Research on Cloud Service Security Measurement Based on Information Entropy

Tilei Gao[1,2], Tong Li[3], Rong Jiang[2], Ming Yang[2], and Rui Zhu[1]
(Corresponding author: Ming Yang)

School of Software, Yunnan University, Kunming 650091, China[1]
School of Information, Yunnan University of Finance and Economics, Kunming 650221, China[2]
Key Laboratory in Software Engineering of Yunnan Province, Kunming 650091, China[3]
(Email: httx133@qq.com)
(Received Aug. 24, 2018; Revised and Accepted Feb. 7, 2019; First Online Sept. 21, 2019)

Abstract

The security of cloud services is one of the most important factors to consider when users choose cloud services. An objective and quantitative measure of cloud services security directly determines whether potential users will choose cloud services or not. Aiming at this measure problem, and on the basis of STC 1.0, ISO/IEC 25010 and CIA security requirement model in the field of information security, cloud service security attribute model (CSSAM) is built. Then, a method to figure up the weights of each attributes in CSSAM is raised based on the information entropy, information gain (IG) and other concepts and formulas. At last, introduce the weights calculation method via case analysis and prove the feasibility and correctness of CSSAM model and weights calculation method.

Keywords: Cloud Service; Information Entropy; Information Gain (IG); Security Attributes

1 Introduction

Authority agency Forrester pointed out that, by 2020, the revenues global SaaS of software will reach $132.6 billion with an average increase of 9.14% each year. IDC indicated that the public cloud spending will be twice as much as the revenue reaching $127.5 billion [23]. Enterprises as the main driving force for Cloud Computing not only access to the opportunities from cloud, such as cost advantages, strategic flexibility, focus on core competencies, access to specialized resources and quality improvements, but salient risks as well, which include: performance risks, economic risks, strategic risks, security risks and managerial risks [3]. For enterprises, especially the small and medium sized enterprises (SMEs), besides the cost, whether cloud services are chosen or not depends on the questions on functionality, usability, integration, security, efficiency [35], real-time, maintainability [9] and so on.

With the rapid development of information technology and network, an increasing number of cloud services have been developed, and remarkable achievements have been made in aspects of functionality, usability and other aspects, and the problem hindering the further development of cloud services ultimately falls on the aspect of cloud service security. As the existing security evaluation and measurement methods are all provided by cloud service producers, agents or cloud service consumers, potential users or new consumers have to search services based on others' comments. Generally, the security of cloud service is positively related to its cost and the higher the security is, the higher the cost will be. But security is made up of many attributes and the highest score service does not always mean the most suitable for specific enterprises. Actually, for different enterprises, there exist differences in the demand for security, and the cloud service product scoring results from outsides are too subjective to reflect the differences in security between different enterprises. Thus, its reference value is greatly questioned.

Based on the problems above, the objective of this paper is to provide a customized method to measure the security of cloud services according to user's security requirements instead of evaluation of service providers or agents.

To achieve the objective, the following tasks will be accomplished in this paper:

1) Divide the personnel involved in cloud computing into two roles: potential users and external personnel. Potential users provide the data reflecting their requirements which will be used to calculate the attributes weights.

2) Collect and collate attributes of cloud service security and build the cloud service security attribute model, CSSAM.

3) Propose the measure method and steps based on entropy and information gain (IG).

4) Verify and validate the correctness and feasibility of the measurement method.

The structure of this paper is as follows: Section 1: The background, content and significance to cloud service security; Section 2: A survey of cloud service, cloud service security and cloud service security measurement methods; Section 3: Definitions, principles and formulas; Section 4: Cloud service security attribute index model CSSAM and specific security measure method; Section 5: A case study and analysis to the feasibility and correctness of the CSSAM model and the proposed measurement method; And Section 6: Conclusion.

2 Related Work

2.1 Cloud Computing and Cloud Computing Security

At present, cloud computing has become one of the research hotspots in the computer field [11]. In addition to the development of cloud services themselves, the cloud service security has increasingly become a hot issue in cloud computing research. The development history of information security has proved that major changes in information technology will directly affect the development process of information security [5]. Cloud Computing, with dynamic distribution of services as its main technical feature, is a major change in the field of information technology, which is bound to have a huge impact on the security sector. Main researches in this major change include trusted cloud computing [1,26,27,36], cloud service data security [10,12,17,21,22] and cloud service resource management security [4,5,18,24,32].

All the researches above focused on either functionality of cloud service or any other single security aspect, and lack overall consideration on cloud computing and cloud computing security. Cloud service security is a systematic project. If any security hole or defect is found, there is no security at all. From above, researches on overall security measurement and detection are also an important aspect to study the security of cloud services. In this regard, this paper proposes a method for measuring the overall security of cloud services which provides reliable, reliable, objective and quantitative basis for users to select products suitable for their own security needs. Meanwhile, the measurement method proposed can also provide reference for cloud service developers to improve their cloud service security.

