses.	The service provider has listed clear compensation clauses, service termination clauses and exemption clauses.
User constraints	More user scenarios are restricted, and user permissions are low.
Persistence of data storage	Data storage persistence is up to 99.99%, and data will not be lost.
Data portability	Data portability depends on the user's own application and cannot be completely migrated.
Data privacy	The service provider does not provide data encryption support, and the data is encrypted by the user himself
Right to know data	The user is not clear about the location and use of data storage.
Data auditability	When it is necessary to review, users can obtain comprehensive operation logs and operation records.
Data destructibility	Server data can be destroyed, but user data cannot be completely destroyed.
Network access performance	The service provider platform only provides basic network defense strategies for the server, and does not provide special DDOS and CC defense support.
Fault recovery capability	If a failure occurs, the service cannot be recovered immediately, and it will take several hours to recover.
Business function	Service providers can provide a large number of services and meet most of users' business needs.
Business availability	The server can operate normally for a long time, with occasional service failure.
Resource allocation capability	Users can quickly expand or reduce computing resources as required.
Measurement accuracy	The measurement of this service is accurate and almost error free.

Table 4. Cloud service case.

		$F_{min}(a_j)$	$F_{max}(a_j)$	$L_{min}(a_j)$	$L_{max}(a_j)$
β_1	α_1	1	2	4	5
	α_2	1	2	3	4
	α_3	2	3	2	4
	α_4	3	4	2	3
β_2	α_5	1	1	4	5
	α_6	2	3	3	4
	α_7	3	5	3	5
	α_8	1	3	1	3
	α_9	1	3	1	3
	α_{10}	3	5	3	4
β_3	α_{11}	4	5	1	3
	α_{12}	2	3	2	5
	α_{13}	2	3	3	4
	α_{14}	2	3	2	4
	α_{15}	1	2	1	3
	α_{16}	1	2	1	3

Table 5. Frequency level and loss severity level of each indicator.

	$\mu_{A_1}(a_j)$	$\mu_{A_2}(a_j)$	$\mu_{A_3}(a_j)$	$\mu_{A_4}(a_j)$		$\mu_{A_1}(a_j)$	$\mu_{A_2}(a_j)$	$\mu_{A_3}(a_j)$	$\mu_{A_4}(a_j)$
α_1	0.000	0.750	0.250	0.000	α_9	0.667	0.333	0.000	0.000
α_2	0.250	0.750	0.000	0.000	α_{10}	0.000	0.167	0.333	0.500
α_3	0.167	0.667	0.167	0.000	α_{11}	0.000	0.500	0.333	0.167
α_4	0.000	0.750	0.250	0.000	α_{12}	0.125	0.500	0.250	0.125
α_5	0.000	1.000	0.000	0.000	α_{13}	0.000	0.750	0.250	0.000
α_6	0.000	0.750	0.250	0.000	α_{14}	0.167	0.667	0.167	0.000
α_7	0.000	0.111	0.222	0.667	α_{15}	0.833	0.167	0.000	0.000
α_8	0.667	0.333	0.000	0.000	α_{16}	0.833	0.167	0.000	0.000

Table 6. The membership degree $\mu_{A_n}(a_j)$ of each indicator.

$$E_{A_1}(\beta_1) = 0.365, E_{A_2}(\beta_1) = 0.838, E_{A_3}(\beta_1) = 0.568, E_{A_4}(\beta_1) = 0.000$$
$$E_{A_1}(\beta_2) = 0.306, E_{A_2}(\beta_2) = 0.634, E_{A_3}(\beta_2) = 0.416, E_{A_4}(\beta_2) = 0.320$$
$$E_{A_1}(\beta_3) = 0.416, E_{A_2}(\beta_3) = 0.838, E_{A_3}(\beta_3) = 0.532, E_{A_4}(\beta_3) = 0.199$$

$$TM(\beta_1) = \left| \begin{array}{cccc} 0.208 & 0.708 & 0.083 & 0.000 \\ 0.104 & 0.729 & 0.167 & 0.000 \\ 0.056 & 0.722 & 0.222 & 0.000 \\ 0.000 & 0.000 & 0.000 & 0.000 \end{array} \right|$$

$$TM(\beta_2) = \left| \begin{array}{cccc} 0.667 & 0.333 & 0.000 & 0.000 \\ 0.222 & 0.449 & 0.134 & 0.194 \\ 0.000 & 0.343 & 0.269 & 0.389 \\ 0.000 & 0.139 & 0.278 & 0.583 \end{array} \right|$$

$$TM(\beta_3) = \left| \begin{array}{cccc} 0.490 & 0.375 & 0.104 & 0.031 \\ 0.326 & 0.458 & 0.167 & 0.049 \\ 0.073 & 0.604 & 0.250 & 0.073 \\ 0.063 & 0.500 & 0.292 & 0.146 \end{array} \right|$$

After calculating $E_{A_n}(\beta_i)$ and $TM(\beta_i)$, the trusted state of each trustworthiness class will be assessed, as shown below.

Assessment of trustworthiness class β_1

According to the ranking of fuzzy entropy $E_{A_n}(\beta_1)$, the value of $E_{A_2}(\beta_1)$ is the largest, which indicates that β_1 has the largest fuzzy degree in state A_2. Therefore, to analyze the trusted state of β_1, it needs to focus on the trusted state changes when β_1 belongs to A_2 or not.

