

Credibility Analysis of Power Cloud Terminal User Based on Set Pair Analysis

Ai-hua Zhou, Jie Ding, Wei Rao
State Grid Smart Grid Research Institute
Beijing, China

Song Deng
Nanjing University of Posts and Telecommunications
Nanjing, China

Tao Chang
State Grid Chongqing Electric Power Company
Chongqing, China

Yun-you Zhu
State Grid Chongqing Information & Telecommunication
Company
Chongqing, China

Abstract—The establishment of cloud computing system can greatly improve the data handling and interacting ability of the electricity network. However, the open operating environment faces significant security challenges. It is very important to effectively determine untrustworthy cloud terminal user so as to ensure the cloud security in complex dynamic environment. In this paper, based on set pair analysis (SPA) theory, we present a convenient method for credibility analysis of power cloud terminal user so as to give the system certain ability to provide differentiated services according to the predefined service policies. Through case study, we demonstrate the effectiveness and simplicity of the SPA-based method.

Keywords—credibility analysis; power cloud; set pair analysis

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1-2]. Combined with the characteristics of the power system and cloud computing technology, we can build up the power cloud to make full use of power system physical network and integrate existing computing power and storage resources. The power cloud can satisfactorily meet the growing application computing needs of data processing, real-time control and advanced analysis.

The power cloud can provide a variety of services to users and power system applications in a transparent manner. It dynamically deploys, allocates/reallocates and real-time monitors the virtualized computing and storage resource pool to provide computing service, data storage service and platform service that meeting the QoS requirement for the terminal user and power system applications [3-4]. With the rapid development of cloud computing, people can enjoy the convenience of reducing operating costs and improving operational efficiency. However, at the same time people have to face more severe information security challenges [5].

Massive important user data that stored in the cloud have a great temptation to attackers. Meanwhile, as to the cloud system provides users an open access interface, the terminal users can directly use the software, operating system, programming environment and network infrastructure of the cloud service provides. So, the impact and damage to cloud resources are more serious than the resource sharing using the Internet. Therefore, the credibility of terminal users who are accessing to cloud resources is important factor to ensure the security of cloud computing. In this paper, based on set pair analysis (SPA), a convenient method of cloud computing security was presented.

II. SET PAIR ANALYSIS

The SPA proposed by Keqin Zhao in 1989 is a modified uncertainty theory considering both certainties and uncertainties as an integrated certain-uncertain system and depicting the certainty and uncertainty systematically from three aspects as identity, discrepancy and contrary [6]. Set pair refers to a couple that consists of two interrelated sets. The basic idea of SPA is to analyze the features of a set pair and set up a connection degree formula of these two sets including identity degree, discrepancy degree and contrary degree under certain circumstances. Based on the connection degree formula, a series of SPA-based researches have been conducted.

Putting together set A and B to form set pair H with respect to the problem W , give the definition of the connection degree of set pair H as:

$$\mu(W) = \frac{S}{N} + \frac{F}{N}i + \frac{P}{N}j \quad (1)$$

where μ is the connection degree of the set pair, N denotes the total number of characteristics of the set pair, S represents the number of identity characteristics, P is the number of contrary characteristics, $F = N - S - P$ is the number of the characteristics of these two sets that are neither identity nor contrary. S/N , F/N and P/N respectively

represent the identity degree, discrepancy degree and contrary degree of these two sets. j is the coefficient of the contrary degree, and is specified as -1. As the coefficient of the discrepancy degree, i is an uncertain value between -1 and 1 in terms of various circumstances. The uncertainty of the discrepancy degree of two sets is eliminated when i is specified as -1 or 1, and will increase when i is approaching zero.

Given $a = S/N$, $b = F/N$, $c = P/N$, Eq. (1) can be rewritten as follows:

$$\mu = a + bi + cj \quad (2)$$

Due to its dialectic characteristics and advantages as a simple mathematic depiction with clear physical meaning, SPA has been applied to some multi-objective decision-making and multi-attribute assessment fields including modern management, applied math, computer science, engineering, social science, environmental assessment and management [7-11].

III. SPA-BASED CREDIBILITY ANALYSIS

A. Overall System Architecture

In the proposed SPA-based credibility analysis system, As shown in figure 1, when the terminal users make service requests to the power cloud computing system, those compliance requests will be sent to the credibility analysis module to determine user credibility level. For simplification, in the following case study we assume that the cloud computing system can determine its different credibility levels based on the application history, the user qualifications and the application task indicators. Of course, depending on the actual application scenario, we can add some necessary judgment indicators.

