Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1499736, 12 pages
https://doi.org/10.1155/2022/1499736

Research Article

A Collaborative Detection Method of Wireless Mobile Network Intrusion Based on Cloud Computing

Xingzhu Wang

School of Computer and Electrical Engineering, Hunan University of Arts and Science, Changde 415000, China

Correspondence should be addressed to Xingzhu Wang; wangxzhu@huas.edu.cn

Received 20 June 2022; Revised 31 August 2022; Accepted 30 September 2022; Published 19 October 2022

Academic Editor: Omprakash Kaiwartya

In order to improve the communication security of wireless mobile network, a collaborative intrusion detection method based on cloud computing is studied. The mobile terminal and the cloud computing platform are connected by the wireless mobile network. The cloud computing platform authentication server adopts a dual server and multifactor authentication scheme for mobile cloud computing to provide authentication services for mobile terminal users. The web server of the cloud computing platform uses the intrusion node detection protocol of the neighbor classification mechanism to provide a communication security protocol for users; Using the HMM algorithm, the intrusion detection module of the computing platform realizes the intrusion detection of wireless mobile network. Finally, using authentication service, security protocol, and intrusion detection module completes the cooperative detection of mobile network intrusion. The experimental results show that this method can realize the cooperative detection of wireless mobile network intrusion, and the detection accuracy is as high as 98%, which ensures the communication security of wireless mobile network.

1. Introduction

With the rapid development of mobile network technology, mobile terminal devices such as smart phones and tablet computers have been widely used in the public. These mobile terminal devices are loved by people due to their mobility, portability, flexibility, and smallness. The effective combination of network technology and mobile terminal equipment has promoted the explosive growth of the number of users [1]. Faced with such a large number of users, relevant industry personnel consider the effective introduction of cloud computing mode and provide users with corresponding services, and then a new type of computing mode has emerged, that is, mobile cloud computing. Using this computing mode, mobile terminal users can access the cloud server through a wireless network connection and then obtain cloud services in an on-demand and easy-to-expand way, which greatly facilitates the user's life, study, and work. The security of the resulting mobile cloud computing data has been highly concerned by the relevant personnel. In this mode, users will generally lose the ability to control data and completely hand over data management to the cloud. How to ensure data security has become the focus technology of the majority of users [2], and data security protection technology for mobile cloud computing came into being. Although the cloud service uses the authentication method to protect the user's data information to a certain extent, because the current research on cloud computing service technology is still in its infancy and the technical level is relatively low, the user data is stored in the process of storage. There are still adverse phenomena such as data loss [3]; so, how to protect user data through the use of related measures such as technological development and innovation presents an urgent problem for researchers in the relevant industry to solve.

With the development of mobile cloud computing, cloud computing has been greatly expanded in its application range. In this mode, application clients can get rid of the constraints of time and space and use mobile device terminals and wireless networks to access rich cloud resources [4]. In the traditional mobile computer environment in the past, users had to perform related data processing and analysis, data storage, and data-intensive computing on mobile devices. However, mobile cloud computing can avoid this

shortcoming [5]. The data storage pulls out the mobile device and regards the mobile device as a simple terminal, which greatly reduces the data processing and resource storage standards for the mobile terminal device. The extremely powerful processing performance of cloud computing, rich and massive service types, and unlimited resources is used [6] to expand the capabilities of mobile terminal devices and achieve high-quality services for low-end mobile devices.

In recent years, the number of mobile communication network users has been increasing, and the storage and control of data information generated by network users require a large physical space, which requires a large amount of investment for mobile communication service providers. The cloud computing service function can reduce the data storage pressure of the communication network terminal [7] and the server load, and the virtualized data management system can improve the information utilization rate and reduce the occupation of the network bandwidth. Because the terminal hardware equipment of the communication network is too large, the professional requirements for manpower and technical personnel required for management and regulation are relatively high. During the peak period of the network usage, the terminal equipment is prone to short-circuit and restart failure due to excessive temperature, which makes network users have a poor sense of online experience. Therefore, the requirements of mobile communication networks for cloud computing services also include the ability to implement deployable system operations for cloud computing, and managers can realize the management and control of the cloud computing platform through software [8] and dynamically grasp the data flow. The demand for cloud computing services of mobile communication networks is not only limited to reducing the load pressure of traditional terminal equipment and grasping communication network data information globally, but more importantly, it can further optimize the communication network through the powerful features of cloud computing and provide more mobile communication service functions. Virtualization is the most prominent feature of cloud computing services. With the help of Internet technology, not only can equipment and systems be virtualized [9] but also all network servers and system operations can be virtualized. The virtualization function can bring great convenience to the optimization of the mobile communication network and reduce the packet loss in the transfer of data hardware devices. Virtualized storage space no longer uses physical devices for storage, which greatly reduces the investment of mobile communication service providers in hard disk storage devices. Under the mobile cloud computing model, different providers have great differences in the security protection capabilities of cloud computing, which makes them eliminated due to their own comprehensive strength in the process of customer service. User's data information processing has become a major problem, and data resource damage is prone to occur in the cloud computing mode. In the process of transferring data resource information to the cloud [10], the user must consider the security service performance of the provider and whether it can satisfy the security of the information to be saved and prevent the loss of data information. In the mobile cloud computing mode, although the cloud environment is free from time and space constraints, it brings a lot of convenience to data storage but also increases the risk of data storage.

At present, many scholars have studied network intrusion detection. Alqahtani proposed a new hybrid optimized long-term and short-term memory (LSTM) method. The convolutional neural network was used to extract the temporal and spatial correlation features of the networked network, and the optimized LSTM was used to predict different attacks in the network. In addition, firefly swarm optimization is combined with LSTM to reduce the computational overhead and improve the prediction accuracy. Nearly 1900503 real-time normal and attack data were collected from the experimental simulation settings based on OMNeT + + – Python – IOT framework. Apply deep learning algorithm to network intrusion detection [11]; Ilyas and Alharbi applied machine learning methods to network intrusion detection and developed five different machine learning classifiers for various attacks. We used the cse-cic-ids2018 data set, which was jointly developed by the communication security agency and the Canadian Network Security Research Institute. It is an extensive network traffic tracking data set, which can capture multiple attacks and is only recently available. The classifier developed in this study relies on a reasonable number of features, and its performance is evaluated for stability and generalization by reporting not only the average performance of 10-fold crossvalidation but also the degree of change from one fold to the next [12]. The above two methods can realize the effective detection of network intrusion, but they have the defects of low detection accuracy and poor real-time detection. In view of the shortcomings of the above two methods applied to network intrusion detection, a collaborative intrusion detection method for wireless mobile networks based on cloud computing is studied, and intrusion detection is realized in wireless mobile networks by using the high-performance computing of cloud computing platform and HMM (hidden Markov model) algorithm. On the basis of basic authentication, dynamic verification code (DVC) and fingerprint information (FP) are added as authentication elements. This paper proposes a lightweight detection protocol with high monitoring probability and strong robustness and uses a variety of methods to achieve cooperative detection of wireless mobile network intrusion. Experiments show that this method can effectively detect wireless mobile network intrusion with high detection accuracy.