- In the first case, when β_1 belongs to A_2, it can be seen from the 2nd row of the matrix $TM(\beta_1)$ that the probability of β_1 still keeping state A_2 unchanged is the maximum;

- In the second case, when β_1 is in other states, the probability of its transition from other states to A_2 is also maximum.

The above results show that in the long-term use of the service, whether β_1 belongs to A_2 or not, it will always transfer to A_2.

In addition, $TM\left(\beta_1\right)$ shows that β_1 only transfers between A_1, A_2 and A_3.In order to further predict and describe the trusted state change trend of β_1,this paper assumes that β_1 belongs to A_1, A_2 and A_3 with equal probability, that is, $\mu_{A_1}\left(\beta_1\right) = \mu_{A_2}\left(\beta_1\right) = \mu_{A_3}\left(\beta_1\right) = 0.333$.Next, substitute the above values into Eq. (5),the trusted state change trend of β_1 can be predicted, as shown in Fig. 4.

Figure 4 reflects the trusted state change trend of β_1. It can be seen from Fig. 4 that the value of $\mu_{A_2}\left(\beta_1\right)$ will gradually increase, and the values of $\mu_{A_1}\left(\beta_1\right)$ and $\mu_{A_2}\left(\beta_1\right)$ will gradually decrease. This change indicates that the trusted state of β_1 will gradually lean towards A_2 over time, namely it will gradually change to a safer state over time.

Assessment of trustworthiness class $$ {\varvec{\beta }}_{2}$$

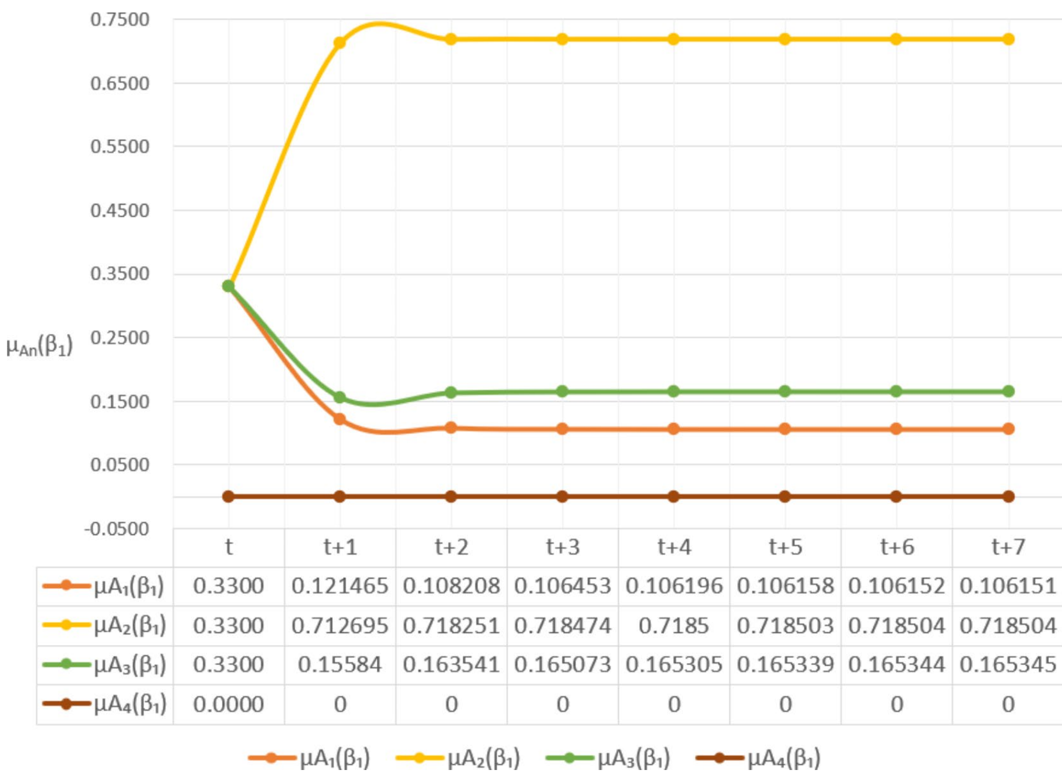
According to the ranking of fuzzy entropy $E_{A_n}\left(\beta_2\right)$, the value of $E_{A_2}\left(\beta_2\right)$ is the largest, which indicates that β_2 has the largest fuzzy degree in state A_2. Therefore, to analyze the trusted state of β_2, it also needs to focus on the trusted state changes when β_2 belongs to A_2 or not.

- In the first case, when β_2 belongs to A_2, it can be seen from the 2nd row of the matrix $TM\left(\beta_2\right)$ that the probability of β_2 still keeping state A_2 unchanged is the maximum;
- In other cases, when β_2 belongs to A_1, it will only transfer between A_1 and A_2. When β_2 belongs to A_3 or A_4, it will have a greater probability to transfer to state A_4.

The above results show that β_2 will have a certain probability to transfer to the more dangerous state A_3 or A_4 during the long-term use. In addition, it can be seen from the 4th row of matrix $TM\left(\beta_2\right)$, once β_2 have transferred to state A_4, it will be difficult to return to a safer state.

Next, in order to further predict and describe the trusted state change trend of β_2, this paper assumes that β_2 belongs to different trusted states with equal probability, $\mu_{A_1}\left(\beta_2\right) = \mu_{A_2}\left(\beta_2\right) = \mu_{A_3}\left(\beta_2\right) = \mu_{A_4}\left(\beta_2\right) = 0.25$ .Then, substitute the above values into Eq. (5),the trusted state change trend of β_2 can be predicted, as shown in Fig. 5.

