Bayesian Network-Based User Behavior Authentication Method for Remote Sensing Clouds: Postprint

Authors: Cheng Luxiao, Yan Jining, Jiao Yang, Ma Yan, Wang Yuzhu

Date: 2018-05-20T00:00:00+00:00

Abstract

Aiming at the intrusion phenomena of untrusted users in remote sensing cloud service platforms, this paper proposes a user behavior authentication scheme that combines the characteristics of remote sensing cloud user behavior with Bayesian network algorithms. The scheme discusses the behavior authentication mechanism for remote sensing cloud platform users and establishes a user behavior authentication set based on user behavior characteristics. By integrating the prediction features of Bayesian network algorithms and user behavior attributes, a Bayesian network model for authentication level prediction is constructed. The weight information of user behavior attributes derived from the model analysis is applied to the user level prediction algorithm, thereby enhancing the algorithm' s security and accuracy for remote sensing cloud user authentication and enabling prediction of user behavior authentication levels. Simulation results demonstrate that this method can accurately identify untrusted users and effectively ensure the security of remote sensing cloud service platforms.

Full Text

Bayesian Network Method for Remote Sensing Cloud User Behavior Authentication

Cheng Luxiao[1], Yan Jining[2], Jiao Yang[1], Ma Yan[3]†, Wang Yuzhu
[1]School of Information Science & Engineering, Yanshan University, Qinhuangdao Hebei 066004, China [2]School of Computer Science, China University of Geosciences, Wuhan 430074, China [3]Institute of Remote Sensing & Digital Earth, Chinese Academy of Sciences, Beijing 100094, China School of Information Engineering, China University of Geosciences, Beijing 100083, China

Abstract

Addressing the intrusion of untrusted users in remote sensing cloud platforms, this paper designs a user behavior authentication scheme that integrates characteristics of remote sensing cloud user behavior with Bayesian network algorithms. The scheme elaborates on the user behavior authentication mechanism for remote sensing cloud platforms and establishes a user behavior authentication set based on user behavior characteristics. By combining the predictive features of Bayesian network algorithms with user behavior attributes, a Bayesian network model is constructed for authentication level prediction. The weight information of user behavior attributes derived from this model is then applied to the user level prediction algorithm, making the algorithm more secure and accurate for remote sensing cloud user authentication, thereby enabling prediction of user behavior authentication levels. Simulation results demonstrate that this method can accurately identify untrusted users and effectively ensure the security of remote sensing cloud service platforms.

Keywords: user behavior authentication; Bayesian network; remote sensing cloud platform; behavior analysis; cloud computing

0 Introduction

While enjoying the high efficiency and low cost brought by cloud computing, users also face severe information security challenges. Remote sensing cloud service platforms, built upon cloud computing technology, package remote sensing data, information products, processing algorithms, and computing resources into metered services. Users can obtain corresponding application and service resources according to their personal needs and preferences through the network [1], primarily including multi-source remote sensing data distribution and sharing, high-performance data processing and product generation, cloud storage, and remote sensing computing platform provisioning. However, since users directly operate the software environment, network infrastructure, and computing platforms provided by cloud service providers, attackers' impact and damage on cloud resources and software/hardware are far more severe than resource sharing via the Internet. For example, in IaaS (Infrastructure as a Service), the service provider offers a shared facility containing components and functions such as storage, operating systems, and servers that are not completely isolated for system users. When attacked, all servers become transparent to the attacker [2]. Similarly, when users access cloud storage services, they must first undergo identity authentication to ensure the correctness and legitimacy of the accessing user. Only through secure and correct user identity authentication can we ensure that subsequent access to and use of remote sensing cloud services are by legitimate users. However, legitimate logged-in users are not necessarily secure users. Therefore, whether user behavior is trustworthy and how to evaluate and predict the credibility of cloud users constitute important content for ensuring cloud computing security today.

In cloud computing application domains, many scholars have studied the application of user behavior trust evaluation methods. For instance, reference [3] proposes a game control mechanism for behavior trust prediction, which first uses Bayesian networks to predict user behavior trust and then derives a Nash equilibrium strategy by combining prediction results with game analysis. Reference [4] presents a method for evaluating trust levels based on user behavior and platform environment characteristics. Reference [5] introduces a cloud security authentication service mechanism based on dynamic trust management, combining PKI technology with dynamic trust management methods to achieve secure authentication in cloud environments. Reference [6] proposes an identity authentication method based on user mouse behavior, employing a hierarchical classification decision model for user identity authentication. However, these authentication mechanisms cannot be tailored to a specific cloud computing service platform. While these models partially solve user trust and evaluation issues in different application contexts, their training set extraction is highly specific, resulting in a lack of flexible trust evaluation mechanisms that cannot accommodate the personalized characteristics required for user behavior assessment in different domains.