2. Materials and Methods

2.1. Overall Architecture of Collaborative Detection of Wireless Mobile Network Intrusion. The overall architecture of the researched collaborative detection method for wireless mobile network intrusion based on cloud computing is shown in Figure 1.

As can be seen from Figure 1, the wireless mobile network is used to connect the mobile terminal and the cloud computing platform. The cloud computing platform uses an authentication server and a web server to provide

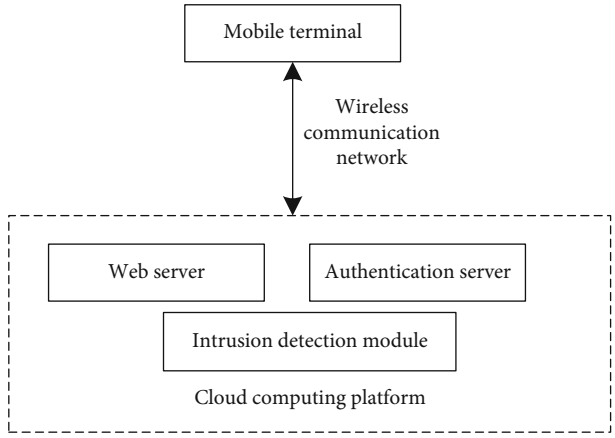

Figure 1: Overall architecture of intrusion collaborative detection.

authentication services and protocols for users of the cloud computing platform. The cloud computing platform has an intrusion detection module, which uses the HMM algorithm to realize the intrusion detection in wireless mobile network, and realizes the collaborative detection of mobile network intrusion through the authentication service of the cloud computing platform, the node intrusion detection protocol, and the HMM algorithm.

2.2. Dual-Server and Multifactor Authentication Scheme for Mobile Cloud Computing. On the basis of the overall architecture of the wireless mobile network intrusion cooperative detection, in order to ensure the operation security of the wireless mobile network and improve the intrusion detection effectiveness of the wireless mobile network, this paper proposes a dual-server and multifactor authentication scheme for mobile cloud computing, which fully considers the characteristics of cloud computing and wireless mobile networks, and improves the communication security of wireless mobile networks through the dual-server and multifactor authentication scheme.

2.2.1. Scenario Description of Mobile Cloud Computing. The mobile payment scenario is a high-security authentication environment involving user property security. This scenario requires the authentication protocol to have the characteristics of efficient and strong authentication. A user registers an account with a cloud computing service provider and then logs into the system through a mobile terminal. By analyzing the behavior of users logging in to the cloud computing platform, we found that the user login behaviors are different and can be basically divided into two categories: one is that users only log in to the cloud computing platform to view account information and do not perform transaction operations; the other class is that users log in to the cloud computing platform and perform transaction operations. In order to improve the user experience and ensure the efficient operation of the mobile cloud computing protocol, authentication schemes with different security levels are provided for these two different user behaviors in the mobile payment scenario.

As for the strength of user authentication, the former type of user behavior does not require transaction information on the cloud computing platform; so, the security requirements for user authentication are relatively low; thus, it is only necessary to provide basic identification of weak authentication, and the traditional username-password authentication method is used to verify the user identity; for the latter type of user behavior, the user needs to perform financial transaction operations on the cloud computing platform [13]; so, strong authentication must be provided to ensure the user's property and privacy information security. On the basis of basic authentication, the dynamic verification code (DVC) and fingerprint information (FP) are added as the authentication factors. The strong security of the transaction process in the cloud computing platform is ensured through multifactor authentication [14, 15]. For the authentication mode of the cloud computing platform server, in order to avoid excessive concentration of risks caused by a single server and meet the high security requirements of mobile payment scenarios, a dual-server mode is adopted to share risks to ensure the robustness and stability of the service [16–19]. The user's fingerprint information is stored in the local trusted execution environment, and the user's fingerprint information does not leave the device, which can prevent security risks caused by the leakage of server fingerprint information [20].

2.2.2. Dual-Server Authentication Scheme for Mobile Cloud Computing. The dual-server and multifactor authentication scheme of mobile cloud computing has two participating entities, the mobile terminal and the cloud. The mobile terminal includes a user, a fingerprint module, and a user agent, and the cloud includes a web server and an authentication server [21–23]. The fingerprint module is embedded in the chip of the mobile terminal and is trusted to perform environmental protection.

Assuming that the security model is as follows: the web server and the mobile terminal are exposed in the open wireless mobile network environment, and the two must ensure the interaction security and achieve the purpose of authentication when communicating. The authentication server and the web server are deployed in the private cloud environment, and it is considered that the web server and the authentication server have been authenticated [24–26]. This solution only needs to focus on ensuring the security of data transmission between the web server and the authentication server.

The identity authentication scheme proposed in this scheme is divided into two stages: user registration and user authentication. Assuming that the mobile device has a fingerprint module, the fingerprint can be securely stored; that is, there is a secure area in the mobile phone, such as the trusted execution environment (TEE) and the security chip (TPM). This scheme includes five parties: user, fingerprint module, user agent, web server, and authentication server. The user, the fingerprint module, and the user agent are all located in the mobile terminal. The fingerprint module is responsible for fingerprint collection, comparison, and secure storage. The user agent is the user APP or browser. Both the web server and the authentication server are deployed in the cloud environment. The web server is

responsible for the communication with the user agent and the forwarding of the authentication data. The authentication server is responsible for verifying the user's identity and saving the user information in the database. The specific process is as follows:

(1) User Registration. In the user registration stage, on the one hand, the user sends the username u, password pw, and mobile phone number phn to the web server, the web server forwards it to the verification server, and the verification server saves $\{u, \text{pw}, \text{phn}\}$ and uses the username as an index; on the other hand, the user performs local registration, that is, the registered user of fingerprint module, and the user enters the fingerprint into the fingerprint module [27–29]. If there is a user fingerprint in the fingerprint module, the fingerprint can be associated with the user account, and the hash value hfp of the user fingerprint information is saved in TEE.

In order to ensure the security of the communication environment in wireless mobile network, it is assumed that the mobile terminal and the web server have their own authentication key pairs and have obtained the public key of the other party. The key pair of the mobile terminal is $\{\text{PK}_u, \text{SK}_u\}$, and the key pair of the web server is $\{\text{PK}_{\text{WS}}, \text{SK}_{\text{WS}}\}$. In the registration phase, the establishment of the communication channel in wireless mobile network has been completed, and the session key between the two is K.