2.2 Reviews on Cloud Service Security Measurement and Evaluation

For the measurement or evaluation of cloud service security, the existing research results are more focused on the measurement or evaluation of security risks. Chhabra and Tangja [6] discussed the risk problems of cloud computing security from the three levels of IaaS, PaaS and SaaS. Tanimoto et al. [30] started their research from the user's point of view and listed the cloud computing security risks that users are concerned about. Meanwhile, for the assessment, solution and response plans of cloud computing security, Saripalli and Walters [28] put forward a framework for cloud computing security risk assessment. Yu and Ji [34] have made a detailed analysis to the purpose, objectives, and risk assessment business processes based on roles, structures, and the context of information systems and proposed a risk assessment method for information system security oriented to business process. Other measure methods like Gini coefficient [16] represents the uncertainty of a randomly selected sample in a subset and can only assess the overall uncertainty of risk.

In order to implement security risk measurement and assessment and identify factors affecting risks, quantification of all factors is a must. The research results in this respect are as follows: risk value model VaR (Value at Risk) [37], actuarial model [7], coherent risk measurement [8, 25], information entropy and Markov chain model [2, 33] and so on. These models and methods provide important reference value for risk measurement and evaluation. In the aspect of risk assessment, existing research results [10,20,31] are mainly for single risk or similar risk analysis. As security analysis is a holistic project, single analysis is bound to lack extensive and relevant analysis, and its effects in system security are limited. In other researches, the results [14, 15, 29] pay more attention to technical risks and the analysis in uncertainty and quantitative of risk factors is inadequate. As a result, the analysis methods lack the objectivity and accuracy to evaluate the overall security of the system.

In summary, on the basis of summarizing the traditional information security demand model and previous research results, this paper starts with the security attributes that affect cloud services, and proposed cloud service security attribute mode, CSSAM, whose initial scores come from the potential users themselves. So, the model proposed reflects the different users' needs for cloud service security. Besides, scores stem from overall security performance of different products, which suggest the integrity principle of cloud service security.

3 Definitions

3.1 Roles in Cloud Computing

In this paper, roles in cloud computing are divided into two kinds: one is planning to use cloud services, named the potential cloud service user (PCSU). This kind of users is up to finish the questionnaires to compute the weights of security attributes. The other one kind is the people who is familiar with cloud services and we named this kind external personnel. The role of external personnel is made up of cloud service user (CSU), cloud service producer (CSP) and cloud service agent (CSA). Based on their own conditions or advantages, such users scored the corresponding cloud service products according to secu-

Table 1: Roles in cloud services

Categories	Role Names	Specific Descriptions
Potential users	potential cloud service user (PCSU)	Organizations or enterprises that have not directly used cloud services which hope to achieve the highest cost performance on the basis of meeting its basic functional requirements. They are always small and medium enterprises. PCSUs are always the ones who will start or add a new business on the internet. After using the services, they will become CSU which belongs to the kind of external personnel.
External personnel	Cloud service producer (CSP)	Providers of cloud services which provide differentiated services of various types and levels, and have flexible charging mode. They can be large scale enterprise and can also be single programmer. When developing a new service, they may also use others' services and then they can also become PCSUs.
	Cloud service user (CSU)	Users who used or are using or experiencing cloud services. The service evaluation data submitted by CSU is an important reference for evaluating cloud services. When new requirements come, they may also become PCSUs to find suitable services.
	Cloud service agent (CSA)	Middlemen of cloud services, who lie between CSP and PCSU. Middlemen have a clear understand of the products from CSP and the needs from PCSU. Due to the drive of value and interest, the evaluation of cloud service products from CSA is more subjective. Usually, CSA is just a service providing platform like apple store.

rity attributes. Descriptions about all roles are shown in Table 1.

3.2 Information Entropy and Information Gain

1) Information entropy

Shannon introduced physical entropy into information theory and defined the magnitude of information, which is used to measure the amount of information and named information entropy. Simply, information entropy is a tool to describe the uncertainty of information before and after communication, and its definition [13] is as follows: Definition (information entropy) Let X be a discrete random variable, and n is the number of its possible values, that means X = x1, x2, ..., xn. For each xi, its probability value is P(xi) and:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i). \quad (1)$$

$H(X)$ is called information entropy of discrete random variable X.

2) Conditional entropy

Definition (Conditional entropy) [19] Let (X, Y) be discrete variable and its joint probability distribution is:

$$P(X = x_i, Y = y_j) = p_{ij}, \quad i = 1, 2, \cdots, n; j = 1, 2, \cdots, m. \quad (2)$$

Conditional entropy H (Y—X) indicates the uncertainty of Y of a random variable under the condition of known random variable X. Actually, conditional entropy H(Y—X) is the mathematical expectation of conditional probability distribution entropy of Y to X under given X condition and the formula is:

$$H(Y|X) = \sum_{i=1}^{n} p_i H(Y|X = x_i). \quad (3)$$

Among it, $p_i = P(X = x_i)$, $i = 1, 2, \cdots, n$.

3) Information gain

Information gain [37] is also called mutual information which indicates the reduction degree of uncertainty of Y when X is confirmed.

Definition (Information gain) For a given set D, which characteristic X is included, the information gain G(D—X) is the difference between the overall information entropy H(D) and the conditional entropy H(D—A).

$$G(D, A) = H(D) - H(D|A). \quad (4)$$

Obviously, $H(D) \geq H(D|A), G(D, A) \geq 0$.

Information gain indicates the effect of an attribute or feature $x_i \in X$, $i = 1, 2, \cdots, n$ on the overall uncertainty of the system. For each attribute of cloud service security, information gain represents the impact of a security attribute on the overall security of the cloud service. So, in this paper, information gain is used to represent as the weight of each security attribute in cloud service. As the criteria for evaluation of cloud services to be selected, the weights can be used to measure the security of cloud services and help PCSU to find the suitable services.

