EPiC Series in Computing

Volume 58, 2019, Pages 378–386

Proceedings of 34th International Conference on Computers and Their Applications

User Behavior and Trust Evaluation in Cloud Computing

Maryam Alruwaythi, Krishna Kambampaty and Kendall E. Nygard
Department of Computer Science
North Dakota State University, Fargo, ND, USA.
{maryam.alruwaythi, k.kambampaty,kendall.nygard@ndsu.edu}

Abstract

Cloud computing helps organizations to dynamically increase the resource needs as and when needed, without the need to purchase them. Security is a basic concern in cloud computing, and threats can occur both internally and externally. Users can access the cloud infrastructure for software, operating system and network infrastructure provided by the Cloud Service Providers (CSP). Evaluating the user behavior in the cloud computing infrastructure is becoming more and more important for both Cloud Users (CSs) as well as Cloud Service Providers The CSPs must ensure the safety of users accessing the cloud. Since user authentication alone is not enough to ensure the safety of users, user behavior trust plays a critical role in ensuring the authenticity of the user as well as safety. In this paper, we present the importance of user behavior in modeling trust, associated evaluation principles and comparison between different trust models.

1 Introduction

Cloud computing architecture provides computing services through the internet on-demand access to a pool of shared resources such as storage, servers, services and applications without physically acquiring them. The cloud computing has become one of the major trends and many industries such as healthcare, banking, education [1][2] etc. are moving towards it.

Cloud computing has three kinds of cloud service models: Infrastructure as a Service(IaaS), Platform as a Service(PaaS), and Software as a Service(SaaS). Figure 1 shows the basic structure of the cloud computing model. The model is comprised of five levels. They are the user professional service provider, information and transportation, cloud service provider and resource provide layers.

2 User Trust Requirements in Cloud Computing

In the cloud computing environment, users can directly access various cloud resources provided by Cloud Service Providers (CSP). User(s) with malicious intent can affect and/or destroy software and hardware resources in the cloud. The damage can occur from a variety of sources like competitors, hackers, etc. For example, in the PaaS service, user can develop and deploy a program to the cloud servers. The malicious user may submit code which attacks other users, occupy CPU time, memory space and other resources [3].

In a cloud environment, the traditional way of authorization is not enough for many reasons. User identity could be stolen, user may behave maliciously to destroy cloud servers or other resources on the cloud. To enhance the security in the cloud computing, user behavior trust plays an essential role.

The remainder of this paper is organized as follows: Section 3 states the principles for evaluating user behavior. Section 4 describes user behavior trust evidence. Section 5 describes the existing models for evaluating user. The Conclusion is in Section 6.

3 Principles for Evaluating User Behavior

In this section, we present the principles which should be considered while modeling user behavior in cloud computing. The following are the overarching principles:

A. The expired user behavior should not be considered. When the behavior recodes are out of date and very old, this implies that the user stopped accessing the cloud or has not accessed in recently. The user should then be evaluated as a strange user.

B. Recent user behaviors affect the trust value:

New behavior must play more important role and affect the trust evaluation more than long-term behavior. This is because in trust calculation, we consider the most recent behavior.

C. Abnormal behavior plays an important role in trust evaluation beyond traditional behavior.

D. Trust evaluation is based on a large user behavior data:

Creditability of trust value is based on a large number of historical users behaviors. The number of users accessing the cloud should be large to ensure that the result is stable. However, if the numbers are small, then the result is not representative and is unstable.

E. Slow –rise strategy to prevent fraud risk in trust evaluation

This strategy is based on a large number of users accessing cloud resources to achieve accurate trust value. This principle prevents users in gaining high trust value when users have a small number of available resources.

F. Punish non-trust user based on Rapid-Decline Strategy:

This strategy punishes user when abnormal behavior is detected. Punishment decreases the trust value quickly.

G. Trust value will decrease whenever repeated malicious behaviors have occurred:

Repeated malicious behavior decreases the trust value more rapidly than the first occurrence.

4 Obtaining Evidence of User Behavior Trust

Different types of evidence should be considered when modeling user behavior in cloud computing, each described below.