Figure 5 reflects the trusted state change trend of β_2. It can be seen from Fig. 5 that the values of $\mu_{A_2}\left(\beta_2\right)$ and $\mu_{A_4}\left(\beta_2\right)$ will gradually increase, and finally $\mu_{A_2}\left(\beta_2\right) > \mu_{A_4}\left(\beta_2\right) > \mu_{A_3}\left(\beta_2\right) > \mu_{A_1}\left(\beta_2\right)$. The change indicates that the trusted state of β_2 is likely to transfer towards A_2 the trusted state of β_2 will also shift towards A_4, indicating that β_2 has a greater potential trustworthiness risk in the long-term use process.



	t	t+1	t+2	t+3	t+4	t+5	t+6	t+7
$\mu A_1(\beta_1)$	0.3300	0.121465	0.108208	0.106453	0.106196	0.106158	0.106152	0.106151
$\mu A_2(\beta_1)$	0.3300	0.712695	0.718251	0.718474	0.7185	0.718503	0.718504	0.718504
$\mu A_3(\beta_1)$	0.3300	0.15584	0.163541	0.165073	0.165305	0.165339	0.165344	0.165345
$\mu A_4(\beta_1)$	0.0000	0	0	0	0	0	0	0

Fig. 4. Assessment of trustworthiness class β_1

Assessment of trustworthiness class $$ {\varvec{\beta }}_{3}$$

According to the ranking of fuzzy entropy $E_{A_n}(\beta_3)$, the value of $E_{A_2}(\beta_3)$ is the largest, which indicates that β_3 has the largest fuzzy degree in state A_2. Therefore, to analyze the trusted state of β_3, it also needs to focus on the trusted state changes when β_3 belongs to A_2 or not.

- In the first case, when β_3 belongs to A_2, it will have a greater probability to transfer to A_1 state or still keeping state A_2 unchanged;
- In other cases, when β_3 does not belong to A_2, it will transfer towards state A_2 in the long-term use process.

Next, in order to effectively predict and describe the trusted state change trend of β_3, this paper assumes that β_3 belongs to different trusted states with equal probability, $\mu_{A_1}(\beta_3) = \mu_{A_2}(\beta_3) = \mu_{A_3}(\beta_3) = \mu_{A_4}(\beta_3) = 0.25$ .Then, substitute the above values into Eq. (5),the trusted state change trend of β_3 can be predicted, as shown in Fig. 6.

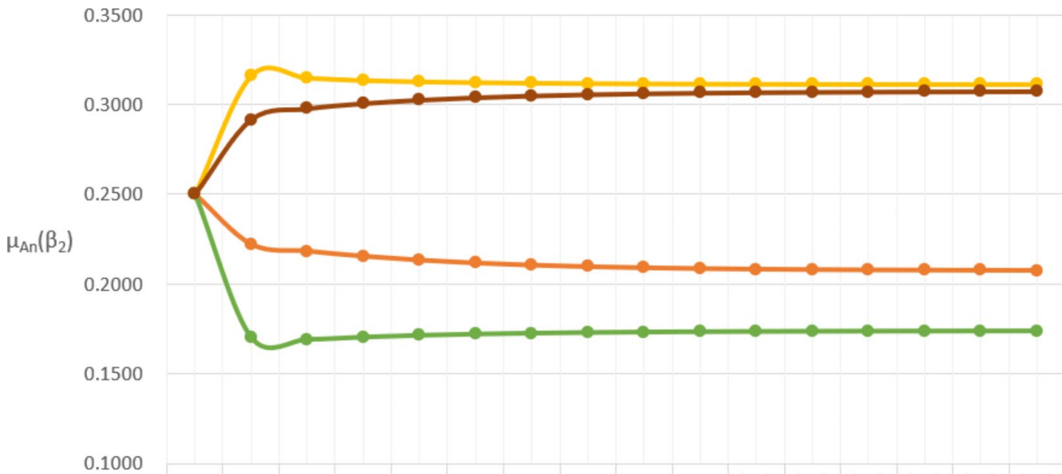
Figure 6 reflects the trusted state change trend of β_3. It can be seen from Fig. 6 that the values of $\mu_{A_1}(\beta_3)$ and $\mu_{A_2}(\beta_3)$ will gradually increase, and finally $\mu_{A_2}(\beta_3) > \mu_{A_1}(\beta_3) > \mu_{A_3}(\beta_3) > \mu_{A_4}(\beta_3)$. This change shows that the trustworthiness of β_3 shows a good change trend, and will gradually transfer towards A_1 or A_2 in the long-term use process.

Summary of assessment results

The results of sections "*Assessment of trustworthiness class β_1*" and "*Assessment of trustworthiness class β_3*" indicate that the trusted states of β_1 and β_3 show a good trend of change. Over time, β_1 and β_3 will transfer towards a more credible state.

The results of section "*Assessment of trustworthiness class β_2*" shows that β_2 of the service has a greater trustworthiness risk. As time goes on, β_2 will have a high probability of having a trusted problem, and once a trusted problem occurs, the service will be difficult to return to normal. In Fig. 7, the Membership degree $\mu_{A_i}(a_j)$ represents the possibility that indicator a_j belongs to the trusted state A_i. The higher the value of $\mu_{A_i}(a_j)$, the higher the likelihood that the trusted state of a_j belongs to A_i. If the probability of the indicator belonging to A_3 andA_4 is higher, it indicates that the indicator may cause the trustworthiness of cloud services to change towards an unfavorable state, resulting in trustworthiness problem.

