ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Fusion of Edge Computing and Hidden Markov Models for Security Assessment of Power IoT

Qiang Li[1,*], *Zhiqi Li*[2], *Jing Chen*[3], *Fusheng Yuan*[4], *Libin Wang*[2], *Zhuo Huang*[4], *Yang Yang*[2], *Shenglong Liu*[2] *and Qin Yin*[2]

[1] National Network Information and Communication Industry Group Co., Ltd., Beijing, 102211, China
[2] State Grid Siji Network Security Technology (Beijing) Co., Ltd., Beijing, 102211, China
[3] Beijing Electric Power Economic and Technical Research Institute Co., Ltd., Beijing, 100037, China
[4] State Grid Information and Communication Industry Group Co., Ltd. Beijing Branch., Beijing, 100031, China

SUMMARY: *This paper proposes a hybrid BW-SOA optimization strategy to increase the sensing layer's reaction time, as well as an enhanced Hidden Markov Model-based method of network security posture evaluation. The efficient use of situational awareness for smart power IoT security monitoring is made possible by the use of edge computing based on deep learning. Experiments have shown that the augmented HMM model improves assessment performance by more successfully identifying security flaws in the system. The state transfer probability of the improved HMM model is more reasonable compared to the original HMM model, S3→S1 is improved from 0.15 to 0.6635, and the concentration of the observation distribution is significantly improved, and the probability of observing V5 in S5 is increased from 0.61 to 0.9962.The converged DL neural network-based edge computation method has an average reward of -39.73, which is 77.17% higher compared to the traditional DDPG.*

KEYWORDS: *power IoT; Hidden Markov Model; BW algorithm; SOA algorithm; edge computing techniques; security posture assessment*

1 Introduction

Power IoT is a network that realizes comprehensive sensing of the massive information that is ubiquitous in all links of the power system [1]. It is deeply integrated with the smart grid through modern technologies such as big data processing, cloud computing, 5G mobile communication, smart city and blockchain, opening up information islands and realizing the extensive interconnection of people and things [2, 3]. Power Internet of Things is an important strategic support for State Grid to build an international leading energy Internet enterprise. However, from the perspective of the security risk of its system operation, the uniqueness of the power IoT information perception and transmission mode makes it easy to be interfered with by external factors in all aspects, in which the security risk of the information communication category is particularly prominent [4-7]. Regarding the security risk of electric power IoT, literature [8] describes that in recent years, due to cyber attacks, large-scale power outages have occurred, which directly affects the power outages have occurred, directly

*liqiang_sgcc@163.com
https://doi.org/10.65102/is2026354
Published: 30 April, 2026

endangering the stability and safety of electricity supply; meanwhile, information security risks have grown increasingly acute. Literature [9] points out that integrating the Internet of Things into power systems can enhance real-time, all-round monitoring, coordinated control, situational perception, and intelligent decision-making, but at the same time, it also makes the power system subject to a variety of cyberattacks, which violates the threat to the power security operation. Literature [10] emphasizes that the application of IoT in smart grid infrastructure has led to a rapid growth in the industry's need for cybersecurity and argues that the current security architecture of the smart grid can no longer satisfy the security needs of the energy sector in the 21st century. Therefore, effective power IoT security assessment is important for the systematic security of power IoT construction. Among them, edge computing and Hidden Markov Models are widely used as typical assessment methods.

As a distributed-computing paradigm, edge computing moves computing and data storage nearer to devices that generate discrete data, thereby reducing data transmission latency and network congestion, while strengthening the efficiency and security of data handling; accordingly, it has been extensively adopted in various industries [11, 12]. In power IoT security assessment, it can sink data-processing functions to the network edge, effectively assess the power IoT security, timely understand the deficiencies in the power grid, and improve it, but it also introduces multidimensional security challenges [13-15]. In recent years, numerous scholars have conducted research on security risk assessment of edge computing IoT and obtained certain results. For example, literature [16] introduces the application of IoT in smart devices brings risks in terms of data security and privacy, and proposes an assessment method of Internet security risk based on edge computing, which verifies that the method improves network security through effective assessment. Literature [17] proposed an IoT- and edge-computing-oriented security assessment model for heterogeneous multi-source systems based on mainstream security assessment standards and architectures, revealing the good performance of the model in security assessment and security ranking. Literature [18] proposed an edge-computing architecture for IoT-driven smart grids to address the limitations of cloud computing models in power systems, many of which have not yet been addressed, such as privacy leakage. Literature [19] pointed out that IoT networks face severe cybersecurity risks and emphasized that the convergence of edge computing with IoT systems significantly improves security and privacy issues in IoT networks. Literature [20] describes a management-and-control framework for ubiquitous power IoT built on edge-cloud collaboration, and the framework is able to cope with issues involving security protection and data security of the power system, which facilitates secure operation and management of the power grid.

The Hidden Markov Model (HMM) is a statistical framework used to characterize a Markov process with hidden-state parameters, which has high application value in the security assessment of power IoT [21]. HMM is able to identify and predict the state of power equipment so as to support security assessment and operational maintenance for power IoT [22]. Regarding the application of HMM in the security assessment of IoT in electric power or other fields, literature [23] introduced a dynamic HMM prediction model so as to effectively assess cybersecurity in electric power systems and established a completely physical based cyber-attack simulation platform, and confirmed the effectiveness of the above model by means of testing. Literature [24] proposed an improved HMM to assess cybersecurity risk and calculated the parameters through the gradient of the parameter space, and the comparative analysis pointed out that the performance of the improved HMM was closer to the real value. Literature [25] pointed out that Internet network security faces many risk challenges, and proposed the use of machine learning based HMM to predict the agility of intrusion detection, and verified that the method has strong predictive performance. Literature [26] proposed a strategy for assessing the reliability together with network security in cloud and IoT systems, which is based

on comparing, selecting and integrating Markov and semi-Markov models, which significantly improves the assessment. Literature [27] proposed a method to fuse the attack graph model with HMM for the network security risk problem, and experimental results indicate that this approach is able to effectively calculate the maximum probability of the state transition sequences, so as to accurately infer the attack intention, and provide a good configuration scheme for safeguarding network security administrators.

When used alone, HMM-based assessment has the limitation that interactions among network nodes are neglected. Therefore, the security assessment method of power IoT that integrates edge computing and Hidden Markov Model can significantly improve the real-time risk assessment capability by combining the advantages of the two methods, utilizing edge computing to achieve localized and fast response to threats, and combining the HMM model to model the timing characteristics of attacks [28, 29]. Of course, beyond the methods discussed above, researchers have also examined the application of other assessment methods. Literature [30] describes that the lack of security protection terminals and related technologies in the power distribution IoT has caused severe network security risks, so it proposes a method for security assessment of power distribution IoT based on entropy power method and cloud modeling theory, and demonstrates the practical effectiveness of the method. Literature [31] in order to solve the problem of information security risk assessment in electric power Internet of Things, put forward a hierarchical-analysis-based security risk assessment method, which can effectively improve the accuracy of the assessment.