When the web server and the authentication server communicate, we think that the authentication server also has its own authentication key pair $\{\text{PK}_{\text{AS}}, \text{SK}_{\text{AS}}\}$, and the web server and the authentication server have obtained each other's public keys.

(2) User Identification of Cloud Computing Platform. When authenticating users of the cloud computing platform, according to the user's scene, the authentication method based on the security level is provided, which is divided into basic authentication and transaction authentication. The user just logs in to his own account, and when viewing the account information, the basic authentication method of username + password with weak security level is adopted; when the user needs to conduct online transactions on the cloud computing platform, the transaction authentication method is adopted; that is, the fingerprint and the dynamic verification code are added as the identity [30–32]. The verification factor is used to identify users, provide strong authentication, and ensure strong security in the transaction process.

In order to avoid repeated statements, when data transmission is performed among the mobile terminal user, the web server, and the authentication server, the data transmission methods of message encryption and decryption, signature, and signature verification are as follows: the sender first encrypts the data to be sent symmetrically with the session key between them, signs the data to be sent with the sender's private key, and finally encrypts the session key with the receiver's public key. After the receiver receives it, it first uses the sender's public key to verify the signature [33, 34]. If the verification fails, the verification fails; otherwise, the verification passes. The private key of the receiver is used to decrypt the session key, and the session key is used to decrypt the data sent by the sender to obtain the data.

When a user has passed basic authentication and requires online transactions, strong authentication of the user's identity is required. The user authentication diagram is shown in Figure 2.

At this stage, we added fingerprints and dynamic verification codes as authentication factors to ensure strong security. When the user requests to conduct online transactions on the cloud computing platform, the local fingerprint identification process is triggered, and the dynamic transaction code identification process is performed.

2.3. Intrusion Node Detection Protocol with Neighbor Classification Mechanism. On the basis of the above two server multifactor authentication scheme for mobile cloud computing, an intrusion node detection protocol with neighbor classification mechanism is implemented. The intruder can search for the communication nodes of the wireless mobile network by means of wireless detection, etc. and invade the wireless mobile network by capturing and cracking the communication nodes, which lays the foundation for the implementation of other intrusion behaviors. The existing detection methods for wireless mobile network intrusion nodes are mostly based on node location information, time synchronization information, and encryption calculation. A lightweight detection protocol with high monitoring probability and strong robustness is proposed: an intrusion node detection protocol based on a neighbor classification mechanism to detect the intrusion behavior of wireless mobile networks. Due to the large amount of data transmitted in wireless mobile networks, the cloud computing platform is used to realize the operation process of the intrusion node detection protocol and improves the detection efficiency of the intrusion node.

2.3.1. Self-Detection Rules of Wireless Mobile Network Nodes. According to the assumptions, when the intruded node x_i' is deployed in a random position, it is possible that it is deployed near the intruded node x_i, that is, $|x_i - x_i'| \le Z$. If the intruded node x_i' sends information to the outside world, the intruded node x_i can search the neighbor classification information for x_i' in its neighbor classification information table, and $x_i = x_i'$, that is, the node x_i finds that there is a neighbor node nearby, and it uses the same node address for communication. At this moment, the node x_i can judge that the wireless mobile network has been invaded, and the address of the invaded node is x_i. A node can judge whether there is an intrusion node in its neighbor nodes by analyzing the classification results of the neighbors. Taking the neighbor classification mechanism based on node cooperative ranging information as an example [35], if a node completes the ranging and classification of neighbor nodes, it finds that the same node identity information exists in different types of neighbors, indicating that its neighbor nodes have intrusion nodes. The node is captured and cracked by the intruder, and the intruder node x_i' has the same node address

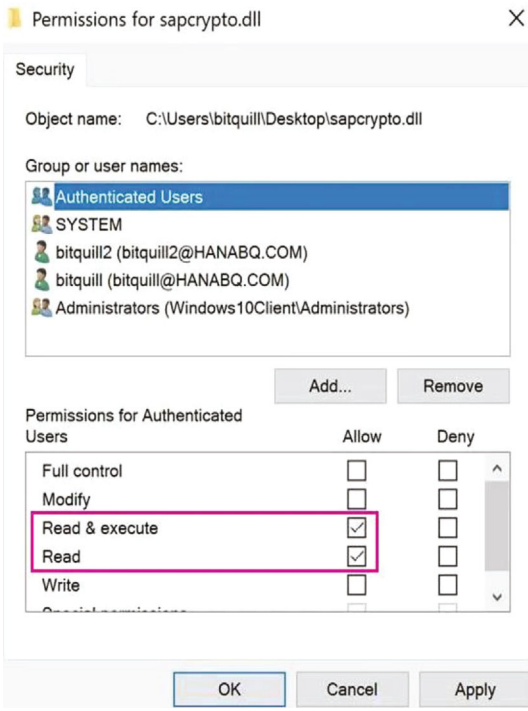

Figure 2: User authentication diagram.

as x' and x_i. At this time, the mutual position and relationship between nodes can be described as $Z < |x_i - x_i'| < Z + Z_f$, $Z_f < |x_i' - x_k| \le Z$, and $|x_i - x_k| \le Z_c$. Therefore, x_i' and x_i will appear in the near neighbor node class and the far neighbor node class in the neighbor classification information table of node x_k, respectively.

2.3.2. Internode Detection Rules. Internode detection rules are the core detection rules of the proposed detection protocol. When detecting wireless mobile network anomalies caused by intrusion nodes, the success rate of internode detection rules is much higher than that of node self-detection rules, and the larger the network scale is, the greater the gap between the two types of detection rules is. The basic idea of internode detection is to find out the abnormal relationship between nodes in the network by comparing the neighbor classification information tables of different nodes.

Let node x_i be the neighbor node $(|x_i - x_{k1}| < Z_c)$ of node x_{k1},and node x_i' be the neighbor node $(|x_i' - x_{k2}| < Z_c)$ of node x_{k2}. Since the intruded node x_i' has the same node address as x_i, the neighbor classification information table of x_{k1} and x_{k2} records the neighbor nodes with the same address (node address $x_i = x'$). According to the Euclidean geometry principle, it can be inferred that they must be adjacent nodes. If x_{k1} and x_{k2} are not adjacent to $(|x_{k1} - x_{k2}| > Z)$, it can be determined that there are intruded nodes in x_i' and x_i, and their shared node address is the intruded node address.