A. Security Evidence

Security evidence presents cloud user's characteristics while utilizing the cloud resources. These evidences are recorded in the user's log file. Some of them are:

i. Scanning of an important port
ii. Traces of viruses
iii. Any unauthorized connections
iv. Whether user Input Security Sensitive keywords
v. Usage of proxy

B. Login

Evidences of user log files are recorded which could represent user's login characteristics. These files assist in tracking user's behavior to prevent any kind of damage to the cloud services and resources.

i. Username and password validation
ii. Number of unsuccessful login attempts and if it exceeded the set limit
iii. Did the login session get created during user's usual activity timeframe.
iv. Login detection of unusual IP address

C. Operation

Operating evidence presents the user's operating characteristics such as:

i. Time spent by the user on the cloud
ii. Functionalities usually used
iii. Usually operation time on the cloud
iv. Frequency of usage
v. Data usage
vi. Usage of other user's account
vii. Any data definition or manipulation performed under different user's account

D. Reliability

Reliability evidence presents user's reliability characteristics. These are recorded on user's log file and they are:

i. Data error rate
ii. IP packet loss rate
iii. Connection establishment failure rate

E. Performance

Users with low performance metric can throttle on resources preventing the usage from other users. Some of the performance characteristics recorded are:

i. CPU and memory occupancy rate
ii. IP transmission delay
iii. Bandwidth occupancy rate
iv. IP packet response time attempt

5 User Behavior Evaluation Models

A. AHP Based Evaluation

There is considerable research which use the Analytic Hierarchy Process (AHP) to build a user evaluation model. AHP is an analysis method for decision science ("divide and treat") based on the hierarchical structure model.

In AHP model, trust evaluation is divided into three levels, the Target layer, Property layer and the Evidence. Figure 1 shows the three different layers. The evidence weight is calculated by comparing each evidence. This value is multiplied with evidence value to obtain user's trust value.

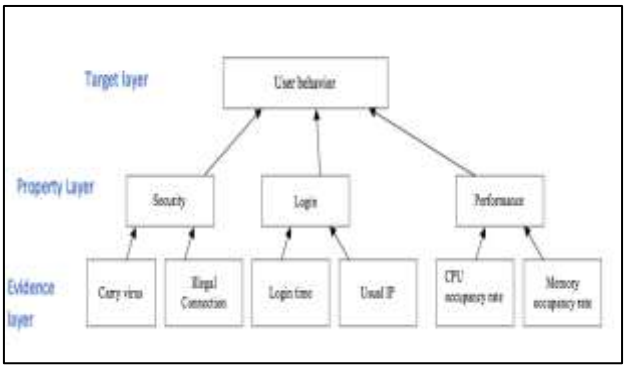

Figure 1: AHP Method

Jun-Jian [4] proposed a dynamic trust evaluation model to evaluate user behavior by combining two methods, entropy with objective weights and AHP with acquired subjective weight.

The advantage with this model is, it can balance between objective and subjective weights to calculate user's trust value. It also calculates which user has consumed the largest amount of resources. This model however has some drawbacks. It does not consider the expiration of trust records, repeated abnormal behavior and recent behavioral changes. In addition, this model does not consider the fraud risk problem. Malicious users obtaining a high trust value with in a short term cannot be prevented using this system

Junfeng et. al. [5] proposed a cloud user behavior authentication model based on multi-partite graphs. This model has three layers: user behavior evidence layer, building behavior multi-partite graphs and behavior authentication layer. This model is a combination of AHP and Graph theory. In addition, they added Identity re-certification and Risk Game to identify malicious users. This enhances authenticity of users and improves the security. This model can distinguish between a malicious and risk user. A malicious user behaves abnormally most of the time, while a risk user behaves abnormally some times. Finally, this model reflects upon the time impact principle.

This model has the similar disadvantages as model in proposed by Jun-Jian.

Lin, Want, Bie and Lei [6], proposed a new model called Mutual Trust-Based Access Control Model (MTBAC) This model has two parts. The first part is to evaluate user behavior using AHP. The second part is to evaluate cloud service provider by applying Ant Colony Algorithm (ACA). In this model, according to the user behavior trust value and CSP's creditability, it assigns multiple users to multiple available CSP. This model solves the trust uncertainty problem.

However, this model does not address the evaluation principles. Thus, the user behavior pattern and trust are not calculated. In addition, this model cannot prevent high trust value for the malicious users.

Ma and Zhang [7], proposed a new method based on Improved AHP method. This model takes into account, the expiration trust record considering three interaction ranges: positive, negative and uncertain. Negative range implies that the behavior is far from current time and should not be included in the trust calculation. Uncertain range means that the record contains uncertain weights in trust calculation. Behavior in Positive range suggests that it is a new behavior and has a high weight in trust calculation. This model applies the time factor and trust fraud risk through the slow-rise and punishment strategy. However, this proposed model fails to evaluate repeated abnormal behavior.