In this study, the Hidden Markov-based network security posture is first built in accordance with network security characteristics. The network security posture will be categorized as the model's hidden component, and filtered alarm data will be included into the model's observation. The problem of parameter optimization algorithms becoming readily trapped in local optimization solutions is addressed by combining the SOA and BW approaches. The value of network security posture may be quantitatively examined once the optimized parameters have been entered into Hidden Markov. An intelligent security monitoring system of the IoT framework for electric power will be created utilizing edge computing to optimize data using deep learning. Conduct a network posture prediction and efficacy verification experiment using LLDOS1.0 as the dataset. To assess the degree of edge computing performance, a power network testing platform will be developed.

2 Network Security Posture Assessment Model Construction Based on Edge Computing and Hidden Markov

Along with the rapid improvement of computer science technology, the informationization and intelligence of the electric power industry have achieved higher maturity. In modern electric power networks, it needs quicker response, real-time fault detection, and quick reaction. Hence, there is a growing demand for a power Internet-of-Things (IoT) safety monitoring system distinct from traditional schemes to increase the system’s response speed while guaranteeing system security and stability. From the present methods, although the Hidden Markov Model (HMM) can simulate the state transition process, the traditional Baum-Welch (BW) parameter estimation algorithm will make the Hidden Markov Model get stuck in a local optimum position. Meanwhile, the traditional cloud computing scheme has high latency and great broadband consumption, which makes it hard to meet the localized perception requirements. Against this backdrop, this paper puts forward a security evaluation strategy that combines edge computing and an improved Hidden Markov Model, expecting to solve the problems of local optimal trap and real-time processing bottleneck encountered in traditional schemes.

2.1 Establishing a Hidden Markov-based Cybersecurity Posture Assessment

In this paper, cyber security characteristics and HMM model are studied and compared and analyzed to find out the common factors and connections between them. Finally, the HMM model for cyber security posture is proposed. The HMM model is defined to be represented by a quintuple $\lambda = (V, S, PI, A, B))$. The five parameters V, S, PI, A, and B in the HMM model will be described separately in the following.

(1) The set space of observable states V

In the set space of observable states, individual elements can be represented by V_M, i.e., $V = (V_1, V_2, \cdots, V_M)$, where V_M describes the states that are directly observable. The set of observable states describes the set of all possible and directly observable state sequences. O denotes the observation sequence, and each element in the observation sequence is denoted by O_i, i.e., $O = (O_1, O_2, \cdots, O_i)$, where the observation sequence denotes the directly observable observation sequences generated in the actual operation. According to the characteristics of the network, it is proposed to take the alarm information as the observable state, and at the same time, considering that the number of alarm information is too large, the types of alarm information are divided into five categories, and each type of alarm information can be corresponded to a category, and then the category of each type of alarm information can be taken as the observable value.

(2) Hidden state set space S

In the set space of hidden states, the individual elements are denoted by S_N, i.e., $S = (S_1, S_2, \cdots, S_N)$, where S_i describes the states that are not directly observable. The set of states describes the set of all possible states that are not directly observable. I denotes the state sequence, and each element in the state sequence is denoted by i_t, i.e., $I = (i_1, i_2, \cdots, i_t)$, where the state sequence describes all the possible sequences of states that can be generated and are not directly observable in actual operation. The network's security condition can be classified into five categories, which would represent the high security condition, the medium-high security condition, the medium security condition, the medium-low security condition, and the low security condition, respectively. Based on the network's properties, it can be said that the security condition of the network should be taken as an unobservable state while simultaneously taking into account the relationship between the alarm data and the security condition of the network. The network's security condition varies depending on the type of attack that is carried out on it; however, these variations would be the general security conditions that occur within the network, which cannot be measured using any tools and could only be assessed by gathering and evaluating the alarm data.

In a network environment, attack behavior within the network can affect overall network security conditions. When an attack behavior occurs, the corresponding alarm information can be detected by the detection tool. Definition state: When the attacker performs an IP scanning form of intrusion behavior on the network, the network is in a high-security state at that moment, which means its security condition remains very good; medium-high state: When the attacker performs a port scanning form of intrusion behavior on the network, the network security state is in the medium-high state at this time, which means that network protection is still relatively good; medium state: When the attacker performs the intrusion behavior of acquiring system privilege on the network, the network security state is in the medium state at this time, indicating an ordinary or moderate security condition; medium-low state: When the attacker performs the intrusion behavior of installing Trojan horse software on the network, the network security state

is in the medium-low state at this time, which means that the network security state at this time is poor; low state: When the attacker performs the intrusion behavior of sending attack commands on the network, the network security state is in the low state at this time, which means that network security has deteriorated to a very poor level. Thus, the hidden states in the HMM can be identified.

(3) Initial hidden state probability distribution matrix PI

The PI describes the probability of the hidden security state of the network at the very beginning in the network environment, which is an initial probability distribution matrix of order $1\times N$, denoted as $PI=\{PI_i\}$, where $PI=P(i_1=S_i)$ and $1\le i\le N$, denotes the probability distribution under the corresponding initial hidden state S_i at the initial moment in the network environment.

(4) State Transfer Probability Distribution Matrix A

A describes the mutual transfer probability distribution between network security situations that are not directly observable in a network environment, noting that $A=\{a_{ij}\}$, where $a_{ij}=P(i_{t+1}=S_j|i_t=S_i)$, $1\le i\le N, 1\le j\le N$, denotes the probability distribution of the downward transfer from the previous moment's state S_i to the next moment's state S_j in the network environment. Considering the actual situation, the probability of the state at $t+1$ not only depends on the state at the moment t, but also depends on the state at the moment $t-1$ also exists, so notate that $a_{xaj}=P(i_{t+1}=S_j|i_{t-1}=S_x,i_t=S_j)$, $1\le x,i,j\le N$, denotes the probability of transferring to the next moment of the state in a network environment by considering the state at both the $t-1$ moment and the t moment.

(5) Observed state probability distribution matrix B

B describes the matrix of observed state probability distributions corresponding to hidden states in the network environment, i.e., the probability that the system is in a certain state when a certain observation is observed, noting $B=\{b_j(k)\}$, where $b_j(k)=P(O_{t+1}=V_k|i_t=S_j)$, $1\le j\le N$, $1\le k\le M$, denoting the directly observable probability distributions of states generated corresponding to being in a certain state in a network environment.