4 Cloud Service Security Measurement Model and Method

4.1 CSSAM

In the traditional information security field, security is embodied in the CIA security requirement model which includes: confidentiality, integrity and availability. Meanwhile, as the extension of traditional information security, other security attributes summarized from Software Trustworthiness Classification Specification and ISO/IEC 25010, such as controllability, non-repudiation, authentication, auditability, survivability and testability, should also be considered.

On the basis of STC 1.0, iso/iec 25010 and CIA security requirement model, we analyzed the characteristics of cloud computing services and users' requirements for security attributes, and then proposed cloud computing security attribute model CSSAM. Definition (CSSAM) CSSAM is a 9-tuple, CSSAM = $< f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9 >$. For each f in CSSAM, it represents the 9 security attributes separately and the specific descriptions of attributes are shown in Table 2.

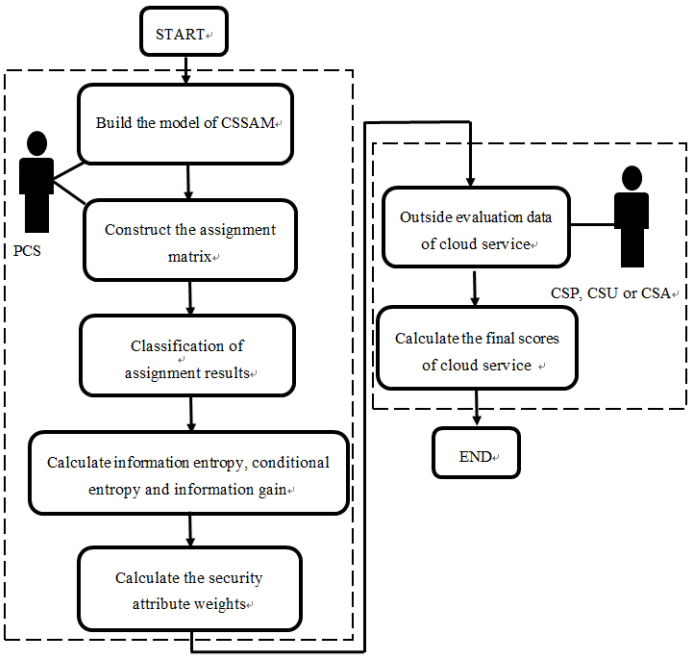

Figure 1: The proposed scheme

4.2 Measurement Method of Cloud Service Security

After building the model of CSSAM, measurement method is given. Method consists of two parts. Part one: according to the PCSU's security requirement, compute the weights on each attribute in CSSAM. The participating role in this part is the staff in PCSU, which helps finish questionnaires for scoring the attributes based on their own business. Part two: compute the final results of cloud service for the PCSU by multiplying weights getting from part one and scores of cloud services getting from external personnel outside PCSU, including CSP, CSU and CSA. Specific steps are shown in Figure 1.

Part one: Calculate the weights of attributes in CSSAM for PCSU. Steps are as follows:

Step 1: According to relevant definitions and descriptions in section 4.1, build CSSAM. Then, design the questionnaire and design the score and grading standard for each attribute in the questionnaire. Potential users PCSU design scoring rules according to their needs, which are going to be used to establish attribute weights. In addition, if having new requirements for security attributes, PCSUs can modify the specific attributes in CSSAM. An example of grading standard table is shown in Table 3. The criteria for comparison among the attributes are based on the scoring method in AHP, and fi means one of the attributes.

Step 2: Statistics the results of each questionnaire after PCSUs finished and use min-max standardization method and Equation (5) to calculate the standard results of security attributes.

$$Y_i = \frac{X_i - X_{min}}{X_{max} - X_{min}} \tag{5}$$

Among the formula, Y_i represents comprehensive score after standardization of each security attribute, and X_{max} represents the maximum value, and X_{min} the minimum value. The results constitute an assignment matrix A:

$$\begin{aligned} A_{n\times m} &= \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \\ &= (\alpha_1, \alpha_2, \cdots, \alpha_m). \end{aligned} \tag{6}$$

In the matrix, n represents the number of products used to get PCSUs' security requirements' data; m represents the number of security attributes; and a_{ij} represents the standardization result of attribute j in product i. Simply speaking, it is the target values of system security attributes based on their daily work. $\alpha_k = (a_{1k}, a_{2k}, \cdots, a_{nk})^T$ and $k = 1, 2, \cdots, m$. Add the values of each row in the matrix to get the security score of each product:

$$\begin{aligned} \beta &= (b_1, b_2, \cdots, b_n)^T \\ &= \left[\sum_{k=1}^{m} a_{1k} \sum_{k=1}^{m} a_{2k} \cdots \sum_{k=1}^{m} a_{nk}\right]^T \end{aligned} \tag{7}$$

