Application and Consideration of Dynamic Security Identity Authentication in Electric Power Business

Lei Chen¹, *, Xianzhou Gao¹, a, Wen Shen¹, b, Xiangqun Wang¹, c, Yuping Tang¹, d and Qigui Yao¹, e

¹Global Energy Interconnection Research Institute co., Ltd. Nanjing, China
²State Grid Zhejiang Electirc Power co., Ltd. Zhejiang, China

*Corresponding author e-mail: chenlei@geiri.sgcc.com.cn,
gaoxianzhou@geiri.sgcc.com.cn, bshenwen@geiri.sgcc.com.cn,
wangxiangqun@geiri.sgcc.com.cn, dtang_yuping@qq.com,
yaoqigui@geiri.sgcc.com.cn

Abstract. This electronic document carries out the analysis of mouse, keyboard fingerprint characteristics and online time and user behaviour, establishes user behavior characteristics database and model of electric power business, realizes the identification and account risk control based on dynamic behavior characteristics, improves the account security of the system, and solves the problems. The former security certification method is single, and the ability of security risk prevention and control is insufficient.

1. Introduction
With the rapid development of mobile Internet and Internet of Things applications, all kinds of network services and network entity identity show explosive growth trend. At the same time, network identity fraud, identity information leakage, account violence cracking, abuse of account authority and other security incidents occur frequently, seriously threatening the healthy development of the Internet industry. In the mobile, ubiquitous, hybrid, wide-area interconnection environment, network security threats and risks have gone beyond the inherent boundaries. The traditional defense architecture based on physical boundaries to build security infrastructure and rely on network location to build security trust has been thoroughly broken. Identity-based authentication and authorization become the trust foundation of the new security defense system. The existing identity authentication in power business system lacks the dynamic management mechanism of the whole life cycle. After user's one-time authentication enters the system, there is no effective identity tracking access control and the correlation strategy between user's behavior and business. The dynamic identity continuous authentication method based on behavior is generally missing.

In view of the limited security and convenience of the existing identity authentication system based on user name and static password technology, this paper carries out the analysis of fingerprint user behavior of mouse and keyboard, establishes the user behavior characteristics database and model of power business, realizes the identification and account risk control based on dynamic behavior characteristics, and focuses on evaluating its practicability in power business system. Upgrading the
account security of the system can solve the problems of single security authentication mode and insufficient security risk prevention and control ability.

2. Current Situation Analysis
At present, the method of identity authentication based on user's behavior characteristics such as keyboard, mouse and sensor has been widely studied. In the existing research on identity authentication, many researchers use the keystroke behavior of users to research user identity authentication. However, with the development of graphical interface of computer system, mouse has become the main device for interaction between users and computer system, and attracted more and more attention from scholars. The Swedish DARPA team devoted 10 years to the research and rebuilt identity authentication as a continuous process, not just a door for users to experience during the login phase.

2.1. Mouse
Mouse behavior analysis, as a behavioral biological feature of using mouse to interact with data, provides user authentication in an accessible and convenient way. In the process of interaction between computer and mouse in daily use, each user has specific mouse behavior characteristics reflected by his or her personal habits or physiological habits [1].

Ryan Kaminsky of the University of Washington, USA, is considering using games to identify current users. Mouse behavior features are extracted from the original data of mouse movement, and the accuracy of final identity authentication varies with the movement available in a particular game.

In 2010, Chao Shen and others of Xi'an Jiaotong University proposed to use users' mouse behavior characteristics for user identity authentication and system monitoring. In 2014, a dimensionality reduction method was proposed to reduce the dynamic changes of mouse behavior and improve the performance of continuous authentication method based on mouse behavior characteristics. In 2016, a multi-pattern biometric recognition system is proposed, which combines keystrokes, face and skin color to continuously verify the identity of the logged-in user. A simple and effective user authentication system was proposed in 2017. Frequent behavior segments were extracted by mining pattern growth to obtain stable and differentiated mouse interaction behavior features. Experiments showed that 0.09% FAR and 1% FRR were achieved [2].