It can be seen from Fig. 7 that a_7 and a_{10} are likely to transfer to A_3 or A_4, indicating that these two indicators are the key factors affecting the trusted state of β_2. When users select and use this cloud service, they need to focus on the control of a_7 and a_{10}. On the one hand, users need to strengthen the detection of their own application vulnerabilities and require service providers to provide encryption transmission mechanisms; On the other hand, the user needs to agree with the service provider in advance which data must be deleted and the time limit for data deletion, so as to avoid the problem of trustworthiness.



	t	t+1	t+2	t+3	t+4	t+5	t+6	t+7	t+8	t+9	t+10	t+11	t+12	t+13	t+14	t+15
$\mu A_1(\beta_2)$	0.25	0.22	0.21	0.21	0.21	0.21	0.21	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20
$\mu A_2(\beta_2)$	0.25	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31	0.31
$\mu A_3(\beta_2)$	0.25	0.17	0.16	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17
$\mu A_4(\beta_2)$	0.25	0.29	0.29	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30

$\mu A_1(\beta_2)$ $\mu A_2(\beta_2)$ $\mu A_3(\beta_2)$ $\mu A_4(\beta_2)$

Fig. 5. Assessment of trustworthiness class β_2.

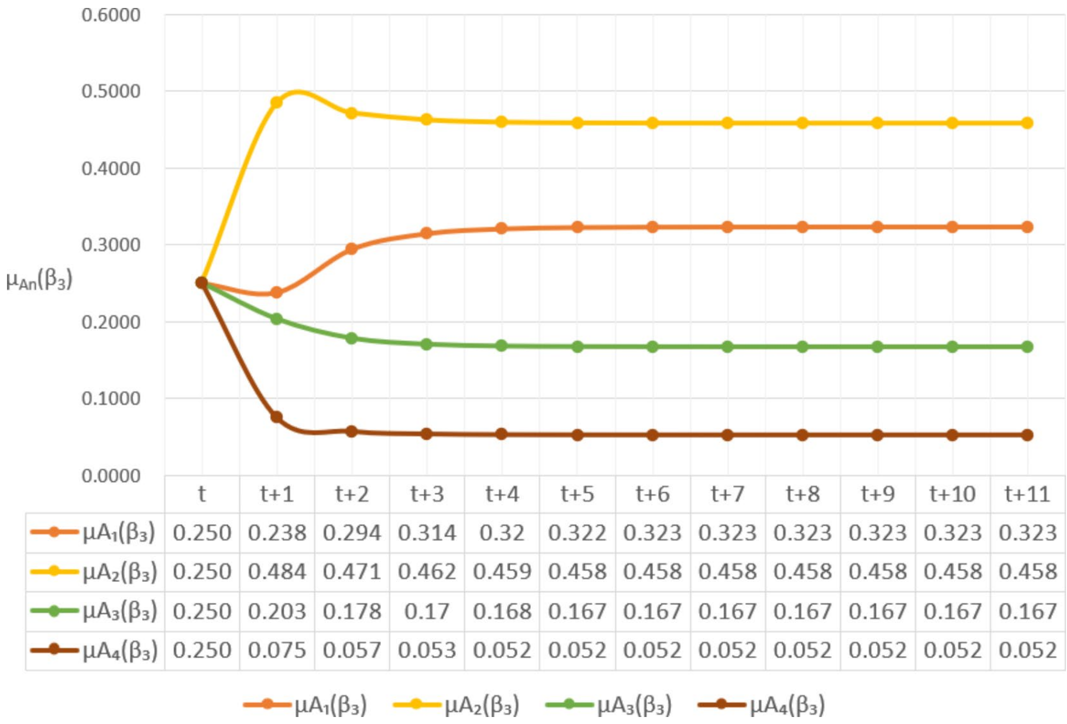


Fig. 6. Assessment of trustworthiness class β_3.