B. Fuzzy Mathematics Based Evaluation of Strategy

Yang et all [8], proposed a model based on the multi-level fuzzy comprehensive evaluation which is a combination of quantitative and qualitative evaluation model. They used AHP method and fuzzy comprehensive evaluation (FCE). This model evaluates the time impact principle which is the number of times user(s) connects with the cloud.

This proposed model doesn't reflect on expiration trust record, repeated abnormal behavior and recent behavior. In addition, this model does not consider fraud risk problem.

Yang [9], suggested a model based on Fuzzy Mathematics theory in Cloud Computing. By using fuzzy mathematics theory, the subjectivity of trust evaluation is reduced. This model combines direct and indirect trust to calculate user's trust value. The direct trust is obtained from local domain and recommendation from the cloud provider. The indirect trust value is obtained from the other cloud service providers.

This model considers the user's trust value from multiple cloud service providers. To prevent the high influence from the indirect trust, different weights have been assigned for direct trust and indirect trust. model doesn't consider expiration of trust records, repeated abnormal behavior, recent behavior and fraud risk problem.

Jaiganesh et. al. [10], proposed a system which used Fuzzy Adoptive Resonance Theory (ART) and Neuro-Fuzzy Techniques. In Fuzzy ART technique, memory, Giga Floating Operation per Second (GELOPS), Disk Space for each virtual client as input factors have been used. Unsupervised learning method is used to train and test the virtual clients. The output classes use fuzzy inference rule.

This model can classify users into four categories namely, Secure, Vulnerable, Modified and Anomaly based on the usage of resources (Memory, GELOPS, and Disk Space) which means this system is able to distinguish between Secure and Anonymous user. This model reflects the time impact principle.

This model doesn't take into account the expiration trust records, repeated abnormal behavior, recent behavior and fraud risk problem

Xiaoxue [11], proposed Reward and Punishment Trust Model (RPTM) to calculate trust value for the user. This model is based on two types of trust: recommendation trust from other users, and user's historical transactions.

RPTM model considers the recommendation trust and applies fraud risk through punishment strategy. This model is effectively able to differentiate between genuine and malicious user. This model considers the time impact principle.

This model doesn't consider the trust record, repeated abnormal behaviors and recent behaviors. In addition, this model is based on one evidence which if the user uses the document successfully on the cloud server.

Berrached, Ali and Korvin [12], proposed a fuzzy algorithm for reinforcing access control based on the history of user behaviors, data being accessed in the cloud and the amount of damage that cloud can tolerate. This model uses different evidences to evaluate user and compute the amount of damage that the cloud can accept.

One of the drawbacks is, this model doesn't consider any of the evaluation principles.

C. Role-Based Access Control Based Evaluation Strategy

Yang et. al. [13], proposed a model which incorporates a role-based access control with user behavior trust. They proposed a multiple context to evaluate the user behavior. This model can provide scalable and flexible authorization strategy. It utilizes multiple contexts in trust evaluation and different trust evaluation methods.

However this model doesn't consider any of the evaluation principles. It is too complex to practice in the cloud computing environment and doesn't have a specific measurement of trust.

Deng and Zhou [14], proposed a Flexible Role Based on Access Control (FRBAC) model. In this model, there is a usage of direct trust between the cloud user (CU) and the Cloud service provider (CSP) based on user's behavior. In addition, they use recommendation trust from other CSP nodes. By combining direct trust and recommended trust, the model produces user trust value. FRBAC model uses AIMD (Additive-Increase, Multiple-decrease) algorithm to punish malicious user. Recommended trust is factored in this model. In addition, by using AIMD algorithm fraud can be identified. It also considers the time impact principle as well.

This model however doesn't consider the expiration trust record, repeated abnormal behavior and recent behavior. In addition, this model does not prevent synergies cheating in recommendation trust.

Xu [15], proposed User Behavior Assessment Based Dynamic Access Control Model (UBADAC). This model has three parts. First, calculating user behavior risk value which based on threat behavior. Secondly, user trust value is calculated based on the risk value of user behavior. Finally, mapping the trust value of user with permission. This value determines the access rights to the cloud resources. This model can calculate the risk value for user behavior based on the assets value, vulnerability degree and threat for each resource in the cloud. It then calculates user trust value based on the risk value. This model takes into account some of the evaluation principles such as time impact and repeated abnormal behavior principles.

However, this model doesn't consider the expiration trust record, repeated abnormal behavior, recent behavior and fraud risk problem.

