Security and Safety, Vol. 3, 2024003 (2024)
https://doi.org/10.1051/sands/2024003
sands.edpsciences.org

Review OPEN ACCESS

Digital Finance

Behavioral authentication for security and safety

Cheng Wang[1,2,3,*], Hao Tang[1,2], Hangyu Zhu[1,2], Junhan Zheng[1,2], and Changjun Jiang[1,2,3,*]

[1] *Department of Computer Science and Technology, Tongji University, Shanghai 201804, China*
[2] *Key Laboratory of Embedded System and Service Computing, Ministry of Education, Shanghai 201804, China*
[3] *Shanghai Artificial Intelligence Laboratory, Shanghai 200232, China*

Received: 7 December 2023 / Revised: 5 March 2024 / Accepted: 18 March 2024 / Published online: 30 April 2024

Abstract The issues of both system security and safety can be dissected integrally from the perspective of behavioral *appropriateness*. That is, a system that is secure or safe can be judged by whether the behavior of certain agent(s) is *appropriate* or not. Specifically, a so-called *appropriate behavior* involves the right agent performing the right actions at the right time under certain conditions. Then, according to different levels of appropriateness and degrees of custodies, behavioral authentication can be graded into three levels, *i.e.*, the authentication of behavioral *Identity*, *Conformity*, and *Benignity*. In a broad sense, for the security and safety issue, behavioral authentication is not only an innovative and promising method due to its inherent advantages but also a critical and fundamental problem due to the ubiquity of behavior generation and the necessity of behavior regulation in any system. By this classification, this review provides a comprehensive examination of the background and preliminaries of behavioral authentication. It further summarizes existing research based on their respective focus areas and characteristics. The challenges confronted by current behavioral authentication methods are analyzed, and potential research directions are discussed to promote the diversified and integrated development of behavioral authentication.

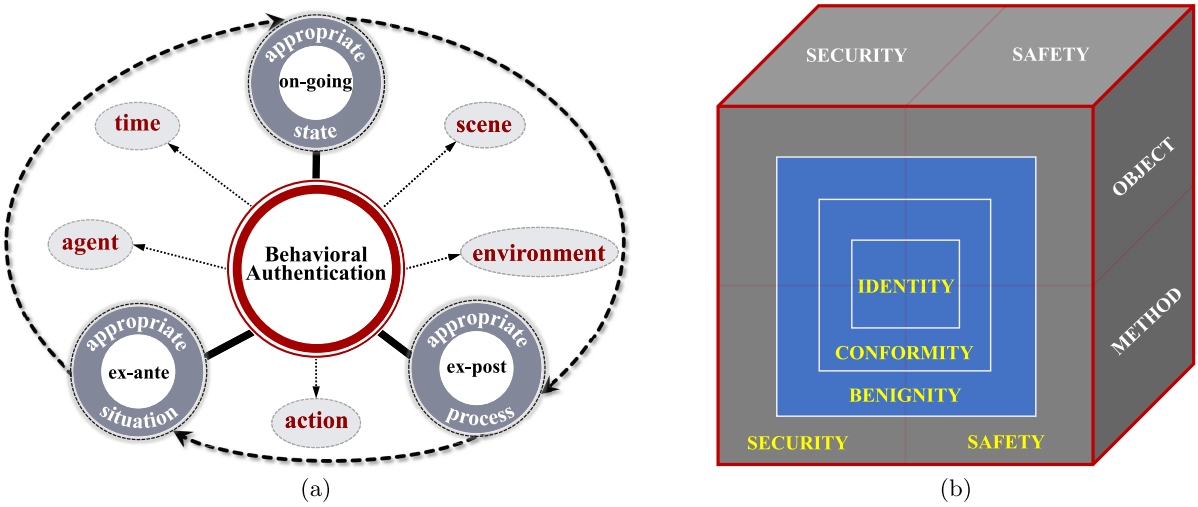
Keywords behavioral authentication, security and safety, behavior modeling, anomaly detection, machine learning, artificial intelligence

Citation Wang C, Tang H, Zhu HY, Zheng JH and Jiang CJ. Behavioral authentication for security and safety. Security and Safety 2024; **3**: 2024003. https://doi.org/10.1051/sands/2024003

1 Introduction

The advantages of frictionlessness, continuousness, synthesizability, and inherence in behavioral authentication have attracted significant attention from the security research community [1–9]. Narrowly defined, behavioral authentication usually refers to *behavioral identity authentication* [10, 11]. It is a technology that has emerged as a result of the continuous development of the artificial intelligence industry and the improvement of computing and storage capabilities in hardware, driven by the increasing dependence of individuals on the convenience provided by devices. Behavioral authentication collects behavioral data implicitly in the background and distinguishes them from others by analyzing unique behavior patterns, as behavior patterns are the intrinsic properties of agents and naturally possess distinct characteristics compared to others. Initially, research on behavioral identity authentication primarily focused on utilizing collected behavioral data to address specific authentication scenarios and meet the essential usability requirements [12–14]. As researchers gain a deeper understanding of behavior, they realize the close correlation between security and behavior [15, 16]. The connotation of security can be described

* Corresponding authors (email: cwang@tongji.edu.cn (Cheng Wang); cjjiang@tongji.edu.cn (Changjun Jiang))



(a) (b)

Figure 1. (a) illustrates the concept of security and safety can be seen as an "appropriate state" during the ongoing detection, an "appropriate process" (sequence of states) in the ex-post evaluation, and an "appropriate situation" (trend in the development of states) in the ex-ante awareness. The essence of studying security lies in examining whether the changing states are secure and the factors inside and outside the state changes are referred to as behavior. (b) describes the conceptual framework of behavioral authentication

from *a behavioral perspective*, where it involves the *right agent* performing the *right actions* at the *right time* under certain conditions (*e.g.*, *scene* and *environment*), as illustrated in Figure 1a. Therefore, the study on security can be essentially implemented by the research on behavior, then the behavior is also regarded as the object of security research [17, 18]. Behavioral identity authentication ensures protection against external malicious attackers and safeguards security. As the scope of behavioral identity authentication applications gradually expands, the importance of non-functional requirements is also increasing. Researchers are paying more attention to the robustness, reliability, and timeliness aspects of behavioral identity authentication [2, 18, 19], which is of great significance to safety.

In real-life business, after verifying the legitimacy of identity, there are still some behaviors that require further behavioral authentication to evaluate their compliance. For example, in the scenario of credit loans [20], some users use their genuine identities, but after being approved, they engage in malicious cash-out activities. In the database system, users access the system through their own account, so the user's identity is normal, but when the user steals database information through this account, the behavior is illegal for the system. We call this type of problem *behavioral conformity authentication*. Behavioral conformity authentication refers to identifying whether behavior patterns conform to the rules within the system during the process of using various intelligent information services under the precondition of a user's legitimate identity. In fact, some studies have already utilized behavioral data as a resource to solve different cybersecurity issues, *e.g.*, online payment anti-fraud [20–22], network system intrusion detection [23], and social network compromised account detection [10, 24, 25].

Furthermore, security and safety issues may arise due to unknown risks and vulnerabilities associated with an agent's behavior, even if its identity is legitimate and its actions comply with regulations. For instance, in the scenario of credit loans, there is the issue of multiple loans, where some users borrow from different platforms using their genuine identities. Their identities are legitimate, and they repay the loans on time initially. However, due to the limited repayment capacity of some borrowers, there is a higher risk associated with borrowing from multiple platforms. In the short term, it may seem like there are no issues, but when the last platform is unable to borrow, it leads to overdue payments and a mounting debt burden, resulting in bankruptcy caused by a cycle of borrowing to repay existing debts. In an industrial Internet scenario, the operational state of a device manifests as an uninterrupted flow of temporal data and is occasionally accompanied by abnormal signals that do not trigger compliance alerts. These signals do not originate from external intrusions upon the device, but the accumulation of occasional abnormal signals over the long term can lead to systemic risks to the system [26–28]. These concerns are called *behavioral benignity authentication*. It refers to detecting any potential risks in user behavior during the

process of using various intelligent information services under the precondition of user identity legitimacy and behavioral compliance.

Considering the aforementioned aspects, behavioral authentication encompasses three main components: behavioral identity authentication, behavioral conformity authentication, and behavioral benignity authentication. We propose the conceptual framework of behavioral authentication, which is shown in Figure 1b. In this work, we first provide an overview of the background and preliminaries of behavioral authentication. Next, we conduct a comprehensive review of existing research and categorize the studies based on their respective focus areas and distinctive characteristics within each category. Moreover, we highlight and discuss the challenges of the current behavioral authentication methods, and propose future research directions to enhance the effectiveness and efficiency of behavioral authentication.

2 Background and preliminaries

2.1 Background

According to the 52nd *Statistical Report on the Development of the Internet in China* [29] released by the China Internet Network Information Center in 2023, as of June 2023, China's Internet user base has reached 1.079 billion people, with an Internet penetration rate of 76.4%. The user base for instant messaging, online video, and short video stands at 1.047 billion, 1.044 billion, and 1.026 billion, respectively, with user adoption rates of 97.1%, 96.8%, and 95.2%. These new digital services have been closely related to people's lives. However, at the same time, digital transformation is also facing severe and complex security and safety challenges, posing real threats to critical infrastructure, systems, and citizen privacy [30, 31]. From the perspective of attack targets, the focus has shifted from networks and systems to business and data, with an increasing number of ransomware and application-based attacks. In terms of attack methods, the trends of automation, intelligence, and concealment in attack tools have become more prominent. Additionally, cybercriminals further enhance the success rate of attacks by illegally acquiring personal data, such as email and physical addresses, phone numbers, and other personally identifiable information. All these factors pose significant challenges to traditional authentication methods. Driven by the security and safety demands of the real world, there is a current need to adopt new technologies to address these challenges. Behavioral authentication is one of the most promising methods, and this innovative approach is moving towards a safer and more secure cyberspace.

The technique of behavior modeling is closely related to behavioral authentication. In fact, there is a rich history of research focused on predicting user characteristics, including attributes, personality, and behavior, through the utilization of behavior modeling techniques. In the years 2013 and 2015, Kosinski *et al.* [32, 33] explored the feasibility of using user behavioral data to infer, predict, and model user attributes, interests, and personality. In terms of user behavior prediction, as early as 2010, Song *et al.* [34] conducted a three-month study and analysis of the travel records of 50 000 anonymous mobile phone users in their publication in *Science*, and found that users' historical travel behaviors followed specific patterns, with an accuracy of up to 93% in predicting users' potential travel behavior. There has been extensive research on the specific application of behavior modeling requirements for internet services. For example, personalized modeling has been implemented by mining users' interests and hobbies based on their behavioral characteristics [35–38]. Behavior trend analysis has been conducted by observing changes in user behavior patterns [39–42]. Malicious accounts have been detected by analyzing account behavioral characteristics [43, 44]. Risk assessment of default has been performed by analyzing user transaction behavior records [45]. Social identity association across different platforms has been addressed by matching user behavior patterns [46–48].

In the field of identity authentication, the majority of current online methods resemble access control methods. Common methods include setting up alphanumeric or graphical passwords for accounts [49–54], utilizing security tokens [53, 55–57], and employing biometric features such as facial and iris recognition [58–62]. Setting passwords for accounts is the simplest and most widely used method of identity authentication while linking mobile phones and emails serves as an effective measure for account protection and recovery. Security tokens are physical devices employed as a means of identity authentication and are currently extensively utilized. Biometric authentication refers to the utilization of unique biological features of individuals to verify their identities. Biometric authentication is considered a relatively reliable method of identity verification. The above-mentioned methods primarily operate during the login

authentication phase of an account. Because these methods typically require additional user operations, they are regarded as intrusive authentication methods. These intrusive methods are hard to meet the high requirements of users for authentication convenience and service experience. When confronted with the issue of managing multiple account passwords, many users tend to adopt complete or partial password reuse strategies, underestimating the threat of password reuse to account security [9, 63, 64]. Furthermore, certain risks exist with certain biometric-based authentication technologies. For instance, in facial recognition, the replicability of facial data (obtainable and replicable in public environments), the instability of facial data (affected by makeup, allergies, injuries, and cosmetic surgeries leading to changes in features), and the security of backend data should be taken seriously (a breach of backend data would have devastating consequences for industries and society).

In the field of conformity authentication, the existing practices mainly rely on establishing conformity authentication systems based on rules [65–69]. The process of setting up rule libraries is time-consuming and incurs high manual costs [70]. Once authentication is granted through rule-based detection systems, these systems tend to persist in granting access to similar requests in the future. However, due to the absence of timely updates to the rule library, identifying new instances of non-conformity becomes challenging. In practical business scenarios, the limitations of rule-based construction have become increasingly apparent. Conformity authentication models sometimes require the input of hundreds of expert features. The manual construction of rules is also challenging to transfer and switch across different application scenarios, resulting in significant manual and time costs and impacting the efficiency of model development and operation. This method is constrained by human expertise and may overlook potential non-conformities, preventing the model from achieving excellent detection performance [71]. Additionally, this time-consuming and labor-intensive approach to constructing conformity models, which may overlook complex risks, no longer meets the requirements of secure, dynamically changing conformity authentication systems. It is of great significance for the development of conformity authentication models to effectively utilize and reuse knowledge, reduce manual and time costs, and establish automated and efficient authentication models.

In terms of benignity authentication, existing methods mainly focus on the static benignity of entities, with limited scalability in dynamic environments. These methods heavily rely on pre-established dependency analysis, equivalence relationships, and protocol state specifications. The trusted formal modeling employed in these methods is predominantly based on cryptographic techniques, which presents several challenges in real-world business scenarios. Cryptographic modeling processes can be time-consuming and hinder the efficiency of authentication procedures. The practicality of these cryptographic methods may be limited due to high hardware requirements for deployment, affecting their efficiency and usability. These methods lack the necessary adaptability and flexibility, which makes it challenging to promptly capture potential risks. For example, coupon clippers may not initially violate regulations, but the large-scale organization of coupon clippers' activities is likely to increase overall transaction and credit costs, ultimately hindering normal business activities. There is a pressing need for more adaptive and flexible approaches in benign authentication that can overcome these limitations and meet the demands of dynamic environments in real-world business scenarios.

2.2 Preliminaries

Experts in the field of cybersecurity have paid attention to the importance of user behavior research in addressing security issues. Dr. Douglas Maughan, the inaugural Office Head for the National Science Foundation (NSF) Convergence Accelerator, and the former Director of the Cyber Security Division at the Science and Technology Directorate of the U.S. Department of Homeland Security, believes that researchers should prioritize viewing cybersecurity issues from a human factors perspective [72]. Professor Angela Sasse of University College London, funded by the British government, is studying cybersecurity issues in the business sector from a novel perspective of social and behavioral science [73]. Professor Stefan Savage of the University of California, San Diego is also researching behavior analysis for the prevention and control of network fraud [74]. *Nature* published an article titled *How to Hack The Hackers: The Human Side of Cybercrime*, highlighting the progress made in representative research efforts and emphasizing the importance of leveraging behavioral science to understand the behavior patterns of both perpetrators and victims for enhancing cybersecurity [75].

For behavioral identity authentication, devices typically collect behavioral data in the background. The collected data is then utilized for training a machine learning model [76]. Features are extracted through the trained machine-learning model based on the collected behavioral data, which form the users' behavior profiles. The identity behavior profile is represented as a matrix U by the model. During the process of behavioral identity authentication, the newly generated credential of the kth user is compared against the stored identity behavior profile matrix to determine the authenticity of the user's identity. Verification involves comparing a provided behavior record with a stored template to determine a level of similarity. It grants access to legitimate users if their presented behavior record exhibits a similarity measure surpassing a predefined threshold. Let x, $g(\cdot)$ and d_k denote the behavior record, the behavioral identity authentication model, and the predefined threshold of user k, respectively. The result of the behavioral identity authentication model $R = \text{True}$ if $g(x) > d_k$ and False otherwise.

Behavioral conformity authentication, refers to the process of ensuring that the internal behavior of users and business activities comply with relevant laws, regulations, and industry standards. Let $\mathcal{X} = \{x_1, x_2, \cdots, x_N\}$ denote the set of behavior records. Behavioral conformity authentication aims to learn a decision function $\phi(\cdot)$: $\mathcal{X} \to \mathbb{R}$ that assigns behavioral conformity scores. The goal is to effectively distinguish non-compliant behavior records from compliant behavior records in the space defined by the behavioral conformity score decision function. By inputting behavioral data into $\phi(\cdot)$, it can directly infer the conformity scores. Larger outputs of $\phi(\cdot)$ indicate a greater degree of non-compliance, which requires the system to take appropriate actions timely to prevent or rectify such behaviors. Certainly, it is necessary to characterize and map the original features of behavior records before inputting them, which is beneficial for obtaining more accurate scores of behavioral compliance.

Researchers have already begun exploring security and safety issues within the scope of behavioral benignity authentication. Relevant research works primarily focus on the following aspects, including traceability of behavior, predictability of risk, consistency of execution, and integrity of record. The traceability of behavior refers to the tracking of individual or entity behavior activities to obtain detailed historical behavioral data, helps verify the legitimacy of user behavior. Predictability of risk involves a comprehensive evaluation of individual or entity behavior activities to timely identify potentially risky behaviors and update the scope of compliance. Consistency of execution evaluates the credibility and detects potential risks without affecting consistent operations in cross-domain interactions over heterogeneous networks. Integrity of record entails protecting user privacy and ensuring consistency in the certification process. These aspects of behavioral benignity authentication provide additional protection for systems.

The behavioral authentication method has the following advantages based on its technical principles:

- **Frictionlessness.** This method operates as a backend program, eliminating the need for user intervention. The collection of data and verification are seamlessly performed without requiring any explicit actions from the user. This frictionlessness of behavioral authentication ensures a smooth and convenient experience.
- **Continuousness.** The method transforms cybersecurity authentication from a one-time process to a continuous one. It allows for ongoing analysis of user behavior over time, ensuring that access remains granted as long as the behavior patterns align with the established user profile. This continuous authentication approach enhances security by detecting any anomalous or suspicious behavior in real time.
- **Synthesizability.** The method directly captures the projection of multiple subspaces of behavior, which exhibits synthesizability among the subspaces. By capturing various dimensions of behavior, it creates a comprehensive and reliable behavior profile. Synthesizability of behavior enhances the accuracy and robustness of the authentication process.
- **Inherence.** The data used for behavioral authentication typically originates from users' inherent characteristics and patterns. Therefore, intruders are unlikely to perfectly mimic the user's behavior patterns, as individual behavior is unique and difficult to imitate convincingly. Furthermore, intruders typically exhibit intrusive actions aimed at stealing benefits, which often deviate from the user's normal behavior.