The observation level and the concealed level are the two levels that typically make up the HMM's structure. State sequences that cannot be directly observed are typically put in the concealed level, whereas observation sequences that can be directly observed are often arranged in the observation level. Additionally, there is a relationship between the state sequences that cannot be directly seen and the observation sequences that can. From the perspective of network security posture characteristics, the network's alarm data will be organized in the observation level, whereas the network security posture will be organized in the concealed level. Next, Fig. 1 will show the network security posture level based on the HMM model.

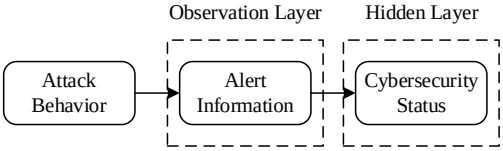


Figure 1: HMM-based network security situation model level

(1) Observation layer

According to the analysis of the characteristics of the network, it can be seen that the alarm information can be detected in the network by various detection tools, and the detected alarm

information is characterized by direct observation, and it is closely related to the current security situation. Therefore, it can be determined that it is the only important basis for analyzing the current network security status, and the detected alarm information can be placed in the observation layer of the HMM-based network security posture model as the observation value.

(2) Hidden Layer

In the actual network environment, we can detect the existence of a large amount of alarm information in the network through detection tools. According to the analysis of the security environment of the network, it can be seen that when some kind of attack behavior occurs in the network, there will correspond to the appearance of matching alarm information, and different alarm information represents that the security status in the network may have changed, and different attack behaviors have different threat levels to the network. Therefore, according to the size of the threat level of the attack behavior on the network, we can determine the impact of this attack behavior on the current network security state. When the attack behavior corresponding to an alarm message has a large degree of threat to the network security, it will reduce the security posture of the current network. When an alarm message corresponds to an attack behavior with a small threat level to network security, it will increase or not change the current network security posture. In summary, the security state of a network can only be obtained by analyzing and judging the network security through directly observable alarm messages. Therefore, the network security posture that cannot be directly observed can be placed as hidden values in the hidden layer of the HMM-based network security posture model.

2.2 SOA-based Hidden Markov Training

The HMM model, usually use BW HMM parameter estimation algorithm is complete, i.e., given an observation sequence values $O = O_1, O_2, \cdots, O_t$, This algorithm can determine A $\lambda = (\pi, A, B)$ such that $P(O/\lambda)$ is maximum. The BW algorithm is implemented by the EM algorithm, which is an optimization algorithm for great likelihood estimation by iteration, and the algorithm can only iterate up to the locally optimal solution, but not to the globally optimal solution. In the situational assessment, the establishment of the observation probability matrix B is the key to the accuracy of the assessment and the main factor affecting the objective function $P(O/\lambda)$, while the parameter π and the parameter A have little effect. Therefore, the value of parameter B should be optimized during the training process of HMM, and the BW algorithm is an iterative process, and the change of parameter B also leads to the change of parameter A, which avoids the algorithm from falling into a local optimum.

SOA is a new population-based heuristic stochastic search algorithm, which analyzes and researches various intelligent behaviors of human beings by studying their stochastic search behaviors, relying on the scientific research results of various disciplines, such as cognitive science, AI, and so on, combining human search behaviors with evolutionary ideas, and modeling human-specific empirical theories in order to determine the search direction, and human-specific fuzzy reasoning theories in order to calculate the step size, complete the update of the position, and realize the global optimization of the solution of the required problem. In order to solve the problem that HMM parameter optimization is easy to fall into the local optimum, this paper combines SOA with BW algorithm, and uses SOA's ability to search globally in the search space to obtain the optimal parameters, so as to improve the accuracy of quantitative model. The total flow of SOA-based HMM for situational assessment is shown in Fig. 2.

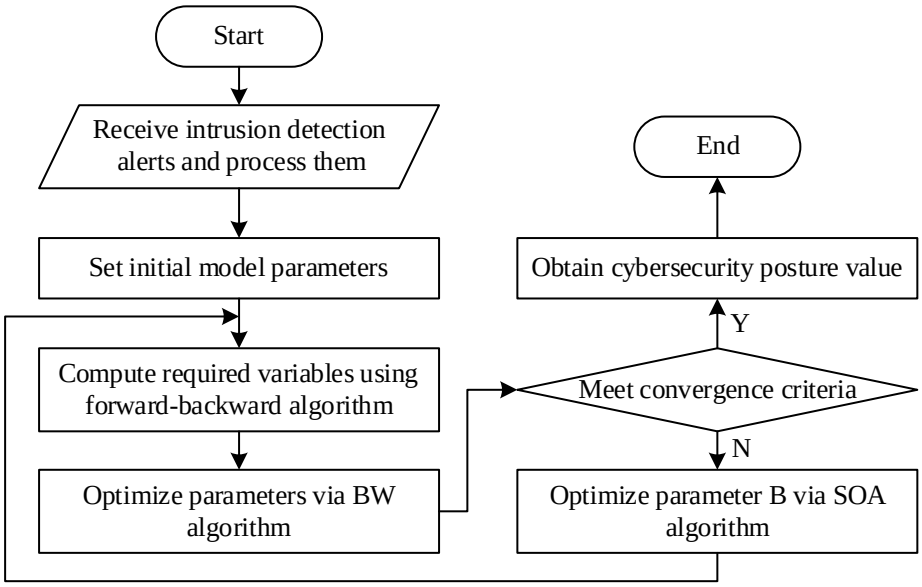


Figure 2: SOA-based HMM situation assessment process

After setting the model's initial parameter values, the BW algorithm is employed to optimize the parameters. Once the convergence criteria are satisfied, the parameters can be substituted directly into the quantitative model to obtain the value of network security posture; otherwise, the parameters B are further optimized through the SOA algorithm, after which they are fed back into the BW algorithm until the convergence requirements are fulfilled. The flowchart of the crowd search algorithm is presented in Figure 3.

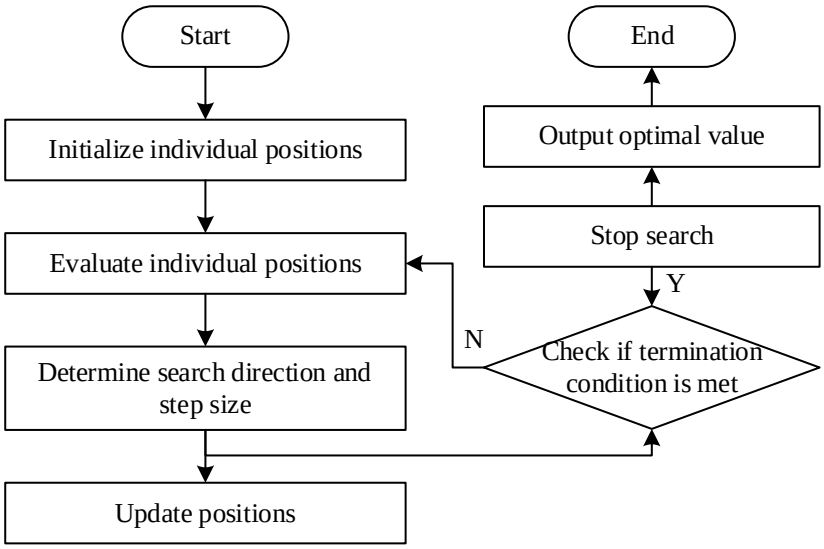


Figure 3: Flow of seeker optimization algorithm

The crowd search algorithm is implemented as follows:

(1) Initialize individual positions

Randomly generate n initial positions in the feasible solution domain, i.e., randomly generate n observation probability matrices B and normalize the matrices.