Then, the original assignment matrix is trans-

Table 2: Security attributes in CSSAM

Nos.	Name of the attributes	Specific Descriptions
f_1	Confidentiality	Ensure that information resources are accessed only by legitimate entities (such as users, processes, etc.) and do not leak information to unauthorized entities.
f_2	Controllability	Ensure that information managers can carry out necessary control and management of information and content transmitted. Authentication, authorization, and monitoring of information and information systems to ensure the authenticity of an entity (user, process, etc.).
f_3	Integrity	Ensure that information resources can only be modified by authorized or authorized means, and not to be accidentally or deliberately altered or forged during storage or transmission.
f_4	Non-Repudiation	Ensure that the sender of information cannot deny part of the information or information that has been sent out, and the receiver of information cannot deny part of the information or information that has been received.
f_5	Survivability	Ensure that computers continue to provide core services in the face of various attacks or errors, and ensure to be able to recover all services in time, and key business functions maintained.
f_6	Auditability	Ensure the behavior of users which can be verified by using security mechanisms such as auditing, monitoring, and non-repudiation, and provide investigation evidence and means for network security problems.
f_7	Availability	Ensure that information resources can be accessed by legitimate users and can be used according to the required characteristics without being denied service.
f_8	Authentication	Ensure that information users and information providers are real claims, preventing attacks from impersonation and repetition.
f_9	Testability	Testability is the ability of software to detect faults and isolate and locate faults and ability of design and testing execution under certain time and cost.

Table 3: An example of marking standard

Levels	Values	Description
Extremely important	8-10	In CSSAM, fi is extremely important
Specially important	6-8	In CSSAM, fi is very important
Very important	4-6	In CSSAM, fi is obviously important
Fairly important	2-4	In CSSAM, fi is a little more important
Unimportant	0-2	In CSSAM, two attributes have the same or similar importance.

formed into $A'_{n\times m}$:

$$A'_{n\times m} = (\alpha_1, \alpha_2, \cdots, \alpha_m, \beta). \tag{8}$$

Step 3: According to the value of β in matrix $A'_{n\times m}$, every attribute has got a security level, which is used to calculate the information entropy in the next step. The specific levels can be set based on the actual needs of PCSU, and security attribute levels can refer to the table in Step 1, and the levels of β values are shown in Table 4.

Table 4: An example of grading

Levels	Scores
UNSAFE	0-30
MEDIUM	30-60
SAFE	60-90

Step 4: The matrix values getting from Step 2 and Step 3, are used to calculate information entropy H(β) using Formula (1) and Formula (3) is used to calculate conditional entropy H($\beta|\alpha_i$) of each security attribute, and Formula (4) is used to calculate information gain G(β, α_i) of each security attribute.

Step 5: Normalize the values of security attributes information gain $G(\beta, \alpha_i)$ getting from Formula (4) and security attribute weight γ_i is obtained. γ_i comes from PCSU's staff, so it reflects the security requirements of PCSU.

Part Two: According to the weights getting from part one, measure the service to be chosen for PCSU. Steps are as follows:

Step 6: Seek evaluation data of cloud services to be selected for PCSU. Usually, the data can be from the roles of external personnel, and the initial data should be standardized by min-max standardization method, and security attribute scores $\delta = (e_1, e_2, \cdots, e_m)$ of some cloud service from external personnel are achieved.

Step 7: For PCSU, the formula for calculating the security score S of the cloud service to be measured is:

$$S = \delta \times \gamma^T.$$

In the formula, γ^T is the transpose of γ and γ is the collection of the 9 security attributes weights and $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6, \gamma_7, \gamma_8, \gamma_9)$.

5 Case Analysis

5.1 Case

To expand its business, some company named E intends to build an online sales management system. As restricted by capital and technology, after investigation, E decides to build their new system by hiring cloud services.

The company used to do online selling in office supplies (B2C), but it found a business opportunity in marketing country agricultural commodities for urban communities (B2B and B2C). This company had to reorganize all the business, transferring to mobile phone client. Owing to the scale, cost and technique, it decided to apply cloud services in order to implement the new business. As the main trade product, fresh product needs more strict standards in technique. If information transmission and processing fail, it will pose a great economic threat to the company. Thus, it needs more strict demands in availability and survivability. On the other hand, the main business is to implement a vital link between village head and property company managers. As for farm product providers or communities, they need to do business through village head or property company managers. In order to guarantee each participant's rights, the company has much higher demands in controllability and auditability of information.

The method proposed in this paper is used to measure the four services for the E company to choose the service which will most satisfy their own security requirements. Measurement processes are as follows:

Step 1: Establish the model of CSSAM and PCSU can select their own security attributes and design the questionnaires for their staff. The grading standard can follow Table 3.

Step 2: Formula (5) is used to calculate the results from PCSU staff questionnaires and put the results into the scoring matrix. Using Formula (7), β is obtained by adding the scores of the 9 attributes and filled in the matrix as well. The scoring matrix A is as shown in Table 5. In Table 5, rows represent the products chosen for test and the columns represent the 9 attributes. The data in the table were scored by 10 front-line staff of E company according to AHP rules for 9 attributes of 15 software products. The company's preference for security attributes can be reflected by the results of scoring different software security by front-line personnel within the company.