In summary, more and more researchers have paid attention to user mouse-based identity authentication, but as far as the current results are concerned, the following problems need to be solved urgently:

1) Existing studies usually use descriptive statistical features of mouse behavior, which describe the intrinsic behavior characteristics of user's mouse behavior. The data acquisition process of dynamic persistent identity authentication based on user's mouse behavior is uncontrollable. Using descriptive statistical features alone cannot effectively represent the original mouse behavior feature space.

2) The existing research does not take into account the variability of user's mouse behavior. At the same time, due to the lack of public data set, the existing identification methods based on user's mouse behavior characteristics cannot compare with previous research on mouse behavior characteristics.

3) Existing research does not have standard test specifications and cannot provide a repeatable and objective evaluation procedure.

2.2. Keyboard
Personal keystroke rhythm mode is difficult to imitate and can be used for identity authentication. According to the keystroke data of personal free text input, the unique keystroke mode can be learned. Based on the detection of user's free text keystroke input, the continuous authentication of user's identity can be completed without affecting user's input. An online learning website named Courrera, uses keystroke features to verify the identity of online students [3].

Based on free text authentication, each user needs at least 10,000 keystroke data, and each test sample needs about 1,000 keystroke data to achieve better recognition effect and reliability.
The Buffalo keystroke data set collected by Yan Sun and Hayreddin Ceker of Buffalo State University of New York in the United States was clustered by Gaussian mixture model. The experimental results show that the equal error rate (EER) of keystroke data is 0.01%.

Tomer Shimshon of Ben-Gurion University in Israel used random forest algorithm to carry out user authentication experiments. Considering the effect of window length on user authentication accuracy, the experiment obtained FAR of 3.47% and FRR of 0%.

From the current research progress at home and abroad, we can see that preliminary exploration has been started on the issue of identity authentication using behavioral characteristics. Stan Salvador of Florida University of Science and Technology and others carry out identity authentication according to users' behavior habits of using specific functions of mobile phones, such as calling, sending text messages, taking photos, etc. But this scheme usually takes a long time to achieve identity authentication. Fabian Monrose of Spyre Laboratory tried to authenticate users according to their keyboard-tapping behavior, but it also needed users to tap continuously for a period of time to achieve it. Davrondzhon Gafiirov et al. made an attempt to authenticate users by using gait, but this scheme is vulnerable to the impact of road conditions, different road conditions and road types, even under the same user. There are also great gait differences, and the TPR of authentication results is low. Alexander De Luca and others of Munich University in Germany have realized the use of gestures to authenticate identity, but the accuracy is low. At the same time, they can only authenticate the identity of two types of users (host and non-host) [4].

3. Research On Mouse Behavior Analysis And Pretreatment In User Environment
The differences of users' habits and physiological habits in the process of mouse operation are analyzed. The mouse behavior characteristics of different users are different, such as the time of single and double mouse click, the use habits of the left and right mouse keys, the speed of mouse movement and so on. The direct reason for these differences lies in the different users' power of moving the mouse, the ability of accurate positioning and the different power of clicking on the mouse's finger. The indirect reason is related to the users' mental state and the users' familiarity with the operation process [5].

The research of mouse behavior characteristics is to monitor the mouse input of computer users, acquire the data of user behavior characteristics when using the mouse, analyze the user's mouse behavior patterns, and then authenticate the user's identity on this basis. Daily mouse actions include mouse movement, left and right key clicks and double clicks, mouse dragging and pulling, mouse scrolling and mouse stationary, etc. Many complex tasks in GUI can be accomplished through a series of simple mouse operations.