We consider typical scenarios to illustrate the connections between different authentication methods. For example, credit loan services are typical data-intensive services, and the synthetic and intrinsic characteristics of behavioral authentication provide support for enhancing representational capabilities and

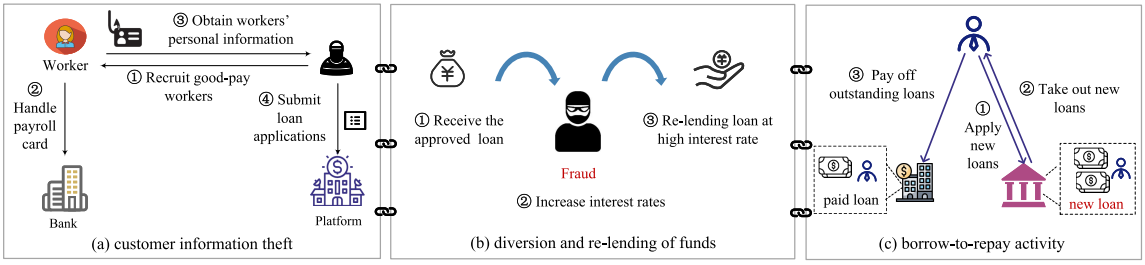


Figure 2. A typical example demonstrates how different levels of behavioral authentication ensure the safety and security of credit loan services. (a) shows criminals collect information from victims and submit loan applications, and it can be addressed by behavioral identity authentication. (b) describes the illicit re-lending of funds activities that occur after the loan has been approved and disbursed, which belongs to the level of behavioral conformity authentication. In the auditing process, timely analyzing the flow of loans among different platforms and ensuring the predictability of lending risks, are the key issues addressed by behavioral benignity authentication, as shown in (c). Behavioral authentication expands through a progressive framework of sub-functions, *i.e.*, identity, conformity, and benignity, to achieve gradual enhancement for the safety and security of credit loan services

breaking down isolated data attributes of credit loan services. During the initial stages of a loan application, some criminals may steal others' information through illegal means for fraudulent loan applications. The specific process is illustrated in Figure 2a. The evaluation of whether the information submitted by a borrower matches the true circumstances falls under the level of behavioral identity authentication, which protects the security of the loan application for financial institutions. While behavioral identity authentication can ensure the legitimacy of a borrower's identity, there are instances of non-compliant behavior after the loan is approved. Diversion and re-lending of funds is one such non-compliant behavior where the borrower does not use the loan funds as intended during the loan application. Instead, after receiving the loan from a financial institution, the borrower engages in illegal lending activities. As shown in Figure 2b, the fraudster further increases the loan interest rates approved by financial institutions and lends the funds to others to profit from the interest rate differential. Detecting such fraud falls under the level of behavioral conformity authentication. It uses methods like behavior tracking to ensure the security of loan flows. Furthermore, in real business processes, there are cases where a borrower's identity is legitimate, and the borrower's behavior complies with platform regulations, but failure to restrict such behavior promptly can increase overall system risks. Figure 2c illustrates the concept of borrow-to-repay activity, which is detrimental to the stable operation of the financial platform. Initially, the borrower only applies for loans on a single platform and can adhere to the repayment policies of that platform. However, later on, due to financial difficulties, the borrower cannot repay the loans on one platform on time. As a result, the borrower applies for new loans on other platforms to repay the outstanding loans. In reality, the borrower's ability to repay loans has declined. The collaborative audit across multiple platforms to promptly detect such behavior not only ensures the security of the business but also further ensures platform safety by timely refining loan strategies and making the controllability of platform risks. They are crucial aspects of behavioral benignity authentication. Safeguarding user identities from theft, monitoring the compliant use of loans, and continuously improving the approval processes provide essential protection for credit loan services. The progressive enhancement of financial market security and safety through the expansion of behavioral authentication sub-functions with the level of identity, conformity, and benignity promotes the development of inclusive finance.

Intelligent transportation information services also involve the extension of different levels of behavioral authentication. As communication and computation-intensive services, the frictionless and continuous characteristics of behavioral authentication help address emerging security and safety challenges, where entities' access is dynamic, devices interact frequently, and cross-domain paths are concealed. During the access phase of different entities, behavioral identity authentication prevents different devices from falling victim to phishing attacks and identity theft, ensuring data and access security for intelligent devices, which is shown in Figure 3a. While some entities have successfully verified their legal identities and registered successfully within the intelligent transportation system, during the process of heterogeneous entity interaction, some entities may not adhere to the standards and regulations of services. Figure 3b illustrates typical non-compliant behavior in intelligent transportation information services.

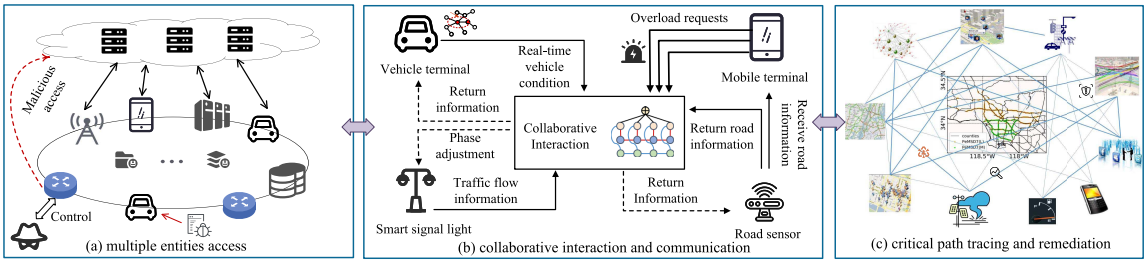


Figure 3. An example illustrating the security and safety issues that different levels of behavioral authentication need to confront in intelligent transportation information services. (a) describes the entity access phase where various entities may face threats such as identity theft and phishing attacks, and it belongs to the level of behavioral identity authentication. (b) illustrates the monitoring of API interface traffic and blocking of non-compliant request entities during collaborative interactions and communication process which falls under the level of behavioral conformity authentication. (c) shows the functionality of behavioral benignity authentication, which identifies and rectifies high-risk paths within the system, enabling internal information protection and proactive defense against malicious activities

During the collaborative development of intelligent transportation information systems, for the convenience of information sharing and resource coordination, different entities open certain interfaces to other interacting entities, based on additional standards. These entities must conform to the specified usage of external cooperative entities' API interfaces according to these additional standards to ensure efficient and stable information sharing and resource allocation in the system. Some access entities have the legitimacy of their identity but generate traffic requests that exceed service standards. This directly leads to network congestion and increases the system's response time. Behavioral conformity authentication is responsible for monitoring the traffic of API interfaces, promptly detecting non-compliant request entities, and safeguarding the overall security and stability of the multi-entity collaborative process. Additionally, some entities have legitimate identities and generate traffic that complies with standards when using open API interfaces. However, in the process of cross-domain access, there may exist potential high-risk access paths. These paths can give rise to undisclosed security vulnerabilities and potentially expose sensitive internal system information. Such vulnerabilities might inadvertently offer attackers opportunities to establish backdoors within the system, as shown in Figure 3c. Behavioral benignity authentication uses traceability analysis to locate the minimum-cost repair points for high-risk access paths, achieving proactive prevention. This further enhances the security of intelligent information networks and safeguards the safety of internal system information. Ensuring the legitimacy of access entities, promptly blocking abnormal traffic, and repairing high-risk access paths, behavioral authentication continuously addresses security and safety issues in various aspects of intelligent transportation information services. This plays a critical supporting role in harnessing the efficiency of transportation infrastructure, improving the operational efficiency and management level of transportation systems, and facilitating smooth public travel.

3 Studies on behavioral authentication

3.1 Behavioral identity authentication

According to the different characteristics of behavioral data, this part categorizes behavioral identity authentication into five major types: keystroke, touch gesture, motion, intrinsic signaling behavior, and user interaction behavior. In addition, in certain specific scenarios, the above different behavioral feature types can be combined into a multi-factor approach to reflect the user behavior, as shown in Figure 4.

Keystroke-based authentication is one of the earlier behavioral identity authentication methods that verifies a user's identity by analyzing the characteristics of the user's input characters on the keyboard, such as keystroke force, keystroke speed, keystroke frequency, keystroke sequence, and keystroke time intervals. Early research into keystroke-based authentication focused on analyzing keystroke force and frequency. Zhu *et al.* [77] proposed a novel approach to authenticate users based on keystroke dynamics while entering passwords. The proposed method leverages a keystroke feature vector which consists of the user's keystroke force and frequency to confirm the user's identity. Subsequently, researchers introduced

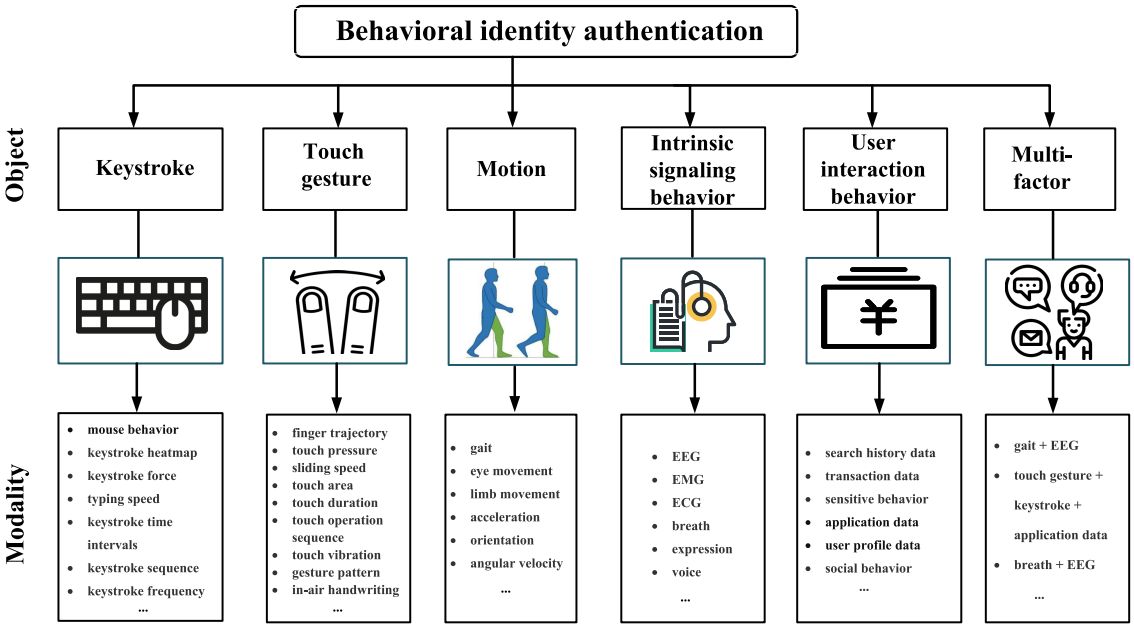


Figure 4. Components of behavioral identity authentication

extra keystroke features to continuously improve the accuracy and security of keystroke-based authentication. Primo *et al.* [78] investigated the effect of music on keystroke behavioral data using two validation techniques: relative and absolute measurements. The researchers analyzed the data based on three dimensions of keystroke behavior: key hold, key press, and inter-key intervals, to understand how music affects user verification performance. Their findings confirmed that a music environment can improve the accuracy of user authentication based on keystroke dynamics. Ho *et al.* [79] introduced a user authentication approach based on keystrokes, which integrates a one-class naive Bayes algorithm (ONENB) and a typing speed inspection in typing skills (SITS) algorithm. The ONENB algorithm computes the probability of keystroke behavioral data, while the SITS algorithm incorporates keystroke patterns to define user keystroke characteristics and builds an authentication model to differentiate legitimate users from impostors. Lee *et al.* [17] designed a parameterized model that utilizes a feature selection method based on the median and interquartile range to extract keystroke dynamics features. The model binds the calculated security measure (FAR) obtained from these keystroke dynamics features for user identity verification. Furthermore, with the development of understanding of keystroke dynamics, many input devices have been used for authentication in similar ideas to ensure the security of user's identity, such as mice, and virtual keyboard. Mao *et al.* [80] developed an innovative real-time identity authentication technique using mouse behavior learning. This approach entails collecting the mouse behavioral feature vectors of each new user during their initial login, both in dynamic and static scenarios, and it compares them with the feature vectors gathered during subsequent login authentication in simulated abnormal scenarios to attain user identity verification. Shen *et al.* [81] proposed a user identification method that involves analyzing mouse behavior. In a controlled environment, data collection is conducted on the mouse operations performed by the user for specific mouse operations. Subsequently, the features are extracted and categorized to accomplish user identity authentication by analyzing the results of the classification. Kang *et al.* [82] expanded the applicability of a dynamic user authentication approach that relies on keystroke dynamics. This approach now enables the authentication of users typing various textual strings across multiple input devices while distinguishing between legitimate and potential imposter users. Inguanez *et al.* [83] developed a user authentication technique for smart touchscreen devices. This method utilizes a multilayer perceptron (MLP) neural network to classify the graph of the user's keystroke behavior and compares it with the characteristics of the keystroke heatmap in order to achieve user authentication. However, keystroke-based authentication still has certain environmental dependencies and limitations. Variable factors such as different input devices and keyboard layouts may require re-establishing authentication

models. The behavioral feature information provided by the keystroke patterns is relatively limited, so more identity authentication methods using other behavioral features have been developed.

With the popularization of smartphones, touch gesture-based authentication methods have been proposed, which make up for the shortcomings of the insufficient use of behavioral characteristics in the keystroke-based authentication methods. Touch gesture refers to the interaction behavior between users and devices through gestures or touches. Existing authentication schemes usually adopt finger trajectory, touch pressure, sliding speed, touch area, and gesture pattern as behavioral features that need to be extracted and analyzed. Cao *et al.* [84] devised a continuous user authentication scheme that uses vibration response as an implicit biometric feature. It applies a high-pass filter to remove noise and segments the vibration data for each touch event to achieve accurate data matching and recognition and proposes a novel centroid vector method to infer the touch position accurately. Shen *et al.* [85] proposed a method to use gesture patterns, touch operation sequences, and other behavioral data for identity verification. It uses a Markov classifier to model the motion sensor data sequence and capture the temporal and dynamic features of the sensor events, which improves the security and applicability of identity verification. Mao *et al.* [86] proposed an implicit continuous authentication model for user authentication on mobile devices through touch behavior. The model uses data from sensors such as accelerometers and gyroscopes to create feature vectors that include both macroscopic and microscopic features. Yang *et al.* [19] designed a touch-based behavioral biometric recognition technique using a single-class support vector machine and independent random forest training models. The technique evaluates the accuracy of each type and then applies Bayes' theorem to estimate the confidence level of each type, which provides a safe and continuous authentication method for mobile applications. Xu *et al.* [3] combined the physical features of finger touch and the biometric features of touch behavior with a feature fusion authentication framework. It utilizes a particular training sample selection strategy to convert signal features into behavior-agnostic features and subsequently applies knowledge distillation in constructing a touch user authentication scheme. Yang *et al.* [87] presented an integrated identity verification scheme that combines passwords and touch behavioral factors which include touch pressure and sliding speed. The scheme utilizes a novel algorithm to differentiate fine-grained finger input and supports different forms of passwords in the frequency domain, which improves the security of authentication. The above-mentioned methods, without exception, are only for the authentication of a single user. In actual scenarios, there may be multiple users on the same device. The aforementioned studies struggle to address this type of authentication issue.

In contrast to keystroke-based and touch gesture-based authentication, motion-based authentication methods emerged later due to the requirement for a multitude of sensors to collect user motion data for analysis. With the development of wearable and mobile devices, more sensors, such as accelerometers and gyroscopes, are built into the devices to meet the needs of users, which also meets the basic conditions of motion-based authentication methods. Existing motion-based authentication schemes typically utilize motion features such as gait, limb movement, acceleration, and orientation to perform identity verification to ensure the security of users' identities. Chen *et al.* [88] proposed a framework for continuous user authentication based on motion behavioral characteristics, including direction, acceleration, and angular velocity. The framework utilizes smartphones' built-in sensors to collect typical daily motion data of users such as time, frequency, and wavelet domains, which achieves relatively accurate user authentication. Lee *et al.* [89] introduced an advanced smartphone authentication system called iAuth, which leverages the capabilities of multiple sensors embedded within smartphones, Bluetooth connectivity, and wearable devices equipped with sensors. By utilizing machining learning methods to capture the user's unique gait behavior pattern in sensor data from different devices, iAuth enables seamless and ongoing authentication of end-users. Zou *et al.* [18] developed a hybrid deep neural network method for identity verification that extracts robust gait features from time series data. The network combines the convolutional output features with the temporal properties of the data, which enhances the gait features and increases the authentication accuracy. He *et al.* [1] developed a gait feature extractor using transfer learning to reduce time costs and enhance the model's robustness. The extractor has undergone pre-training for user identification tasks. Song *et al.* [90] developed an authentication system based on eye movement. The system verifies the user's identity by capturing the features of human eye movement from the front camera of the smartphone. In terms of multi-user authentication, the authentication schemes need to solve the problem of changing motion features to ensure the system's safety. Kong *et al.* [91] presented an optimized method for user identification based on gait features. To accurately capture the behavioral characteristics of gait data, their method employs a spatial transformation algorithm to optimize coordinate drift and

utilizes a support vector machine algorithm to address the issue of gait feature changes when switching between users. Compared to keystroke-based authentication methods, motion-based authentication methods involve multiple sensor data that may be leaked during transmission, thereby compromising the safety of the system. Wang *et al.* [4] proposed a novel behavioral authentication framework for user motion characteristics to address issues including behavioral dynamics, data privacy, and side-channel leakage. The framework accelerates feature transfer speed on mobile devices mitigates potential side-channel leakage, and improves security during transmission. In summary, motion-based authentication schemes introduce more sensors to capture behavioral features, which makes full use of user behavioral features but also brings greater computational overhead and sensor data leakage problems that necessitate optimization and resolution.

Compared with touch gesture and motion, intrinsic signals, such as EEG, EMG, ECG, breath, facial expression, voice, and others, are highly unique in behavioral recognition, making it more difficult for attackers to accurately replicate. Moreover, existing research also focuses on these sequences of behavioral signals which typically reflect an individual's behavior patterns. Chauhan *et al.* [92] proposed the ContAuth system, which targets inherent behavioral signals of users, such as breath and EEG, obtained from sensors using a class-incremental learning method. It combines deep learning models with online learning models to enhance the robustness of behavior-based authentication. Perera *et al.* [15] designed a sparse representation-based multi-user mobile active authentication scheme according to the dynamic facial expressions of users that automatically adjusts the parameters using the extremum distribution mechanism. It also includes an extension algorithm for applying the scheme in a single-user scenario. Lu *et al.* [93] studied the acoustic Doppler effect of user speech and created a lip-reading-based user authentication system called LipPass that operates in noisy environments. Ji *et al.* [94] introduced a position-sensitive identity verification mechanism called NAuth with nonlinear enhancement. This verification scheme ensures consistent device identity verification by extracting acoustic nonlinear patterns (ANP). Implementing intrinsic signal authentication often requires specialized hardware, which may not be available on all devices. Also, acquiring these signals often requires stable physical and emotional states, and changes in signals caused by emotions or illness may affect the performance of the system.