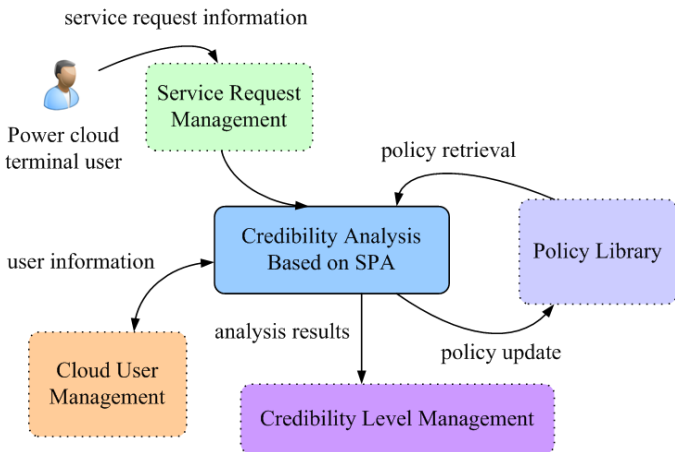


Fig. 1 The architecture of credibility analysis system

Hereafter the power cloud computing system according to the predefined service policies in the policy library provides differentiated services to these terminal users. Accordingly, we can succinctly achieve an effective terminal user security implementation in the dynamic complex cloud computing system environments.

B. SPA-based Analysis Algorithm

Considering the following two identity-discrepancy-contrary vectors:

$$\mu_1 = (a_1, b_1, c_1) \quad (3)$$

$$\mu_2 = (a_2, b_2, c_2) \quad (4)$$

the cosine of the angle θ between vector μ_1 and μ_2 can be defined as:

$$\cos \theta = \frac{[\mu_1, \mu_2]}{\|\mu_1\| \|\mu_2\|} \quad (5)$$

where $[\mu_1, \mu_2] = a_1 a_2 + b_1 b_2 + c_1 c_2$ ($\mu_1 \neq 0, \mu_2 \neq 0$) is the inner product of vector μ_1 and μ_2 . The norm of vector μ_i ($i = 1, 2$) can be calculated by the following formula:

$$\|\mu_i\| = \sqrt{a_i^2 + b_i^2 + c_i^2} \quad (6)$$

According to the above definition, the cosine of the angle θ reflects the closeness of the two identity-discrepancy-contrary vectors. Obviously, the difference between these two vectors is smaller and the similarity is larger if the cosine of the angle θ is larger. Conversely, the difference between these two vectors is larger and the similarity is smaller if the cosine of the angle θ is smaller.

Therefore, the credibility analysis algorithm of power cloud terminal user based on SPA can be described as follows:

- Select the attributes set of terminal user. Generally speaking, we give a superior or inferior judgment conclusion to an object depending on the preset criteria. These criteria must be able to reflect the pros and cons of objects to be judged and these changes that may exist. Therefore, there is no fixed judgment standard. Generally, we select terminal user attributes set based on the practical application scenarios.
- Determine attribute weight coefficient. For an object to be judged, its attributes have different importance in the evaluation process and different role in the evaluation results. So, we use the weight coefficient to represent the importance of various attribute in the judgment process.
- Preset the ideal attribute set according to application scenario. The so-called ideal attribute refers to the optimum attribute set of these objects to be judged. The ideal attribute set can be obtained by manually setting or by mathematical calculation using certain algorithms.
- Execute attribute aggregation. Based on the identity-discrepancy-contrary vector multiplication algorithm of the set pair analysis theory, we aggregate multi-attributes selected in step (1) according to the attribute

weight coefficient determined in step (2) so as to obtain the whole identity-discrepancy-contrary vector.

- Calculate the similarity between actual vector and ideal vector. We calculate the cosine of the angle between the whole identity-discrepancy-contrary vector and the preset ideal attribute vector in step (3), and obtain the vector similarity to perform the final judgment decision.

IV. CASE STUDY

The grid information system is a huge collection of various power information services involving very complex users. These existing power clouds are usually running on top of closed information systems within power enterprises. In the future, the trend of smart grid development requires open or semi-open mode to build the power cloud. So, this requires cloud management center to provide effective security mechanism to ensure the safety of the power cloud computing service system.

We use the credibility analysis of power cloud terminal users based on SPA theory to provide a security assurance measure in the complex dynamic service environment.

Provide we have known that in credibility level 1, the application history identity-discrepancy-contrary vector is $\mu_{11} = 0.9 + 0.06i + 0.04j$, the user qualifications vector is $\mu_{12} = 0.8 + 0.1i + 0.1j$, the application task vector is $\mu_{13} = 0.7 + 0.2i + 0.1j$. According to the multiplication rules of SPA, we can have the contact degree of credibility 1:

$$\begin{aligned}\mu_1 &= \mu_{11} \cdot \mu_{12} \cdot \mu_{13} \\ &= (0.9 + 0.06i + 0.04j) \cdot (0.8 + 0.1i + 0.1j) \cdot (0.7 + 0.2i + 0.1j) \\ &= 0.5 + 0.3i + 0.2j\end{aligned}$$

Similarly, in credibility 2, the application history identity-discrepancy-contrary vector is $\mu_{21} = 0.5 + 0.3i + 0.2j$, the user qualifications vector is $\mu_{22} = 0.6 + 0.3i + 0.1j$, the application task vector is $\mu_{23} = 0.4 + 0.4i + 0.2j$, we can have the contact degree of credibility 2:

$$\begin{aligned}\mu_2 &= \mu_{21} \cdot \mu_{22} \cdot \mu_{23} \\ &= (0.5 + 0.3i + 0.2j) \cdot (0.6 + 0.3i + 0.1j) \cdot (0.4 + 0.4i + 0.2j) \\ &= 0.1 + 0.7i + 0.2j\end{aligned}$$

In the power cloud computing system, when a terminal user applies for system services, we first examine three indicators: the application history, the user qualifications and the application task.