Table 5: Scoring matrix

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	β
1	10	9	8	6	7	5	6	8	8	67
2	6	8	7	4	3	6	4	5	3	46
3	7	5	6	4	5	3	2	5	5	42
4	6	3	6	3	1	0	1	4	3	27
5	6	6	8	7	7	4	3	6	8	55
6	8	7	9	9	8	6	8	6	7	68
7	9	9	8	9	8	6	8	5	8	69
8	10	8	9	8	9	8	4	6	6	68
9	5	5	8	6	6	8	4	3	5	50
10	8	5	7	9	7	3	2	5	4	50
11	8	8	10	9	9	4	6	7	9	71
12	7	9	6	5	5	2	5	3	7	50
13	6	1	5	3	3	0	1	3	5	27
14	8	4	7	8	7	4	4	4	8	54
15	6	4	7	6	8	2	4	5	8	50

Step 3: Scores in Table 5 are divided into different grades according to the standards in Table 3 and Table 4 and the dividing results are as shown in Table 6. In the table, EI means extremely important; SI means specially important; VI means very important; FI means fairly important; UI means unimportant.

Step 4: Formula (1) is used to calculate information entropy $H(\beta) = 0.97$. Formula (3) is used to calculate the conditional entropy $H(\beta|\alpha_i)$ of each security attribute in Table 6 and then, information gain $G(\beta, \alpha_i)$ of each attribute is got by using Formula (4). The results are as shown in Table 7.

Step 5: Normalize the results of $G(\beta, \alpha_i)$ in Table 7 and weight of each security attribute is obtained. The results are shown in Table 8. γ_i means the weight of attribute f_i.

Table 6: Grades of each attributes

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	β
1	EI	EI	EI	VI	SI	VI	SI	EI	EI	SAFE
2	SI	EI	SI	VI	FI	SI	VI	VI	FI	MEDIUM
3	SI	VI	SI	VI	VI	FI	FI	VI	VI	MEDIUM
4	SI	FI	SI	FI	UI	UI	UI	VI	FI	UNSAFE
5	VI	VI	EI	SI	SI	VI	FI	SI	EI	MEDIUM
6	EI	SI	EI	EI	EI	SI	EI	SI	SI	SAFE
7	EI	EI	EI	EI	SI	SI	EI	VI	SI	SAFE
8	EI	EI	EI	SI	EI	EI	VI	SI	SI	SAFE
9	VI	VI	EI	SI	SI	EI	VI	FI	VI	MEDIUM
10	SI	VI	SI	EI	SI	FI	FI	VI	VI	MEDIUM
11	EI	EI	EI	EI	EI	VI	SI	SI	EI	SAFE
12	SI	EI	SI	VI	VI	FI	VI	FI	SI	MEDIUM
13	SI	UI	VI	FI	FI	UI	UI	FI	VI	UNSAFE
14	EI	FI	SI	EI	SI	VI	VI	VI	SI	MEDIUM
15	SI	VI	SI	SI	SI	FI	VI	VI	EI	MEDIUM

Table 7: The results of conditional entropy and information gain

Security Attributes	$H(\beta\|\alpha_i)$	$G(\beta,\alpha_i)$
f_1	0.46	0.51
f_2	0.35	0.62
f_3	0.47	0.50
f_4	0.52	0.45
f_5	0.28	0.69
f_6	0.40	0.57
f_7	0.18	0.79
f_8	0.65	0.32
f_9	0.65	0.32

Table 8: Weights of each attribute indexes

Security Attributes	γ_i
f_1	0.11
f_2	0.13
f_3	0.10
f_4	0.09
f_5	0.14
f_6	0.12
f_7	0.17
f_8	0.07
f_9	0.07

Step 6: According to the attributes in CSSAM, seek the security evaluation data of the four cloud services (CS1, CS2, CS3, CS4) and Table 9 is established. The data in the table were the mean value which were calculated from scores of external personnel (include 10 CSAs, 10 CSPs and 30 CSUs) according to AHP rules for nine attributes of the four products. Each score means the sum of each attribute of each cloud service product.

The scores of the four cloud services are based on the AHP rules of 50 external personnel (include 10 CSAs, 10 CSPs and 30 CSUs). Because of the exclusiveness of security attributes, the strength of some attributes will inevitably lead to the decline of other attributes. Four service products have different emphasis on nine security attributes. CS1 focuses on authentication, non-repudiation, survivability and testability; CS2 focuses on availability and survivability; CS3 focuses on confidentiality, controllability availability and authentication; CS4 focuses on availability, testability, survivability, auditability and controllability. As CS2 only performs well in availability and survivability, other attribute scores are very low, resulting in the lowest total score in the four products.

Table 9: Scores getting from external personnel

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	Scores
CS1	8	6	8	9	9	7	5	10	9	70
CS2	6	5	3	3	9	5	10	6	5	52
CS3	10	10	7	5	5	5	10	9	8	69
CS4	4	9	3	6	9	9	10	8	10	67

Step 7: The four services' final scores S for E company

will be gotten using Formula (9) and results are shown in Table 10.

From Table 8, we can get that, f_7, f_5 and f_2 are the most concerned security factors, that means, compared with others, E company pay more attention to the availability, survivability and controllability. And attributes like authentication and testability do not have much concern.

5.2 Comparison and Analysis

In the case, we have calculated the weights of the 9 attributes of the E company. According to the scores of four cloud services given by external personnel staff, the results that meet the company's security requirements are calculated, as is shown in Table 10. We choose two commonly used weight calculation methods: average method and AHP scoring method, and compare them with information gain method proposed in this paper.

1) Average method (AVG). Assuming that each security attribute has the same weight, that means $\gamma_i = 1/9$, $i = 1, 2, \cdots, 9$, and $\gamma_{avg}^T = (0.11, 0.11, \cdots, 0.11)$.