2.3.3. Free Node Detection Rules. Free nodes are usually deployed at the edge of the detection area or in areas with sparse distribution of nodes. Free nodes have no neighbors; so, the internode detection rules cannot be used to judge the authenticity of their identities, and additional detection rules need to be designed to detect free nodes. In order to prevent intruders from using the characteristics of free nodes to bypass protocol detection, it is stipulated that each free node can choose one of its neighbor nodes as its proxy node, this node forwards the data of the free node, and other neighbor nodes do not need to process and forward data from free nodes. When free nodes are captured by intruders and implement intrusion behaviors based on the information contained in them, they can be detected by analyzing and comparing the information provided by proxy nodes [36]. Among them, $x_{d_1}, x_{d_2}, x_{d_3}$ are three free nodes, $x_{d_1}{}'$ and $x_{d_2}{}''$ are two intruder nodes deployed by the intruder in the network, and they all disguise themselves as free nodes. Suppose that x_{a_1} is the proxy node for x_{d_1} and $x_{a_1}{}'$ is the proxy node for $x_{d_1}{}'$, since the protocol stipulates that the free node can only select one neighbor node as the proxy node, and when two different nodes are selected as the proxy node of the same free node (same node address), it can be determined that there is an intrusion node in the network, and the address is the address of the intruded node. On the other hand, the intruded node $x_{d_2}{}''$ can disguise itself as a free node by reducing the wireless transmission power, but it can still detect its real identity by analyzing the neighbor classification information table of its proxy node. The free node detection rule will cause the connectivity of the free node area to decrease, but considering the limited number of free nodes in the wireless mobile network [37] and the limited connectivity, the impact of the decreased connectivity of free nodes on the wireless mobile network is almost negligible.

2.4. HMM-Based Intrusion Detection Method of Wireless Mobile Network. On the basis of the intrusion node detection protocol with neighbor classification mechanism mentioned above, intrusion detection of wireless mobile network is carried out based on the HMM model. HMM (hidden Markov model) is a double stochastic process, including the state transition of the model and the randomness of observable events in a specific state. It is used to describe a Markov process with hidden unknown parameters and is a statistical Markov model in which the modeled system is considered to be a Markov process with unobserved states.

The HMM model is a random model obtained by extending the Markov chain, which can realize the intrusion detection of wireless mobile networks. HMM is a double-random process, that is, a Markov chain and a random process. The Markov chain represents the unobserved finite state chain representing the transition of the state, and the general random process represents the relationship between the state and the observation sequence.

The random events described by the HMM model satisfy the following assumptions: the current state is completely determined by the previous state and has nothing to do with the historical state; the transition probability between states

does not change with time [38]; the observed value is only related to the current state.

The HMM model can usually be expressed as a 5-tuple, namely, $\alpha = (S, O, \pi, A, B)$, where the state value set is $S = \{s_1, s_2, \cdots, s_n\}$, and n represents the total number of states of the HMM; the observation value is $S = \{v_1, v_2, \cdots, v_m\}$, and m is the number of observations; the initial distribution vector is $\pi = \{\pi_1, \pi_2, \cdots, \pi_N\}$, $\pi_i = P\{s_1 = \theta_i\}$, which means the probability of observing θ_i in state s_1 and satisfying $\sum_{i=1}^{n} \pi_i = 1$; the observation symbol probability matrix $A = [a_{ij}]_{N \times N}$ is the state transition probability matrix, a_{ij} can represent the probability of transitioning from state θ_i to θ_j at the current moment, $a_{ij} = P(s_{t+1} = \theta_j | s_t = \theta_i)$, where $i, j = 1, 2, \cdots, n$, and it satisfies $\sum_{j=1}^{n} a_{ij} = 1$;

Observation probability matrix is $B = [b_{ij}]_{N \times M}$, and $b_{ij} = b_i(o_j) = P(o_j = v_j | s_j = \theta_j)$ represents the probability of being in state θ_j at time t and random observation v_j.

The training of the HMM model is parameter estimation, which is to estimate the model parameter $\alpha_1 = (A, B, \pi)$. According to the classification result of each sample data by Mahalanobis distance, the intrusion category is determined [39–41], and the posterior probability $P(\alpha_k | o_t)$ of the intrusion category corresponding to each sample is assigned as 1; the value of each observation probability in the observation probability matrix $B = [b_{ij}]_{N \times M}$ is obtained by Bayesian reasoning formula:

$$P(o_j = v_j | s_j = \theta_j) = \frac{P(s_j = \theta_j | o_j = v_j) P(o_j = v_j)}{s_j \pi_j o_j}. \quad (1)$$

In formula (1), $P(o_j = v_j)$ is the reciprocal of the observation time length T, and the value of $P(s_j = \theta_j | o_j = v_j)$ is $P(\alpha_k | o_t)$.

According to the forward evaluation rule and the backward evaluation rule, the initial distribution vector pπ and the state transition probability matrix $A = [a_{ij}]_{N \times N}$ are updated. According to the forward evaluation algorithm and the backward evaluation algorithm, we can get

$$P(O|\alpha) = \sum_{i=1}^{N} \alpha_t(i) \beta_t(i) \pi_j. \quad (2)$$

In formula (2), let $\alpha_t(i)$ represent the probability that model α is in state q_i at time t, and the output observation sequence is $o_1, o_2, \cdots, o_t$; $\beta_t(i)$ represents the probability that model α is in state q_i, and output observation sequence is $o_{1+1}, o_{2+2}, \cdots, o_T$ at time t. Taking the largest posterior probability as the target, it can be expressed as

$$K = -\log \frac{P(\alpha_1, O|\alpha)}{P(O|\alpha)}. \quad (3)$$

Deriving π_i and a_{ij} in formula (3) can get π and $A = [a_{ij}]_{N \times N}$ as

$$\frac{\partial K}{\partial \pi_i} = \left[\frac{1 - \delta}{P\{O|\alpha\} P\{\alpha_1, O|\alpha\}} \right] b_i(O_1) \delta \beta_1(i), \quad (4)$$

$$\frac{\partial K}{\partial \pi_i} = \left[\frac{1 - \delta}{P\{O|\alpha\} P\{\alpha_1, O|\alpha\}} \right] \sum_{t=1}^{T} \beta_1(i) \delta b_j(O_t) \alpha_{t-1}(i). \quad (5)$$

According to formula (6), it can judge whether the HMM training is end:

$$|\lg (P(O|\alpha_{k+1})) - \lg (P(O|\alpha_k))| \le \varepsilon. \quad (6)$$

In formula (6), ε is the end threshold. When the end condition is satisfied, the current model α is used as the final intrusion detection model of wireless mobile network. Otherwise, it should enter the next sample and continue training each model parameter.