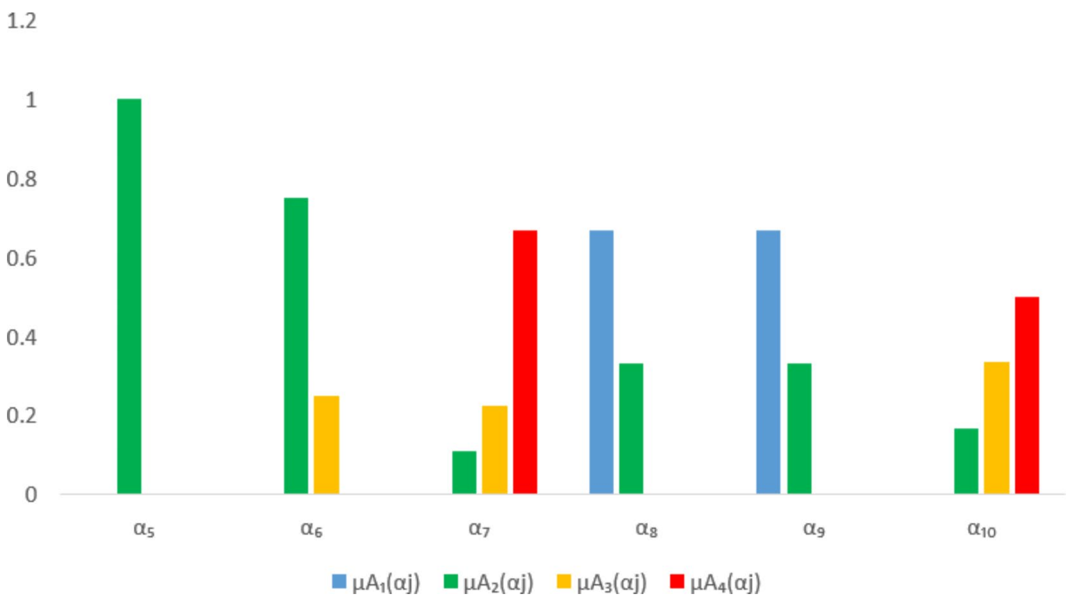


Fig. 7. The membership degree of each indicator a_j included in β_2.

Method comparison

The above case analysis shows the method proposed in this paper is feasible. Next, this paper will compare the proposed method with other mature methods to illustrate the characteristics of this method. These methods are assessment methods based on information entropy[21–23], assessment methods based on AHP[15,16,44], assessment methods based on risk matrix[37,38] and assessment methods based on D-S evidence theory[26–28]. These methods are relatively mature assessment methods, which suitable for assessing uncertain systems with multiple objectives.

This paper will continue to use the cloud services shown in Table 4 as a reference, and discuss the characteristics of different methods from five aspects: objectivity, comprehensiveness, cost, scalability, and decision support. Through the comparison with these methods, it will be able to reflect the characteristics of the method proposed in this paper.

Method	reflect the random trusted environment	reduce the influence of human subjective factors	solve the problem of opinion conflict
Information entropy	*No*	*Yes*	*Yes*
AHP	*No*	*Yes*	*No*
Risk matrix	*No*	*No*	*No*
D-S evidence theory	*No*	*Yes*	*Yes*
The method of this paper	*Yes*	*Yes*	*Yes*

Table 7. Objective comparison of each method.

Method	Can assess the trustworthiness of indicator a_j	Can assess the trustworthiness of class β_i	Can assess the trustworthiness of the entire cloud service	Can assess the change of service trusted state
Information entropy	*Yes*	*Yes*	*Yes*	*No*
AHP	*Yes*	*Yes*	*Yes*	*No*
Risk matrix	*Yes*	*Yes*	*No*	*No*
D-S evidence theory	*Yes*	*Yes*	*Yes*	*No*
The method of this paper	*Yes*	*Yes*	*Yes*	*Yes*

Table 8. Comprehensiveness comparison of each method.

- **Objectivity.** It refers to whether the assessment results can objectively reflect the cloud service trustworthiness. The higher the objectivity, the closer the assessment results are to the real trustworthiness environment.
- **Comprehensiveness.** It refers to the comprehensiveness of the assessment results. The more assessment results the method can provide, the more comprehensive the method is.
- **Cost.** It refers to the input of assessment, including the difficulty of expert assessment, number of tasks, difficulty in data acquisition, etc.
- **Scalability.** It refers to the performance of the method when dealing with new assessment requirements. The higher the scalability, the less adjustment the method needs to make in the face of new assessment requirements.
- **Decision support.** It refers to the support of assessment results to decision-making. The greater the reference value of the assessment results, the greater the decision support.

Objectivity comparison
It is known that the objectivity of assessment results will be affected by subjective factors and expert opinions, and it needs to be able to effectively reflect the random trusted environment of cloud services. Therefore, in order to visually compare the objectivity of various methods, this paper compares them around the following three aspects. As shown in Table 7.

Comprehensiveness comparison
Around the trustworthiness attribute model shown in Fig. 1, this paper compares the comprehensiveness of each method based on the assessment of the following four contents. As shown in Table 8.

Cost comparison
As shown in Tables 9 and 10, in order to visually compare the cost of each method, this paper compares the content that needs to be processed and their average time complexity when using different methods for assessment.

Scalability comparison
Take the service assessed in this paper as a reference. When new indicators a_j are introduced, the scalability of each method is compared as follows. The more content that needs to be recalculated when new assessment indicators are introduced, the lower the scalability of the method. As shown in Table 11.

Decision support comparison
In order to effectively compare the decision support of each method, this paper continues to use the cloud service described in section "Case analysis" as a reference, and compares the content that each method can provide for decision support, as shown in Table 12.

In summary, according to the comparison results in Tables 7, 8, 9, 10, 11 and 12, $\{high = 3, medium = 2, low = 1\}$t is used to compare and describe the characteristics of the above methods. The final comparison result is shown in Fig. 8.

Figure 8 shows that the method proposed in this paper has high objectivity, comprehensiveness and decision support, but its cost is high and its scalability is medium.

Method	Need assess the occurrence frequency level and loss severity level of each indicator a_j	Need assess the occurrence frequency level and loss severity level of each class β_i	Need calculate the membership $\mu_{A_n}(a_j)$ of each indicator a_j	Need calculate the fuzzy entropy $E_{A_n}(\beta_i)$ and trusted state matrix $TM(\beta_i)$	Need calculate the service uncertainty	Need calculate the weight judgment matrix of each indicator a_j	Need calculate the weight judgment matrix of each class β_i	Need check the consistency of the assessment results	Need fuse the assessment results of multiple experts
Information entropy	*Yes*	*No*	*No*	*No*	*Yes*	*No*	*No*	*No*	*No*
AHP	*No*	*No*	*No*	*No*	*No*	*Yes*	*Yes*	*Yes*	*No*
Risk matrix	*Yes*	*Yes*	*No*	*No*	*No*	*No*	*No*	*No*	*No*
D-S evidence theory	*Yes*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*Yes*
The method of this paper	*Yes*	*No*	*Yes*	*Yes*	*No*	*No*	*No*	*No*	*No*

Table 9. Cost comparison of each method.