In addition to the above-mentioned methods relying on devices or sensors for identity authentication, some methods can achieve identity authentication only through user interaction data. With the advancement of big data, machine learning, artificial intelligence, and other technologies, these methods have received more and more attention and research. User interaction behavior, such as social networking, financial transactions, and information browsing has generated a series of data that includes but is not limited to search history data, transaction data, user profile data, sensitive behaviors, and social behaviors. Ruan *et al.* [95] introduced a user authentication scheme that relies on social behavioral characteristics. They extracted and classified social behavioral features such as user browsing and clicking on OSN websites, determined metrics for each feature, and constructed user behavior profiles. Finally, they validated the accuracy of distinguishing genuine users from impostors using user behavior profiles. Shi *et al.* [96] presented an implicit identity verification scheme based on user behavior patterns, leveraging history data on smartphones and movement data collected by sensors to extract behavioral features for user authentication. Skravcic *et al.* [97] presented an implicit authentication scheme centered around user behavior patterns. This approach employs classification models that are built using vast amounts of user transaction data, call records, and email correspondences from various systems, such as banking and social networks, to identify legitimate and malicious users. By leveraging these behavior patterns, the scheme effectively distinguishes between these two user categories. Yang *et al.* [12] designed a wind vane module to achieve lightweight implicit authentication. This module determines the amount of data needed to be collected at different times based on the user's identity legitimacy and interactive behavior habit and adjusts the sampling rate accordingly, which provides an energy-efficient solution for real-time implicit authentication on mobile devices. Shi *et al.* [13] developed an end-point identity authentication technology based on the analysis of user-associated behaviors. The approach employs an interactive behavior common-subsequence similarity algorithm, which extends the traditional behavior common-subsequence (BCS) sequence pattern, and considers the maximum overlap of user behavior sequences and the short sequence overlaps at different time intervals to better identify any anomalies during each user's login session. Wu *et al.* [14] proposed a Hidden Markov Model (HMM) to detect malicious user interactive behavior in network systems by extracting relevant features and defining the observation symbols and hidden states based on the user's access behavior patterns. It maps the user's behavior to an HMM chain

Table 1. Summary of behavioral identity authentication

Object	Description	Characteristics	Issues
Keystroke [17, 77–83]	Keystroke refers to the action of a user inputting information through a keyboard, a keypad, or even a mouse.	(1) Without reliance on additional devices. (2) Extra layer of security for password. (3) Non-invasive continuous authentication.	Data quality easily affected by environmental and user conditions.
Touch gesture [3, 19, 84–87]	Touch gesture refers to the interaction between users and devices through gesture or touch.	(1) Covering multiple dimensional features to improve the security of verification. (2) Ensuring frictionless authentication.	(1) Difficulty in distinguishing and identifying multiple behavior patterns. (2) Cross-platform versatility limited by inconsistent behavioral data formats.
Motion [1, 4, 18, 88–91]	Motion refers to the various postures and movements made by users while using wearable or mobile devices.	(1) Utilization of broader behavioral features. (2) Non-invasive continuous authentication. (3) Less prone to variation caused by external factors.	(1) Multi-device dependency. (2) Privacy risks posed by sensor attacks.
Intrinsic signaling behavior [15, 92–94]	Intrinsic signaling behavior refers to the signals emitted by human organs during the interaction between users and devices.	High biometric uniqueness.	(1) High device dependency. (2) Data quality largely affected by emotions, diseases, etc.
User interaction behavior [12–14, 95–97]	User interaction behavior refers to the behavior of users interacting with applications.	(1) No requirement for sensor data collection and conversion. (2) A wider range of behaviors beyond keystroke or motion.	(1) Suffering from data privacy problem and breach risk. (2) The increasing probability of misjudgments of the model due to adversarial attacks.
Multi-factor [2, 98–100]	Multi-factor refers to the use of multiple categories of behavioral data or a combination of conventional methods with behavioral authentication to verify a users identity.	(1) Flexible combination of authentication methods. (2) The addition of cross-validation for an extra layer of security. (3) Reducing reliance on a single piece of sensitive data.	(1) The challenge of seamlessly integrating various behavioral features and authentication technologies. (2) Imbalanced data from various behavioral features.

and identifies any abnormal or harmful actions to ensure the security of network systems. Such methods need to collect, analyze, and store user interaction behavioral data, especially for behaviors containing sensitive data, which may involve privacy issues. Furthermore, such methods are prone to adversarial attacks. When the attacker adds fake historical data to the training samples, the model will not be able to perform correct authentication.

With the further development of authentication technology, some studies realized that multi-factor authentication systems, which rely on multiple factors to provide robust and accurate results, have stronger security compared with systems that only consider a single behavioral feature. Dasgupta *et al.* [98] proposed a multi-factor authentication system that considers various combinations of different data features through a subset of available authentication modalities, which ensures efficiency in dynamic environments. They conducted tests on one-time and continuous authentication for smartphone users and confirmed that there is complementarity between different signals, which can enhance the performance of the authentication system. Zhang *et al.* [2] designed a multi-modal biometric authentication system that combines EEG and gait data and leverages their unreplicated characteristic. This system uses a doubly authenticated method to improve the anti-counterfeiting and security of the authentication process. Wazzeh *et al.* [99] devised an authentication scheme for mobile devices utilizing federated learning (FL). This scheme allows each user to keep their private data locally for safety and trains models to capture their multi-modal behavioral data with a server for global aggregation. Liu *et al.* [100] presented a user authentication method for smartphones by analyzing user interaction behavior. The approach establishes a behavioral characteristic classification model using data such as the user's touchscreen interaction method, motion, and phone power consumption to enable continuous user identity verification. However, when designing multi-factor authentication methods, suitable algorithms are needed to solve problems such as multi-factor data fusion and data imbalance, and it is technically challenging to seamlessly integrate various factors.

Based on the aforementioned analysis, characteristics and issues of different objects of behavioral identity authentication are summarized in Table 1.

3.2 Behavioral conformity authentication

Behavioral conformity authentication aims to identify potential security and safety risks within a system that fall outside the scope of behavioral identity authentication. The risky objects detected by behavioral conformity authentication mainly include five typical categories, *i.e.*, fraud, malicious intrusion, insider threat, unfair discrimination, and privacy leakage, as shown in Figure 5.

Fraud risks commonly occur in industries such as telecommunications, healthcare, and finance, with a particularly significant impact observed in the financial field. In the financial domain, user identity authentication is typically subjected to heightened scrutiny. This is attributed to the involvement of substantial funds and sensitive information in financial transactions, necessitating the assurance of transactional security and accuracy. Despite the stringent measures, instances of loan fraud still occur, even when identity authentication processes are in place. For fraudulent behavior in the financial sector, some methods can detect non-compliant activities and transactions by monitoring customer transactions and behavior patterns. Jiang *et al.* [101] developed a more comprehensive network for embedding location information, called the Fuller Location Information Embedding Network. The network employs self-supervised learning to characterize the address features of users, with a focus on analyzing the relationship between address information, behavioral information, and customer fraudulent behavior in loan applications, effectively improving the performance of loan fraud detection models. Wu *et al.* [102] proposed a two-stage detection model for identifying fraudulent agents on online large-scale loan platforms. The model extracts 26 features from activity records such as communication logs and application activity histories of agents and borrowers, as well as loan histories. Based on these 26 features, the model characterizes the behavior patterns of the classification objects in detail and achieves high accuracy in identifying fraudulent agents. Awotunde *et al.* [103] proposed an artificial neural network-based detection method for fraud in bank loan management. They extracted a series of borrower-related and loan-related information data as features for identification and classification, in order to detect fraudulent behavior in loan transactions. Chang *et al.* [104] presented a general model for detecting financial fraud using natural language processing technology to accurately detect and classify fraud. As an instance of the model, they implemented an anti-fraud chatbot on a widely used social network service. Nevertheless, certain advanced fraudulent activities transcend the actions of solitary individuals, involving collaboration among multiple users or intermediary agents. In view of these scenarios, a number of research studies have been dedicated to investigating the correlations within the behaviors of multiple users. Xu *et al.* [105] proposed a novel graph neural network with a role-constrained conditional random field (GRC) for loan fraud detection. The model utilizes a graph neural network to detect individual user loan fraud and collusion fraud based on borrower role information and network social relationships. Experimental results demonstrate that the model performs well in detecting loan fraud on Alipay. Wang *et al.* [23] proposed a graph-based approach for behavior modeling called behavior identification graph (BIG). This method delves into the property-level associations in behavioral data and integrates the inter and intra-behavioral correlations into a unified space. Furthermore, they introduced a property graph to describe fine-grained correlations between properties, where the structure of the graph corresponds to the topology information of behavior events. Based on the property graph, they designed an event-property composite model and used network representation learning algorithms to extract fine-grained associations at the behavioral property level. The behavior patterns are represented in a multidimensional spatial distribution of behavioral properties. The effectiveness of this method has been verified in various network threat detection scenarios, particularly in the fraud detection scenario. In addition, some research has focused on purchase fraud and misinformation. He *et al.* [106] proposed a novel malicious user detection system, called Datingswc, that aims to address fraudulent activities such as misinformation or illegal information on dating applications. The system utilizes user profiles, comments, and other relevant information to establish behavior patterns using machine learning models, such as MLP and LSTM. These behavior patterns are then combined and inputted into an attention module to automatically detect suspicious activities following these behavior patterns. Wang *et al.* [107] designed a novel graph-based fraud detection framework to detect fraudulent orders placed by employment fraud teams. The framework comprises two parts: the DPP module, which

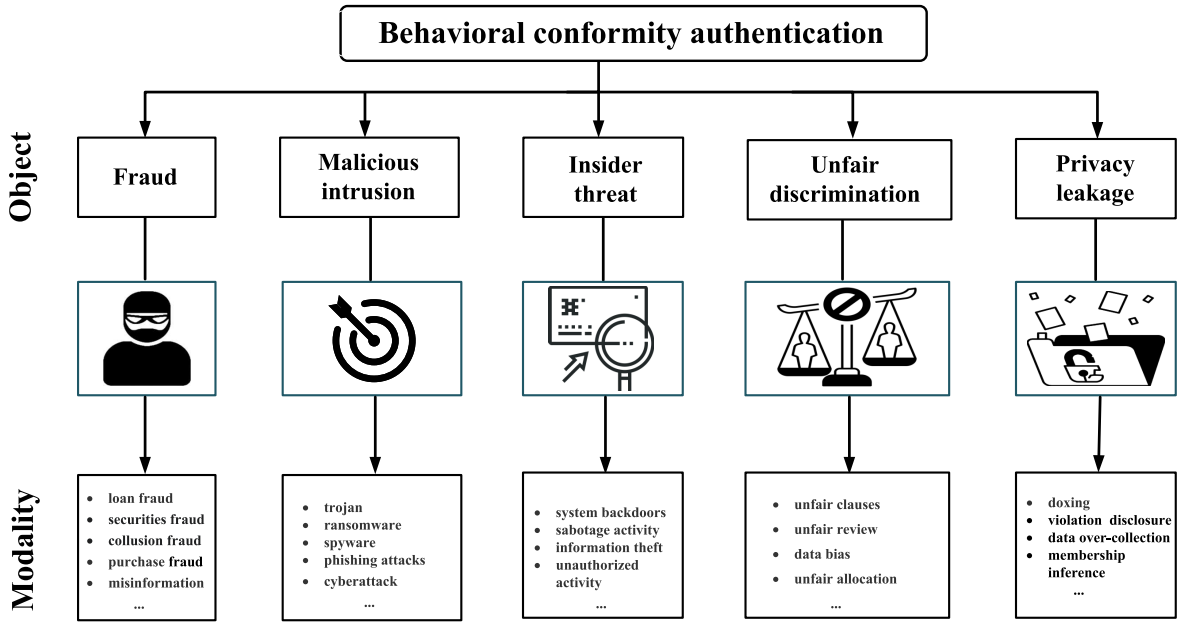


Figure 5. Components of behavioral conformity authentication

extracts feature sequences of user click locations from the website, and the GSR module, which performs neighborhood sampling and information aggregation. The effectiveness of this framework has been validated through purchase fraud detection on the JD platform. Wang *et al.* [5] developed an interactive fraud detection dialogue system, which actively engages in conversations with clients by means of intelligent voice interactions. The system employs imitation learning to master the dialogue strategy and accurately assesses the risk of actual payment, thereby reducing the likelihood of misjudging payment behavior without actual risk. However, behavior-based fraud detection methods still exhibit certain shortcomings and face a set of challenges. Constructing a fraud model necessitates the inclusion of user privacy data, which requires the consent and authorization of both the regulatory platform and the user. Once privacy data is acquired, the model confronts the difficulty of addressing the inherent imbalance between instances of fraudulent and normal behavior during the training phase. Furthermore, the trained model must contend with the ever-evolving deceptive techniques, thereby necessitating regular updates to accommodate the identification of emerging fraud patterns.

Different from fraud with deceptive features, the malicious intrusion has evident attack-oriented features. This type of behavior poses substantial risks, not only to personal computers but also to smartphones, Internet of Things (IoT) devices, and even to network security as a whole. The category of malicious intrusion spans a broad spectrum, including trojans, ransomware, spyware, phishing attacks, and cyberattacks. Existing intrusion detection frameworks often utilize machine learning algorithms to extract features from network behavior, aiding in the differentiation between normal and malicious activities. Chen *et al.* [108] presented an efficient Network-Based Anomaly Detection (NBAD) algorithm using a combination of Deep Belief Network (DBN) and Long Short-Term Memory (LSTM) network for cyberattack detection. Firstly, on the premise of maintaining accuracy, the DBN method is utilized to automatically extract the features of the original data nonlinearly, so as to express the features of the original data with a lower dimension. Furthermore, the classification results, as the basis for identifying anomalous network behavior, are obtained through a lightweight LSTM network. Chen *et al.* [109] presented an automated ransomware pattern extraction and early detection tool. The tool analyzes discovered malware samples and generates a log, from which it extracts sequences of events triggered by ransomware. It also ranks the features of ransomware and detects malicious activity from the learned behavior, which effectively enhances the security of infrastructures. Hamid *et al.* [110] designed a hybrid feature selection method for detecting phishing attack behavior, which combines content-based and behavior-based analysis. The method analyzes the content and ID tags of phishing emails to identify characteristics of

attacker behavior and subsequently detects phishing attacks. Qin *et al.* [111] devised a novel unsupervised network behavior anomaly detection framework, which combines real-time high-order host state in a dynamic interactive environment with dialogue patterns between hosts. It automatically generates high-order features from a series of basic features extracted from the graph neural network (GNN) and identifies various cyberattack behaviors more effectively. Jiang *et al.* [112] proposed a behavior-based method for intelligent recognition and security supervision of unmanned aerial vehicles (UAVs). The method uses location tracking and flight data from the onboard black box to collect real-time behavioral data on UAVs. Then, it identifies suspected intrusion and attack behaviors of UAVs through behavior modeling and issues warnings in potential illegal situations. Garg *et al.* [8] addressed the issue of high false alarm rates in existing real-time anomaly detection by proposing a hybrid detection model that utilizes grey wolf optimization (GWO) and convolutional neural networks (CNN). The model improves the feature selection and anomaly classification capabilities. In the first stage, improved grey wolf optimization (ImGWO) is used for feature selection to minimize the feature set. In the second stage, an optimized convolutional neural network (ImCNN) is used for more effective anomaly classification. Pajouh *et al.* [113] devised a novel intrusion detection model that uses two layers of dimensionality reduction and two layers of classification modules to identify malicious activities such as User to Root and Remote Local attacks. The model uses Naive Bayes and the Deterministic-KNN version to detect suspicious behavior. Wang *et al.* [114] proposed a security detection system (IoT-Praetor) for malicious attacks on IoT devices. The system uses a novel DUD model to construct norms for the interaction and communication behavior of IoT devices. A behavior rule engine is employed to detect device behavior in real time, enabling the identification of behaviors that damage devices through malicious network communication. Some studies also consider the security of data privacy and the safety of the detection framework while striving for accurate detection of malicious behavior. Pei *et al.* [115] devised a personalized federated anomaly detection framework in order to take into account privacy protection in the process of detecting anomalous network traffic. It archives a personalized detection model by fine-tuning the model structure of different systems, which improves the data utility on the premise of protecting privacy and takes into account the safety of the method while improving efficiency. Mothukuri *et al.* [116] presented a federated learning-based method for detecting malicious attacks in IoT. The method utilizes decentralized device data to proactively identify intrusion behaviors in IoT networks, achieves privacy preservation of terminal devices, and performs better in attack detection than non-federated learning methods. Kurt *et al.* [6] devised a data-driven method to detect UDP flooding and spam attacks in IoT networks. To ensure the privacy of node data, the scores are encrypted and perturbed before being sent to the network operator for aggregation of statistical information, followed by anomaly detection through generalized accumulation and algorithms. Intrusion detection methods still have some deficiencies and challenges. Similar to fraud detection, the model of intrusion detection also has the problem of imbalanced training data. When the intrusion detection model needs to be deployed on multiple devices, the problem of heterogeneous data fusion is also considered.

The above-mentioned fraud and malicious intrusion are both behaviors that occur outside the system, while insider threats are relatively intuitive risk behaviors inside the system, which may also lead to system collapse or huge economic losses. System backdoors and equipment failures are relatively common insider threats. Ji *et al.* [117] designed an active anomaly detection network for mobile robots to address system malfunctions caused by outdoor environmental factors. The network effectively integrates multiple sensor signals to ensure robust anomaly detection even in the presence of sensor obstruction in the field environment. Cui *et al.* [118] introduced a blockchain-supported decentralized and asynchronous FL framework for anomaly detection in IoT systems. This framework ensures data integrity, avoids single-point failures, and improves the security of the system. Luo *et al.* [119] first introduced autoencoder neural networks to solve anomaly detection problems in wireless sensor networks. By constructing a three-layer autoencoder neural network, they overcame the huge demands for network resources that deep learning requires. This method is mainly used to detect IoT device failures and changes in the environment. Li *et al.* [120] proposed an active learning and contrastive-based detection model, which monitors the system performance indicators such as CPU utilization, and latency to form a multivariate time series. It models the abnormal and normal sequences based on the VAE model to recognize the abnormal sequences and discover the potential security backdoors in the system. In addition, information theft, unauthorized activity, and even sabotage activity by system insiders are also insider threats. Modell *et al.* [121] devised an incremental approach to analyze anomalous user behavior in event logs. It employs graph embedding to acquire a

vector representation of the users, which is updated over time and utilized to model the configuration profiles of user-accessed resources and builds the formation of a dynamic, interactive network comprising users and resources. The method is applicable for identifying suspicious or unauthorized user behavior in enterprise networks. Hou *et al.* [7] proposed a lightweight framework for detecting abnormal driving behavior. The framework utilizes IoT devices as carriers and captures video and image data using cameras. Based on the analysis of this data, the framework identifies dangerous behaviors such as fatigued driving and erratic driving. Mazzawi *et al.* [122] proposed a machine learning algorithm for detecting malicious user activity in databases, which is used to detect suspicious behaviors, such as information theft and unauthorized activity. The algorithm consists of two primary components: one is responsible for generating models using user behavior, and the other focuses on clustering similar behaviors to detect abnormal patterns that might be shared among a group of users. The current detection methods rely on high-quality behavioral data to ensure models' performance. When encountering sporadic zero-day backdoors or highly covert unauthorized activities, these existing detection methods have difficulty adapting rapidly to newly emerging threats due to a lack of behavioral data.