When the HMM model is trained, an independent model is obtained for different intrusion categories. When the intrusion class is α, the resulting HMM model can be expressed as α_1, α_2, ..., α_g. At this time, the unlabeled sample data that has undergone data preprocessing is input into the model α_1, α_2, ..., α_g to obtain a set of posterior probability densities, namely, $P(O|\alpha_1)$, $P(O|\alpha_2)$, ..., $P(O|\alpha_g)$, and the mode α with the largest probability value is selected as the corresponding intrusion category.

3. Results

The detection performance of the wireless mobile network intrusion detection method based on cloud computing is tested by experiments, 10 mobile terminals are selected as the user terminal, the user terminal is connected to the cloud computing platform, and the intrusion data in the network intrusion data set is selected as the intrusion data in the experimental test process.

10 nodes in the wireless mobile network are randomly selected, and the method in this paper is used to detect the detection results of wireless mobile network intrusion. A new hybrid optimized long and short-term memory (LSTM) method proposed in document [11] and a network intrusion detection method based on machine learning proposed in document [12] are taken as comparison methods. The comparison results are shown in Table 1.

It can be seen from the experimental results in Table 1 that the method in this paper can effectively detect the intrusion nodes in the wireless mobile network. The experimental results in Table 1 verify that the method in this paper can not only achieve effective detection of wireless mobile network intrusion but also has a high detection accuracy. The methods of reference [11] and reference [12] detect 10 random nodes in wireless mobile networks, and there are cases where the intrusion nodes are detected as normal nodes. The detection accuracy of the method in this paper is significantly higher than the other two methods, which verifies that the method in this paper has a high performance of intrusion detection in the wireless mobile network.

For applications on a mobile terminal, since the mobile terminal is a resource-limited device, the operation time of

Table 1: Intrusion detection results of wireless mobile network.

Node serial number	The method of this paper	Reference [11] method	Reference [12] method	Actual results
1	Normal node	Normal node	Normal node	Normal node
2	Intrusion node	Intrusion node	Normal node	Intrusion node
3	Normal node	Normal node	Normal node	Normal node
4	Intrusion node	Intrusion node	Intrusion node	Intrusion node
5	Normal node	Normal node	Normal node	Normal node
6	Intrusion node	Normal node	Intrusion node	Intrusion node
7	Normal node	Normal node	Normal node	Normal node
8	Normal node	Normal node	Normal node	Normal node
9	Normal node	Normal node	Normal node	Normal node
10	Normal node	Normal node	Normal node	Normal node

Table 2: Encryption and decryption performance of this method.

File size	Generate encryption key time/ms	Generate ciphertext time/ms	Time to generate decryption key/ms	Generating plaintext time/ms
1 KB	1	2	1	5
10 KB	1	3	1	10
100 KB	1	5	1	38
1 MB	1	20	1	126
10 MB	1	156	1	568
100 MB	1	345	1	1052
200 MB	1	1845	1	2064
1000 MB	1	13584	1	10234

connecting the mobile terminal to the cloud computing platform is very important. In order to verify whether the method in this paper can improve the security performance of the wireless mobile network, when designing the experimental encryption and decryption performance, the computing time of the mobile terminal and the private cloud during the encryption process are measured, respectively, and nine rounds of encryption and decryption are performed. The performance of encrypting and decrypting of different sizes files are tested when using the method in this paper to detect wireless mobile network intrusion. Since mobile terminals are resource-constrained devices and can only perform lightweight operations, a 1 GB file can already be considered a large file. Five aspects of the encryption key generation time, ciphertext generation time, decryption key generation time and plaintext generation time, etc., with file sizes of 1 KB, 10 KB, 100 KB, 1 MB, 10 MB, 100 MB, 200 MB, 500 MB, and 1000 MB are tested, respectively. The encryption and decryption performance test results of the method in this paper are shown in Table 2.

When selecting the data, the files of each size are tested 5 times, and then the average is taken to ensure the objective and accurate experimental data. From the experimental results in Table 2, it can be seen that as the file size increases, the time to generate the decryption key and the time to generate the plaintext gradually increase, but the time to generate the encryption key and the decryption key remains basically unchanged. That is to say, as the size of encrypted files increases, the computing burden on the private cloud increases, while the computing burden on the mobile terminal remains basically unchanged. Through the remote encryption process, no matter how large the file needs to be encrypted, the mobile terminal only needs to generate the encryption and decryption keys, and the computational burden is very low, only a few milliseconds. Especially when the file is large, the contribution of the method in this paper to reduce the burden of mobile terminals is more prominent, and the performance is also superior. The heavy computing burden is transferred to the private cloud, which greatly reduces the workload of the mobile terminal and achieves the original intention of transferring the workload of the mobile terminal. The experimental results in Table 2 verify that when using the cloud computing technology in the method of this paper to detect wireless mobile network intrusion, the computing performance of cloud computing technology can improve the detection performance of intrusion detection, shorten the time of applying this method to detect wireless mobile network intrusion, and improve the real-time performance of intrusion detection on wireless mobile network.

The number of information discarded by using the method in this paper to detect intrusion behaviors on wireless mobile network is counted, and the method in this paper is compared with the method in the reference [11] and the method in the reference [12]. The comparison results are shown in Figure 3.

From the experimental results in Figure 3, it can be seen that for the method in this paper used to detect the intrusion

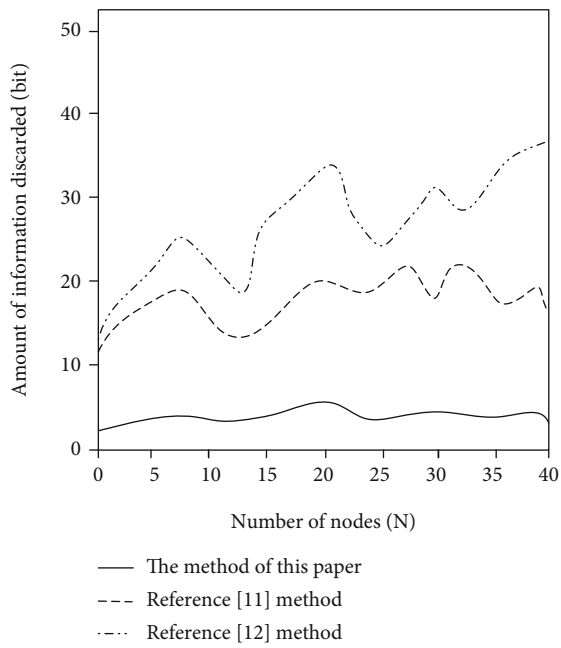

Figure 3: Comparison of the number of information discarded.

behavior of wireless mobile network, when the number of nodes is different, the number of information discarded is less than 5 bits; when the method of reference [11] and reference [12] are used to detect the intrusion behavior of wireless mobile network, the number of discarded information is significantly higher than the proposed method. The comparison results in Figure 2 verifies that when the method in this paper is used to detect the intrusion behavior of wireless mobile network, the number of discards during data transmission on wireless mobile network is guaranteed to be the lowest. The method in this paper can not only realize the effective detection of intrusion behavior in wireless mobile network but also ensure that the wireless mobile network has high communication performance, which verifies the high applicability of the method in this paper.