To ensure the security of remote sensing cloud service platforms, in addition to deploying firewalls at the resource layer and monitoring virtual computing clusters at the computing layer, user behavior feature monitoring is also required above the business layer. This paper addresses remote sensing cloud service platform user behavior characteristics by proposing a user behavior authentication method based on a Bayesian network model, combining traditional identity authentication with behavior authentication mechanisms.

1 Remote Sensing Cloud Service Platform

For any specific system or service platform, each user' s behavioral state and operational habits follow certain patterns. For example, reasonable behavior trajectories in remote sensing cloud platforms include standard remote sensing data and product retrieval, browsing, ordering, downloading, and transferring [9], followed by utilizing the high-performance remote sensing data processing and product generation platform for online data processing and product generation, or customizing personal remote sensing virtual computing environments for data processing, with final results stored in personal cloud storage. When user behavior anomalies occur, user behavior authentication is required, and service is denied if authentication fails.

The remote sensing cloud service platform integrates various remote sensing information and technical resources based on cloud computing technology, providing one-stop spatial information cloud services to users through the network by packaging remote sensing data, information products, application software, and computing and storage resources as public service facilities. Developed on the OpenStack cloud computing framework, the platform architecture consists of five layers from bottom to top: resource layer, management layer, comput-

ing layer, business layer, and service layer, as shown in [Figure 1: see original paper].

The resource layer constructs virtualized resource pools by connecting numerous computing, network, and storage resources via network, forming virtual resources such as virtual CPUs, virtual memory, virtual disks, virtual object storage spaces, and virtual networks that can be uniformly managed within the remote sensing cloud system. The management layer primarily adopts the OpenStack computing framework, utilizing its core components to manage virtual resources. The computing layer provides virtual cluster computing environments, including massive remote sensing data storage, cluster computing and scheduling, and computing environment monitoring services. The business layer mainly comprises multi-center remote sensing data management and high-performance computing platforms for remote sensing data processing and product generation. Additionally, based on SaltStack management tools, automatic deployment and system scaling of virtual computing environments can be achieved. The service layer provides users with services including remote sensing data services, information product services, remote sensing data processing services, cloud platform services, and cloud storage services. Remote sensing data services refer to the collection, storage, retrieval, and download of multi-source remote sensing data; information product services refer to the production and distribution of remote sensing information products [7]; remote sensing data processing services, based on MPI parallel computing mechanisms, can achieve high-performance online processing of massive remote sensing data according to user-submitted processing requirements and can scale computing resources based on task volume; cloud platform services are responsible for creating virtual computing resources and customizing remote sensing computing template instances or personalized instances according to user requirements for virtual remote sensing computing environments; cloud storage services primarily meet the needs of remote sensing cloud data storage and enable dynamic scaling of personal cloud storage based on demand.

[Figure 2: see original paper] shows the main interface of the final implemented remote sensing cloud prototype system.

2 User Behavior Authentication Scheme

User behavior authentication comprises two components: identity authentication and behavior authentication. Based on the personalized behavior characteristics of remote sensing cloud users, a more fine-grained behavior trust authentication scheme is designed. The design concept involves extracting user behavior data information by combining server logs with client data, including obtaining user browsing and ordering data and service information through Web logs, and acquiring user browsing behavior records on the remote sensing cloud platform through server logs. When users submit system access requests, they must first undergo identity authentication. If identity authentication fails, service is directly denied. If identity authentication succeeds, the process enters

the behavior authentication phase. Behavior authentication refers to the server obtaining real-time user behavior evidence and matching it against the behavior authentication set stored in the database [8]. During behavior authentication, the system locates specific behavior authentication sets based on behavior evidence and calculates the trust level of each behavior authentication set using Bayesian networks combined with real-time behavior evidence. Finally, the user behavior trust level is calculated based on a decision algorithm. [Figure 3: see original paper] illustrates the specific process of the remote sensing cloud service platform user behavior authentication scheme. The detailed steps are as follows:

a) When an end user sends a service request to the server, the behavior authentication mechanism first performs identity authentication. For users who pass identity authentication and are not first-time logins, access is granted and real-time behavior monitoring is implemented, proceeding to step b). For users who pass identity authentication but are first-time visitors to the cloud platform, authorized access is granted with enhanced behavior monitoring, proceeding to step d). For users who fail identity authentication, service access is denied.