Unlike insider threats, the risk of unfair discrimination might not be immediately apparent, but rather, it accumulates gradually within the system over time. For instance, within certain machine learning models, data bias could propagate unfairness to model decisions. In cloud environments, resources might be unfairly distributed due to scheduling or allocation mechanisms. If the resources allocated to maintain the security of the environment fall short, the environment will gradually fall into a perilous situation. Additionally, on some network platforms, there may be unfair user clauses. Existing research mainly focuses on detecting or optimizing problems such as data bias, imbalanced distribution, and unfair clauses. Li *et al.* [123] designed a q-Fair Federated Learning (q-FFL) optimization method that enables fairer performance allocation among devices in large-scale federated networks. This method can also be applied to other related problems such as meta-learning, which helps in fair initialization across multiple tasks. Mohri *et al.* [124] developed a novel unbiased Federated Learning framework to address the issue of model bias among different clients in Federated Learning scenarios. This framework is also applicable to learning scenarios such as cloud computing, domain adaptation, and data drift. Wei *et al.* [125] designed a method for optimizing resource balance distribution in cloud services. First, they employed a binary integer programming approach to address the resource allocation optimization problem among independent applicants. Second, they used evolutionary programming to modify the reuse strategy of initial optimal solutions of different applicants. This method provides a solution for resolving the complex issue of resource balance distribution in cloud computing. Lin *et al.* [126] proposed a combined approach of single-layer dominant and max-min fair (SDMMF) allocation and multilayer dominant and max-min fair (MDMMF) allocation to address the issue of fair resource allocation in Intrusion Detection Systems (IDS) in edge computing. The IDS architecture is divided into six layers, and SDMMF allocation is executed recursively starting from the first layer until resources are assigned to the bottom layer, resulting in the equitable allocation of resources that achieves both single-layer and multi-layer fairness in terms of multiple resources. Lippi *et al.* [127] proposed a machine learning and natural language method for detecting unfair clauses in applications or websites. They defined unfair terms and expanded the corpus of clauses in order to better train the model. In addition, the model can not only perform classification tasks but can also identify more information in the clauses and detect and classify the implicit unfair semantics of clauses in the terms. Dolly *et al.* [128] designed a scheme for detecting unfair reviews. This scheme uses sentiment analysis algorithms and supervised techniques to determine the overall semantics of customer comments based on the positive or negative emotions reflected in them. All of the above detection or optimization methods do reduce the unfairness of the target, but the selection of fairness indicators, such as α-fairness [123], has certain subjectivity. The fairness indicators vary depending on different models and scenarios. Therefore, universally applicable fairness indicators should be further studied to promote the formulation of universal fairness clauses.

With the emergence of privacy protection standards such as CCPA [137] and GPDR [138], people pay more attention to the security of private data. Privacy leakage has become a prevalent security concern. Specifically, privacy leakage may arise not only due to malicious intrusion or insider threat but also user disclosure. All these activities will lead to the result of system or user privacy leakage. Current research predominantly centers on two key aspects: the detection of privacy leakage and the enhancement of privacy protection measures. In terms of detection, several studies have explored issues related

Table 2. Summary of behavioral conformity authentication

Object	Description	Characteristics	Issues
Fraud [5, 23, 101–107]	Fraud refers to the behavior of fraudsters for obtaining illegal benefits through fraudulent means, such as concealing facts and stealing information.	(1) Ensuring process security by detecting suspicious activity during transactions. (2) Uncovering hidden fraud networks through behavioral correlation analysis.	(1) Possible leakage and illegal use of user privacy data. (2) Imbalanced training data. (3) Hard to deal with new fraud patterns timely.
Malicious intrusion [6, 8, 108–116]	Malicious intrusion refers to attacks from outside the system, posing threats to personal computers, mobile phones and even the entire network.	(1) Ensuring system security by detecting malicious activity. (2) Timely alerts and responses.	(1) Difficulty in detecting advanced persistent threats. (2) Imbalanced training data.
Insider threat [7, 117–122]	Insider threat refers to the risks existing in the system, affecting the safety of the system from the inside.	(1) Enhancing network safety and system availability. (2) Strengthening the compliance of systems, such as enterprise networks.	(1) Dependencies on high-quality behavioral data. (2) Difficult to address zero-day backdoors.
Unfair discrimination [123–128]	Unfair discrimination refers to unfairness or imbalance within a system, which gradually become apparent as the system runs.	Detecting patterns of unfair discrimination at an early stage allows system personnel to intervene and correct such practices timely, which avoids the cumulative risk of unfair discrimination.	The scarcity of data complicates the comprehensive selection of fairness indicators and hinders the establishment of universally applicable fairness metrics.
Privacy leakage [129–136]	Privacy leakage usually refers to the exposure of users' private data due to security issues, but it also includes disclosure by a second party, a third party, or even other users.	(1) The discovery of external threats and enhancement of system security through privacy leak detection. (2) The improvement of privacy safety through privacy protection measures.	Under data constraints, such as scenarios where there are no clearly defined levels of privacy data, establishing an efficient detection model is a subsequent challenge.

to privacy leakage. Li *et al.* [129] proposed a static taint analyzer for detecting sensitive data leaks during data propagation between application components. This method focuses on contextual information regarding data propagation between multiple components, which allows for higher performance. Liu *et al.* [130] conducted a study on the problem of privacy leakage caused by background access to location in location-based service applications. Their research shows that accessing locations in the background of an application can generate user movement trajectory data, thereby identifying personal information and resulting in privacy leakage. Mehdy *et al.* [131] proposed a hybrid neural network model with multiple inputs and outputs for detecting privacy leaks. The model incorporates pre-trained language models, semantic analysis, linguistics, and other knowledge to accurately identify personal information related to health, finance, and social relationships that Twitter users may disclose when posting tweets. This enables the detection of privacy disclosures by users. Shokri *et al.* [132] conducted a study on the privacy implications of machine learning models, specifically focusing on membership inference attacks that can lead to data leakage. They conducted experiments using a dataset that contained hospital-related information and analyzed various factors that influence privacy leakage. Additionally, they evaluated different strategies to mitigate these privacy risks. Karimi *et al.* [133] proposed an automated method for detecting privacy violations on Twitter. The approach utilizes contextualized string embedding to detect sensitive information in tweets, specifically targeting second-party and third-party doxing and malicious information disclosure, while excluding instances of self-disclosure by users and privacy disclosures not targeting any specific identity. In addition, some researches are dedicated to the improvement of privacy protection. Wang *et al.* [134] developed a new solution for the challenges faced in the collection of multidimensional data under Local Differential Privacy (LDP), including high communication costs and noise issues. The solution includes a Multivariate k-ary Randomized Response (kRR) mechanism called multi-kRR to reduce communication cost, a Markov-based dynamic privacy budget allocation mechanism called Markov-kRR to mitigate the impact of noise, and an improvement on Markov-kRR flipping times threshold to optimize data utility. Rahat *et al.* [135] developed a convolutional neural network-based privacy policy classification model to assess compliance with the privacy policies of various websites. They

used the General Data Protection Regulation (GDPR) as a standard and identified 18 labels from it to annotate and classify the privacy policy dataset. Their experiments demonstrated that very few source websites in the dataset strictly followed the GDPR standards. Li *et al.* [136] proposed a mobile cloud framework to prevent applications from over-collecting user data. This framework stores all user data in the cloud and restricts application access to user data in the cloud, proactively eliminating instances of data over-collection. However, different application services have different protection levels for private information, and the existing privacy leakage detection models are only established for specific scenarios and lack of sufficient scenario transferability. Confronted with scenarios where there are no clearly defined levels of privacy data, the detection model may struggle to yield satisfactory outcomes. Establishing an efficient detection model under such data constraints is a subsequent challenge.

From the above analysis, characteristics and issues of different objects of behavioral conformity authentication are summarized in Table 2.

3.3 Behavioral benignity authentication

The study of behavioral benignity authentication can be mainly divided into the following four aspects: predictability of risk, consistency of execution, traceability of behavior, and integrity of record, as shown in Figure 6.

Predictability of risks is one of the important attributes of a secure network or system. By analyzing and assessing potential risks, the system can identify possible threats and vulnerabilities in advance and take preventive measures. Even in cases where risk threats cannot be entirely mitigated, early warnings can significantly reduce the impact of risk events. Many studies, aimed at risk prediction, have introduced methodologies encompassing risk quantification and credibility assessment. Hu *et al.* [139] proposed a new threat identification method and risk quantification model for predicting threats in multimedia communication networks. The threat recognition method uses a dynamic Bayesian attack graph-based threat prediction algorithm, which aims to predict threat scenarios using complete information. The risk quantification model quantifies the risk status of the entire network and individual hosts by analyzing the security risks at the host and network levels. Wang *et al.* [140] proposed a network behavior risk measurement method by analyzing network traffic. They considered traffic data as network behavior and characterized the network traffic and network topology information. Additionally, they introduced the theory of differential manifolds to measure the behavior risk of the network system. Li *et al.* [141] developed a trust-based model for detecting suspicious behavior in network groups. Firstly, the model constructs a trust matrix between network nodes utilizing network topology information. Secondly, it calculates the similarity matrix of nodes based on their trust levels. Finally, the model clusters the nodes utilizing the similarity matrix to identify potential malicious groups. This approach has a high distinction rate for hidden risks in the network. There are also some studies that indirectly conduct risk prediction through network situation prediction methods. Yang *et al.* [142] proposed a network security situational assessment method based on attack intent distinction. They analyzed the correlation between the attack phase, network configuration information, and attack intent. The method distinguishes the attacking intent and predicts the next attack, which does not rely on historical sequences and is more effective in predicting network security situational assessments. Ghazel *et al.* [143] proposed a global model involving the LC (Logistics Center) region's railway and road transportation, where each model describes the behavior of components throughout the LC environment. By employing the Monte Carlo principle, the global system behavior can be simulated. They also give some solutions for risk mitigation according to the simulation. Vulnerability discovery plays a crucial role in mitigating potential risks within a system, and it has witnessed significant advancements with the progress of detection technologies. Liu *et al.* [144] introduced a software vulnerability detection system, which leverages deep learning and domain adaptation techniques to address the challenge of software vulnerability detection. The system harnesses the automatic feature representation capabilities of deep learning and the domain adaptation framework to discover various vulnerabilities in heterogeneous projects and reduce software security risks. Wan *et al.* [145] proposed a dynamic testing method for semantic denial-of-service vulnerabilities and accurately discovered nine unknown vulnerabilities in the planning of the actual open-source autonomous driving system. Code reuse leads to the propagation of vulnerabilities. Luo *et al.* [146] developed an intermediate representation function model to achieve cross-architecture binary code search through an entropy-based

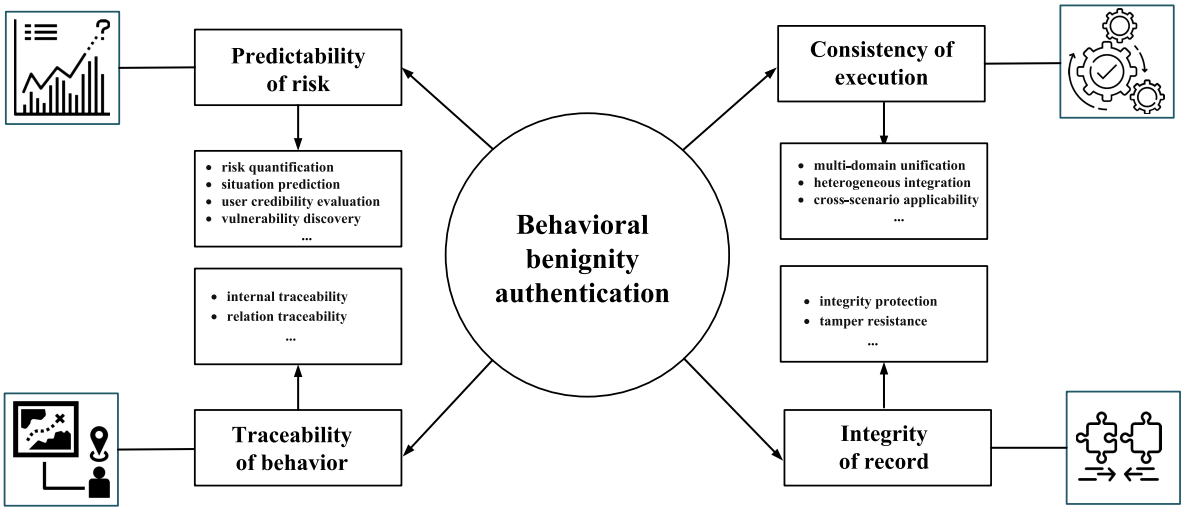


Figure 6. Components of behavioral benignity authentication

adapter and progressive search strategy and tested it on seven different tasks to prove the robustness of the model. Cui *et al.* [147] proposed an automated vulnerability detection framework VRust for Solana smart contracts. The framework automatically detects potential vulnerabilities in contracts by analyzing the intermediate representation of translated Rust source code and program data flow. However, in real scenarios, network or system risk prediction faces more difficulties and challenges, and it is necessary to enhance the robustness of risk prediction in terms of consistency of execution, traceability of behavior, and integrity of record. These aspects can significantly improve the reliability and effectiveness of network or system risk prediction.

Consistency of execution helps ensure smooth collaboration among multiple systems or entities involved in cross-domain risk detection. In real scenarios, achieving unified execution operations in cross-domain interactions over heterogeneous networks contributes to informed risk management and resource optimization. Ding *et al.* [148] designed a resource management algorithm for heterogeneous integrated networks. During the process of collecting and managing heterogeneous resources in the heterogeneous network, the algorithm uses information security transmission technology to ensure the safe collection of resources and uses the improved management algorithm of heterogeneous resources to realize the security management of heterogeneous integrated network resources. Guo *et al.* [149] introduced a reliable cross-domain authentication mechanism applied to the IoT. To achieve cross-domain authentication between heterogeneous IoT domains, the mechanism uses a master-slave blockchain architecture to ensure cross-domain privacy security. To achieve trusted authentication, an improved Byzantine fault-tolerant device based on the reputation value model (RIBFT) is used to conduct a credible assessment. Xuan *et al.* [150] devised a certificate-less cross-domain authentication scheme that possesses the capability to distinguish parameters. The scheme relies on the principles of certificate-less public key cryptography and smart contract technology, which allows for the use of differentiated cryptographic system parameters for authentication between heterogeneous IoT networks, thus enhancing the security of cross-domain authentication for heterogeneous IoT networks. Hao *et al.* [151] proposed a lightweight architecture for consortium blockchain. The architecture utilizes a token accumulation mechanism for authentication of data access control and trust evaluation of requesting nodes. It supports cross-domain data sharing among Internet of Things users from different geographical locations. Li *et al.* [152] introduced a trust mechanism hierarchy that relies on cooperative detection among blockchain nodes. Firstly, they employed federated learning to train a cross-domain unified behavior detection model which broke down data barriers and achieved cross-domain unified evaluation of device behavior trust. Based on this, they designed a layered trust mechanism based on federated detection combined with the transaction performance of blockchain. By dynamically evaluating devices based on behavior detection and blockchain transaction detection, graded trust management of devices is implemented. Sheff *et al.* [153] aimed at the problem of safe scheduling in a federated environment and implemented a static detection compiler and a system that

introduced a phased commit protocol to ensure the consistency and security of scheduling. Chen *et al.* [154] proposed an efficient and privacy-preserving cross-domain authentication scheme, named XAuth, to address the cross-domain authentication issue in Public Key Infrastructure (PKI). The scheme utilizes Multiple Merkle Hash Trees to ensure the responsiveness of cross-domain data management and employs zero-knowledge proof algorithms to ensure privacy in cross-domain authentication. Lin *et al.* [155] designed a time-aware cross-scenario keystroke dynamic authentication mechanism to address the issue of collecting a large amount of data every time the authentication scenario switches. The method improves the quality of data by selectively learning and encoding time information to achieve efficient behavior pattern transfer across scenarios. The method improves data diversity and cross-scenario applicability through a local Gaussian data augmentation method to enable consistent authentication across different scenarios. However, objectives such as cross-domain communication and heterogeneous integration still face several challenges. Cross-domain and heterogeneous networks typically entail distinct security policies and mechanisms. Achieving unified execution operations necessitates overcoming conflicts between diverse security requirements while ensuring that cross-domain operations do not introduce novel security vulnerabilities.