To describe our approach, assuming the application history identity-discrepancy-contrary vector of the power cloud terminal user is $\mu_{01} = 0.5 + 0.2i + 0.3j$, the user qualifications vector is $\mu_{02} = 0.7 + 0.1i + 0.2j$, the application task vector

is $\mu_{03} = 0.6 + 0.2i + 0.2j$, we can have the contact degree of the terminal user:

$$\begin{aligned}\mu_0 &= \mu_{01} \cdot \mu_{02} \cdot \mu_{03} \\ &= (0.5 + 0.2i + 0.3j) \cdot (0.7 + 0.1i + 0.2j) \cdot (0.6 + 0.2i + 0.2j) \\ &= 0.2 + 0.4i + 0.4j\end{aligned}$$

Given $\mu_1 = (0.5, 0.3, 0.2)$, $\mu_2 = (0.1, 0.7, 0.2)$, $\mu_0 = (0.2, 0.4, 0.4)$, the cosine of the angle $\theta_{(1,0)}$ between vector μ_1 and μ_0 can be calculated as follows:

$$\cos \theta_{(1,0)} = \frac{[\mu_1, \mu_0]}{\|\mu_1\| \|\mu_0\|} = \frac{0.30}{0.37} = 0.81$$

Similarly, the cosine of the angle $\theta_{(2,0)}$ between vector μ_2 and μ_0 can be calculated as follows:

$$\cos \theta_{(2,0)} = \frac{[\mu_2, \mu_0]}{\|\mu_2\| \|\mu_0\|} = \frac{0.38}{0.55} = 0.69$$

Obviously, $\cos \theta_{(1,0)} > \cos \theta_{(2,0)}$, so we can conclude the terminal user in credibility level 1. Then the power cloud computing system provides appropriate services to the terminal user according to predefined policies.

V. CONCLUSIONS

The Construction of cloud computing system can integrate large-scale heterogeneous computing resources for solving the problems of grid information system in order to address the future challenges of the intelligent power system. But the application of cloud computing technology will bring about the power information system some risks and challenges.

Based on SPA theory, we present a convenient method for credibility analysis of power cloud terminal user so as to give the system certain ability to provide differentiated services according to the predefined service policies in the policy library. Through case study, we demonstrate the effectiveness and simplicity of the method. In the subsequent research, we will consider the time-varying factors in the credibility dynamic analysis based SPA theory.

REFERENCES

- [1] Frederico Durao, Jose Fernando S. Carvalho, Anderson Fonseca, et al. A systematic review on cloud computing. *The Journal of Supercomputing*, 2014, 68(3): 1321-1346.
- [2] David C. Chou. Cloud computing: A value creation model. *Computer Standards & Interfaces*, 2015, 38: 72-77.
- [3] Dragan S. Markovic, Dejan Zivkovic, Irina Branovic, et al. Smart power grid and cloud computing. *Renewable & Sustainable Energy Reviews*, 2013, 24(10): 566-577.
- [4] Lianshun Mu, Lizhong Cui, Ning An. Research and practice of cloud computing center for power system. *Power System Technology*, 2011, 35(6): 171-175.
- [5] Rabia Latif, Haider Abbas, Saïd Assar et al. Cloud computing risk assessment: A systematic literature review, *Future Information*

- Technology, Lecture Notes in Electrical Engineering, 2014, 276: 285-295
- [6] Keqing Zhao. Set pair analysis and its preliminary application. *Exploration of Nature*, 1994, (1): 67-72.
- [7] Yunliang Jiang, Congfu Xu. Advances in set pair analysis theory and its applications. *Computer Science*, 2006, 33(1): 205-209.
- [8] Jingjing Xue, Lei Shen, Litao Liu, et al. Energy supply security assessment of China and the influencing factors based on set pair analysis. *Geographical Research*, 2014, 33: 842-852.
- [9] Qiang Zou, Jianzhong Zhou, Chao Zhou, et al. Comprehensive flood risk assessment based on set pair analysis-variable fuzzy sets model and fuzzy AHP. *Stochastic Environmental Research & Risk Assessment*, 2012, 27(2): 525-546.
- [10] Wei Wu, Yanying Wei. Land Ecological Security Assessment of Yangzhou Municipal City--the Fuzzy Set Pair Analysis Method. *Journal of Shanxi Agricultural Sciences*, 2013, 41(6): 582-589.
- [11] Meirong Su, Zhifeng Yang, Bin Chen. Set pair analysis for urban ecosystem health assessment. *Communications in Nonlinear Science and Numerical Simulation*, 2009, 14: 1773-1780.