D. Other Evaluation Strategies

Alguliev et. al. [16] proposed a system to detect masquerader in the cloud computing environment. This system has two phases: creating user's profile phase and detecting phase. Creating phase consists of two components. In the first phase user event log is recorded and feature extraction is done. In the profile creating phase, three values were used (expectation Ex, entropy En and excess entropy). In the detection phase, cosine similarity method has been used to compare a normal behavior with new behavior. Collaborative filtering method evaluates any deviation from the normal behavior. This model is simple to model and can very well detect the masquerader user.

Drawbacks of this model are that it doesn't identify the actual behavior pattern and behavior trust.

Kalaskar and Gayatri have proposed a system which combines two technologies. One is user profiling technology to monitor user behavior and secondly to distinguish between real and fake user. User profile technology is based on those evidences which have been mentioned in the evidence section.

The advantage of this system is, it combines two techniques which can provide enhanced security in the cloud. In addition, this system is able to detect fake user and send bogus data without the knowledge of the fake user. However, this model doesn't consider any of the evaluation principles.

Chen et all [18] proposed a trust evaluation model based on the user behavior data. In this model, authors have come up with a set of trusted behaviors of the cloud user from data and set weight for each behavior's category which will use to calculate direct trust. In addition, recommendation trust is

calculated based on the interaction between the user and other users on the cloud. Then by giving the historical trust value, comprehensive trust is calculated which is based on the direct, recommended, and historical trust. This model considers expiration of trust records, time impact and fraud risk problem. However, it does not consider repeated abnormal behavior.

Reena [19] proposed a system which uses two technologies. First, user behavior profiling to compute user trust value. User profiling is based on how, when, and how much user accesses information. The Second technique is decoy technology which is used to download decoy file to the untrusted user instead of a genuine file. This system can detect abnormal user access and create decoy files by scrambling content of the genuine file. This system fails in all the evaluation principles

Table 1 provides a taxonomy of the principles that apply for trust measurement.

REFERNCE NUMBER	*PRINCIPLES*	*EVIDENCES USED*
4	The time impact	Security Evidence: Illegal connection, Using proxy, security sensitive keywords. Performance Evidence: CPU occupancy rate Login Evidence: Login time Reliability Evidence: User IP packet loss rate
5	The time impact	Operation Evidence: Operation time Performance Evidence: User's IP transmission delay Reliability Evidence: User IP packet loss rate
6		Security Evidence: Illegal connection Login Evidence: Exceed authority attempt Reliability Evidence: User data error rate, Connection establishment failure rate
7	The time impact, and trust fraud risk through slow rise and punishment strategy.	Security Evidence: Illegal connection, Number of carrying virus Performance Evidence: CPU occupancy rate, Bandwidth utilization Reliability Evidence:User data error rate
8	The Time impact	Login Evidence: Login Certification, Login path, IP address,login time Operation Evidence: Common function, duration operation, operation time, Data volume
9		Login Evidence: Exceed authority attempt. Reliability Evidence:User data error rate, Connection establishment failure rate
10	The Time impact	Performance Evidence: CPU occupancy rate Memory occupancy rate
11	The time impact and trust fraud risk	Operation Evidence: Download files.
12		Login Evidence: Login Certification Login path, IP address,login time

13		Login Evidence: Login Certification, Login path, IP address, login time
14	The time impact, and trust fraud risk	Login Evidence: Exceed authority attempt. Performance Evidence: User's storage resource occupancy rate Reliability Evidence: User IP packet loss rate
15	The time impact, Repeat abnormal behavior	Operation Evidence: User Method to deal with cloud resource
16		Operation Evidence: Common operation
17		Operation Evidence: Common function, duration operation, operation time, data volume
18	The expiration trust record, time impact and fraud risk problem	Login Evidence : Login certification, IP address, login time Operation Evidence: Retrieve files, upload files, search
19		Login Evidence: Login Certification, IP address, login time Operation Evidence: Common function, duration operation, operation time, data volume

Table 1. Trust Principles

6 Conclusion

In the world of cloud computing, an attacker could hide as a legitimate user by stealing a user's identity or the user himself could behave abnormally to destroy cloud resources. So, it is important to evaluate the user behavior and compute trust value for the cloud user to improve security in the cloud. In this paper, we presented the importance of evaluating user behavior in the cloud, principle to evaluate user, evidence to use to evaluate user. Finally, we presented the existing models to evaluate user behavior. In the future research, we will implement a model that considers the principles and evidences to improve security in the cloud.