2) AHP scoring method (AHP). Collate the scoring results of 20 external personnel (include 5 CSAs, 5 CSPs and 10 CSUs) and obtain the weights of the 9 security attributes, $\gamma_{AHP}^T = (0.20, 0.12, 0.18, 0.02, 0.16, 0.03, 0.20, 0.04, 0.05)$.

According to Formula (9), the scores of four CSs using different weight calculation methods are calculated, and the results are shown in Table 11 and Table 12. In the two tables, S represents the total score of four cloud service products calculated by the two methods.

Combining the results calculated in Table 10, the results of scoring four cloud service products by three methods are shown in Table 13 and Figure 2.

In Figure 2(a), (b) and (c) are the final scores of the four cloud services calculated by multiplying the weights obtained by using information gain, average value and AHP method with the results of external personnel scoring in Table 9. Figure 2(b) directly reflects the external measurement results of the security of four products. External recognition of the security of four products is in the figure, that is, $CS1 > CS3 > CS4 > CS2$. This only shows the degree of recognition of various cloud service products by the outside world, but does not reflect the security needs preferences of specific users.

Figure 2(c) is the weight of each security attribute derived by the external staff associated with cloud services according to their awareness of security attributes. According to the objective score data of each cloud service, the final result is $CS3 > CS1 > CS4 > CS2$. This reflects the industry's recognition of security attributes. Combining the scores of four cloud service products, the professional evaluation of four cloud services by professionals is given. Its reference value is higher than the average method. In this method, CS3 products perform best in attributes that experts value, so it gets obvious high scores. The service of CS3 may have got a good score in most situations, but still may not be perfect for a special application scenario.

Figure 2(a) is the result of the method presented in this paper. The weights are calculated by the internal personnel analysis, which reflects the user's own security needs. Combined with the evaluation of four cloud services given by the outside world, the results not only reflect the objective degree of product security, but also reflect the degree of conformity of the cloud services to the company's security needs.

For company E, the result calculated with the method proposed in this paper is: $CS4 > CS1 > CS3 > CS2$. Obviously, CS4 has the highest score and should be the most suitable service for E. Compared with the scores from other methods, the calculated scores are more consistent with E's own business security requirements, and the advantages of CS4 focuses on the attributes of controllability, survivability, auditability, availability and testability, which meet the needs of E's security requirements in the practical application process.

6 Conclusion

As one of the most crucial attributes, the security of cloud services also becomes the most dominant element for traditional users to choose cloud services. An objective and quantitative measure of cloud services security directly determines whether potential users will choose cloud services. In the existing literature, researchers only measured and evaluated the product itself and ignored the specific security needs of users. Therefore, for specific users, existing methods will not meet their customized security requirements. Regarding the objective quantitative measure problem, different users in different field or one user in different application environments have diverse demand in cloud services security.

To solve the problem above, the following contributions have been made: (1) We have introduced the roles and roles' classification in cloud computing, containing potential users (PCSU), cloud services providers (CSP), cloud services users (CSU) and cloud services agents (CSA). (2) On the basis of STC 1.0, ISO/IEC 25010 and CIA security requirement model in the field of information security, a cloud service security attribute model CSSAM has been proposed, which includes 9 security attributes for measurement. (3) A method based on the entropy, information gain (IG) and other concepts and formulas has been raised to define weights of each attributes in user CSSAM. (4) A case study has been introduced which proved the feasibility and correctness of CSSAM model and weights calculation method in practice. Our work has enriched the application scenarios of information entropy and information gain (IG) theory. In practical application, it has also made some contributions to objectively measure cloud services and help SMEs choose suitable cloud ser-

Table 10: Final scores of 4 cloud services

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	S
CS1	0.83	0.79	0.80	0.84	1.30	0.84	0.83	0.67	0.60	7.50
CS2	0.64	0.63	0.31	0.28	1.30	0.59	1.66	0.40	0.34	6.16
CS3	2.04	1.31	0.69	0.45	0.72	0.57	0.33	0.61	0.56	7.27
CS4	0.43	1.18	0.31	0.52	1.30	1.05	1.66	0.54	0.65	7.64

Table 11: AVG scores of 4 cloud services

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	S
CS1	0.89	0.67	0.89	1.00	1.00	0.78	0.56	1.11	1.00	7.89
CS2	0.67	0.56	0.33	0.33	1.00	0.56	1.11	0.67	0.56	5.78
CS3	1.11	1.11	0.78	0.56	0.56	0.56	1.11	1.00	0.89	7.67
CS4	0.44	1.00	0.33	0.67	1.00	1.00	1.11	0.89	1.11	7.56

Table 12: AHP scores of 4 cloud services

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	S
CS1	1.60	0.70	1.44	0.17	1.44	0.22	1.00	0.42	0.47	7.45
CS2	1.20	0.59	0.54	0.06	1.44	0.15	1.99	0.25	0.26	6.48
CS3	2.00	1.17	1.26	0.09	0.80	0.15	1.99	0.38	0.42	8.27
CS4	0.80	1.06	0.54	0.11	1.44	0.28	1.99	0.33	0.52	7.07