b) Obtain user behavior state information and perform authentication based on the behavior state authentication set. Users who fail state authentication are denied access; those who pass are granted authorized access and proceed to step c).

c) Retrieve user historical behavior authentication information. If the historical behavior authentication status is "trusted," the user is allowed authorized access and real-time behavior monitoring is implemented, proceeding to step b). If the historical behavior authentication status is "generally trusted," the user enters a warning and prevention state, granted authorized access but subject to enhanced real-time behavior monitoring, proceeding to step d). If the historical behavior authentication status is "untrusted," access is denied.

d) Obtain real-time user behavior evidence to implement authentication of behavior content authentication sets and behavior habit authentication sets. Calculate the trust level of each behavior authentication set based on the Bayesian network model, and finally compute the user behavior trust level based on the decision method. If the result is "trusted" and the user continues accessing, proceed to step b). If the result is "trusted" or "generally trusted" and the user terminates access, proceed to step e). If the result is "generally trusted" and the user continues accessing, grant access with enhanced real-time behavior monitoring and proceed to step b). If the result is "untrusted," terminate user access. Update the user behavior authentication set and user historical trusted authentication status information.

e) Update the user behavior authentication set and user historical trusted authentication status information.

2.1 User Behavior Authentication Set

User behavior authentication sets have personalized characteristics and are crucial for ensuring authentication accuracy. Therefore, determining the behavior authentication set is one of the most important aspects of the behavior authentication process [9]. During authentication, real-time user behavior evidence must be obtained and compared with user behavior authentication sets. The probability of successful user behavior authentication depends on the division and definition of behavior authentication sets and the coverage rate of behavior-related sets.

The user behavior authentication set includes the following aspects: State Authentication set (SA), Content Authentication set (CA), and Habit Authentication set (HA). The State Authentication set comprises behavior attributes that trigger behavior state anomalies, such as sudden inconsistencies in user login location, client IP address, operating system version, and access time compared to historical behavior states. Both PaaS and SaaS layers require behavior state anomaly verification against operating system, IP address, and access time evidence attributes. Since the IaaS layer only provides infrastructure services, it does not require authentication of the client operating system evidence attribute. Behavior content primarily includes user resource usage, such as types and quantities of resources used. In different service models of cloud computing environments, resource content varies: at the IaaS layer it mainly refers to basic computing resources like processing, storage, and network; at the PaaS layer it refers to development environments like servers, operating systems, and middleware. Under normal circumstances, the quantity and type of resources used by end users do not change significantly. If substantial changes occur, user behavior may be abnormal and require authentication [10]. Particularly in the SaaS service model, different end users have different specific behavior content. Behavior habits mainly include frequently visited websites, habitual page references for entering resources, and habitual accessed resources.

2.2 User Behavior Authentication Process

The user behavior authentication process consists of three main phases:

a) Pre-behavior user identity authentication and behavior state authentication.

b) Real-time dynamic state authentication during behavior, including behavior state authentication, behavior content authentication, and behavior habit authentication.

c) Post-behavior evidence authentication set update in preparation for the next behavior authentication.

The user authentication mechanism is shown in [Figure 4: see original paper]. The specific steps are:

1) Obtain real-time user behavior through the client and transmit behavior evidence via the network to the user behavior authentication server;
2) The user behavior authentication server authenticates the captured user behavior;
3) Perform behavior authentication using behavior authentication sets on the server and return authentication results;
4) Return authentication results.

When users access the system, they first undergo identity authentication. If the user' s identity is untrusted, service is directly denied. If the user' s identity is trusted and it is not their first visit, the process enters the behavior authentication phase. If the user' s identity is trusted and it is their first visit, authorized access is granted with enhanced real-time behavior monitoring. Behavior authentication involves submitting real-time behavior evidence obtained from user-system interaction to the corresponding server, which matches the submitted behavior evidence against the user behavior authentication set stored in the database [10]. Based on the authentication results, the server determines whether user behavior is trustworthy. If the authentication result is trusted, information services are provided to the user; if untrusted, information services are denied.