Traceability of behavior plays a key role in risk detection. There is a great deal of uncertainty in the task of risk prediction. In instances of prediction failure, it is necessary to promptly trace the risk behavior to address vulnerabilities and minimize losses. The traceability of behavior is mainly categorized into two types: internal traceability and relation traceability. Internal traceability involves tracing user behavior within the network environment to distinguish potential risk behaviors or to trace the source of suspicious behavior that has already occurred. Relation traceability refers to analyzing a series of behaviors within the network environment, tracing suspicious associated behaviors, or tracing attacks from outside the network environment. Zhang *et al.* [156] presented a secure s-health system designed for cloud service environments. The system introduces a decryption component that is integrated with the user's information during key retrieval. Once integrated, the component remains fixed and prevents key owners from re-randomizing, thereby establishing a binding between the user's information and enabling the tracking of a series of user behaviors. Lin *et al.* [157] proposed a method for detecting internal threats in cloud environments based on behavior traceability. First, the method analyzes the call rules of the cloud service interface to construct the complete behavior process of the call. Then, it uses the behavior tree construction algorithm to generate a legitimate behavior tree describing the behavior of cloud users. Subsequently, behavior trace points are set up to capture call behavior information on the service invocation interface of cloud services. Finally, user interface call information is matched with legitimate behavior trees through keyword matching to trace the source of malicious user behavior. Yu *et al.* [158] proposed a blockchain-enhanced security access control scheme to support traceability and revocability in IoT. Specifically, the scheme involves blockchain-based authentication to store all user information and public keys. Subsequently, system parameters are issued by administrators to users, along with a unique parameter embedded in private keys. The scheme enables tracing malicious behavior by utilizing the parameter in private keys and revoking malicious users accordingly. Wang *et al.* [159] proposed a method for tracing associated events using a composite blockchain structure. Firstly, a storage structure model for the composite blockchain was constructed to achieve data association storage. Secondly, by obtaining the source entity block, an event association graph was constructed by using a source tracing method based on the Apriori algorithm. Finally, the entities were subjected to risk assessment using reinforcement learning. Zhu *et al.* [160] proposed an Ethereum attack traceability method based on graph analysis. They applied graph analysis techniques to analyze the behavioral characteristics of attackers and the relationships among them. Additionally, they used RPC mechanisms to trace the related attackers and attack sources. Behavioral tracing also encounters several challenges. More sophisticated attack behaviors excel at concealing their attack features, rendering themselves indistinguishable from normal behavior patterns. As a result, these behaviors can lurk within the system for an extended duration, which is currently difficult to trace.

Integrity of record can provide a reliability and accuracy guarantee for risk prediction and behavior traceability. Integrity of record includes integrity, accuracy, and tamper resistance of data. Current research is mainly focused on data integrity protection and tamper resistance. Li *et al.* [161] integrated the trusted execution environment SGX with blockchain technology to construct a privacy-preserving multimedia authentication system. The system utilizes SGX to create a trusted execution environment and employs PhotoChain's hybrid storage mode to only store the hash values of the photos on the

Table 3. Summary of behavioral benignity authentication

Object	Description	Characteristics	Issues
Predictability of risk [139–147]	Predictability of risk refers to the distinction of potential behavioral risks in the network environment.	(1) Prevention of potential attacks. (2) Remediation of exploitable vulnerabilities. (3) Reduction of losses through early warning.	Due to the inherent uncertainty of evolving threats, ensuring the robustness of risk prediction needs to be complemented with other security technologies.
Consistency of execution [148–155]	Consistency of execution primarily refers to the method of credibility evaluation and potential risk detection that can perform consistent operations across complex and diverse networks.	Ensuring the seamless execution of operations across various domains and heterogeneous networks in multiple scenarios facilitates unified risk management and resource optimization.	Achieving consistency of execution requires compatibility with different resource forms and operating mechanisms in cross-domain interactions over heterogeneous networks.
Traceability of behavior [156–160]	Traceability of behavior refers to the traceability of potential risks or suspicious behaviors in the network environment.	(1) Tracing suspicious behavior before it becomes a threat. (2) Tracing malicious behavior back to its source and close loopholes. (3) Tracing the source of related behaviors to reveal hidden attack chains.	More sophisticated attackers excel at hiding their attack signatures and making attack behaviors indistinguishable from normal behaviors so that they lurk in systems for extended periods of time to carry out continuous attacks.
Integrity of record [161–165]	Integrity of record means that user data in a trusted network environment should remain complete, accurate, and non-tamperable.	(1) Improvement of risk prediction accuracy through complete and accurate data. (2) Enhancement of traceability analysis reliability.	Protecting record integrity faces multiple data tampering attacks and introduces performance overhead and system complexity like data protection in distributed systems.

blockchain. By using blockchain to ensure data integrity, the system does not add a storage burden to the blockchain. Javaid *et al.* [162] proposed a solution based on Physically Unclonable Functions (PUFs) and blockchain, known as BlockPro, for enhancing the security of data sources and ensuring data integrity in IoT environments. Specifically, the characteristics of PUFs can be used to establish a data source to ensure a unique source, and the data storage method of Ethereum ensures data integrity. Patil *et al.* [163] proposed an efficient privacy-protecting authentication protocol that combines blockchain technology and PUFs. The protocol employs a decentralized digital ledger using blockchain smart contracts to resist attacks from data tampering, thereby ensuring security in an IoT environment. Additionally, by integrating the uniqueness and tamper-proof properties of PUFs with blockchain, the protocol ensures unique device IDs and data integrity in the IoT. Barbareschi *et al.* [164] proposed a mutual authentication scheme relying on the use of PUFs. The scheme employs PUFs' characteristics of being unclonable, unique, and tamper-evident to protect edge nodes in IoT from physical attacks and data tampering. Wei *et al.* [165] proposed a solution to address data security concerns in cloud computing by integrating blockchain technology. The approach involves deploying a distributed virtual machine proxy model in the cloud through the use of mobile agents, which ensures reliable data storage. Furthermore, the solution leverages a blockchain-based data integrity protection framework and generates hash values for corresponding files using the Merkle hash tree. Data alterations are then monitored via smart contracts and alerts are triggered in case of any tampering. In the process of data integrity protection for cross-domain transmission, researchers need to find a balance between security and efficiency, so as to provide more reliable support for risk prediction and behavior traceability.

Based on the aforementioned analysis, characteristics and issues of different objects of behavioral benignity authentication are summarized in Table 3.

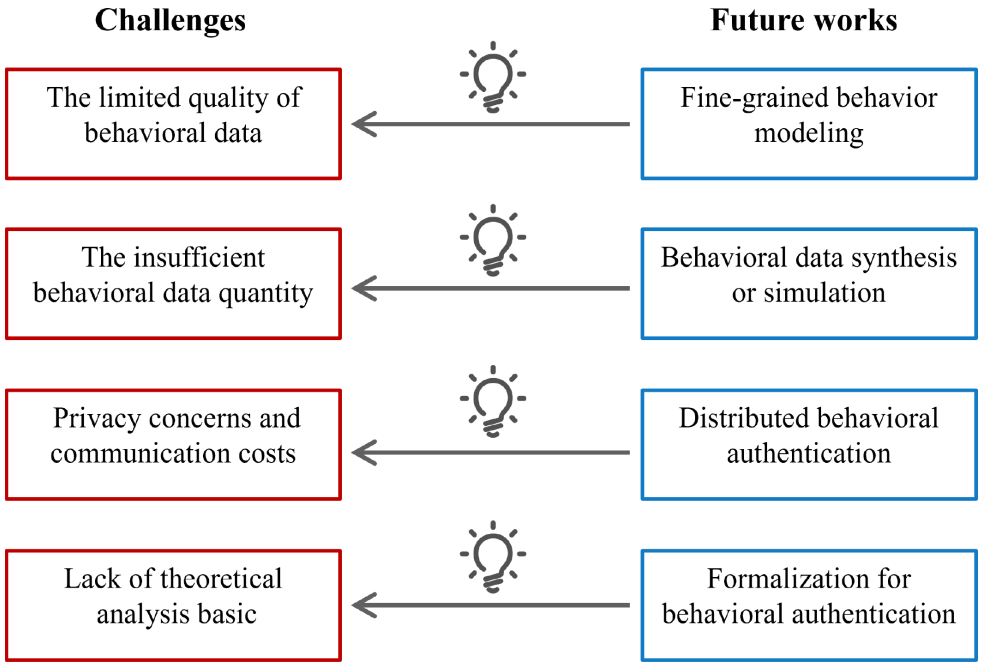


Figure 7. Overview of main challenges and future research directions for behavioral authentication

4 Challenges and future research directions

We thoroughly examine the main limitations associated with existing behavioral authentication methods and discuss innovative research directions that have the potential to significantly augment the applicability and effectiveness of behavioral authentication. A comprehensive overview of limitations and future research directions is shown in Figure 7.

4.1 Challenges of behavioral authentication

4.1.1 The limited quality of behavioral data

How to overcome the limitations of behavioral data quality in the modeling process remains a primary concern. These limitations can be generally attributed to three factors: behavioral data collection and processing, privacy protection, and business attributes. In terms of data collection and processing, inherent difficulties in behavioral data collection or processing can result in low data quality [166]. For example, during the collection of behavioral data, issues such as duplicate or missing data may arise due to unreliability in collection equipment or inconsistencies in data sources, leading to inaccurate or even erroneous results in behavioral data analysis. These undesirable results have a direct impact on the quality and effectiveness of behavior modeling. Therefore, to guarantee the high quality of behavior modeling, it is imperative to have a rigorous process of data cleaning and validation. In terms of business attributes, the inherent characteristics of commercial activities pose challenges in effectively modeling user behavior [167, 168]. In scenarios such as online payment services, the highly imbalanced ratio of fraudulent accounts to legitimate accounts presents significant difficulties in behavior modeling. For interaction data across diverse terminal devices, the distinction between normal and abnormal data is frequently ambiguous. Relying solely on attribute data has limited effectiveness. Designing feasible data augmentation methods is a key prerequisite for achieving effective behavioral authentication and aims to establish high-quality behavior models using low-quality behavioral data.

4.1.2 The insufficient behavioral data quantity

Behavioral authentication is also data-driven, and insufficient behavioral data quantity may influence the effectiveness of behavioral authentication systems. With limited behavioral data available for training, it becomes difficult to create robust behavioral authentication models capable of accurately distinguishing between legitimate and malicious behaviors. This scarcity also increases the risk of biased or unfair models, as they may learn from a narrow subset of behaviors, leading to decreased reliability in authentication performance. Furthermore, the attackers may not repeat previously detected or blocked methods to attack the system, which also intensifies the risks associated with the system [169]. The lack of behavioral data inhibits the generalizability of authentication systems, as models may struggle to adapt to new or evolving threats without comprehensive training data. Therefore, addressing the challenge of insufficient behavioral data quantity is crucial for the development of highly reliable behavioral authentication systems.

4.1.3 Privacy concerns and communication costs

Under stricter privacy protection regulatory constraints, such as CCPA, GPDR, and DSL [137, 138, 170], behavioral data are more tightly controlled. People are also increasingly valuing privacy as they become more aware of the risks associated with data breaches and unauthorized surveillance. Heightened concerns about personal information security have motivated individuals to demand greater transparency and control over how their data is collected and used. These changes directly lead to the difficulty of implementing existing centralized authentication methods for collecting behavioral data from different agents. Despite the advancements in hardware technology and the development of 5G technology, the current computational resources and latency in behavioral authentication also face significant challenges. Behavioral data exists in various forms such as text, voice, and video, and the required models for training are of high complexity [171]. This leads to excessive consumption of computational resources and significant communication costs. For example, when there is a change in the existing behavioral authentication patterns, it becomes necessary to update the entire model, which not only affects the usability of authentication but also results in unnecessary waste of computational resources. It is of great significance to determine models that are compatible with resource constraints and establish an efficient knowledge transfer mechanism of multimodal behavioral data. Regarding authentication latency, current mainstream authentication schemes still rely on the transmission of frequent behavioral data packets to achieve centralized behavior modeling. However, there is distance between different terminal devices, and centralized collection takes time to transmit behavioral data. Even a delay of a few milliseconds, while browsing the internet or attempting to connect to a smart refrigerator, may only affect user experience. Additionally, the centralized authentication relies on a single centralized entity, leading to excessive concentration of authority, and single-point failures can result in severe system issues. However, in scenarios such as automated remote surgery or autonomous driving [172, 173], a few milliseconds of latency could lead to fatal accidents. Therefore, establishing more flexible deployment schemes for behavioral authentication not only ensures lower latency but also avoids unnecessary network congestion and reduces unnecessary bandwidth costs.

4.1.4 Lack of theoretical analysis basic

The existing foundational theoretical efforts primarily focus on conducting specialized theoretical analysis from specific perspectives, considering the constrained conditions of user behavioral data. On one hand, these studies excessively rely on the employed models, making it hard to perform prior evaluation and analysis of data utility. This circumstance prevents accurate anticipation of model performance before data utilization and hinders the determination of whether the chosen models possess sufficient applicability for particular tasks or applications. On the other hand, the data-driven paradigm is difficult to cover or traverse all possible scenarios, consequently impeding the attainability of a general applicable theoretical framework. The diverse requirements arising from different data sources and tasks may necessitate distinct methods and models for conducting behavioral authentication. In summary, the existing relevant research lacks theoretical analysis basic of behavioral authentication, which makes it difficult to evaluate the performance of behavioral authentication in practical applications and hampers the provision of theoretical guidance for optimizing approaches. Hence, the exploration of the formalization for behavioral authentication holds significant significance, akin to the guiding role of information theory's

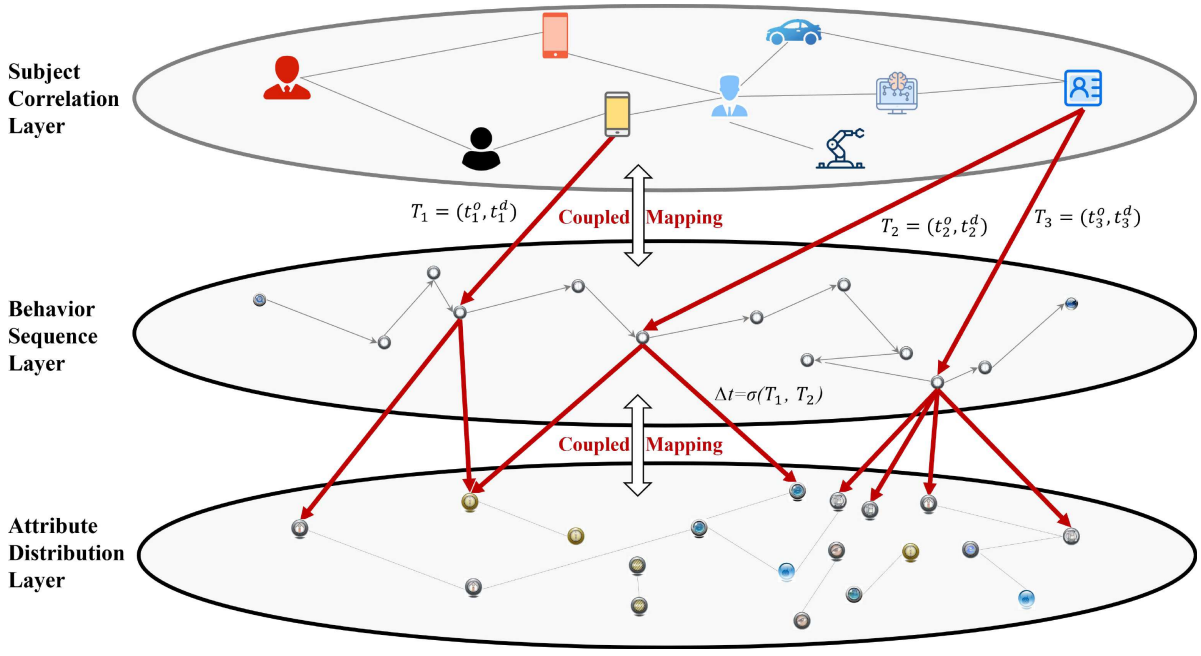


Figure 8. The fine-grained behavior modeling framework consists of the subject correlation layer, behavior sequence layer, and attribute distribution layer. The subject correlation layer reflects the association between subjects and is coupled with a mapping relationship to the behavior sequence layer. There is a time-annotated edge with time information $T = (t^o, t^d)$ between each subject and behavior, where time T indicates the starting time t^o and ending time t^d when the subject initiates the behavior. In the behavior sequence layer, different behaviors occur in a clear sequence, and we denote $\Delta t = \sigma(T_1, T_2)$ as the time difference between two behaviors T_1 and T_2. A behavior is described in detail by several attributes, and their associations are reflected as the coupling mapping between the behavior sequence layer and the attribute distribution layer

fundamental limits in digital communication technology. It will not only offer architectural guidance for high-performance models and algorithm design in behavioral authentication but will also provide systematic metrics for evaluating specific performances. Simultaneously, it will provide a theoretical foundation and analytical methodologies for understanding the mechanisms of behavior modeling in typical services, holding particular importance for estimating data utility in the data handover phase. Efforts towards addressing this issue contribute to a better comprehension of essential issues and drive the advancement and progress of the entire field.

4.2 Future research directions of behavioral authentication

4.2.1 Fine-grained behavior modeling

Future research should focus on developing a behavior modeling method that fully utilizes limited data, taking into account the interaction and collaboration between behaviors from a fine-grained perspective. Fine-grained behavior modeling leverages deep and rich information from the behavior data, which can provide accurate and reliable behavior distribution for behavioral identity, conformity, and benignity authentication.

We are committed to proposing a fine-grained behavior modeling framework to enhance the limited behavior data. It considers the associations of behavior across multiple dimensions such as behavior sequences, subject correlations, and attribute distributions from complex and diverse behavioral data in both virtual and real spaces. Through holistic learning of abundant behavioral information, we can better understand the underlying semantic meanings in behavioral data, and subsequently apply the learned semantics to enhancing the authentication performance.

Correspondingly, as shown in Figure 8, a potential solution is to establish a three-layer knowledge graph structure, including the subject correlation layer, behavior sequence layer, and attribute distribution layer. In the subject correlation layer, subject correlation associations are modeled by introducing the similarity between subjects and their social relevancies. Specifically, the behavior sequence layer

and attribute distribution layer provide a characterization of the latent behavior space encompassing all behaviors, allowing the generalization of subjects from instantiated modeling objects in network services to any behavioral attributes (such as population, individual, and class-based subjects). Multi-dimensional intelligent synthesis strategies are designed to cooperatively generalize the distribution of subject models, thereby mitigating the technical bottleneck of insufficient data in security and safety authentication. In the behavior sequence layer, the temporal relationships of behaviors, such as the order in which behaviors occur, are modeled. We aim to propose a variable-length sequences modeling solution that specifically can be divided into prefix, infix, and suffix partitions based on behavioral order, and adaptive partitions based on behavioral windows. Compared to traditional sequence modeling techniques, it combines behavior intent recognition and time dependency learning. By Extracting information from behavioral context and intent alleviates the inefficiency issues of authentication techniques on limited data. In the attribute distribution layer, co-occurrence associations between attributes from the same behavior are extracted. For example, multiple attributes that appear together in a behavior can serve as co-occurrence relationships between attributes. We conceptualize behavior as a stable system composed of internal associations at the topological level. By designing customized behavioral scanners, we quantify the associations between fine-grained behavioral attributes as measurable graph objects. It excludes confounding information arising from knowledge-driven interference within behaviors, focusing instead on potentially internal associations between fine-grained behavioral attributes as driven by the data. So it can eliminate behavioral noise caused by erroneous or outdated human annotation. Based on the three customized layers, two types of coupled mapping, *i.e.*, subject behavior mapping and behavior attribute mapping, are devised. The former realizes the effect of subject-collaborative filtering through the interaction between subjects and behaviors. Subjects with similar preferences are reflected in the subject correlation layer. The correlations between subjects are further described by the interaction with time between subjects and behaviors. The latter realizes the effect of content collaborative filtering through the interaction between behaviors and attributes, which reflects behaviors with similar attributes in the behavior sequence layer. Through hierarchical modeling of behavior, in addition to introducing more associations to enrich the description of behavior, we can perform customized behavioral authentication based on specific associations within each layer. The coupled mapping between layers further allows aggregating information from other layers into a single layer, thereby obtaining high-density behavioral semantics (information stacking and reduced information carriers jointly improve density) under limited behavioral data to support different authentication tasks.