4. Research On Keyboard Behavior Analysis And Pretreatment In User Environment
The traditional keyboard behavior of users is mainly embodied in the user's keystroke behavior. The keystroke behavior of different users has certain regularity, and the user's behavior will change slowly with the passage of time. The main feature of keystroke behavior is time feature. Two of the main features are the keystroke latency and the duration of the key. At present, in the study of time-based keystroke characteristics, the method of collecting time data is based on the time when the keyboard issues interrupt requests to the host computer. When a key on the keyboard is pressed, the keyboard sends an interrupt request to the host and sends out a 'close code'. When the keyboard is raised, the keyboard also sends an interrupt request to the host, and at the same time sends out a 'disconnect code'. The keystroke time acquisition method can calculate the keystroke time by measuring the number of
CPU cycles experienced between the two interrupts and cooperating with the CPU frequency of the host computer [7].

When users log in with mobile devices, the mobile devices will shift when different users tap the soft keyboard on the touch screen. This project marks the user's identity by using the angle and size of the displacement. When the user taps the input button on the touch screen, a button action can be divided into two successive processes: pressing and lifting. With the pressing and releasing of the finger, the mobile phone will also produce acceleration and acceleration of physical displacement, and the built-in value of the action sensor will change significantly. The process of inferring user identity from motion sensor data consists of two parts: ①Acquisition and storage of mobile phone built-in motion sensor data; ②Extraction of eigenvectors from sensor data. The process is as follows:

**Figure 1.** The Process of User Identity Judgment Based on Action Sensor Data Inference.

5. Dynamic Identity Authentication And Risk Prevention

5.1. Dynamic Identity Recognition

When user identification is carried out, the validity of unique information is judged firstly. When the unique information is not available, the configuration information features or models composed of user's mouse and keyboard behavior characteristics are needed to identify. Because the feature information may not match the identity feature or model completely, it is necessary to judge the credibility of the identity feature or model submitted by this authentication. This paper designs a method of calculating identity credibility. This method can reflect the difference of various feature information elements in identity features or models, and has a certain dynamic learning function based on environment. In the application environment, the credibility calculation of identity features or models can be divided into two situations: when the features or models carried by an identity match with the trusted features or models, the credibility of the features or models can be considered to be 100%; when the identity features or models are different from the trusted features or models, it is believed that the modification of the identity features or models by trusted users is trustworthy. Then the credibility of identity features or models is equal to the probability of being changed by trusted users. Assuming that the values of each feature or model are not related and independent events, the reliability of the whole feature or model can be expressed by the product of the independent credibility of each feature or model element pi [8].

The advantage of this method is that if the calculation of each component Pi is independent, we can use different calculation methods for different components, which is a feature or model overall credibility calculation framework independent of each feature or model credibility.

In order to store user information and trusted device information, it is necessary to store user's basic information in the database, as well as the characteristics or model information with the binding. In this way, whenever the authentication request information with the current feature or model is received, the reliability of the feature or model of the trusted device that has been bound to the user in the database
can be calculated, and the identity credibility of the authentication request can be calculated by the algorithm based on statistical data and Bayesian method.

5.2. Risk Prevention and Control of Abnormal Behavior

On the basis of realizing user identification, aiming at the abnormal behavior of some account users, active alarm notification and access permission change measures are taken to realize the prevention and control of account risk.

![Diagram](image)

**Figure 2.** Identity Recognition of Dynamic Behavior Characteristics and Account Risk Prevention and Control Process.

5.2.1. Active Alarm Technology Based on Application Protocol. The paragraph text follows on from the subsubsection heading but should not be in italic. When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

This method uses the signature of data message to identify protocol. At present, for the unencrypted network protocol, it is more mature and efficient. However, it does not take into account that the characteristic part of the protocol is the process of stately transition.

Traditional protocol recognition methods based on message content do not record the status of recognition when dealing with data messages. In some of their implementations, some of them match the feature fields (fixed string feature fields and feature fields described by regular expressions) with the content of the message. Once the matching is successful, they decide that they belong to the protocol. Others collect the application-level data of the first several network messages as a long string, and then match the feature fields with it. For example, L7-filter for each network protocol, there is only one regular expression. Although the expression can have "or", its matching mode is still in the above two ways. Because of the shortcomings of traditional protocol recognition methods based on message content, this paper proposes a method based on protocol recognition state of finite automata and signature recognition, which is based on the following points:

a) There are several signatures in the network protocol, which may be more than one.