3 User Behavior Trust Level Prediction

3.1 Bayesian Network Model for User Behavior Trust Prediction

User behavior trust prediction is based on historical interaction behavior evidence combined with current real-time behavior to predict user trust levels. A Bayesian network is a directed acyclic graph composed of nodes representing variables and directed edges connecting these nodes [11,13]. The Bayesian network for user behavior trust level prediction is constructed as shown in [Figure 5: see original paper], where variable nodes include the user behavior authentication sets to be predicted and their constituent behavior attribute sets. The behavior authentication sets include State Authentication set (SA), Content Authentication set (CA), and Habit Authentication set (HA). Child nodes of behavior authentication sets are corresponding user behavior attributes: for example, the State Authentication set SA includes client information, IP information, and login information; the Content Authentication set CA includes remote sensing data processing software usage types, quantity of downloaded remote sensing data, types of ordered remote sensing products, and types of ordered remote sensing virtual computing environments (agricultural thematic, forestry thematic, mineral thematic, ocean thematic, etc.); the Habit Authentication set HA includes frequently accessed remote sensing cloud service types, frequently downloaded remote sensing data or product types, frequently ordered remote sensing virtual computing environment types, and page references.

Bayesian networks can intuitively represent user behavior trust level prediction and user behavior attributes using directed graphs [3], while incorporating user

historical and real-time behavior statistics as conditional probabilities. This seamlessly combines prior knowledge with posterior data. Moreover, nodes in a Bayesian network influence each other, and changes in any node' s value affect other nodes, thereby satisfying the fine-grained combinatorial reasoning and prediction requirements for different needs.

3.2 Prior Probability of User Behavior Attribute Levels

When using Bayesian networks for user behavior authentication, prior probabilities of user behavior attributes must first be calculated. This paper divides user behavior trust T, behavior state SA, behavior content CA, behavior habit HA, and behavior attributes of each authentication set into L trust levels, assigning numbers i(i = 1,2,3···,L) from high to low. Array subscripts represent different value ranges, where Ti, SAi, CAi, HAi, and Si respectively represent the ranges of overall behavior trust, behavior state authentication set, behavior content authentication set, behavior habit authentication set, and behavior attributes. |Ti|, |SAi|, |CAi|, |HAi|, and |Si| respectively represent the number of times the predicted user' s interaction history values fall within the ranges of Ti, SAi, CAi, HAi, and Si. n represents the total number of interactions, while P(Ti), P(SAi), P(CAi), P(HAi), and P(Si) represent their probabilities. These symbols apply throughout the paper.

The prior probability calculation formula for user behavior authentication set levels is:

$$\sum_{i=1}^{L} P(T_i) = 1 \text{ and } \sum_{i=1}^{L} P(S_i) = 1$$

The prior probability of user behavior attribute set levels is calculated similarly to that of user behavior authentication set levels. The prior probability P(Si) of behavior attribute trust level is:

$$P(S_i) = \frac{|S_i|}{n}$$

3.3 Conditional Probability of Behavior Authentication Sets

In addition to prior probabilities, conditional probabilities of each behavior authentication set level are required. The conditional probability calculation formula is:

$$p(e|h) = \frac{p(e,h)}{p(h)}$$

which represents the probability of satisfying condition e given condition h. Taking p(Si|CAj) as an example, it represents the probability that a behavior at-

tribute node falls within range Si given that the behavior content authentication level is j. The calculation formula is:

$$p(S_i|CA_j) = \frac{|S_i \cap CA_j|}{|CA_j|}$$

Based on the prior probabilities and conditional probabilities obtained from the above calculation methods, the trust level probabilities of behavior authentication sets can be derived. Below, we predict the trust level of the behavior content authentication set under single behavior attribute conditions as an example; other behavior authentication set calculations are similar. The probability that the behavior content authentication level is i given that the behavior attribute node in the behavior content authentication set falls within range Sj is P(CAi|Sj). Using Bayes' formula:

$$P(CA_i|S_j) = \frac{P(S_j|CA_i)P(CA_i)}{\sum_{i=1}^{L} P(S_j|CA_i)P(CA_i)}$$

For multiple behavior attribute conditions, we use the prediction of behavior content authentication set as an example; other behavior authentication set trust level predictions are similar. Assume the behavior content authentication set contains four behavior attributes S1, S2, S3, and S4, falling within ranges S1j, S2k, S3m, and S4n respectively. The trust level prediction of behavior authentication set CA under the conditions of S1j, S2k, S3m, and S4n is calculated as:

$$p(CA_i|S_1, S_2, S_3, S_4) = \frac{|S_1 \cap S_2 \cap S_3 \cap S_4 \cap CA_i|/n}{|S_1 \cap S_2 \cap S_3 \cap S_4|/n}$$

3.4 Calculation Method for Behavior Trust Level

After calculating the trust level of each behavior authentication set, the weight information of each behavior authentication set is analyzed from the graphical Bayesian network. Finally, the user behavior trust level T is calculated using the polynomial calculation method:

$$T = \sum_{i=1}^{n} W_i C_i$$

where Ci represents the trust level of the ith behavior authentication set, and Wi represents the weight of the ith behavior authentication set.