4.2.2 Behavioral data synthesis or simulation

The challenge of insufficient behavioral data consists of two parts. On the one hand, in scenarios with a defined process, behavioral data synthesis methods are required to supplement the datasets, especially samples of illegal behavior. Data synthesis methods can be utilized to expand existing datasets with data of the same distribution, and the gap between normal behavior samples and illegal behavior samples could be narrowed. On the other hand, in scenarios with complex interactive processes, the interactions of individuals lead to chaos so that there does not exist a fixed distribution of illegal behaviors. Therefore, synthesis methods creating behavioral data of the same distribution no longer work, and we suggest behavioral simulation as an effective resolution.

For the synthesis of behavioral data, the existing methods exhibit sensitivity to outliers, which may compromise the quality of generated samples in the latent space. A potential approach to address these limitations is to combine a generator and two discriminators. The generator incorporates an autoencoder to map the data into a high-dimensional space, where the outlier characteristics of abnormal behavior are accentuated through a specially designed mapping function. The interaction between the generator and the first discriminator enhances the similarity between the generated data distribution and the real data distribution, while the interaction between the generator and the second discriminator enhances the separation between the distributions of normal and illegal behaviors. The adversarial training between the first discriminator and the second discriminator further enhances the distinction of illegal behaviors. Simulation technologies have developed for many decades, consistently regarded as a powerful tool for analyzing complex systems. Agent-based modeling simulation (ABMS) represents an advanced simulation approach, characterized by the generation of individual-level behaviors for both items and agents [174]. In

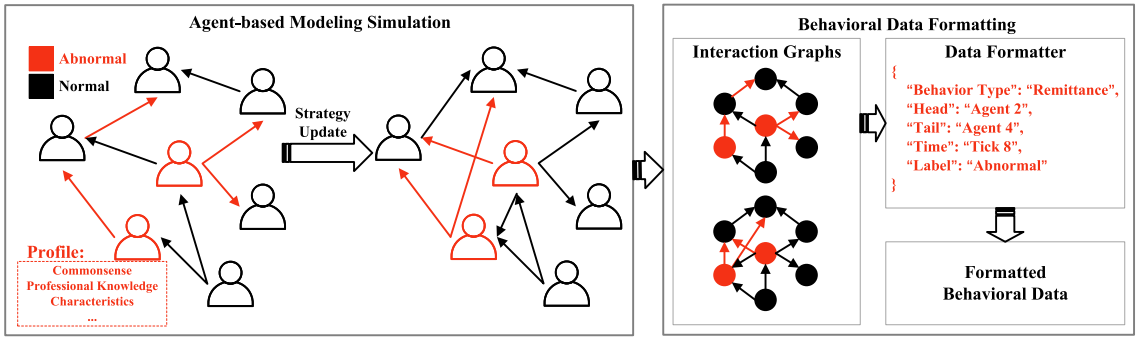


Figure 9. The illustration of behavioral data simulation. First, agents with open-domain reasoning ability and detailed profiles are launched in an ABMS system. Second, the interactions between agents are converted into interaction graphs. Third, these graphs are formatted into the required form through a data formatter. Finally, these data are regarded as simulated behavioral data to supplement the origin dataset

the era of data science, deep learning models have been harnessed to enhance the authenticity of individual behavior generation. This paradigm falls short in addressing the challenge of dynamic distributions, as agents empowered by deep learning models remain constrained by historical data and limited behavior sets. To enhance ABMS for simulating diverse behavioral data, we suggest a novel simulation framework centered around agents endowed with reasoning and learning capabilities. Notably, large language models (LLMs) have demonstrated open-domain reasoning abilities as agents. Leveraging these agents for simulating security scenarios (as depicted in Figure 9), we provide them with security-related knowledge and detailed profiles encompassing motivation, behavior preferences, and other relevant factors, using a variety of models. Through the combination of foundational models with smaller-scale models, each agent is effectively characterized to respond thoughtfully to situational cues. Furthermore, these agents possess learning abilities, enabling them to devise novel strategies beyond historical data, similar to real-world attackers and defenders. In summary, an ABMS built upon this new type of agent equipped with hierarchical knowledge structures and adaptive learning mechanisms offers a promising resolution for simulating behavioral data in complex scenarios.

4.2.3 Distributed behavioral authentication

In general, the effectiveness of behavioral authentication methods often relies on centralized data collection to construct classification models. However, with the increasing emphasis on stricter privacy protection regulations and the need for local data processing in distributed environment, the control and transmission of behavioral data become more challenging. It is necessary to develop distributed behavioral authentication models across different devices while minimizing the costs associated with transmitting privacy-sensitive behavioral data between devices. The concept of a computing power network has been implemented as the infrastructure continues to improve, enabling behavioral data to transition from single central deployment to diverse distributed deployment. This shift from centralized scheduling to distributed collaborative scheduling has provided a favorable opportunity for the advancement of behavioral authentication in near-real-time processing. Sensitive behavioral data can be processed and stored locally, while other behavioral data can be decoupled, allowing for selective interaction with servers in different physical locations. Even if the parties involved in data sharing do not have identical definitions of sensitive behavioral information, negotiations can be conducted to determine the optimal approach for decoupling the sensitivity levels of behavioral information. Distributed behavioral authentication systems can bring enhanced processing capabilities and reduce response time, which improves the effectiveness and reliability of the authentication process significantly.

Therefore, as an essential computational paradigm, distributed learning holds great potential in designing viable architectures for behavioral authentication to achieve a balance among authentication performance, user privacy, and communication costs. An objective is to improve cloud-edge-terminal collaboration to fully leverage the centralized and intensive deployment capabilities of the central cloud, the low latency and high flexibility of edge servers, and the local processing power of the terminal devices.

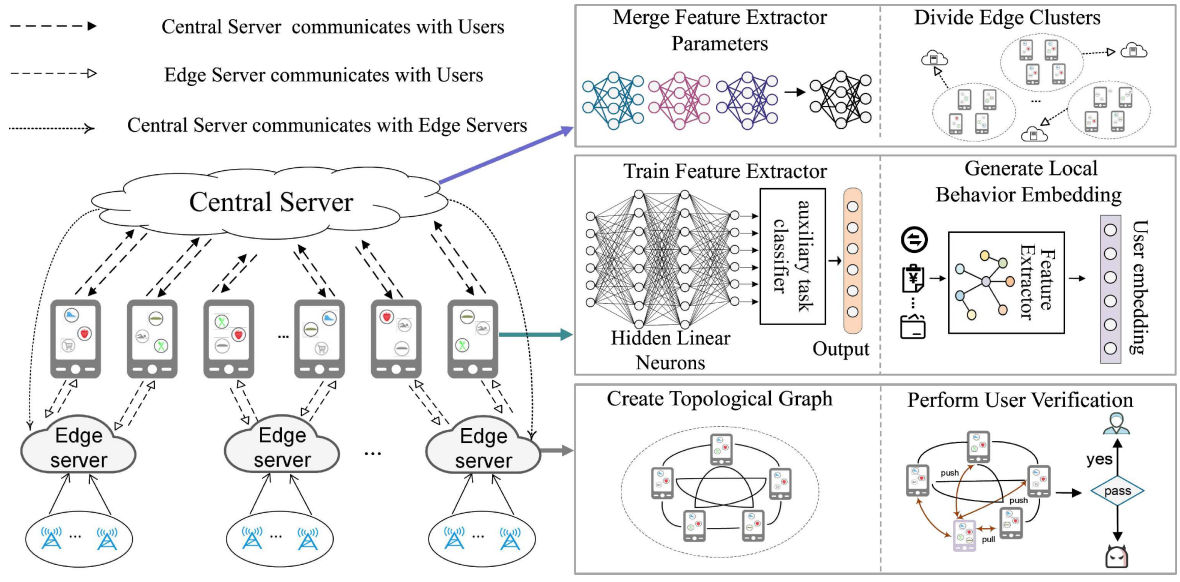


Figure 10. The overall architecture of distributed behavioral authentication. The central server is responsible for collaborating with the terminals to construct feature extractors and coordinating the unified scheduling of edge servers. Edge servers are responsible for deploying specific authentication credentials and partitioning user clusters, as well as responding to specific authentication requests. Terminals are responsible for storing private sensitive data and initiating relevant requests during the verification process

The collaboration approach enhances the safety of behavioral data interactions. Through the collaboration of cloud computing, edge verification, and local data processing, it reduces the processing burden on the cloud center, lowers bandwidth load and authentication latency, and mitigates behavioral data transmission costs.

Correspondingly, as shown in Figure 10, a distributed behavioral authentication framework that leverages cloud-edge-device collaboration has been established, further expanding the application scenarios of behavioral authentication. Specifically, the central server and devices work together to construct a feature extractor. To achieve this, an auxiliary task is defined to obtain behavioral embedding vectors based on a deep neural network. During this process, terminal data remains to be stored locally without the risk of privacy leakage. The local devices share the partial model parameters with the central server to ensure the measurability of different behavioral embedding vectors. If the learning rate of the device is l when the global parameters are updated in the t round, each device will perform parameters updates locally through ${w_{t+1}}^k = {w_t}^g - l\nabla g_k$. The central server uses the operation of ${w_{t+1}}^g = \sum_{k=1}^{K} \frac{n_k}{\sum_{k=1}^{K} n_k} \cdot {w_{t+1}}^k$ to aggregate parameters, and returns ${w_{t+1}}^g$ to different devices. The device updates the local model with the new parameters for the next training round. Once the feature extractor has been built and deployed to various devices, corresponding behavioral vectors are generated locally by different devices, and then different devices send these vectors to the central server. When the central server receives behavioral representation vectors from various terminals, it calculates the similarity between these vectors. Subsequently, the authentication service is deployed to the optimal edge locations based on demand. For the deployment of edge servers, the optimization objective is centered around minimizing latency by: $\min \mathcal{L}(r) = \sum_{s_k \in S} \sum_{a_i \in Z_k} q(a_i, s_k; r)$, where r represents one certain feasible edge deployment scheme, Z_k represents all base stations covered by current authentication server s_k, S represents all edge authentication servers, and $q(a_i, s_k)$ signifies the latency from base station a_i to edge authentication server s_k. Furthermore, each edge server establishes a topological graph. For terminals with similar patterns, corresponding behavior profiles are created, and based on the results, a topological graph $G = (V, E)$ is constructed. The node set is denoted as $V = \{x | x \in X\}$, where X represents the terminals within that cluster, and $E = \{(x, y) | x, y \in V\}$, where (x, y) represents an edge between two terminals. The connection strength of credentials between different terminals is calculated and stored on the edge server. During the verification phase, the k-th terminal generates new behavioral data. For the privacy-sensitive data of this terminal, the input data is processed through the trained feature extractor to generate a

vector representation, denoted as Φ_{k_i}, which is then sent to the edge server. The final authentication result is returned by the edge server. This approach achieves distributed behavioral authentication by the collaboration of cloud, edge, and devices, which significantly reduces authentication latency while ensuring authentication performance.

The proposed framework represents initial efforts towards enabling distributed behavioral authentication, which possesses good flexibility and compatibility. In scenarios where datasets from different clients are highly heterogeneous and non-independently distributed, local model structures and model training strategies can be replaced in our framework. Personalized feature extractors can be trained through techniques such as model decoupling and global model personalization [175, 176]. Additionally, the framework can be used in conjunction with many other technologies. When addressing privacy concerns, our framework can employ technologies such as differential privacy [177] to alleviate privacy issues. Simultaneously, it can utilize existing robust adversarial defense techniques [178, 179] to defend against security threats during the behavior modeling process. Furthermore, when there is distrust among multiple clients, our framework can address this issue by introducing blockchain technology [180, 181]. It is orthogonal to our framework, and thus can be incorporated into our framework for storing behavior profiles.

4.2.4 Formalization for behavioral authentication

Inspired by the formal hypotheses and principles in information theory, we analogize behavioral authentication to concurrent network communication since both the problems of behavioral authentication and concurrent network communication share the common goal of eliminating uncertainty. The fundamental problem in communication is for one end of communication to accurately or approximately reproduce the message selected by the other end.

We give the formalization method for behavioral authentication, which satisfies the formal hypotheses. As shown in Figure 11, we encode the complex features of data to obtain behavior representations, which extract meaningful information and behavior event structures. Ultimately, behavioral authentication aims to eliminate the uncertainty of behaviors. Similar to the Signal-to-Interference-plus-Noise Ratio (SINR) in communication, this uncertainty can be measured as follows:

$$\mathrm{SINR}(b, P_I) = \frac{\sum_{p_i \in P_I} \mathrm{Sim}(b, p_i)^{-\alpha} \cdot \exp(-H_{p_i})}{N_0 + \sum_{p_j \in \mathcal{P} - P_I} \mathrm{Sim}(b, p_j)^{-\alpha} \cdot \exp(-H_{p_j})},$$

where P_I denotes the set of behavior patterns of the user to be verified, $\mathcal{P}$ represents the set of all behavior patterns, and H_{p_i} represents the behavior entropy of the current matched user. The function Sim() measures the similarity between behaviors. The impact on behavioral authentication performance arises from interference by users with similar behavior patterns and the noise inherent in the data itself. For different levels of behavioral authentication, the elements contained in P_I have distinct meanings. Taking behavioral identity authentication as an example, the set P_I degenerates into a singleton set, containing only the user with a deterministic behavior pattern. The signal strength of behavioral identity authentication can be measured by calculating the stability and similarity between the given behavior and the behavior pattern of the user to be verified.

Building upon the formalization for behavioral authentication described above, we conduct a preliminary exploration of the fundamental limits of data utility for behavioral authentication [182]. Specifically, from the perspective of data distribution, we introduce a data utility function based on conditional entropy. We analogize behavioral authentication to the problem of signal transmission in communication channels. By establishing the relationship between conditional entropy and authentication accuracy, we derive upper bounds on accuracy for behavioral authentication: the Shannon upper bound and Rényi upper bound. The former is based on Shannon entropy and is obtained by transforming the Fano inequality; the latter utilizes conditional entropy defined on Rényi entropy and is derived by applying Jensen's inequality and the principle of maximum discrete entropy. When the order of Rényi entropy is greater than 1, the Rényi upper bound can be expressed as follows: where $\boldsymbol{X}$ denotes the attribute combination, N refers to the number of categories of the label Y, e denotes the average authentication error probability, H_α denotes the Rényi entropy, and H_S denotes the Shannon entropy. When the order of Rényi entropy tends to 1, the Rényi upper bound degenerates to the Shannon upper bound. On the real-world business dataset after privacy protection, we obtain the achievable bounds on accuracy for behavioral

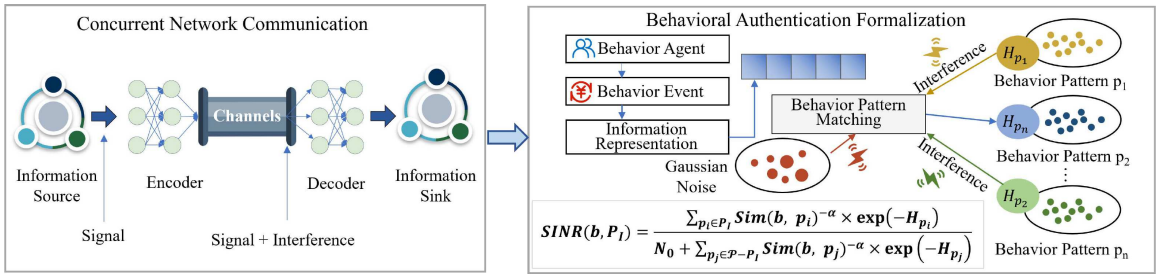


Figure 11. The formalization for behavioral authentication. Inspired by the formal hypotheses and principles in information theory, the ultimate essence of behavioral authentication is the elimination of behavioral uncertainty. This uncertainty can be quantified using a metric similar to the Signal-to-Interference-plus-Noise Ratio (SINR) commonly found in communication. The impact on behavioral authentication performance arises from interference by users with similar behavior patterns and the noise inherent in the data itself

authentication using state-of-the-art and representative ensemble learning and deep learning models. By comparing the theoretical upper bound with the achievable bound, we observe that the theoretical upper bound is higher than the achievable bound, and they are very close to each other. This indicates that the theoretical upper bound provides valuable insights for optimizing the achievable bound.

Furthermore, in the field of communication, there have been initial advancements in semantic communication paradigms [183, 184], which improve the transmission efficiency and reduce the latency of communication systems. In the future, incorporating semantic information into our proposed formalization method for behavioral authentication holds the potential to push the fundamental limits of behavioral authentication.

5 Discussions and conclusion

5.1 Applications

Behavioral authentication has already been applied in practical applications such as financial risk control, healthcare, and intelligent transportation.

In financial transaction services, behavioral authentication can deduce invariant behavioral patterns from changing behavioral data. By integrating multiple factors such as the financial chain, consumption patterns, timing, and location of ordinary consumers, fragmented information is used to accomplish behavioral modeling of consumers. This forms the basis for constructing a comprehensive risk prevention and control system. Behavioral authentication technologies have been implemented in the risk prevention systems of banks and Ant Group [23, 185]. It enables early detection and prevention of fraudulent activities.

In healthcare applications, smart wearable devices from companies like Apple and Huawei use your behavioral data to assess your physical health status [186, 187]. Behavioral authentication provides continuous monitoring and important guidance for the user's health. The industry has witnessed the emergence of behavioral capture and analysis products, such as fall detection vests for the elderly. When the walking patterns, accelerations, and other behavioral features of elderly individuals deviate from their normal patterns, the vest automatically activates a protective mode to mitigate the impact of a potential fall and prevent injuries [188, 189].

In intelligent transportation services, leading automotive companies such as Byd and Tesla have implemented real-time behavior detection of drivers in their onboard systems [190, 191]. When non-benign behaviors are detected, such as abrupt lane changes without signaling or tailgating at an unsafe distance, the onboard system intervenes to mitigate potential risks. This intervention can take the form of audible warnings, visual alerts, or even automated corrective actions, such as gentle steering corrections or adaptive cruise control adjustments. The implementation of behavioral authentication in intelligent transportation services helps to cultivate safer driving habits and reduce the likelihood of accidents.