Method	Assess the occurrence frequency level and loss severity level of each indicator a_j	Assess the occurrence frequency level and loss severity level of each class β_i	Calculate the membership $\mu_{A_n}(a_j)$ of each indicator a_j	Calculate the fuzzy entropy $E_{A_n}(\beta_i)$ and trusted state matrix $TM(\beta_i)$	Calculate the service uncertainty	Calculate the weight judgment matrix of each indicator a_j	Calculate the weight judgment matrix of each class β_i	Check the consistency of the assessment results	Fuse the assessment results of multiple experts
Information entropy	$O(n)$	-	-	-	$O(n)$	-	-	-	-
AHP	-	-	-	-	-	$O(n^2)$	$O(n^2)$	$O(n)$	-
Risk matrix	$O(1)$	$O(1)$	-	-	-	-	-	-	-
D-S evidence theory	$O(n)$	-	-	-	-	-	-	-	$O(n)$
The method of this paper	$O(n)$	-	$O(n)$	$O(n^2)$	-	-	-	-	-

Table 10. Comparison of the average time complexity of each calculation step in the assessment process of each method.

Method	Content that needs to be recalculated
Information entropy	①The entropy values of new indicators a_j ②The entropy values of different classes β_i ③The service uncertainty
AHP	①The weight judgment matrix of each indicator a_j ②The weight judgment matrix of each class β_i ③The consistency of the assessment results
Risk matrix	①The occurrence frequency level and loss severity level of new indicators a_j ②The occurrence frequency level and loss severity level of each class β_i
D-S evidence theory	①The occurrence frequency level and loss severity level of new indicators a_j ②Refuse the assessment results of multiple experts
The method of this paper	①The occurrence frequency level and loss severity level of new indicators a_j ②The membership $\mu_{A_n}(a_j)$ of the new indicators a_j ③The fuzzy entropy $E_{A_n}(\beta_i)$ and trusted state matrix $TM(\beta_i)$

Table 11. Scalability comparison of each method.

Conclusion

This paper establishes a trusted attribute hierarchy model of cloud service based on YDB144-2014 standard. Based on this model, this paper defines the trustworthiness level of cloud service, proposes an effective trusted state representation method, constructs a membership function of the cloud service trusted state based on fuzzy entropy, finally proposes an effective trusted state assessment method of cloud service by combining fuzzy entropy and Markov chain. This paper provides a reference model for the trustworthiness assessment of cloud service, reduces the assessment difficulty of expert by combining the fuzzy entropy theory, and uses the

Method	Content that can be provided for decision-making
Information entropy	①The uncertainty of different indicators a_j ②The uncertainty of different classes β_{i}
AHP	①The trustworthiness impact weights of different indicators a_j ②The trustworthiness impact weights of different classes β_{i} ③Check the consistency of the assessment results
Risk matrix	①The trustworthiness level of different indicators a_j with strong subjectivity ②The trustworthiness level of different classes β_{i} with strong subjectivity
D-S evidence theory	①The trustworthiness level of different indicators a_j with certain objectivity ②The trustworthiness level of different classes β_{i} with certain objectivity
Methods of this paper	①The trustworthiness level of different indicators a_j ②The fuzzy degree of different trustworthiness classes β_{i} ③The cloud service trusted state change trend

Table 12. Decision support comparison of each method.

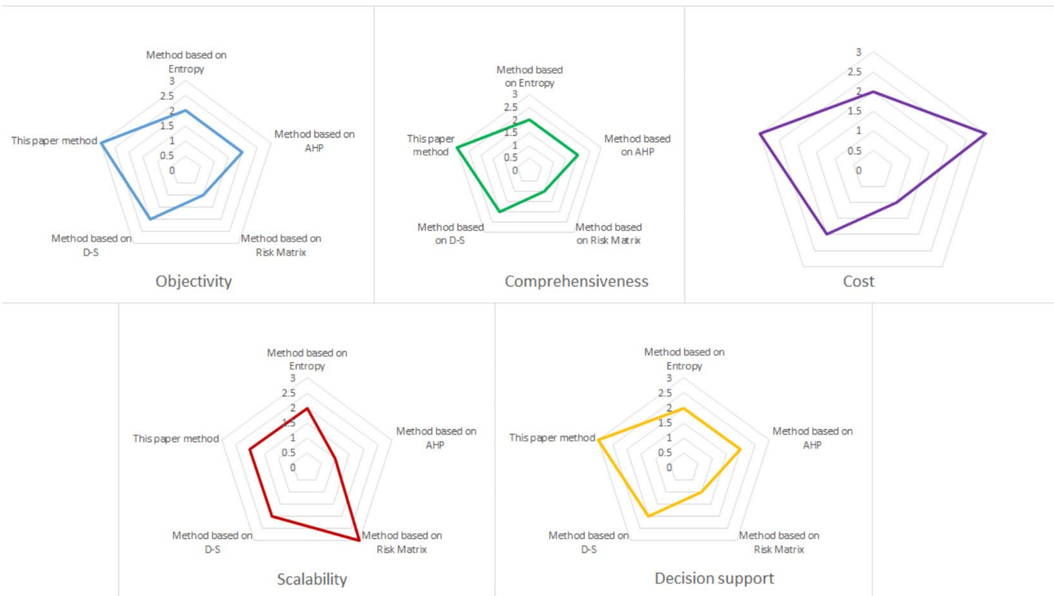


Fig. 8. Characteristics comparison of each method.