4 Security Analysis of Authentication Method

Security is the most important issue in authentication methods. The security of this behavior authentication scheme is mainly reflected in two aspects: First, from the perspective of the entire authentication process, more specific strategies are provided for different situations. For users who pass identity authentication, behavior trust prediction is performed for each behavior request, and the user' s behavior request operation is denied if it exceeds the trusted range, ensuring authentication security from the process flow. Second, from the perspective of the authentication algorithm, the behavior attribute weight information analyzed through the Bayesian network model constructed from user behavior is combined with the Bayesian network algorithm, avoiding subjectivity and uncertainty in the algorithm and making it more targeted and secure for the platform. This enables more accurate prediction of malicious behavior users on remote sensing cloud platforms, ensuring the security of the entire authentication process.

5 Example and Analysis of User Behavior Trust Level Prediction

Based on the user behavior trust level prediction method proposed above, this section demonstrates the effectiveness of the prediction model through an example. According to 207 sets of interaction statistics between user U and the remote sensing cloud service platform, at a certain moment, user U requests to access server S. The model predicts the user' s behavior trust level under specific behavior attribute authentication set conditions. Behavior trust is divided into three levels: trusted, generally trusted, and untrusted. The behavior content trust level prediction process for this user is presented below, where the frequency of the user' s behavior evidence falling within different behavior attribute intervals (S1, S2, S3 representing three different behavior attributes) is shown in .

1) Calculation of Behavior Authentication Set Trust Level

Based on the user behavior interaction data information obtained above, prior probabilities of each node in the network can be calculated using the formula. The prior probabilities of behavior attribute nodes are shown in , and similarly, the conditional probability table of behavior authentication level node T is shown in . The conditional probability of each evidence attribute is then calculated using the formula to obtain the Conditional Probability Table (CPT) for each evidence attribute. With all nodes' prior probabilities and child nodes' conditional probabilities obtained, corresponding prior probabilities and conditional probabilities can be used for any set of observed values when calculating behavior authentication set trust level predictions. Substituting them into the formula yields all posterior probabilities, and the maximum probability value is taken as the trust level of each behavior authentication set.

2) Calculation of User Behavior Trust Level

According to the user behavior trust level prediction steps mentioned above, the Bayesian network model analysis yields the Bayesian network structural relationship diagram of each behavior attribute, as shown in [Figure 6: see original paper]. The weight information of each behavior attribute for the final user behavior trust level prediction is analyzed from this Bayesian network structure diagram. The weight distribution diagram of user behavior attributes in this experiment is shown in [Figure 7: see original paper], with the obtained weight values for each behavior attribute being: page reference weight 0.225, browsing URL weight 0.190, access time weight 0.190, byte count weight 0.165, resource usage weight 0.225, and client information weight 0.072. Based on these behavior attribute weight values, the weight value of each behavior authentication set is calculated using a weighted average algorithm. The weights obtained in this experiment are: State Authentication set weight Ws = 0.392, Content Authentication set weight Wc = 0.402, and Habit Authentication set weight Wh = 0.206.

After this session ends, the final predicted behavior trust level for user U is calculated as 2 (“generally trusted”) using the formula based on the analyzed weight values. After the session ends, the behavior evidence database is updated in preparation for the next user behavior authentication. Simultaneously, if the user continues to access, each operational behavior request is re-authenticated to ensure the trustworthiness of the user’ s behavior and guarantee user security.

This experiment establishes three types of user behavior authentication sets based on remote sensing cloud service platform user behavior characteristics. According to the conditional independence assumption characteristics of Bayesian networks and the causal relationship between behavior authentication and behavior attributes, a Bayesian network model is established to predict user behavior trust levels. The model enables fine-grained trust level predictions for user behavior authentication sets. The paper uses Bayesian network analysis to derive weight information of user behavior attributes for trust level prediction results, and finally calculates user trust levels using a decision method.