(2) Evaluate individual positions

Calculate the objective function value, i.e., $P(O/\lambda)$ value, for each location.

(3) Calculate the search direction and step size for each individual i in each dimension j

Adopt linear affiliation function to determine the relationship between the objective function value and step size according to fuzzy inference:

$$\mu_i = \mu_{\max} - \frac{s - I_i}{s-1}\left(\mu_{\max} - \mu_{\min}\right), i = 1, 2, \cdots, s \tag{1}$$

$$\mu_{ij} = rand\left(\mu_{ij}, 1\right), j = 1, 2, \cdots, D \tag{2}$$

$$\alpha_{ij} = \hat{\delta}_{ij}\sqrt{-\ln\left(\mu_{ij}\right)} \tag{3}$$

where $\mu_{\max} = 1.0$ and $\mu_{\min} = 0.0111$ are the best affiliation and the worst affiliation, respectively, μ_i is the affiliation of the individual i, and μ_{ij} is the affiliation of the individual i in the j-dimensional direction; I_i is the $P(O/\lambda)$ number after sorting in descending order; D is the direction dimension; s is the individual size; α_{ij} is the step size of the j-dimensional direction; and $\hat{\delta}_{ij}$ can be determined by the following equation:

$$\hat{\delta}_{ij} = \omega \cdot abs\left(\vec{x}_{\min} - \vec{x}_{rand}\right) \tag{4}$$

$$\omega = (T_{\max} - t)/T_{\max} \tag{5}$$

where $x_{\min}$ is the best position of the individual, and x_{rand} is the randomly generated position of the individual that is different from the best position in the individual; ω is the change weight, which decreases linearly as T increases; t is the current number of evolutions; and $T_{\max}$ is the maximum number of evolutions; The function $abs(\ )$ is the function to take the absolute value.

The search direction $\vec{d}_i(t)$ is jointly determined by the self-interested direction (Eq. (6)), the altruistic direction (Eq. (7)), and the premovement direction (Eq. (8)):

$$\vec{d}_{i,ego}(t) = \vec{p}_{i,best} - \vec{x}_i(t) \tag{6}$$

$$\vec{d}_{i,alt}(t) = \vec{g}_{i,best} - \vec{x}_i(t) \tag{7}$$

$$\vec{d}_{i,pro}(t) = x_i(t_1) - x_i(t_2) \tag{8}$$

$$\vec{d}_i(t) = sign\left(\omega\vec{d}_{i,ego} + \varphi_1\vec{d}_{i,alt} + \varphi_2\vec{d}_{i,pro}\right) \tag{9}$$

where $x_i(t_1)$ and $x_i(t_2)$ are the best position in $\{x_i(t-2), x_i(t-1), x_i(t)\}$ respectively; $\vec{g}_{i,best}$ is the ith individual history best position; $\vec{p}_{i,best}$ is the global best position; $sign(\ )$

is the sign function; φ_1 and φ_2 are randomly generated numbers between 0 and 1; and ω is the change weights, which decreases linearly with T . .

(4) Individual position update

Update each individual position according to the following formula:

$$\Delta x_{ij}(t+1) = \alpha_{ij}(t) d_{ij}(t) \tag{10}$$

$$x_{ij}(t+1) = x_{ij}(t) + \Delta x_{ij}(t+1) \tag{11}$$

2.3 Edge computing based security situational awareness deployment

Edge computing is able to solve the problem of large-scale heterogeneous networks and transmission and processing delays by providing intelligent services to process data from nearby sensor and controller nodes. Deep learning has sensing and decision-making capabilities to obtain information directly from the environment and make decisions to control it. On top of providing detection capabilities, deep learning autonomously pushes the security action strategies of the security situational assessment system to maximize long-term returns. To this end, this paper proposes edge computing technology based on deep learning, which makes full use of historical data and deep learning at the edge end to improve the accuracy of fault monitoring, which can effectively alleviate the huge and redundant data volume brought about by traditional IoT data processing, thus further improving the response speed of the system and reducing the latency, and at the same time, due to the characteristics of the deep learning neural network, it can effectively ensure the reliability of data transmission that reduces data loss and avoids affecting the robustness of the system. The deep learning (DL) neural network is trained using the steepest descent algorithm (GD). We use back propagation (BP) to train the neural network to calculate the gradient of the neural network cost function. Where regularized logistic regression, the cost function is defined as shown in equation (12):

$$\begin{aligned} J(\theta) = & \frac{1}{2m} \sum_{i=1}^{m} \sum_{k=1}^{K} \left[-y_k^{(i)} \log\left(h_\theta(x^{(i)})_k\right) - \left(1 - y_k^{(i)}\right) \times \log\left(1 - h_\theta(x^{(i)})_k\right) \right] \\ & + \frac{\alpha}{2m} \left[\sum_{j=1}^{10} \sum_{k=1}^{2} \left(\theta_{jk}^{(1)}\right)^2 + \sum_{k=1}^{10} \left(\theta_k^{(2)}\right)^2 \right] \end{aligned} \tag{12}$$

Intelligent sensors are utilized to monitor the operating status of the power system, and deep sensing is carried out through the parameters set by the cloud platform of the monitoring system, the acquired data are transmitted to the edge computing terminal, and the deep learning neural network is distributed in the output ports of the edge computing terminal to carry out the data analysis, and then the analysis results are uploaded to the communication backbone network, and the structure of this edge computing based on deep learning is shown in Fig. 4.