References

[1] Rabi Prasad Padhy.P, Rabi et al. "Cloud Computing: Security Issues and Research Challenges". International Journal of Computer Science and Information Technology & Security,2011

[2] S.giri, Mahesh, et al. "A Survey on Data Integrity Techniques in Cloud Computing." International Journal of Computer Applications, vol. 122, no. 2, 2015, pp. 27–32., doi:10.5120/21674-4762.

[3] Tian, Li-Qin, et al. "Evaluation of User Behavior Trust in Cloud Computing." 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), 2010, doi:10.1109/iccasm.2010.5620636.

[4] Jun-Jian, Li, and Tian Li-Qin. "Users Behavior Trust Evaluate Algorithm Based on Cloud Model." 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), 2015, doi:10.1109/imccc.2015.123.

[5] Junfeng, Tian, and Cao Xun. "A Cloud User Behavior Authentication Model Based on Multi-Partite Graphs." Third International Conference on Innovative Computing Technology (INTECH 2013), 2013, doi:10.1109/intech.2013.6653686.

[6] G. Lin, D. Wang, Y. Bie, and M. Lei, "MTBAC: A mutual trust based access control model in cloud computing," Communications, China, vol. 11, no. 4, pp. 154–162, 2014.

[7] J. Ma and Y. Zhang, "Research on Trusted Evaluation Method of User Behavior Based on AHP Algorithm," in 2015 7th International Conference on Information Technology in Medicine and Education (ITME), 2015, pp. 588–592.

[8] Yang, Ruilan, and Xuejun Yu. "Research on Way of Evaluating Cloud End User Behaviors Credibility Based on the Methodology of Multilevel Fuzzy Comprehensive Evaluation." Proceedings of the 6th International Conference on Software and Computer Applications - ICSCA 17, 2017, doi:10.1145/3056662.3056677.

[9] A. Mohsenzadeh, H. Motameni, and M. J. Er, "A New Trust Evaluation Algorithm between Cloud Entities Based on Fuzzy Mathematics," International Journal of Fuzzy Systems, pp. 1–14, 2015.

[10] Jaiganesh, M., et al. "Neuro Fuzzy ART-Based User Behavior Trust in Cloud Computing." Asian Journal of Information Technology, 2016,ISSN:1682-3915.

[11] Xiaoxue, Ma, et al. "Trust Model Based on Rewards and Punishment Mechanism." 2010 Second International Workshop on Education Technology and Computer Science, 2010, doi:10.1109/etcs.2010.337.

[12] Berrached, Ali, and A. D. Korvin. "Reinforcing Access Control Using Fuzzy Relation Equations." International Conference on Security &Management, Sam 2006, Las Vegas, Nevada, Usa, June DBLP, 2006:489-493.

[13] Yang, Ran, et al. "Trust Based Access Control in Infrastructure-Centric Environment." 2011 IEEE International Conference on Communications (ICC), 2011, doi:10.1109/icc.2011.5963329.

[14] W. Deng and Z. Zhou, "A Flexible RBAC Model Based on Trust in Open System," in Intelligent Systems (GCIS), 2012 Third Global Congress on, 2012, pp. 400–404.

[15] Jing, Xu, et al. "A Cloud-User Behavior Assessment Based Dynamic Access Control Model." SpringerLink, Humana Press, 22 Dec. 2015, link.springer.com/article/10.1007/s13198-015-0411-1.

[16] Alguliev,R and Abdullaeva ,F. "User Profiles and Identifying User Behavior in the Cloud Computing Environment." Universal Journal of Communications and Network 2(5): 87-92, 2014, doi: 10.13189/ujcn.2014.020501.

[17] Kalaskar, Gayatri, et al. "FOG Computing: Preventing Insider Data Theft Attacks in Cloud Using User Behavior Profiling and Decoy Information Technology." International Journal of Engineering Trends and Technology, vol. 32, no. 7, 2016, pp. 352–355., doi:10.14445/22315381/ijett-v32p266.

[18] Chen, Zhenguo, et al. "Trust Evaluation Model of Cloud User Based on Behavior Data." International Journal of Distributed Sensor Networks, vol. 14, no. 5, 2018, p. 155014771877692., doi:10.1177/1550147718776924.

[19] Reena, K.m., et al. "Security Implementation in Cloud Computing Using User Behaviour Profiling and Decoy Technology." 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), 2017, doi:10.1109/icicct.2017.7975242.