The security of wireless mobile network when using the method in this paper to detect the intrusion behavior of wireless mobile network is counted, and the method in this paper is compared with the methods in reference [11] and reference [12]. The comparison results are shown in Table 3.

From the experimental results in Table 3, it can be seen that the method in this paper can ensure the forward security of the wireless mobile network, ensure the confidentiality and integrity of the wireless mobile network when transmitting data, and can resist replay intrusion and biological template intrusion. The user's biometrics are stored in the trusted execution environment of the local device. When performing transaction authentication, the server authenticates the user's device, not the user, thus realizing user anonymity and resisting biological template intrusion. The method of reference [11] saves the biometric template in the server, and the method of reference [11] submits the biometric template to the server when the user registers; so, when the server data is leaked, the security of the user's biometric template in the method of reference [11] and the method of reference [12] will be compromised and therefore cannot be protected against this intrusion. Since the server does not save any data related to the user's biometrics, the method in this paper can resist intrusion, improve the security of user data, and protect user privacy. The method in this paper adopts the dual-server authentication method to disperse security risks, and the stability and robustness are improved. The method in this paper provides authentication methods with different security levels according to the authentication scenario where the user is located, provides weak authentication in the basic authentication scenario, and provides strong authentication in the transaction authentication scenario. From the perspective of the user, the user experience is improved, and the authentication efficiency is improved. It is more practical and feasible.

The intrusion detection accuracy within 24 hours of operation when using the method in this paper to detect wireless mobile network intrusion is tested. The method in this paper is compared with the method in the reference [11], the method in the reference [12], and the method in the reference [13], and the comparison results are shown in Figure 4.

It can be seen from the experimental results in Figure 4 that the method in this paper is used to realize the collaborative detection of wireless mobile network intrusion, which can improve the detection accuracy of wireless mobile network intrusion. The detection accuracy of the collaborative detection of wireless mobile network intrusion achieved by the method in this paper is higher than 98%, and the detection accuracy of the intrusion detection in wireless mobile network by the other three methods is obviously lower than that of the method in this paper. The experimental results verify that the method in this paper has high performance of intrusion detection in wireless mobile network and can be applied to the actual detection of wireless mobile network intrusion. This is because the cloud computing platform is used in this method, and the authentication server adopts the dual server and multifactor authentication scheme for mobile cloud computing to provide authentication services for mobile terminal users. The web server of cloud computing platform uses the intrusion node detection protocol of neighbor classification mechanism to provide communication security protocol for users.

4. Discussion

In this paper, a collaborative detection method for wireless mobile network intrusion based on cloud computing is researched, using cloud computing technology to detect achieve wireless mobile network intrusion. Mobile cloud computing is an important way for mobile networks to provide services to users. The security protection technologies often used in cloud computing are as follows:

4.1. Identity Authentication Technology. In the implementation of cloud computing, since service providers have different forms of existence, there is a lot of room for users to choose, and there can be multiple forms of user service presentation, which will easily lead to forgetting or confusion.

Table 3: Comparison of wireless mobile network security under different methods.

Performance test name	The method of this paper	Reference [11] method	Reference [12] method
Information confidentiality	High	Medium	Medium
Information integrity	High	High	Medium
Forward security	High	Low	High
Key guessing attack resistance	High	High	Low
Intrusion attack level	High	Medium	Medium
Server-side data confidentiality	High	Low	Medium
Safety level certification	High	Low	High
Creature template attack	High	High	Low
Defend against unreliable users	High	Medium	High

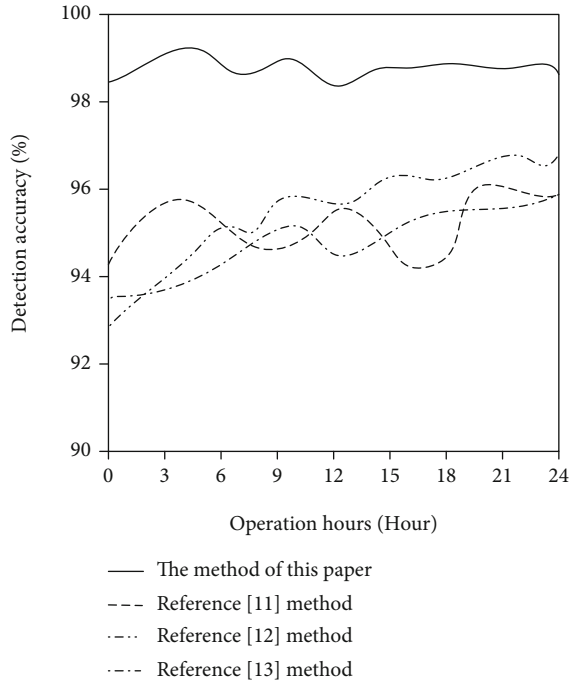

Figure 4: Intrusion detection accuracy.

In order to provide users with a better experience, single sign-on is often used in cloud computing authentication. Single sign-on is the ability to transfer all the security of the identity system to the cloud service, which requires strengthening its own identity authentication management system. After one registration is completed, all users do not need to register and log in to each cloud service, which can reduce the burden on users. The authentication of federated identity is to establish a federated identity database between different service providers. Users can log in once on the platform and then access the multicloud platform to reduce the repeated login problem of cloud platform login. The realization of this technology is mostly based on single sign-on.

4.2. Static Storage Data Protection Technology. The existence of cloud service is cloud storage service, which is a basic storage method, especially storage technology developed in the field of distributed or virtualized computers. This storage technology is a huge storage resource formed after integrating more storage media to allocate and shield data. When users rent storage resources, they often use remote access systems. During the opening of storage activities, the data mostly exists in a static way. Due to the confidentiality and privacy of the data, these storage methods can save the data in a static form. At the same time, the research on the implementation of security technology in storage mostly focuses on encrypting user data to ensure the confidentiality of data. However, it should be noted that when the data privacy is questioned, the cloud service provider needs to retrieve the results on the one hand and obtain the corresponding data content on the other hand, so as to ensure that the user privacy is not violated when analyzing the data content. Users should sign a confidentiality agreement with the service provider when using it. If the data is damaged, they need to be held accountable for the problem in a timely manner.