6 Conclusion

User behavior is an important research direction in the field of network security in cloud computing environments. Identity authentication is the foundation of entire information security in user behavior authentication, but traditional identity authentication cannot prevent malicious behavior intrusion by legitimate users. This paper elaborates on the remote sensing cloud service platform user behavior authentication process based on Bayesian networks, integrating Bayesian network inference technology to solve user behavior trust level problems. By combining identity authentication with a Bayesian network model, user behavior authentication is achieved. Bayesian network inference technology decomposes behavior trust level problems based on causal dependency relation-

ships between variables and attributes. Due to the conditional independence assumption feature of Bayesian networks, Bayesian network inference technology only needs to consider the relationship between current nodes and their parent nodes when solving problems, simplifying calculations and facilitating accurate probability distribution estimation, thereby improving prediction accuracy. However, such schemes will face many attacks in the future. Due to lack of research and usage experience, the attacks they may face and feasible defense solutions require further research.

References

[1] Li Xiaoning, Li Lei, Jin Lianwen, et al. Building private cloud computing platform based on OpenStack [J]. Telecommunications Science, 2012, 28(9): 1-8.

[2] Reichert A. The future, applications, and security of PaaS [EB/OL]. (2014-9-02) [2017-09-05]. https://searchcloudcomputing.techtarget.com.cn/5-10646/.

[3] Tian Liqin, Lin Chuang. A game control mechanism based on behavior trust prediction in trusted networks [J]. Chinese Journal of Computers, 2007, 30(11): 1930-1938.

[4] Zou Bingyu, Zhang Huanguo, Guo Xi, et al. A fine-grained authorization model based on credibility in trusted network connection [J]. Journal of Wuhan University: Natural Science Edition, 2010, 56(2): 147-150.

[5] Zhu Lirong, Chen Ningjiang, He Peicong, et al. Cloud user behavior authentication service system based on dynamic trust management [J]. Journal of Guangxi University: Natural Science Edition, 2015, 40(6): 1485-1493.

[6] Xu Jian, Li Mingjie, Zhou Fucai, et al. Identity authentication method based on user mouse behavior [J]. Computer Science, 2016, 43(2): 148-154.

[7] Li Liang, Tian Liqin, Li Junjian. Authentication and prediction of user behavior in cloud computing environment [J]. Computer Systems & Applications, 2016, 25(6): 125-130.

[8] Chen Yarui. Research on user behavior authentication and security control in cloud computing environment [D]. Beijing: University of Science and Technology Beijing, 2012.

[9] Chen Yarui, Tian Liqin, Yang Yang. Mechanism, model and analysis of dynamic user behavior authentication in cloud computing environment [J]. Journal of System Simulation, 2011, 23(11): 2302-2307.

[10] Zhao Jie, Xiao Nanfeng, Zhong Junrui. Behavior trust control based on Bayesian network and behavior log mining [J]. Journal of South China University of Technology: Natural Science Edition, 2009, 37(5): 94-100.

[11] Tian Liqin. Security trust analysis and control of network user behavior [M]. Beijing: Tsinghua University Press, 2011: 144-152.

[12] Wei Zhongqiang, Xu Hongzhe, Li Wen, et al. Bayesian network structure learning algorithm based on maximal information coefficient [J]. Application Research of Computers, 2014, 31(11): 3261-3265.

[13] Wang Xiaoju, Tian Liqin, Zhao Jingxiong. User behavior authentication mechanism and analysis based on Internet of Things [J]. Journal of Nanjing University of Science and Technology: Natural Science Edition, 2015, 39(1): 70-77.

[14] Tang H, Mantao W. User identity authentication based on the combination of mouse and keyboard behavior [J]. International Journal of Security and Its Applications, 2016, 10(6): 29-36.

[15] Mu Chundi, Ye Jun. Bayesian network based on data mining [J]. Journal of Software, 2000, 11(5): 660-666.

[16] Abramson M, Aha D W. User authentication from Web browsing behavior [C]// Proc of FLAIRS Conference. 2014.

[17] Tian L Q, Lin C, Ni Y. Evaluation of user behavior trust in cloud computing [C]// Proc of IEEE International Conference on Computer Application and System Modeling. 2010: V7-567-V7-572.

[18] Feng Dengguo, Zhang Min, Zhang Yan, et al. Research on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83.

[19] Goel N K, Jha C. Analyzing users behavior from Web access logs using automated log analyzer tool [J]. International Journal of Computer Applications, 2013, 62(2): 29-33.

[20] Brosso I, Neve A L, Bressan G, et al. A continuous authentication system based on user behavior analysis [C]// Proc of IEEE Ares' 10 International Conference on Availability, Reliability, and Security. 2010: 380-385.

Note: Figure translations are in progress. See original paper for figures.