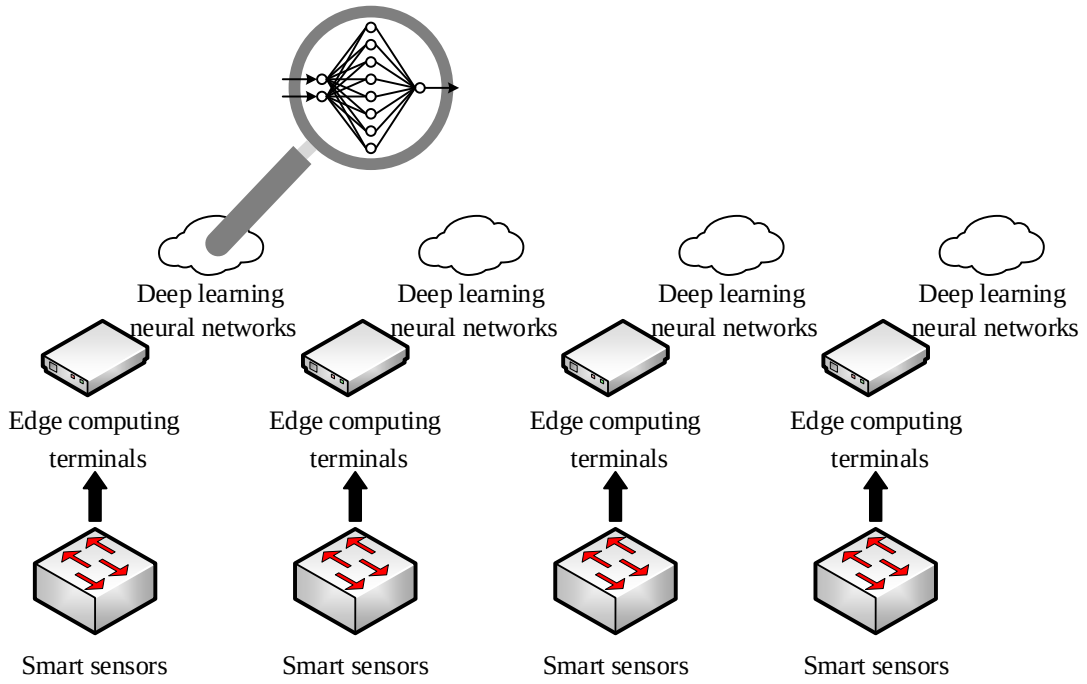


Figure 4: Edge computing structure based on deep learning

3 Simulation and result analysis of security assessment model for power IoT

LLDOS1.0 from the classical dataset DARPA2000 is selected as the experimental dataset.LLDOS1.0 is a test set of DDOS attack scenarios.The scenarios simulate the number of phases of an attack as 6.For different phases, different attacks or security events will put the network in different security states.

3.1 Network posture prediction and algorithm validation

3.1.1 Analysis of the effects of state forecasting

In this paper, we use wireshark to analyze the dump file and set filtering rules by wireshark to obtain various service information in the file. In order to avoid obtaining more or less power security observation data due to overlapping time periods or large time interval, which affects the power network posture assessment, this paper utilizes the counter algorithm to obtain security observation data. The width of the time window $\triangle t$ is set to 10min, the size of the sub-window is 2min, the sliding step is 2, and the threshold of each sub-window is set to 30, which means that when the number of alarms in the sub-window exceeds 30, the sliding stops, or else the sliding to the right is carried out with a step of 2.

Using the improved HMM algorithm in this paper to calculate the probability of being in different states at moment t, the results of the probability distribution of each state are shown in Figure 5. In each state probability distribution graph, if there is a state probability maximum in a certain moment, it is judged to be currently in the state. The total time of the scenario simulation attack is 400min, and the whole experimental process is the initial network security is in a high state, and the network is in a high state for the first 20min. It can be seen that the first 20min are in high state has the highest probability. Then it starts to get the list of power network attacks, then it starts to perform network pre-attacks to find the weak hosts. The next

approximately 100min, when the network is in a medium-high state, medium state has the highest probability. After the constant attacks and finding the weak hosts, the intrusion of the hosts through the vulnerabilities starts, so as to achieve the purpose of controlling the weak hosts. For the next 50 min, the network remains in a medium-low security state. When controlling the weak host, according to the description of the attack scenario, the attacker gained the system privileges of the host when t=180 min, and the network security condition at that point should be medium-low state. Then the probability that the system is in the low state at 180 min reaches its maximum. At t=180 min, the likelihood of the low state is much greater than that of the other states, with a high probability value of 0.72, while the other states have very low probability values, so at this point it can be determined to be in the low state. Then, the network defense started after the network attack action stopped the network takedown, and the network security condition gradually began to recover. Then, another round of server attacks is launched by the attacker, and the network security state begins to deteriorate again. However, due to the network security's own defense, it is not cyber-attacked, and after the server attacks are stopped, the network returns to a relatively stable state. During the subsequent period, the network security state changes from low to medium-low to medium again. However, due to the server attack, the network state started to change to medium-low state again. After the server attack stops, it slowly changes to medium again and the network state gradually improves.

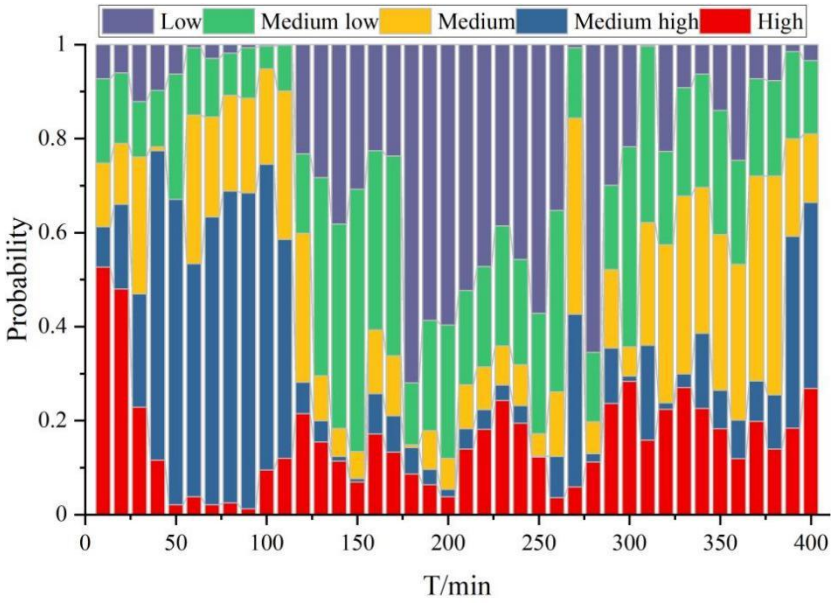


Figure 5: Results of probability distribution of each state

Based on the probability values of different states at different moments already calculated in Figure 5, the accuracy of each state can also be derived, and the results of the accuracy of the five states are shown in Figure 6. The prediction accuracy for the high state is 86.65%, the prediction accuracy for the medium-high state is 96.12%, the prediction accuracy for the medium state is 90.66%, the prediction accuracy for the medium-low state is 92.08%, and the prediction accuracy for the low state is 100%. The above data shows that the method can accurately predict the trend change of the attacked state, and also the prediction of other states is relatively accurate. It can be shown that it is more accurate to judge the state that the network is in by this method.