4.3. Dynamic Data Isolation Protection Technology. When dynamic data is encrypted and protected, the isolation mechanism is used to isolate and protect cloud applications. By using the application permissions in the Prophet system, the interference and damage of data to the environment can be reduced. In the cloud technology system, the most important security mechanism is the access control mechanism, which can effectively protect the data resources in the rights management and avoid authorized access. Due to the heterogeneity, openness, and dynamics of the meta-computing system, different security strategies must be considered in the process of data protection.

4.4. Trusted Cloud Computing Protection. In the cloud computing environment, through the use of trusted computer technology, service operators can provide continuous services to users in a reliable manner, so that a good trust relationship can be established between operators and service providers. At present, this is also an important research direction in the field of cloud computing security. The purpose of the trusted computing organization is to establish a good hardware security module in the computer's communication system, which enables the trusted computer platform to directly enter the boundary guarantee system of extended trust from the initial stage. It is well known that the construction of a trusted computer platform is shown in Figure 1, which is completed by cloud computing in a

virtual environment. Therefore, it is necessary to explore whether a secure and trusted platform in a virtual environment can become the basic guarantee of computer platform security. The current credibility of the virtual environment mainly starts from the following aspects: the first is the security design of the virtual machine monitor; the second is the protection mechanism of the virtual machine monitor; and the third is the isolation mechanism of the virtualized environment software.

5. Conclusion

Cloud computing is a new form of future development of science and technology. Due to the emergence of cloud computing, the data era ushered in a new situation of vigorous development. At present, computer technology continues to develop. Affected by factors such as large amounts of data and data informatization, cloud storage mode has become the main storage method used by people. However, the use of the cloud storage mode also has many drawbacks and dangers; therefore, it should use the cloud computing mode to understand the data, better protect the use of data information, develop the security of data information, and ensure the development of enterprises. In this paper, the collaborative detection method of wireless mobile network intrusion based on cloud computing is researched, to detect the intrusion behavior in the data transmission process of wireless mobile network and improve the transmission security of wireless mobile network. The implementation of cloud computing services in mobile communication networks can improve and optimize the current mobile network environment for users and provide and develop more business models for mobile communication service providers. The specific implementation of cloud computing services should start from the infrastructure of cloud computing technology, set up basic servers according to the different service contents of mobile communication service providers, fully consider the technical characteristics of cloud computing services in the network structure design, and better integrate its service functions. In the mobile communication network environment, it provides support for the optimization and improvement of the communication network. The realization of cloud computing services in mobile communication networks is a process of continuous development and improvement, which requires the participation of service providers and network users to effectively promote the implementation of cloud computing services. The experiment proves that the method adopted in this paper realizes the cooperative detection of wireless mobile network intrusion and improves the accuracy of wireless mobile network intrusion detection. The detection accuracy of wireless mobile network intrusion detection realized by this method is higher than 98%. In the future development, advanced artificial intelligence technology and information technology will be introduced to detect wireless mobile network intrusion.

Symbols

$\{PK_u, SK_u\}$: The key pair of the mobile terminal
$\{PK_{WS}, SK_{WS}\}$: The key pair of the web server
K: The session key between the two
x_i': Deployed in a random position
x_i: The intruded node
x_k: The neighbor classification information table of node
n: The total number of states of the HMM
$S = \{s_1, s_2, \cdots, s_n\}$: The state value set
$S = \{v_1, v_2, \cdots, v_m\}$: The observation value
m: The number of observations
$\pi = \{\pi_1, \pi_2, \cdots, \pi_N\}$: The initial distribution vector
θ_i: The probability of observing
$A = [a_{ij}]_{N\times N}$: The state transition probability matrix
$B = [b_{ij}]_{N\times M}$: Observation probability matrix
$P(o_j = v_j)$: The reciprocal of the observation time length T
$\alpha_t(i)$: The probability that model α is in state q_i at time t
$\beta_t(i)$: The probability that model α is in state q_i
$o_1, o_2, \cdots, o_t$: The output observation sequence
ε: The end threshold
α: The intrusion class.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

It is declared by the author that this article is free of conflict of interest.

Acknowledgments

The research is supported by the Natural Science Foundation of Hunan Province, China (Grant No. 2020JJ6062).

References

[1] G. Ramsay, "A cloud-computing platform for developing and evaluating vocal biomarkers based on home audio recordings: resources for large-scale data processing and analysis," *The Journal of the Acoustical Society of America*, vol. 148, no. 4, pp. 2791–2791, 2020.

[2] Y. D. Lin, D. T. Truong, A. Ali, C. Y. Li, and T. Dinh, "Proxy-based federated authentication: a transparent third-party solution for cloud-edge federation," *IEEE Network*, vol. 34, no. 6, pp. 220–227, 2020.

[3] M. Ghose, S. Kaur, and A. Sahu, "Scheduling real time tasks in an energy-efficient way using vms with discrete compute capacities," *Computing*, vol. 102, no. 1, pp. 263–294, 2020.

[4] M. Marimuthu, J. Akilandeswari, and P. R. Chelliah, "Identification of trustworthy cloud services: solution approaches and research directions to build an automated cloud broker," *Computing*, vol. 104, no. 1, pp. 43–72, 2022.

[5] L. Kenyereye, J. Y. Hwang, Q. V. Pham, and J. S. Song, "Meix: evolving multi-access edge computing for Industrial Internet-

of-Things services," *IEEE Network*, vol. 35, no. 3, pp. 147–153, 2021.

[6] Z. P. Luo, Y. C. Jiang, and Z. J. Hu, "Cloud computing virtual resource enhanced multipoint secure transmission simulation," *Computer Simulation*, vol. 38, no. 1, pp. 158–161+166, 2021.

[7] C. Blatti, A. Emad, M. J. Berry, L. Gatzke, and S. Sinha, "Knowledge-guided analysis of "omics" data using the knoweng cloud platform," *PLoS Biology*, vol. 18, no. 1, pp. e3000583–e3000588, 2020.

[8] Y. Huang, X. Qiao, P. Ren, L. Liu, and J. Chen, "A lightweight collaborative deep neural network for the mobile web in edge cloud," *IEEE Transactions on Mobile Computing*, vol. 21, pp. 2289–2305, 2020.

[9] P. Zhao and G. Dan, "Joint resource dimensioning and placement for dependable virtualized services in mobile edge clouds," *IEEE Transactions on Mobile Computing*, vol. 21, pp. 3656–3669, 2021.

[10] M. Grami, "An energy-aware scheduling of dynamic workflows using big data similarity statistical analysis in cloud computing," *The Journal of Supercomputing*, vol. 78, no. 3, pp. 4261–4289, 2022.