"trusted state" to describe the cloud service trustworthiness and its change in combination with Markov chain. It makes up for the shortcomings of assessment method which only using a single fuzzy entropy in the assessment process, and realizes the assessment of cloud service trustworthiness and its change.

This method combines fuzzy entropy and Markov chain, provides a new method for cloud service trustworthiness assessment, and is of great significance to the research of cloud service trustworthiness assessment. In the subsequent research, with the development of trustworthiness research, when the number of trustworthiness indicators of cloud service increases, the scalability of this method needs to be further improved.

Data availability

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

Received: 23 March 2024; Accepted: 27 November 2024
Published online: 03 December 2024

References

1. Geppert, T. et al. Trusted execution environments: Applications and organizational challenges. *Frontiers in Computer Science* **4**, 930741 (2022).
2. Group, T. C. *Trusted computing platform alliance (TCPA) main specification version 1.1b* (2001). http://www.trustedcomputinggroup.org.
3. ISO/IEC. *15408-1:2005 Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model* (2005).
4. Association, C. C. S. Cloud service agreement reference framework. In *China Communications Standardization Association: China*, Vol. YDB144-2014 (2014).
5. Guo-Hua, S. et al. Survey on software trustworthiness evaluation: Standards, models and tools. *Journal of Software* **27**(4), 955–968 (2016).