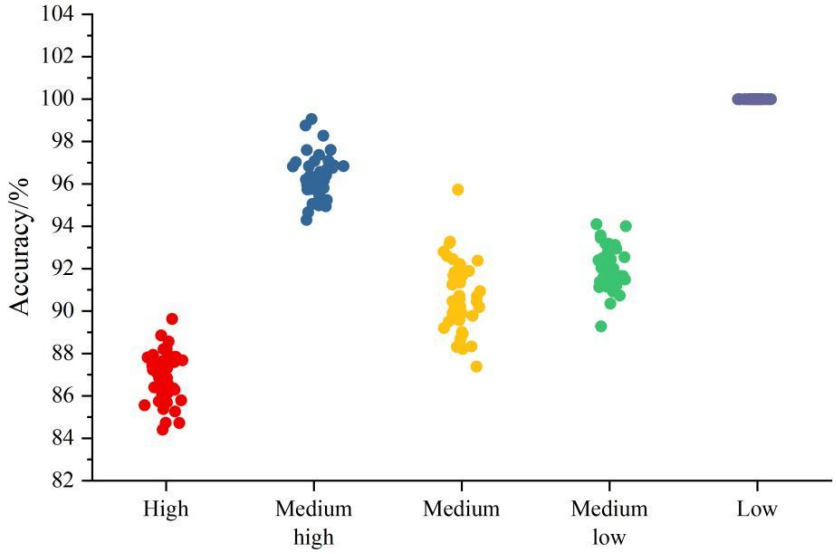


Figure 6: Accuracy results of four states

In order to verify the accuracy of the posture prediction, this paper divides the data in the dataset by directly adopting the number of alerts per 6 hours of the dataset as the posture value. Specifically, the number of alerts at 12 test moments in the last 7 days is selected to predict the number of alerts in the next 12 hours, and then the posture value is obtained. The cybersecurity posture prediction results are shown in Fig. 7. The prediction of network security posture using the improved HMM algorithm is closer to the actual value, and the gap with the real posture value is kept within 0.025, even if the trend of the posture value is more obvious, it is also basically consistent with the actual posture change, which is a good proof of the validity of the method proposed in this paper.

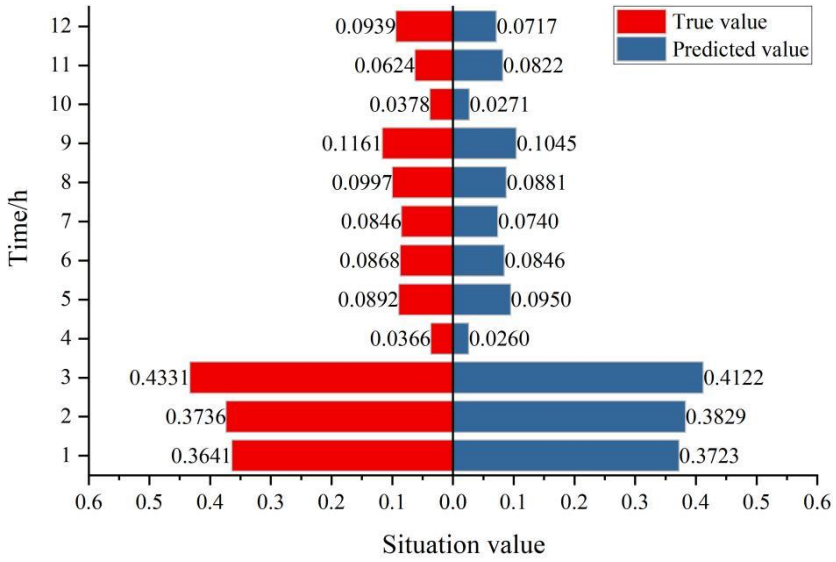


Figure 7: Results of network security situation prediction

3.1.2 Comparative analysis with existing methods

To verify the superiority of the improved HMM model proposed in this paper over other algorithms in situational prediction, the simple Markov model prediction method and the RBF model prediction method are both chosen for comparative experiments. The prediction results

of different algorithms for network security posture are presented in Figure 8. Compared with other algorithms, the network security posture prediction method based on the improved HMM algorithm in this paper produces results that are closer to the actual posture values, and its accuracy continues to improve over time relative to the other methods. In particular, when compared with the HMM algorithm, the proposed algorithm achieves an average absolute error that is 19.23% lower, mainly due to the hybrid optimization strategy combining BW and SOA. At the same time, it can also be observed that the posture prediction MAE of the improved HMM algorithm in this paper outperforms that of the other algorithms.

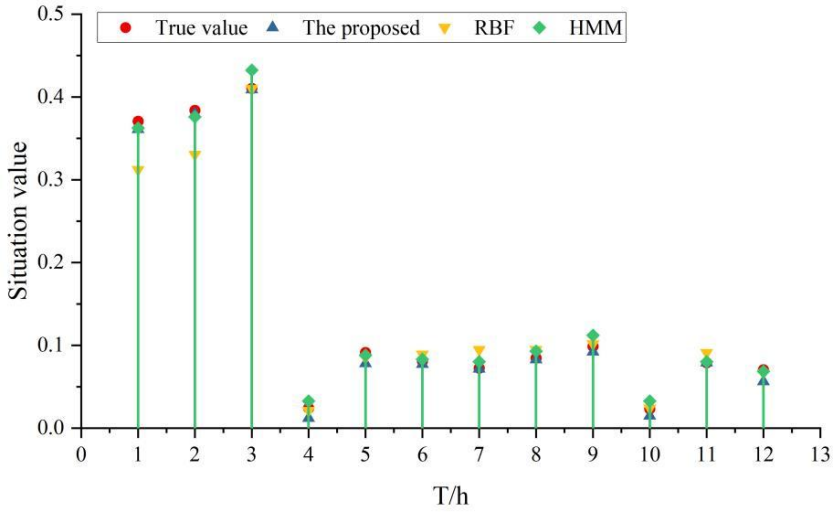
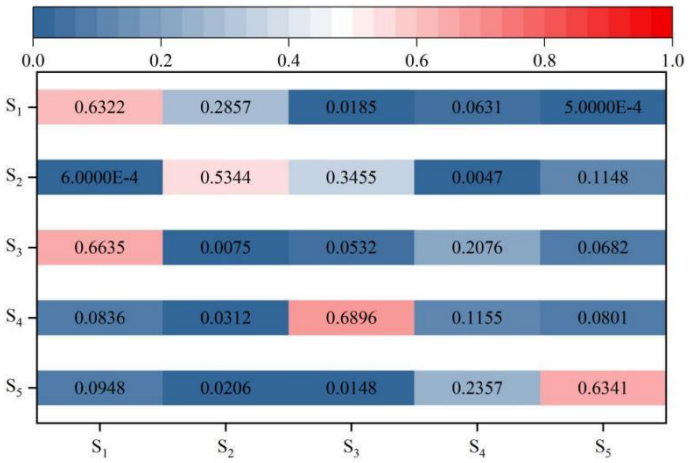