[11] A. S. Alqahtani, "Fso-lstm ids: hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks," *The Journal of Supercomputing*, vol. 78, no. 7, pp. 9438–9455, 2022.

[12] M. U. Ilyas and S. A. Alharbi, "Machine learning approaches to network intrusion detection for contemporary internet traffic," *Computing*, vol. 104, no. 5, pp. 1061–1076, 2022.

[13] M. E. Khansari and S. Sharifian, "A modified water cycle evolutionary game theory algorithm to utilize qos for iot services in cloud-assisted fog computing environments," *The Journal of Supercomputing*, vol. 76, no. 7, pp. 5578–5608, 2020.

[14] L. N. Fan, "Hybrid intrusion data mining method for multichannel ship wireless mobile communication network," *Ship Science and Technology*, vol. 43, no. 14, pp. 166–168, 2021.

[15] B. Cao, S. Fan, J. Zhao et al., "Large-scale many-objective deployment optimization of edge servers," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3841–3849, 2021.

[16] A. Pellegrini, N. Stephens, M. Bruce et al., "The arm neoverse n1 platform: building blocks for the next-gen cloud-to-edge infrastructure soc," *IEEE Micro*, vol. 40, no. 2, pp. 53–62, 2020.

[17] B. Cao, Z. Sun, J. Zhang, and Y. Gu, "Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3832–3840, 2021.

[18] Z. Lv, L. Qiao, and I. You, "6G-enabled network in box for internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5275–5282, 2020.

[19] F. Liu, G. Zhang, and J. Lu, "Multi-source heterogeneous unsupervised domain adaptation via fuzzy-relation neural networks," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 11, pp. 3308–3322, 2020.

[20] J. Dong, Y. Cong, G. Sun, Z. Fang, and Z. Ding, "Where and how to transfer: knowledge aggregation-induced transferability perception for unsupervised domain adaptation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 1, p. 1, 2021.

[21] D. Li, H. Yu, K. P. Tee, Y. Wu, S. S. Ge, and T. H. Lee, "On time-synchronized stability and control," *IEEE Transactions on Systems Man Cybernetics-Systems*, vol. 52, no. 4, pp. 2450–2463, 2021.

[22] L. Zhang, H. Zhang, and G. Cai, "The multi-class fault diagnosis of wind turbine bearing based on multi-source signal fusion and deep learning generative model," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, 2022.

[23] H. Kordestani, C. Zhang, S. F. Masri, and M. Shadabfar, "An empirical time-domain trend line-based bridge signal decomposing algorithm using Savitzky–Golay filter," *Structural Control and Health Monitoring*, vol. 28, no. 7, 2021.

[24] A. Yildirim, E. Zeydan, and I. O. Yigit, "A statistical comparative performance analysis of mobile network operators," *Wireless Networks*, vol. 26, no. 2, pp. 1105–1124, 2020.

[25] G. Liu, "Data collection in MI-assisted wireless powered underground sensor networks: directions, recent advances, and challenges," *IEEE Communications Magazine*, vol. 59, no. 4, pp. 132–138, 2021.

[26] M. Zhang, Y. Chen, and W. Susilo, "PPO-CPQ: a privacy-preserving optimization of clinical pathway query for E-healthcare systems," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10660–10672, 2020.

[27] X. Wu, W. Zheng, X. Chen, Y. Zhao, T. Yu, and D. Mu, "Improving high-impact bug report prediction with combination of interactive machine learning and active learning," *Information and Software Technology*, vol. 133, article 106530, 2021.

[28] W. Zheng, Y. Xun, X. Wu, Z. Deng, X. Chen, and Y. Sui, "A comparative study of class rebalancing methods for security bug report classification," *IEEE Transactions on Reliability*, vol. 70, no. 4, pp. 1658–1670, 2021.

[29] K. Liu, F. Ke, X. Huang et al., "DeepBAN: a temporal convolution-based communication framework for dynamic WBANs," *IEEE Transactions on Communications*, vol. 69, no. 10, pp. 6675–6690, 2021.

[30] C. Zong and Z. Wan, "Container ship cell guide accuracy check technology based on improved 3D point cloud instance segmentation," *Brodogradnja: Teorija i Praksa Brodogradnje i Pomorske Tehnike*, vol. 73, no. 1, pp. 23–35, 2022.

[31] C. Zong, H. Wang, and Z. Wan, "An improved 3D point cloud instance segmentation method for overhead catenary height detection," *Computers & Electrical Engineering*, vol. 98, article 107685, 2022.

[32] A. Li, D. Spano, J. Krivochiza et al., "A tutorial on interference exploitation via symbol-level precoding: overview, state-of-the-art and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 796–839, 2020.

[33] A. Li, C. Masouros, A. L. Swindlehurst, and W. Yu, "1-bit massive MIMO transmission: embracing interference with symbol-level precoding," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 121–127, 2021.

[34] J. Yan, H. Jiao, W. Pu, C. Shi, J. Dai, and H. Liu, "Radar sensor network resource allocation for fused target tracking: a brief review," *Information Fusion*, vol. 86-87, pp. 104–115, 2022.

[35] R. S. Krishnan, E. G. Julie, Y. H. Robinson, R. Kumar, and H. V. Long, "Modified zone based intrusion detection system for security enhancement in mobile ad hoc networks," *Wireless Networks*, vol. 26, no. 2, pp. 1275–1289, 2020.

[36] T. Shawly, M. Khayat, A. Elghariani, and A. Ghafoor, "Evaluation of hmm-based network intrusion detection system for multiple multi-stage attacks," *IEEE Network*, vol. 34, no. 3, pp. 240–248, 2020.

[37] S. He, W. Huang, J. Wang, J. Ren, and Y. Zhang, "Cache-enabled coordinated mobile edge network: opportunities and challenges," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 204–211, 2020.

[38] Y. Mu, "Design of network psychological feature prediction system based on cloud computing technology," *Electronic Design Engineering*, vol. 30, no. 1, pp. 56–60, 2022.

[39] P. Bedi, N. Gupta, and V. Jindal, "I-siamids: an improved siam-ids for handling class imbalance in network-based intrusion detection systems," *Applied Intelligence*, vol. 51, no. 2, pp. 1133–1151, 2021.

[40] Z. Wang, D. Jiang, L. Huo, and W. Yang, "An efficient network intrusion detection approach based on deep learning," *Wireless Networks*, vol. 5, pp. 1–14, 2021.

[41] Y. Alharbi, A. Alferaidi, K. Yadav, G. Dhiman, and S. Kautish, "Denial-of-service attack detection over IPv6 network based on KNN algorithm," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 8000869, 6 pages, 2021.