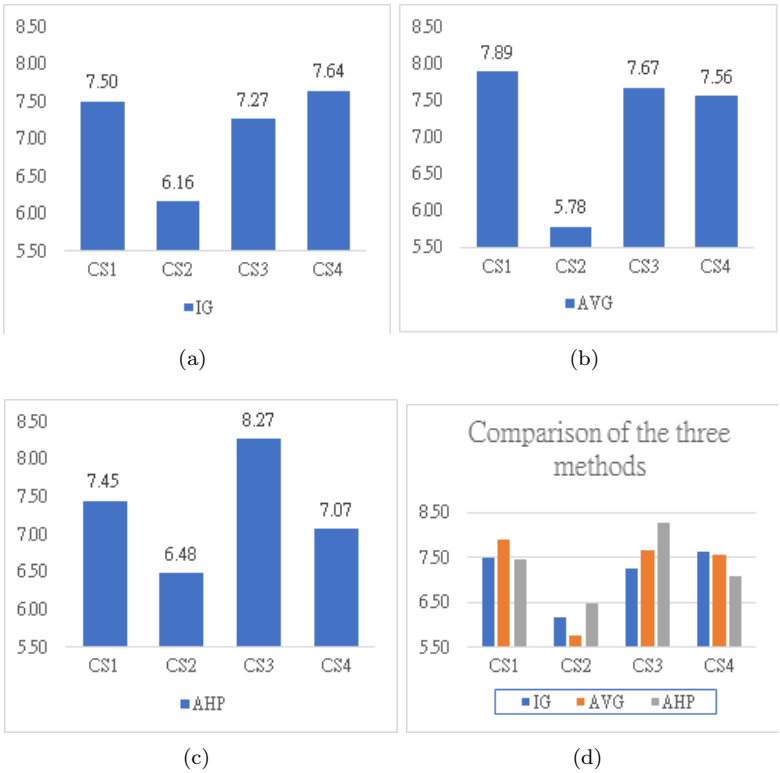

Figure 2: The comparison of the 3 methods

Table 13: AVG scores of 4 cloud services

	CS1	CS2	CS3	CS4
IG	7.50	6.16	7.27	7.64
AVG	7.89	5.78	7.67	7.56
AHP	7.45	6.48	8.27	7.07

vices. While the attributes in CSSAM will develop or change with the environment and society, in the future, cloud computing and cloud services will continue to be further studied, and we will further improve and refine security attributes in CSSAM and give more reasonable and detailed security attributes and descriptions to better measure the security of cloud services and provide more reliable basis for PCSU to selected suitable cloud services.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Nos.61379032, 61763048, 61263022, 61303234, 61662085), National Social Science Foundation of China (No.12XTQ012), Science and Technology Foundation of Yunnan Province (No.2017FB095), Yunnan Province Applied Basic Research Project(No.2016FD060), Science Research Project of Yunnan Education (Nos.2017ZZX001, 2017ZZX227), Key Project of Scientific Research of Yunnan Education (2015Z018), Provincial Scientific and Technological Innovation Team Project of Yunnan University (2017HC012), the 18th Yunnan Young and Middle-aged Academic and Technical Leaders Reserve Personnel Training Program (No.2015HB038). The authors would like to thank the anonymous reviewers and the editors for their suggestions.

References

[1] D. S. AbdElminaam, "Improving the security of cloud computing by building new hybrid cryptography algorithms," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 40-48, 2018.

[2] M. H. R. Al-Shaikhly and H. M. El-Bakry and A. A. Saleh, "Cloud security using markov chain and genetic algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 96-106, 2018.

[3] A. Benlian, and T. Hess, "Opportunities and risks of software-as-a-service: Findings from a survey of it executives," *Decision Support Systems*, vol. 52, no. 1, pp. 232-246, 2012.

[4] P. Bonatti, S. D. C. di Vimercati, P. Samarati, "An Algebra for Composing Access Control Policies," *ACM Transactions on Information and System Security*, vol. 5, no. 1, pp. 1-35, 2002.

[5] S. Bulusu, and K. Sudia, "A Study on Cloud Computing Security Challenges," *DiVA Portal*, 2012. (`https://www.diva-portal.org/smash/get/diva2:830115/FULLTEXT01.pdf`)

[6] S. P. Chandran, and M. Angepat, "Cloud computing: Analysing the risks involved in cloud computing environments," *Ornitologia Neotropical*, vol. 12, 2001.

[7] M. Eling, and N. Loperfido, "Data breaches: Goodness of fit, pricing, and risk measurement," *Insurance Mathematics & Economics*, vol. 75, pp. 126-136, 2017.

[8] H. Föllmer, and I. Penner, "Consistent risk measures and a non-linear extension of backwards martingale convergence," in *Interdisciplinary Mathematical Sciences & Festschrift Masatoshi Fukushima* pp. 183-202, 2015.

[9] J. Espadas, A. Molina, G. Jiménez, M. Molina, R. Ramírez, D.Concha, "A tenant-based resource allocation model for scaling; Software-as-a-service applications over cloud computing infrastructures," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 273-286, 2013.

[10] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of "big data" on cloud computing: Review and open research issues," *Information Systems*, vol. 47, no. C, pp. 98-115, 2015.

[11] C. Hoffa, G. Mehta, T. Freeman, E. Deelman, K. Keahey, B. Berriman, and J. Good, "On the use of cloud computing for scientific workflows," in *IEEE Fourth International Conference on Escience*, 2008. DOI: 10.1109/eScience.2008.167.