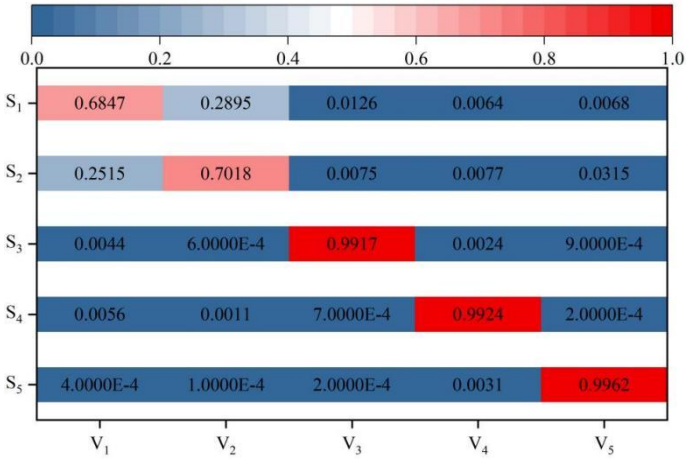
Figure 8: Network security situation prediction results of different algorithms

3.1.3 Analysis of the effectiveness of improvement strategies

To evaluate the effectiveness of the method proposed in this study, the predictions generated by the improved HMM model in this paper are compared with the predictions of the HMM model to determine parameter initial values in λ. The state transfer probability matrix P and the observed state probability distribution matrix Q of this paper's method are shown in Fig. 9 and, correspondingly, the initial values of P and Q of the original method are shown in Fig. 10 (a-b), respectively. The state transfer probabilities in the original HMM model are symmetrically dispersed distribution and are not precise enough. While the improved HMM enhances the S3→S1 probability to 0.6635 by adjusting the transfer path, and the S5→S5 self-transfer is enhanced to 0.6341. Taking S5 as an example, the observed V5 probability of the original method is 0.61, which jumps to 0.9962 after the improvement and the probabilities of non-target observations are all decreased by more than 50%. This indicates that the improved method optimizes the state transfer mechanism and enhances the match between observation and state.

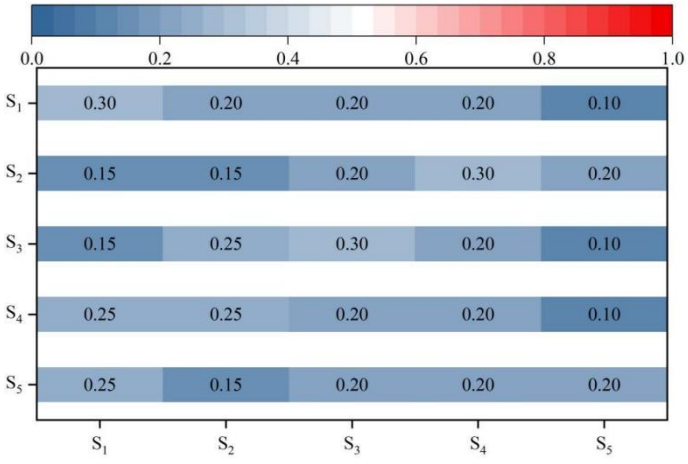


(a)P

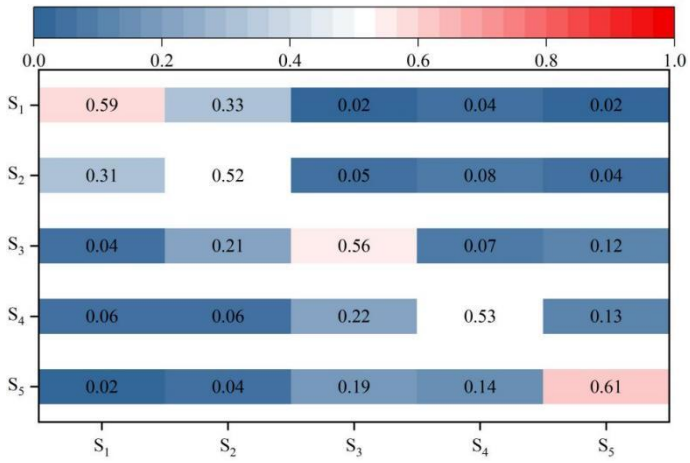


(b)Q

Figure 9: Initial values of P and Q for the proposed method



(a)P



(b)Q

Figure 10: Initial values of P and Q for the original method

3.2 Simulation experiment analysis

The power network system's test platform is established in this chapter. Intelligent metering systems, microgrid control centers, relay protection systems, and charging stations are among the power network terminals. The edge agent receives port traffic and log data from these devices in a proactive manner. The edge agent simultaneously identifies the power network terminals' vulnerabilities and attack details.

The total reward values obtained from this paper's DP neural network-based edge computing method and traditional DDPG are compared. The detection error rates of the posture elements are all set to 0.005, i.e., only up to one error is allowed after 200 actions taken by the edge agent, and then 20,000 iterations are performed for this paper's method and the DDPG-based method, respectively. The results of the comparison of the total reward values of different methods in the same initial situational awareness environment are shown in Fig. 11. Both achieve convergence after reaching 2000 sets. The reward values obtained by this paper's method are concentrated between -70 and 0, while DDPG is between -225 and -100. This indicates that the proposed DL neural network based edge computing method rewards are better than the traditional DDPG method in terms of post-training stability, and it also proves that the proposed method in this paper achieves lower penalty for sensory failure and processing cost.

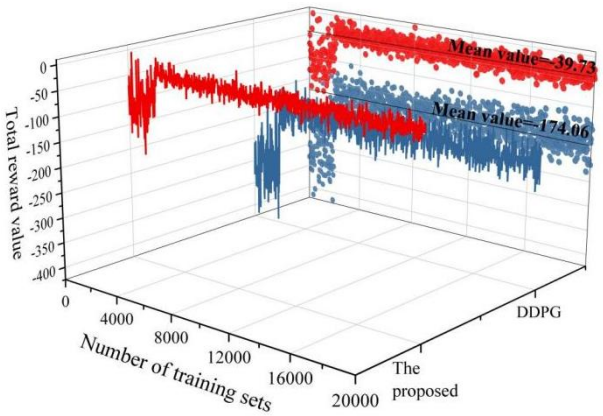


Figure 11: Comparison results of total reward values for different methods

4 Conclusion

In this paper, based on the improved HMM model and combined with the edge computing method based on DL neural network, the cybersecurity posture of LLDOS 1.0 dataset and simulation platform test is evaluated.