b) There is some dependence between the internal signatures of the protocol.

c) There may be identical signatures between protocols, which means that at the initial stage of communication, different protocols may produce network messages with identical data characteristics.
5.2.2. Privilege Change of User Abnormal Behavior. The paragraph text follows on from the subsubsection heading but should not be in italic. When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

When changing the role's permission, the non-relational change method of type needs to be dealt with in two situations according to the type's position in the type hierarchy. If the type does not have a parent type, revoke its permissions directly, that is, change the type and change the permissions that belong to that type only and not to any other type in the permission domain. If the type has a parent type, it does not revoke its privileges directly, but marks the type as non-assignable, and at the same time marks the privileges that belong only to the marked type but not to other types as inaccessible in the corresponding permission domain, that is to say, the type has not changed from the type level, and the privileges that belong only to the type have not changed from the type level. Changes in permission domains, but this type cannot be assigned to users and user groups, and similarly these permissions cannot be granted. Marked as an unassigned type, although it cannot be assigned to the user, it can still be used to connect its parent type to its child type. After the type of non-correlation algorithm is changed, it can ensure that the hierarchical position of each type and the relationship between each type remain unchanged. In practical application, the advantages of non-correlation algorithm are as follows:

a) The privilege information of the type marked as non-assignable is not displayed, but the relationship between other types will not be affected.

b) When the system needs to restore the type in the future or add other types in the location of the type.

Since the hierarchical relationship has not changed, and the type has not been changed, it is possible to directly change the type of non-assignable marker or extract the type of non-assignable marker and change it to a new type of relevant information. The non-associated change strategy improves the simplification of work steps, the flexibility of authorization and the convenience of type management to a certain extent.

6. Conclusion
This paper analyses the physiological and behavioral characteristics of keyboard and mouse, puts forward the key technologies of dynamic identity security authentication and risk control suitable for power business scenarios, realizes multi-dimensional identity security authentication based on users' physiological characteristics perception and continuous risk control of accounts, and provides users with more convenient and better identity authentication based on improving the security management capability of power business.

Acknowledgments
This work was financially supported by the science and technology project of State Grid Corporation of China: "Research on Key Technologies of Dynamic Identity Security Authentication and Risk Control for Electric Power Business" (Grand No. 5700-201972227A-0-0-00) fund.

References
[1] Shen Chao, Cai Zhongmin, Guan Xiaohong, Fang Chao, Du Youtian. User Identity Authentication and Monitoring Based on Mouse Behavior Characteristics [J]. Journal on Communication, 2010, 31 (7): 68 - 75.
[2] Wang Xin, Wang Mengyin, Liang Jin. Identity Authentication Based on Mouse and Keyboard Behavior. China's Educational Technology Equipment [J]. 2014, 22: 50 - 53.
[3] Fang Chao, Cai Chao, Cai Zhongmin, Shen Chao. User Identity Authentication and Monitoring Based on Mouse Dynamics Model [J]. Journal of Xi'an Jiaotong University, 2008 (10): 1235.
[4] GAMBOA H, FRED A. A behavioral biometric system based on human computer interaction [J]. Proceedings of SPIE, 2004, 54: 4 - 36.

[5] PUSARA M, BRODLEY C E. User re-authentication via mouse movements [C]. Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, DMSEC Session. Washington DC, USA: 2004: 1 - 8.

[6] Guo Xiaojing. Research and Improvement of Identity Authentication Algorithms for Keystroke Sequences Based on Statistics [D]. Beijing: Beijing University of Posts and Telecommunications, 2013.

[7] Yue Bing, Huo Baofeng, Tian Bing. Research on Network Intrusion Behavior Model in Journal of Tianjin University [J]. 2003, 36 (2) 254 - 256.

[8] Jin Qianqian, Chen Chunlin, Yu Xiaowen, Liao Peng. Pre-warning method of abnormal user behavior in power information intranet based on similarity analysis [J]. Computer Systems & Applications, 2017, 26 (12): 220 - 26.