[12] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," *Journal of Systems and Software*, vol. 86, no. 3, pp. 716-727, 2013.

[13] E. T. Jaynes, "Information theory and statistical mechanics," *Physical Review*, vol. 106, no. 4, pp. 620-630, 1957.

[14] C. Joshi, and U. K. Singh, "Information security risk management framework for university computing environment," *International Journal of Network Security*, vol. 19, no. 5, 2017.

[15] M. Jouini, and L. B. A. Rabai, "Comparative study of information security risk assessment models for cloud computing systems," *Procedia Computer Science*, vol. 83, pp. 1084-1089, 2016.

[16] W. Kalmijn, Gini Coefficient: Springer Netherlands, 2014.

[17] S. Kalra, and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive & Mobile Computing*, vol. 24, pp. 210-223, 2015.

[18] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64-67, 2013.

[19] H. Li, *Statistical Learning Method: Tsing University Press*, 2012. (`https://www.amazon.com/Statistical-learning-methods-LI-HANG/dp/7302275955`)

[20] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650-666, 2016.

[21] L. Liu, W. Kong, Z. Cao and J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 110-115, 2017.

[22] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT," *Future Generation Computer Systems*, vol. 49, no. C, pp. 58-67, 2015.

[23] Z. Ma, R. Jiang, M. Yang, T. Li, and Q. Zhang, "Research on the measurement and evaluation of trusted cloud service," *Soft Computing*, vol. 22, no. 6, pp. 1-16, 2016.

[24] J. Mclean, "The specification and modeling of computer security," *Computer*, vol. 23, no. 1, pp. 9-16, 1990.

[25] S. Mitra, Sovan, "Efficient option risk measurement with reduced model risk," *Insurance Mathematics & Economics*, vol. 72, pp. 163-174, 2017.

[26] A. R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing: Secure outsourcing of data and arbitrary computations with lower latency," in *International Conference on Trust and Trustworthy Computing*, 2010. DOI:10.1007/978-3-642-13869-0.

[27] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in *International Conference on Hot Topics in Cloud Computing*, 2009. (`https://people.mpi-sws.org/~gummadi/papers/trusted_cloud.pdf`)

[28] P. Saripalli, and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in *IEEE International Conference on Cloud Computing*, 2010. DOI: 10.1109/CLOUD.2010.22.

[29] F. U. Sha, Y. Z. Xiao, and M. H. Liao, "An approach for campus information systems security risk assessment based on fuzzy set and entropy weight," *Information Science*, 2013. (`http://en.cnki.com.cn/Article_en/CJFDTotal-QBKX201309023.htm`)

[30] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, "Risk Management on the Security Problem in Cloud Computing," in *First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, 2011. DOI: 10.1109/CNSI.2011.82.

[31] J. Wang, J. Liu, and H. Zhang, "Access control based resource allocation in cloud computing environment," *International Journal of Network Security*, vol. 19, no. 2, pp. 236-243, 2017.

[32] D. Wijesekera, and S. Jajodia, "A propositional policy algebra for access control," *ACM Transactions on Information & System Security*, vol. 6, no. 2, pp. 286-325, 2003.

[33] M. Yang, R. Jiang, T. Gao, W. Xie and J. Wang, "Research on cloud computing security risk assessment based on information entropy and markov chain," *International Journal of Network Security*, vol. 20, no. 4, pp. 664-673, 2018.

[34] Z. Yu, and Z. Ji, "A survey on the evolution of risk evaluation for information systems security," *Energy Procedia*, vol. 17, 1288-1294, 2012.

[35] K. K. F. Yuen, "Software-as-a-service evaluation in cloud paradigm: Primitive cognitive network process approach," in *IEEE International Conference on Signal Processing, Communication and Computing*, 2012. DOI: 10.1109/ICSPCC.2012.6335719.

[36] X. Zhang, T. Li, X. Wang, Q. Yu, Y. Yu, and R. Zhu, "Formal Analysis to Non-Functional Requirements of Trustworthy Software," *Journal of Software*, vol. 26, no. 10, pp. 2545-2566, 2015.

[37] Z. Zhang, L. Yang, H. Li, and F. Xiang, "A quantitative and qualitative analysis-based security risk assessment for multimedia social networks," *International Journal of Network Security*, vol. 18, no. 1, pp. 43-51, 2016.

Biography

Tilei Gao is a lecturer at the school of information,Yunnan University of Finance and Economics. He is also a Ph.D candidate in system analysis and integration at the school of software at Yunnan University. His main research interests include software engineering and information management.

Tong Li is a professor and Ph. D. supervisor at school of software, Yunnan University, China. He received his Ph.D. from De Montfort University in 2007. His main research interests include software process, software engineering, etc.

Rong Jiang is a professor and Ph. D. supervisor at the school of information, Yunnan University of Finance and Economics, China. He received his Ph.D. from the school of software at Yunnan University. His main research interests include cloud computing, big data, software engineering, information management, etc.

Ming Yang, Corresponding author, is a lecturer at the school of information, Yunnan University of Finance and Economics, China. He received his Ph.D. from the school of software at Yunnan University. His main research interests include information management and data mining.

Rui Zhu is a lecturer at software school, Yunnan University, China. He received his Ph.D. from the school of software at Yunnan University. His main research interests include software process, software engineering, etc.