(1) The prediction accuracy of the improved HMM model for all five states is above 85%, which is closer to the actual posture values than other algorithms, and becomes more and more accurate relative to other algorithms as time changes. The improvement strategy in this paper realizes the rationalization of the transfer path and the improvement of the observation discrimination by reconstructing the state transfer matrix and the observation probability distribution. The correlation of HF states S3-S1 and S5-S5 of the improved HMM model is enhanced, and the conditional probabilities of target observations are significantly concentrated, reducing the risk of state confusion.

(2) After convergence, the fluctuation range of reward value of DL neural network based edge computing method is not more than 70, while the fluctuation range of DDPG is around 125, and the average processing cost of this paper's method is lower than that based on traditional DDPG.

About the Author

Qiang Li was born in Mudanjiang, Heilongjiang, China, in 1966. Now he is mainly engaged in multi station integration, power and energy internet, smart grid and other work in State Grid Information and Communication Industry Group Co., Ltd.

References

[1] Rastogi, S., Sharma, M., & Varshney, P. (2016). Internet of Things based smart electricity meters. International Journal of Computer Applications, 133(8), 13-16.

[2] Liu, Y., Yang, X., Wen, W., & Xia, M. (2021). Smarter grid in the 5G Era: A framework integrating power internet of things with a cyber physical system. Frontiers in Communications and Networks, 2, 689590.

[3] Jiang, A., Yuan, H., Li, D., & Tian, J. (2019). Key technologies of ubiquitous power Internet of Things-aided smart grid. Journal of Renewable and Sustainable Energy, 11(6).

[4] Vaccari, I., Cambiaso, E., & Aiello, M. (2019). Evaluating security of low-power internet of things networks. International Journal of Computing and Digital Systems, 8(02), 101-114.

[5] Zhang, Y., Zou, W., Chen, X., Yang, C., & Cao, J. (2014, October). The security for power internet of things: Framework, policies, and countermeasures. In 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (pp. 139-142). IEEE.

[6] Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2018). Challenges of securing Internet of Things devices: A survey. Security and Privacy, 1(2), e20.

[7] Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), 586-602.

[8] Hou, R., Ren, G., Zhou, C., Yue, H., Liu, H., & Liu, J. (2020). Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things. Computer communications, 158, 64-72.

[9] Sarjan, H., Ameli, A., & Ghafouri, M. (2022). Cyber-security of industrial internet of things in electric power systems. IEEE Access, 10, 92390-92409.

[10] Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. Future Generation Computer Systems, 93, 849-859.

[11] Ahmed, E., & Rehmani, M. H. (2017). Mobile edge computing: opportunities, solutions, and challenges. Future Generation Computer Systems, 70, 59-63.

[12] Liang, B., Wong, V. W. S., Schober, R., Ng, D. W. K., & Wang, L. C. (2017). Mobile edge computing. Key technologies for 5G wireless systems, 16(3), 1397-1411.

[13] Shen, S., Zhang, K., Zhou, Y., & Ci, S. (2020). Security in edge-assisted Internet of Things: challenges and solutions. Science China Information Sciences, 63(12), 220302.

[14] He, D., Chan, S., & Guizani, M. (2018). Security in the Internet of Things supported by mobile edge computing. IEEE Communications Magazine, 56(8), 56-61.

[15] Liu, D., Liang, H., Zeng, X., Zhang, Q., Zhang, Z., & Li, M. (2022). Edge computing application, architecture, and challenges in ubiquitous power internet of things. Frontiers in Energy Research, 10, 850252.

[16] Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A survey on security and privacy issues in edge-computing-assisted internet of things. IEEE Internet of Things Journal, 8(6), 4004-4022.

[17] Guo, Z., Lu, Y., Tian, H., Zuo, J., & Lu, H. (2023). A security evaluation model for multi-source heterogeneous systems based on IOT and edge computing. Cluster Computing, 26(1), 303-317.

[18] Chen, S., Wen, H., Wu, J., Lei, W., Hou, W., Liu, W., ... & Jiang, Y. (2019). Internet of things based smart grids supported by intelligent edge computing. IEEE access, 7, 74089-74102.

[19] Rupanetti, D., & Kaabouch, N. (2024). Combining edge computing-assisted internet of things security with artificial intelligence: Applications, challenges, and opportunities. Applied Sciences, 14(16), 7104.

[20] Gong, Y., Chen, C., Liu, B., Gong, G., Zhou, B., & Mahato, N. K. (2019, November). Research on the ubiquitous electric power Internet of Things security management based on edge-cloud computing collaboration technology. In 2019 IEEE Sustainable Power and Energy Conference (iSPEC) (pp. 1997-2002). IEEE.

[21] Mor, B., Garhwal, S., & Kumar, A. (2021). A Systematic Review of Hidden Markov Models and Their Applications. Archives of computational methods in engineering, 28(3).

[22] Liao, Y., Zhao, G., Wang, J., & Li, S. (2020). Network security situation assessment model based on extended hidden Markov. Mathematical Problems in Engineering, 2020(1), 1428056.

[23] Zhang, B., Liu, X., Zheng, H., & Song, Y. (2024). Hidden Markov model based cyberattack prediction in power systems. IEEE Transactions on Smart Grid.

[24] Li, X. (2016). Network security risk assessment method based on the improved hidden Markov model. International Journal of Simulation–Systems, Science & Technology, 17(36).

[25] Muhati, E., & Rawat, D. B. (2021). Hidden-Markov-model-enabled prediction and visualization of cyber agility in IoT era. IEEE Internet of Things Journal, 9(12), 9117-9127.

[26] Kharchenko, V., Ponochovnyi, Y., Ivanchenko, O., Fesenko, H., & Illiashenko, O. (2022). Combining Markov and semi-Markov modelling for assessing availability and cybersecurity of cloud and IoT systems. Cryptography, 6(3), 44.

[27] Liu, S. C., & Liu, Y. (2016, May). Network security risk assessment method based on HMM and attack graph model. In 2016 17th IEEE/ACIS international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD) (pp. 517-522). IEEE.

[28] Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. Sensors, 25(1), 213.

[29] Sefati, S., & Navimipour, N. J. (2021). A qos-aware service composition mechanism in the internet of things using a hidden-markov-model-based optimization algorithm. IEEE Internet of Things Journal, 8(20), 15620-15627.

[30] Cai, S., Wei, W., Chen, D., Ju, J., Zhang, Y., Liu, W., & Zheng, Z. (2022). Security risk intelligent assessment of power distribution internet of things via entropy-weight method and cloud model. Sensors, 22(13), 4663.

[31] Sun, Y., Zhuang, L., Jia, T., Cheng, D., Zhao, X., & Guo, J. (2025). A risk assessment method for power internet of things information security based on multi-objective hierarchical optimisation. IET Smart Grid, 8(1), e12208.