5.2 Conclusion

Technological advancements have ushered humanity into an unprecedented era of artificial intelligence. Behavioral authentication has emerged as a promising authentication solution in many scenarios and has been successfully and widely applied in practice. It has gradually become a fundamental problem in the field of authentication. This work summarizes the background and applications of behavioral authentication. In particular, it introduces the concept of behavioral authentication including behavioral identity authentication, behavioral conformity authentication, and behavioral benignity authentication. The paper presents a comprehensive review of work conducted in these three levels of behavioral authentication, establishes a clear framework for categorization, and summarizes their corresponding characteristics and issues. The main challenges in current behavioral authentication are analyzed, and key research directions for the future are pointed out including fine-grained behavior modeling, distributed behavioral authentication, and formalization for behavioral authentication. Obviously, with the increasing sophistication of artificial intelligence in various fields and a greater emphasis on user experience, behavioral authentication will display even stronger vitality and play an increasingly important role.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Cheng Wang and Changjun Jiang designed the research. Cheng Wang and Hao Tang articulated the concept of behavioral authentication and divided it into three different levels, and wrote the paper. Hangyu Zhu established a preliminary framework for fine-grained behavioral modeling in the future work. Junhan Zheng participated in the literature review of existing studies. All authors read and approved the final manuscript.

Acknowledgements

We thank the anonymous reviewers for their helpful comments.

Funding

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 62372328, in part by the National Key Research and Development Program of China under Grant 2022YFB4501704, in part by the Program of Shanghai Academic Research Leader under Grant 22XD1423700, in part by the Shanghai Science and Technology Innovation Action Plan Project under Grant 22511100700, in part by the Leadership Project under the Oriental Talent Program, and in part by the Open Fund of Key Laboratory of Industrial Internet of Things and Networked Control, Ministry of Education, under Grant 2021FF08.

References

[1] He L, Ma C, Tu C, et al. Gait2vec: continuous authentication of smartphone users based on gait behavior. In: 25th IEEE International Conference on Computer Supported Cooperative Work in Design, Hangzhou, 2022, 280–285

[2] Zhang X, Yao L, Huang C, et al. Deepkey: a multimodal biometric authentication system via deep decoding gaits and brainwaves. ACM Trans Intel Syst Technology (TIST) 2020; **11**: 1–24

[3] Xu X, Yu J, Chen Y, et al. Touchpass: towards behavior-irrelevant on-touch user authentication on smartphones leveraging vibrations. In: Proceedings of the 26th Annual International Conference on Mobile Computing and Networking, London, 2020, 1–13

[4] Wang C, Xiao Y, Gao X, et al. A framework for behavioral biometric authentication using deep metric learning on mobile devices. IEEE Trans Mob Comput 2021; **22**: 19–36

[5] Wang Z, Yang M, Jin C, et al. Ifdds: An anti-fraud outbound robot. In: Proceedings of the AAAI Conference on Artificial Intelligence, 2021, 16117–16119

[6] Kurt MN, Yılmaz Y, Wang X, et al. Online privacy-preserving data-driven network anomaly detection. IEEE J Select Areas Commun 2022; **40**: 982–998

[7] Hou M, Wang M, Zhao W, et al. A lightweight framework for abnormal driving behavior detection. Comput Commun 2022; **184**: 128–136

[8] Garg S, Kaur K, Kumar N, et al. A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Trans Network Service Management 2019; **16**: 924–935

[9] Lyastani SG, Schilling M, Fahl S, et al. Better managed than memorized? studying the impact of managers on password strength and reuse. In: 27th USENIX Security Symposium, Baltimore, 2018, 203–220

[10] Wang C, Zhu H, Yang B. Composite behavioral modeling for identity theft detection in online social networks. IEEE Trans Comput Soc Syst 2022; 9: 428–439

[11] Li Z, Yang X, Wang C, et al. Crowd-learning: A behavior-based verification method in software-defined vehicular networks with MEC framework. IEEE Internet Things J 2022; **9**: 1622–1639
[12] Yang Y and Sun J. Energy-efficient w-layer for behavior-based implicit authentication on mobile devices. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, Atlanta, 2017, 1–9
[13] Shi C, Du M, Lu W, et al. Identity authentication with association behavior sequence in machine-to-machine mobile terminals. Mobile Networks Appl 2022; 1–13
[14] Wu Z, Tian L, Wang Z, et al. Network user behavior authentication based on hidden markov model. In: 2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE), Chengdu, 2021, 76–82
[15] Perera P and Patel VM. Face-based multiple user active authentication on mobile devices. IEEE Trans Inf Forensics Secur 2018; **14**: 1240–1250
[16] Shen C, Chen Y and Guan X. Performance evaluation of implicit smartphones authentication via sensor-behavior analysis. Inf Sci 2018. **430**: 538–553
[17] Lee H, Hwang JY, Lee S, et al. A parameterized model to select discriminating features on keystroke dynamics authentication on smartphones. Pervasive Mobile Comput 2019; **54**: 45–57
[18] Zou Q, Wang Y, Wang Q, et al. Deep learning-based gait recognition using smartphones in the wild. IEEE Trans Inf Forensics Secur 2020; **15**: 3197–3212
[19] Yang Y, Guo B, Wang Z, et al. Behavesense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. Ad Hoc Networks 2019; **84**: 9–18
[20] Wang C, Zhu H, Hu R, et al. Longarms: Fraud prediction in online lending services using sparse knowledge graph. IEEE Trans Big Data 2023; **9**: 758–772
[21] Wang C, Chai S, Zhu H, et al. Caesar: An online payment anti-fraud integration system with decision explainability. IEEE Trans Dependable Secure Comput 2022; **20**: 2565–2577
[22] Wang C, Wang C, Zhu H, et al. LAW: Learning automatic windows for online payment fraud detection. IEEE Trans Dependable Secure Comput 2021; **18**: 2122–2135
[23] Wang C and Zhu H. Wrongdoing monitor: A graph-based behavioral anomaly detection in cyber security. IEEE Trans Inf Forensics Security 2022; **17**: 2703–2718
[24] Ring M, Wunderlich S, Scheuring D, et al. A survey of network-based intrusion detection data sets. Comput Security 2019; **86**: 147–167
[25] Shu K, Mahudeswaran D, Wang S, et al. Fakenewsnet: A data repository with news content, social context, and spatiotemporal information for studying fake news on social media. Big Data 2020; **8**: 171–188
[26] Charles G and Mori N. Loan repayment performance of clients of informal lending institutions: Do borrowing histories and dynamic incentives matter? Int J Develop Issues 2017
[27] Bailey C, Brody R and Sokolowski M. Fraudulent loans and the united states paycheck protection program. J Financ Crime, 2022; **29**: 519–532
[28] Wang C and Zhu H. Representing fine-grained co-occurrences for behavior-based fraud detection in online payment services. IEEE Trans Dependable Sec Comput 2022; **19**: 301–315
[29] 52th Statistical Report on the Development of the Internet in China. https://www.gov.cn/yaowen/liebiao/202308/content_6900651.htm, 2023.
[30] Chen X, Wang C, Yang Q, et al. Locally differentially private high-dimensional data synthesis. Sci China Inf Sci 2023; **66**
[31] Chen X, Wang C, Cui J, et al. Incorporating prior knowledge in local differentially private data collection for frequency estimation. IEEE Trans Big Data, 2023; **9**: 499–511
[32] Youyou W, Kosinski M and Stillwell D. Computer-based personality judgments are more accurate than those made by humans. Proc Nat Academy Sci 2015; **112**: 1036–1040
[33] Kosinski M, Stillwell D and Graepel T. Private traits and attributes are predictable from digital records of human behavior. Proc Nat Acad Sci 2013; **110**: 5802–5805
[34] Song C, Qu Z, Blumm N, et al. Limits of predictability in human mobility. Science 2010
[35] Yin H, Hu Z, Zhou X, et al. Discovering interpretable geo-social communities for user behavior prediction. In: 2016 IEEE 32nd International Conference on Data Engineering (ICDE), Helsinki, 2016, 942–953
[36] Hashemi SH and Kamps J. Where to go next? exploiting behavioral user models in smart environments. In: Proceedings of the 25th Conference on User Modeling, Adaptation and Personalization, Bratislava, 2017, 50–58
[37] Zhou C, Bai J, Song J, et al. Atrank: An attention-based user behavior modeling framework for recommendation. In: Proceedings of the AAAI conference on artificial intelligence, New Orleans, 2018, 4564–4571
[38] Wang Q, Yin H, Wang H, et al. Tsaub: a temporal-sentiment-aware user behavior model for personalized recommendation. In: Databases Theory and Applications: 29th Australasian Database Conference (ADC), Gold Coast, 2018, 211–223
[39] Nai W, Liu L, Wang S, et al. Modeling the trend of credit card usage behavior for different age groups based on singular spectrum analysis. Algorithms 2018; **11**: 15
[40] Yang J, Qiao Y, Zhang X, et al. Characterizing user behavior in mobile internet. IEEE Trans Emerg Top Comput 2014; **3**: 95–106
[41] Huo C, Zhao Y and Ren W. User behavior sequence modeling to optimize ranking mechanism for e-commerce search. In: Proceedings of the 3rd International Conference on Communication and Information Processing, Tokyo, 2017, 164–169
[42] Zhu Y, Li H, Liao Y, et al. What to do next: Modeling user behaviors by Time-LSTM. In: Proceedings of the 26th International Joint Conference on Artificial Intelligence (IJCAI), Melbourne, 2017, 3602–3608
[43] Cao Q, Yang X, Yu J, et al. Uncovering large groups of active malicious accounts in online social networks. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, 2014, 477–488

[44] Zhang Y, Lv S and Fan D. Research on abnormal account detection methods in online social networks. J Comput Res Develop 2015; **38**: 2011–2027
[45] Wang Z, Jiang C, Ding Y, et al. A novel behavioral scoring model for estimating probability of default over time in peer-to-peer lending. Electr Comm Res Appl 2018; **27**: 74–82
[46] Liu S, Wang S, Zhu F. Structured learning from heterogeneous behavior for social identity linkage. IEEE Trans Knowledge Data Eng 2015; **27**: 2005–2019
[47] Wang Q, Shen D, Feng S, et al. Comprehensive perspective feature combined with crowdsourcing cross-social network user identification. J Softw 2018; **29**
[48] Zafarani R and Liu H. Connecting users across social media sites: a behavioral-modeling approach. In: Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Chicago, 2013, 41–49
[49] Pearman S, Thomas J, Naeini PE, et al. Let's go in for a closer look: Observing passwords in their natural habitat. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, 2017, 295–310
[50] Ye G, Tang Z, Fang D, et al. Cracking android pattern lock in five attempts. In: Proceedings of the 24th Network and Distributed System Security Symposium (NDSS), California, 2017
[51] Constantinides A, Belk M, Fidas C, et al. An eye gaze-driven metric for estimating the strength of graphical passwords based on image hotspots. In: Proceedings of the 25th International Conference on Intelligent User Interfaces, Cagliari, 2020, 33–37
[52] Constantinides A, Belk M, Fidas C, et al. On the accuracy of eye gaze-driven classifiers for predicting image content familiarity in graphical passwords. In: Proceedings of the 27th ACM Conference on User Modeling, Adaptation and Personalization, Larnaca, 2019, 201–205
[53] Pal U, Roy RK, Roy K, et al. Indian multi-script full pin-code string recognition for postal automation. In: 2009 10th International Conference on Document Analysis and Recognition, Barcelona, 2009, 456–460
[54] Bonneau J, Herley C, VanOorschot PC, et al. Passwords and the evolution of imperfect authentication. Commun ACM 2015; **58**: 78–87
[55] Turner S and Housley R. Implementing Email and Security Tokens: current Standards, Tools, and Practices. John Wiley & Sons, 2008
[56] Hallsteinsen S, Jorstad I, et al. Using the mobile phone as a security token for unified authentication. In: Proceedings of the Second International Conference on Systems and Networks Communications (ICSNC), Cap Esterel, 2007, 68–68
[57] Bonneau J, Herley C, VanOorschot PC, et al. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: IEEE Symposium on Security and Privacy, San Francisco, 2012, 553–567
[58] Ruiz-Blondet MV, Jin Z, Laszlo S. Cerebre: A novel method for very high accuracy event-related potential biometric identification. IEEE Trans Inf Forensics Security 2016; **11**: 1618–1629
[59] Sitová Z, Šeděnka J, Yang Q, et al. Hmog: New behavioral biometric features for continuous authentication of smartphone users. IEEE Trans Inf Forensics Security 2015; **11**: 877–892
[60] Bicego M, Lagorio A, Grosso E, et al. On the use of sift features for face authentication. In: IEEE Conference on Computer Vision and Pattern Recognition Workshop (CVPRW), New York, 2006, 35–35
[61] Clancy TC, Kiyavash N and Lin DJ. Secure smartcardbased fingerprint authentication. In: Proceedings of ACM SIGMM Workshop on Biometrics Methods and Applications, Berkley, 2003, 45–52
[62] Kumar A and Passi A. Comparison and combination of iris matchers for reliable personal authentication. Pattern Recognition, 2010; **43**: 1016–1026
[63] Das A, Bonneau J, Caesar M, et al. The tangled web of password reuse. In: 21st Annual Network and Distributed System Security Symposium (NDSS), San Diego, 2014, 23–26
[64] Sun HM, Chen YH and Lin YH. opass: A user authentication protocol resistant to password stealing and password reuse attacks. IEEE Trans Inf Forensics Security 2011; **7**: 651–663
[65] Xu J, You J and Liu F. A fuzzy rules based approach for performance anomaly detection. In: Proceedings of IEEE Networking, Sensing and Control, 2005, 44–48
[66] Cao L. Domain-driven data mining: Challenges and prospects. IEEE Trans Knowledge Data Eng 2010; **22**: 755–769
[67] Tandon G and Chan PK. Learning rules from system call arguments and sequences for anomaly detection. In: Proceedings of ICDM Workshop on Data Mining for Computer Security, 2003
[68] Pan D, Liu D, Zhou J, et al. Anomaly detection for satellite power subsystem with associated rules based on kernel principal component analysis. Microelectron Reliability 2015 **55**: 2082–2086
[69] Li X, Han J, Kim S, et al. Roam: Rule-and motif-based anomaly detection in massive moving object data sets. In: Proceedings of the 17th SIAM International Conference on Data Mining, Minneapolis, 2007, 273–284
[70] Lin XX, Lin P and Yeh EH. Anomaly detection/prediction for the internet of things: State of the art and the future. IEEE Network 2020; **35**: 212–218
[71] Tandon G and Chan PK. Weighting versus pruning in rule validation for detecting network and host anomalies. In: Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Jose, 2007, 697–706
[72] WALDROP MM. Cybercrime. Nature, 2016, 533.
[73] Krol K, Spring JM, Parkin S, et al. Towards robust experimental design for user studies in security and privacy. In: The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER), San Jose, 2016, 21–31
[74] Pearce P, Dave V, Grier C, et al. Characterizing large-scale click fraud in zeroaccess. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, 2014, 141–152
[75] Waldrop MM. How to hack the hackers: The human side of cybercrime. Nature 2016; 533
[76] Abuhamad M, Abusnaina A, Nyang D, et al. Sensor-based continuous authentication of smartphones users using behavioral biometrics: A contemporary survey. IEEE Internet Things J 2020; **8**: 65–84

[77] Zhu M, Zhou J and Wang J. A novel method of user identity authentication based on keystroke features. Comput Eng 2002; **28**: 138–139
[78] Primo A. Keystroke-based continuous authentication while listening to music on your smart-phone. In: 8th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, 2017, 217–225
[79] Ho J and Kang DK. One-class naïve bayes with duration feature ranking for accurate user authentication using keystroke dynamics. Appl Intell 2018; **48**: 1547–1564
[80] Mao C, Cheng Y and Yu W. Research on the method of dynamic real-time identity authentication. Chin J Network Inf Security 2016; **2**: 76–85
[81] Shen C, Cai Z, Guan X, et al. User authentication through mouse dynamics. IEEE Trans Inf Forensics Security 2012; **8**: 16–30
[82] Kang P and Cho S. Keystroke dynamics-based user authentication using long and free text strings from various input devices. Inf Sci 2015; **308**: 72–93
[83] Inguanez F and Ahmadi S. Securing smartphones via typing heat maps. In: IEEE 6th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), Berlin, 2016, 193–197
[84] Cao H, Jiang H, Liu D, et al. Evidence in hand: Passive vibration response-based continuous user authentication. In: 41st IEEE International Conference on Distributed Computing Systems (ICDCS), Washington DC, 2021, 1020–1030
[85] Shen C, Li Y, Chen Y, et al. Performance analysis of multi-motion sensor behavior for active smartphone authentication. IEEE Trans Inf Forensics Security 2017; **13**: 48–62
[86] Mao R, Ji H, Cheng D, et al. Implicit continuous authentication model based on mobile terminal touch behavior. In: IEEE Symposium on Computers and Communications (ISCC), Rhodes, 2022, 1–7
[87] Yang X, Yang S, Liu J, et al. Enabling finger-touch-based mobile user authentication via physical vibrations on iot devices. IEEE Trans Mobile Computing, 2021, **21**: 3565–3580
[88] Chen Y, Shen C, Wang Z, et al. Modeling interactive sensor-behavior with smartphones for implicit and active user authentication. In: IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), New Delhi, 2017, 1–6
[89] Lee WH and Lee R. Implicit sensor-based authentication of smartphone users with smartwatch. In: Proceedings of the Hardware and Architectural Support for Security and Privacy 2016, 2016, 1–8
[90] Song C, Wang A, Ren K, et al. Eyeveri: A secure and usable approach for smartphone user authentication. In: 35th Annual IEEE International Conference on Computer Communications (INFOCOM), San Francisco, 2016, 1–9
[91] Kong J, Guo Y, Liu C, et al. Gait feature recognition method based on smartphone motion sensor. J Comput Appl 2019; **39**: 1747
[92] Chauhan J, Kwon YD, Hui P, et al. Contauth: Continual learning framework for behavioral-based user authentication. Proc ACM on Int Mobile Wearable Ubiquitous Technol 2020; **4**: 1–23
[93] Lu L, Yu J, Chen Y, et al. Lippass: Lip reading-based user authentication on smartphones leveraging acoustic signals. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications, Honolulu, 2018, 1466–1474
[94] Ji X, Zhou X, Yan C, et al. A nonlinearity-based secure face-to-face device authentication for mobile devices. IEEE Trans Mobile Comput 2020; **21**: 1155–1171
[95] Ruan X, Wu Z, Wang H, et al. Profiling online social behaviors for compromised account detection. IEEE Trans Inf Forensics Security 2015; **11:** 176–187
[96] Shi E, Niu Y, Jakobsson M, et al. Implicit authentication through learning user behavior. In: Information Security 13th International Conference, Boca Raton, 2010, 99–113
[97] Skračić K, Pale P and Kostanjčar Z. Authentication approach using one-time challenge generation based on user behavior patterns captured in transactional data sets. Comput Security 2017; **67**: 107–121
[98] Dasgupta D, Roy A and Nag A. Toward the design of adaptive selection strategies for multi-factor authentication. Comput Security 2016; **63**: 85–116
[99] Wazzeh M, Ould-Slimane H, Talhi C, et al. Privacy-preserving continuous authentication for mobile and iot systems using warmup-based federated learning. IEEE Network, 2022
[100] Liu X, Shen C and Chen Y. Multi-source interactive behavior analysis for continuous user authentication on smartphones. In: Biometric Recognition: 13th Chinese Conference, CCBR 2018, Urumqi, 2018, 669–677
[101] Jiang J, Ni B and Wang C. Financial fraud detection on micro-credit loan scenario via fuller location information embedding. In: Companion Proceedings of the Web Conference 2021, 2021, 238–246
[102] Wu Y, Xie Z, Ji S, et al. Fraud-agents detection in online microfinance: a large-scale empirical study. IEEE Trans Dependable Secure Comput 2022; **20**: 1169–1185
[103] Awotunde JB, Misra S, Ayeni F, et al. Artificial intelligence based system for bank loan fraud prediction. In: Hybrid Intelligent Systems: 21st International Conference on Hybrid Intelligent Systems (HIS 2021), 2021, 463–472
[104] Chang JW, Yen N and Hung JC. Design of a nlp-empowered finance fraud awareness model: the anti-fraud chatbot for fraud detection and fraud classification as an instance. J Ambient Intell Humanized Comput 2022; **13**: 4663–4679
[105] Xu B, Shen H, Sun B, et al. Towards consumer loan fraud detection: Graph neural networks with role-constrained conditional random field. In: Proceedings of the AAAI Conference on Artificial Intelligence, 2021, 4537–4545
[106] He X, Gong Q, Chen Y, et al. Datingsec: Detecting malicious accounts in dating apps using a content-based attention network. IEEE Trans Dependable Secure Comput 2021; **18**: 2193–2208
[107] Wang S, Liu Y, Zheng C, et al. Purchase pattern based anti-fraud framework in online e-commerce platform using graph neural network. In: Artificial Intelligence: Second CAAI International Conference, CICAI 2022, Beijing, China, August 27–28, 2022; 112–123
[108] Chen A, Fu Y, Zheng X, et al. An efficient network behavior anomaly detection using a hybrid DBN-LSTM network. Comput Security 2022; **114**: 102600