6. Yue, C. A software trustworthiness evaluation methodology for cloud services with picture fuzzy information. *Applied Soft Computing* **152**, 111205 (2024).
7. Tang, C. et al. A two-dimensional time-aware cloud service recommendation approach with enhanced similarity and trust. *Journal of Parallel and Distributed Computing* **190**, 104889 (2024).
8. Tofighy, S., Rahmanian, A. A. & Ghobaei-Arani, M. An ensemble CPU load prediction algorithm using a Bayesian information criterion and smooth filters in a cloud computing environment. *Software: Practice and Experience* **48**(12), 2257–2277 (2018).
9. Salimian, M., Ghobaei-Arani, M. & Shahidinejad, A. Toward an autonomic approach for Internet of Things service placement using gray wolf optimization in the fog computing environment. *Software Practice and Experience* **51**(8), 1745–1772 (2021).
10. Shahidinejad, A., Farahbakhsh, F., Ghobaei-Arani, M., Malik, M. H. & Anwar, T. Context-aware multi-user offloading in mobile edge computing: A federated learning-based approach. *Journal of Grid Computing* **19**(2), 18 (2021).
11. Ghobaei-Arani, M. & Souri, A. LP-WSC: A linear programming approach for web service composition in geographically distributed cloud environments. *The Journal of Supercomputing* **75**(5), 2603–2628 (2019).
12. Alam, K. A., Ahmed, R., Butt, F. S., Kim, S. G. & Ko, K. M. An uncertainty-aware integrated fuzzy AHP-WASPAS model to evaluate public cloud computing services. *Procedia Computer Science* **130**, 504–509 (2018).
13. Li, C., Wang, S., Kang, L., Guo, L. & Cao, Y. Trust evaluation model of cloud manufacturing service platform. *International Journal of Advanced Manufacturing Technology* **75**(1–4), 489–501 (2014).
14. Ping, L., Yuan, L., Hu, J., Yan, J. & Jian, F. A comprehensive assessment approach to evaluate the trustworthiness of manufacturing services in cloud manufacturing environment. *IEEE Access* **6**, 30819–30828 (2018).
15. Fattahi, R. & Khalilzadeh, M. Risk evaluation using a novel hybrid method based on FMEA, extended MULTIMOORA, and AHP methods under fuzzy environment. *Safety Science* **102**, 290–300 (2018).
16. Fagundes, M., Keler, T. C., Teles, E. O., Melo, S. & Freires, F. Multicriteria decision-making system for supplier selection considering risk: A computational Fuzzy AHP-based approach. *IEEE Latin America Transactions* **19**(9), 1564–1572 (2021).
17. Li, Z. & Jie, R. Cloud service trust evaluation algorithm optimization based on multi-level structure model. *Journal of Nanjing University of Science and Technology* **44**(1), 55–60 (2020).
18. Zeqian, C., Xiaotong, S., Najing, Z. & Shuo, Y. Construction and application of evaluation index for public cultural cloud service. *Library, Document & Communication* **2020**(6), 54–66 (2020).
19. Tilei, T. & Ming, R. Research on a trustworthiness measurement method of cloud service construction processes based on information entropy. *Entropy* **21**(5), 462 (2019).
20. Gao, T., Li, T., Jiang, R., Yang, M. & Zhu, R. Research on cloud service security measurement based on information entropy. *International Journal of Network Security* **21**(6), 1003–1013 (2019).
21. Guesmi, H., Kalghoum, A., Ghazel, C. & Saidane, L. A. FFED: A novel strategy based on fast entropy to detect attacks against trust computing in cloud. *Cluster Computing* **66**, 1–10 (2021).
22. Sharma, A., Munjal, P. & Banati, H. Entropy-based classification of trust factors for cloud computing. *International Journal of Grid and Utility Computing* **11**(6), 747–754 (2020).
23. Nie, S. A novel trust model of dynamic optimization based on entropy method in wireless sensor networks. *Cluster Computing* **22**(5), 11153–11162 (2019).
24. Wei, L., Lu-Kun, Z., Yuan-Jie, B. A., Guang-Li, L. I. & Zhi-Gang, Z. A relevance aware cloud service trust model based on convex evidence theory. *Computer Engineering & Science* **41**(001), 47–55 (2019).
25. Zuan-shi, L. & Xiu-li, G. Trusted cloud service evaluation method research based on D–S theory. *Computer Engineering and Applications* **53**(17), 70–76 (2017).
26. DX, W. & Q, W. Trustworthiness evidence supporting evaluation of software process trustworthiness. Journal of Software **29**(11), 178–200 (2018).
27. Yang, M., Gao, T., Xie, W., Jia, L. & Zhang, T. The assessment of cloud service trustworthiness state based on DS theory and Markov chain. *IEEE Access* **10**, 68618–68632 (2022).
28. Xu, W., Yang, W. & Yao, Y. Multi-dimensional trust evaluation method based on D–S evidence theory. *Computer and Digital Engineering* **47**(2), 7 (2019).
29. Ratnayake, R. & Antosz, K. Development of a risk matrix and extending the risk-based maintenance analysis with fuzzy logic. *Procedia Engineering* **182**, 602–610 (2017).
30. Albery, S., Borys, D. & Tepe, S. Advantages for risk assessment: Evaluating learnings from question sets inspired by the FRAM and the risk matrix in a manufacturing environment. *Safety science* **89**, 180–189 (2016).
31. Shang, W. & Xing, X. ICS software trust measurement method based on dynamic length trust chain. *Scientific Programming* **2021**(5), 1–11 (2021).
32. Yang, Z., Yin, C., Fang, Z., & Zhao, N. In trust chain model and credibility analysis in software systems. In *2020 5th International Conference on Computer and Communication Systems (ICCCS) 2020* (2020).
33. Jayasinghe, U., Lee, G. M., Macdermott, I. & Rhee, W. S. TrustChain: A privacy preserving blockchain with edge computing. *Wireless Communications and Mobile Computing* **2019**(1), 1–17 (2019).
34. Song, Y., Wang, Y. & Jin, D. A Bayesian approach based on bayes minimum risk decision for reliability assessment of web service composition. *Future Internet* **12**(12), 221 (2020).
35. Ping, C., Xinjian, W. & Depeng, D. Construction of model based on Petri net and reliability analysis based on Bayes net of Web Service transaction. *Journal on Communications* **39**(S1), 99–104 (2018).
36. Shuangyang, Q., Zhe, C. & Yuanxu, L. Cloud service reliability prediction method based on improved Bayes. *Computer Applications and Software* **34**(11), 6 (2017).
37. Hassan, H., El-Desouky, A. I., Ibrahim, A., El-Kenawy, E. & Arnous, R. Enhanced QoS-based model for trust assessment in cloud computing environment. *IEEE Access* **99**, 1 (2020).
38. Gan-zhi, H. & Xi-ping, L. A service selection method with QoS synthetic evaluation. *Computer Technology and Development* **27**(8), 164–170 (2017).
39. Xin-qi, X. & Xi-ping, L. A trusted QoS selection method based on evaluation classification. *Computer Technology and Development* **28**(8), 114–119 (2018).
40. Huo, X., Yang-Yang, Z., Yong-Jun, J. & Kun, S. Multidimensional reputation calculation method based on feedback reliability in MAS environment. *Journal of Software* **31**(2), 374–394 (2020).
41. Xiao-yu, W. & Liang-lun, C. Study of credible guarantee mechanism of multi-source information resources cloud services model on cloud computing. *Application Research of Computers* **31**(9), 2741–2745 (2014).
42. Ruzhong, D., Chunxiang, H., Junfeng, T. & Xia, T. Evaluation of trusred cloud services based on third-party regulation. *Journal of Information Security Research* **3**(4), 344–352 (2017).
43. Gao, T., Jia, X., Jiang, R., He, Y. & Yang, M. SaaS service combinatorial trustworthiness measurement method based on Markov theory and cosine similarity. *Security & Communication Networks* **6**, 66 (2022).
44. Wang, Q., Wang, H. & Qi, Z. An application of nonlinear fuzzy analytic hierarchy process in safety evaluation of coal mine. *Safety Science* **86**, 78–87 (2016).

Author contributions

All authors contributed to the study conception and design. Material preparation, data collection, and analysis were performed by Jia Wang, Gui Bin and Leijin Long. First draft of the manuscript was written by Ming Yang and Rong Jiang, and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding
This research was supported by the National Natural Science Foundation of China (no. 72261033), Yunnan Fundamental Research Projects (nos. 202101AT070211, 202201AT070142) and the Foundation of Yunnan Key Laboratory of Service Computing (no. YNSC23110).

Declarations

Competing interests
The authors declare no competing interests.

Ethical statement
I certify that this manuscript is the original and has not been published. During the submission period, it will not be submitted to other places for publication. The authors declare that they have no conflict of interest. This article does not contain any studies with human participants or animals performed by any of the authors.

Additional information
Correspondence and requests for materials should be addressed to J.W.