[109] Chen Q, Islam SR, Haswell H, et al. Automated ransomware behavior analysis: Pattern extraction and early detection. In: Science of Cyber Security: Second International Conference, SciSec 2019, Nanjing, 2019, 199–214
[110] AHamid IR and Abawajy J. Hybrid feature selection for phishing email detection. In: Algorithms and Architectures for Parallel Processing: 11th International Conference, ICA300 2011, Melbourne, Australia, October 24–26, 2011, 266–275
[111] Qin ZQ, Xu HZ, Ma XK, et al. Interaction context-aware network behavior anomaly detection for discovering unknown attacks. Security Commun Networks, 2022
[112] Jiang C, Fang Y, Zhao P, et al. Intelligent uav identity authentication and safety supervision based on behavior modeling and prediction. IEEE Trans Indus Inf 2020; **16**: 6652–6662
[113] Pajouh HH, Javidan R, Khayami R, et al. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks. IEEE Trans Emerging Top Comput 2016; **7**: 314–323
[114] Wang J, Hao S, Wen R, et al. Iot-praetor: Undesired behaviors detection for iot devices. IEEE Internet Things J 2020; **8**: 927–940
[115] Pei J, Zhong K, Jan MA, et al. Personalized federated learning framework for network traffic anomaly detection. Comput Networks 2022; **209**: 108906
[116] Mothukuri V, Khare P, Parizi RM, et al. Federated-learning-based anomaly detection for iot security attacks. IEEE Internet Things J 2021; **9**: 2545–2554
[117] Ji T, Sivakumar AN, Chowdhary G, et al. Proactive anomaly detection for robot navigation with multi-sensor fusion. IEEE Robot Autom Lett 2022; **7**: 4975–4982
[118] Cui L, Qu Y, Xie G, et al. Security and privacy-enhanced federated learning for anomaly detection in iot infrastructures. IEEE Trans Ind Inf 2021; **18**: 3492–3500
[119] Luo T, Nagarajan SG. Distributed anomaly detection using autoencoder neural networks in wsn for iot. In: 2018 IEEE International Conference on Communications (ICC), Kansas City, 2018, 1–6
[120] Li Z, Zhao Y, Geng Y, et al. Situation-aware multivariate time series anomaly detection through active learning and contrast vae-based models in large distributed systems. IEEE J Selected Areas Commun 2022; **40**: 2746–2765
[121] Modell A, Larson J, Turcotte M, et al. A graph embedding approach to user behavior anomaly detection. In: 2021 IEEE International Conference on Big Data (Big Data), Orlando, 2021, 2650–2655
[122] Mazzawi H, Dalal G, Rozenblatz D, et al. Anomaly detection in large databases using behavioral patterning. In: IEEE 33rd International Conference on Data Engineering (ICDE), San Diego, 2017, 1140–1149
[123] Li T, Sanjabi M, Beirami A, et al. ArXiv preprint [arXiv:1905.10497], 2019
[124] Mohri M, Sivek G, Suresh AT. Agnostic federated learning. In: Proceedings of the 36th International Conference on Machine Learning, Long Beach, 2019, 4615–4625
[125] Wei G, Vasilakos AV, Zheng Y, et al. A game-theoretic method of fair resource allocation for cloud computing services. J Supercomput 2010; **54**: 252–269
[126] Lin F, Zhou Y, An X, et al. Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of internet of things devices. IEEE Consumer Electronics Mag 2018; **7**: 45–50
[127] Lippi M, Pałka P, Contissa G, et al. Claudette: an automated detector of potentially unfair clauses in online terms of service. Artif Intell Law 2019; **27**: 117–139
[128] DollyNithisha M, DivyaSri B, LekhyaSahithi P, et al. Unfair review detection on amazon reviews using sentiment analysis. In: High Performance Computing and Networking: Select Proceedings of CHSN 2021, Springer, 2022, 295–306
[129] Li L, Bartel A, Bissyandé TF, et al. Iccta: Detecting inter-component privacy leaks in android apps. In: 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Florence, 2015, 280–291
[130] Liu D, Gao X and Wang H. Location privacy breach: Apps are watching you in background. In: 2017 IEEE 37th international conference on distributed computing systems (ICDCS), Atlanta, 2017, 2423–2429
[131] Mehdy A and Mehrpouyan H. A multi-input multi-output transformer-based hybrid neural network for multi-class privacy disclosure detection. ArXiv preprint [arXiv:2108.08483], 2021
[132] Shokri R, Stronati M, Song C, et al. Membership inference attacks against machine learning models. In: 2017 IEEE symposium on security and privacy (SP), San Jose, 2017, 3–18
[133] Karimi Y, Squicciarini A, Wilson S. Automated detection of doxing on twitter. Proc ACM Human-Computer Interaction 2022; **6**: 1–24
[134] Chen X, Wang C, Yang Q, et al. The opportunity in difficulty: A dynamic privacy budget allocation mechanism for privacy-preserving multi-dimensional data collection. ACM Trans Manag Inf Syst 2023; **14**: 1–24
[135] Rahat TA, Le T, Tian Y. Automated detection of gdpr disclosure requirements in privacy policies using deep active learning. ArXiv preprint [arXiv:2111.04224], 2021
[136] Li Y, Dai W, Ming Z, et al. Privacy protection for preventing data over-collection in smart city. IEEE Trans Comput 2015; **65**: 1339–1350
[137] Stallings W. Handling of personal information and deidentified, aggregated, and pseudonymized information under the california consumer privacy act. IEEE Security Privacy 2020; **18**: 61–64
[138] Godinhode Matos M, Adjerid I. Consumer consent and firm targeting after gdpr: The case of a large telecom provider. Management Science, 2021
[139] Hu H, Zhang H, Yang Y. Security risk situation quantification method based on threat prediction for multimedia communication network. Multimedia Tools Appl 2018; **77**: 21693–21723
[140] Wang Q, Zhao X, Guo J, et al. Research on network behavior risk measurement method based on traffic analysis. Security Commun Networks 2023.
[141] Li Q, He H, Fang B, et al. Abnormal behavior discovery of network groups based on trust. J Comput Sci Technol 2014; **37**: 1–14
[142] Yang H, Zhang Z, Xie L, et al. Network security situation assessment with network attack behavior classification. Int J Intell Syst 2022; **37**: 6909–6927

[143] Ghazel M. Using stochastic petri nets for level-crossing collision risk assessment. IEEE Trans Intell Trans Syst 2009; **10**: 668–677
[144] Liu S, Lin G, Qu L, et al. Cd-vuld: Cross-domain vulnerability discovery based on deep domain adaptation. IEEE Trans Dependable Secure Comput 2020; **19**: 438–451
[145] Wan Z, Shen J, Chuang J, et al. Too afraid to drive: systematic discovery of semantic dos vulnerability in autonomous driving planning under physical-world attacks. In: 29th Annual Network and Distributed System Security Symposium (NDSS), San Diego, 2022
[146] Luo Z, Wang P, Wang B, et al. Vulhawk: Cross-architecture vulnerability detection with entropy-based binary code search. In: 30th Annual Network and Distributed System Security Symposium (NDSS), San Diego, 2023
[147] Cui S, Zhao G, Gao Y, et al. Vrust: Automated vulnerability detection for solana smart contracts. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS), Los Angeless, 2022, 639–652
[148] Ding L, Wang Z, Wang X, et al. Security information transmission algorithms for iot based on cloud computing. Comput Commun 2020; **155**: 32–39
[149] Guo S, Wang F, Zhang N, et al. Master-slave chain based trusted cross-domain authentication mechanism in IoT. J Network Comput Appl 2020; **172**: 102812
[150] Xuan S, Xiao H, Man D, et al. A cross-domain authentication optimization scheme between heterogeneous iot applications. Wireless Commun Mobile Comput 2021; **2021**: 1–14
[151] Hao X, Ren W, Fei Y, et al. A blockchain-based cross-domain and autonomous access control scheme for internet of things. IEEE Trans Serv Comput 2022; **16**: 773–786
[152] Li C, Yang H, Sun Z, et al. Federated hierarchical trust-based interaction scheme for cross-domain industrial IoT. IEEE Internet Things J 2022; **10**: 447–457
[153] Sheff I, Magrino T, Liu J, et al. Safe serializable secure scheduling: Transactions and the trade-off between security and consistency. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, 2016, 229–241
[154] Chen J, Zhan Z, He K, et al. Xauth: Efficient privacy-preserving cross-domain authentication. IEEE Trans Dependable Secure Comput 2021; **19**: 3301–3311
[155] Lin C, He J, Shen C, et al. Crossbehaauth: Cross-scenario behavioral biometrics authentication using keystroke dynamics. IEEE Trans Dependable Secure Comput 2022; **20**: 2314–2327
[156] Zhang Y, Li J, Zheng D, et al. Towards privacy protection and malicious behavior traceability in smart health. Personal Ubiquitous Comput 2017; **21**: 815–830
[157] Lin L, Li S, Lv X, et al. Btdetect: An insider threats detection approach based on behavior traceability for iaas environments. In: 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), New York, 344–351
[158] Yu K, Tan L, Aloqaily M, et al. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE Trans Ind Inf 2021; **17**: 7669–7678
[159] Wang J, Li S, Wanting J, et al. A composite blockchain associated event traceability method for financial activities. Peer-to-Peer Networking Appl 2023; 1–20
[160] Zhu H, Niu W, Liao X, et al. Attacker traceability on ethereum through graph analysis. Security Commun Networks 2022; **2022**: 3448950:1–3448950:12
[161] Li X, Wei L, Wang L, et al. A blockchain-based privacy-preserving authentication system for ensuring multimedia content integrity. Int J Intell Syst 2022; **37**: 3050–3071
[162] Javaid U, Aman MN, Sikdar B. Blockpro: Blockchain based data provenance and integrity for secure IoT environments. In: Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, Shenzhen, 2018, 13–18
[163] Patil AS, Hamza R, Hassan A, et al. Efficient privacy-preserving authentication protocol using pufs with blockchain smart contracts. Comput Security 2020; **97**: 101958
[164] Barbareschi M, DeBenedictis A, LaMontagna E, et al. A puf-based mutual authentication scheme for cloud-edges IoT systems. Future Gen Comput Syst 2019; **101**: 246–261
[165] Wei P, Wang D, Zhao Y, et al. Blockchain data-based cloud data integrity protection mechanism. Future Gen Comput Syst 2020; **102**: 902–911
[166] Jing C, Wang C and Yan C. Thinking like a fraudster: Detecting fraudulent transactions via statistical sequential features. In: Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, 588–604
[167] Bauder RA and Khoshgoftaar TM. The effects of varying class distribution on learner behavior for medicare fraud detection with imbalanced big data. Health Inf Sci Syst 2018; **6**: 1–14
[168] Kaur P and Gosain A. Comparing the behavior of oversampling and undersampling approach of class imbalance learning by combining class imbalance problem with noise. In: ICT Based Innovations: Proceedings of CSI 2015, 23–30
[169] Eisenberg L and Noe TH. Systemic risk in financial systems. Manage Sci 2001; **47**: 236–249
[170] Chen J and Sun J. Understanding the chinese data security law. Int Cybersecurity Law Rev 2021; **2**: 209–221
[171] Phan-Minh T, Grigore EC, Boulton FA, et al. Covernet: Multimodal behavior prediction using trajectory sets. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, 2020, 14074–14083
[172] Derman E and Salah AA. Continuous real-time vehicle driver authentication using convolutional neural network based face recognition. In: 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, 577–584
[173] Gupta R, Tanwar S, Tyagi S, et al. Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions. IEEE Network, 2019; **33**: 22–29

[174] Smith ER and Conrey FR. Agent-based modeling: A new approach for theory building in social psychology. Personality Soc Psychol Rev 2007; **11**: 87–104
[175] Tan AZ, Yu H, Cui L, et al. Towards personalized federated learning. IEEE Trans Neural Networks Learn Syst 2022
[176] Collins L, Hassani H, Mokhtari A, et al. Exploiting shared representations for personalized federated learning. In: International Conference on Machine Learning, PMLR, 2089–2099
[177] Wei K, Li J, Ding M, et al. Federated learning with differential privacy: Algorithms and performance analysis. IEEE Trans Inf Forensics Security 2020; **15**: 3454–3469
[178] Chen P, Yang J, Lin J, et al. A practical clean-label backdoor attack with limited information in vertical federated learning. In: 2023 IEEE International Conference on Data Mining (ICDM), IEEE, 41–50
[179] Huang A, Liu Y, Chen T, et al. Starfl: Hybrid federated learning architecture for smart urban computing. ACM Trans Intell Syst Technol (TIST) 2021; **12**: 1–23
[180] Shayan M, Fung C, Yoon CJ, et al. Biscotti: A blockchain system for private and secure federated learning. IEEE Trans Parallel Distributed Syst 2020; **32**: 1513–1525
[181] Lu Y, Huang X, Dai Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial iot. IEEE Trans Ind Inf 2019; **16**: 4177–4186
[182] Yang Q, Wang C, Wang C, et al. Fundamental limits of data utility: A case study for data-driven identity authentication. IEEE Trans Comput Soc Syst 2020; **8**: 398–409
[183] Dong C, Liang H, Xu X, et al. Semantic communication system based on semantic slice models propagation. IEEE J Selected Areas Commun 2022; **41**: 202–213
[184] Dai J, Wang S, Tan K, et al. Nonlinear transform source-channel coding for semantic communications. IEEE J Selected Areas Commun 2022; **40**: 2300–2316
[185] Roa L, Correa-Bahnsen A, Suarez G, et al. Super-app behavioral patterns in credit risk models: Financial, statistical and regulatory implications. Expert Syst Appl 2021; **169**: 114486
[186] Kunchay S and Abdullah S. Watchover: using apple watches to assess and predict substance co-use in young adults. In: Adjunct Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers 488–493
[187] Xiao X, Li L, Zeng L, et al. Fatigue risk management based pilot sleep monitoring validation experiment. In: Seventh International Conference on Traffic Engineering and Transportation System (ICTETS 2023). SPIE, 13064, 370–376
[188] Ramachandran A, Karuppiah A, et al. A survey on recent advances in wearable fall detection systems. BioMed Res Int 2020; 2020
[189] Pei K, Wang S, He Y, et al. Elderly care stm32-based intelligent anti-fall vest for the elderly. In: 2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), IEEE 5; 413–418
[190] Xun Y, Qin J and Liu J. Deep learning enhanced driving behavior evaluation based on vehicle-edge-cloud architecture. IEEE Trans Veh Technol 2021; **70**: 6172–6177
[191] Ma Xc, Lu J, Wong YD, et al. Exploring the behavior-driven crash risk prediction model: the role of onboard navigation data in road safety. J Adv Trans 2023; 2023

Cheng Wang received a master's degree from the Department of Applied Mathematics at Tongji University, Shanghai, China, in 2006 and a Ph.D. degree from the Department of Computer Science at Tongji University in 2011. He is currently a Professor and the Head of the Department of Computer Science at Tongji University. His research interests include distributed learning, cyberspace security, and intelligent information services.

Hao Tang received a bachelor's degree in engineering at the Department of Computer Science from Chongqing University of Posts and Telecommunications in 2020. He is currently pursuing a Ph.D. degree at the Department of Computer Science at Tongji University in Shanghai, China. His research interests include privacy-preserving learning and intelligent information services.

Hangyu Zhu received a master's degree from the Department of Computer Science and Technology, Tongji University, Shanghai, China, in 2021, where he is currently pursuing a Ph.D. degree with the Department of Computer Science. His research interests include anomaly detection and network representation learning.

Junhan Zheng received a bachelor's degree in computer science from Tongji University, Shanghai, China, in 2023, where he is currently working towards a master's degree from the Department of Computer Science and Technology. His research interests include anomaly detection and attack investigation.

Changjun Jiang received a Ph.D. degree from the Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 1995. He is currently the Leader of the Key Laboratory of the Ministry of Education for Embedded System and Service Computing, Tongji University, Shanghai, China. He is also an Honorary Professor with Brunel University London, Uxbridge, England. Dr. Jiang is also an IET Fellow. He is an Academician of the Chinese Academy of Engineering. His research interests include concurrence theory, Petri nets, formal verification of software, cluster, grid technology, intelligent transportation systems, and service-oriented computing.