ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Study on a collaborative governance framework for cybersecurity capability enhancement in non-regulated operations

Qijing Zhang[1,*], *Renmeng Lu*[1] *and Yu Lu*[1]

[1] Digitalization Department, Guizhou Power Grid Co., Ltd., Guiyang, Guizhou, 550000, China

SUMMARY: *In order to cope with the diversified security challenges faced by non-regulatory business networks, it is particularly important to construct a comprehensive network security protection system. In this paper, a new hybrid kernel function is constructed, the parameters of the support vector machine are optimized by genetic algorithm, and a network security posture indicator system is proposed to realize the network security posture assessment model based on GA-SVM. And the ARIMA model is used to predict the network security posture. The empirical results tabulate that compared with the two prediction models of RBF and PSO-SVM, the accuracy, AUC value, and F1 value of the GA-SVM network security posture assessment model are 89.47%, 0.8792, and 0.8644, respectively, which are able to accomplish the network security assessment in a better way.The results of ARIMA in the task of network security posture prediction have a better fitting effect. Therefore, network security posture assessment and prediction can be used to monitor the security status in the non-regulated business network environment in real time, discover potential threats and abnormal behaviors in a timely manner, and predict possible security risks in the future.*

KEYWORDS: *cybersecurity posture assessment; cybersecurity posture prediction; GA-SVM; ARIMA; non-regulated business*

1 Introduction

The rapid iteration of information technology is reconfiguring the basic shape of global cyberspace [1]. From the autonomous decision-making of intelligent algorithms to the cross-domain circulation of data elements, the defense boundaries, threat patterns and governance logic of traditional cybersecurity are facing fundamental changes, making cybersecurity an important challenge for all types of business [2]. Especially in the field of non-regulatory business, the weakness of network security is more and more significant. Non-regulated business units often lack sufficient security protection capabilities and standardized management systems, becoming high-risk targets of network attacks, which not only pose a threat to the normal operation of the unit, but also may affect the security and stability of the entire company. Therefore, upgrading the cybersecurity capability of non-regulated business units and building a sound security management system are necessary measures to realize information system security, guarantee business continuity and improve overall operational efficiency.

In terms of cybersecurity governance, foreign scholars mostly focus on the construction of institutional frameworks, regulations and standards to safeguard the openness and security of

*zhangqijing1989@163.com
https://doi.org/10.65102/is2026700
Published: 30 April, 2026

cyberspace [3]. Borghard and Lonergan analyze the connotation of coercive dynamics in cyberspace, that is, the state uses the Internet technology as an independent tool to coerce opponents, and the cyberspace is becoming a field in which a state uses the threat of force against its opponents in order to achieve political purposes, and the coercive dynamics have a wider striking area and more destructive power than the traditional field of war [4]. Maleh et al. study proposed a capability maturity framework designed to help organizations assess and improve their cybersecurity governance to ensure that their security strategies and policies are consistently and measurably implemented in a dynamically changing threat environment [5]. Yusif and Hafeez-Baig pointed out that cybersecurity, as a multidimensional problem involving individual and organizational Internet activities, can be systematically addressed through a governance framework, for which a cybersecurity governance model for dynamic assessment and continuous optimization was constructed with the aim of providing organizations with a structured and measurable governance path [6]. Azmi et al. conducted a coding analysis on 12 cybersecurity frameworks and found that the differences among these frameworks mainly lay in the four dimensions of "promoting actions", "drivers", "framework environment" and "target audience". At the same time, they summarized three common concepts, namely "joint actions", "network pillars" and "framework life cycle", which provided a theoretical basis for constructing a universal cybersecurity framework model [7]. Savaş and Karataş pointed out that network governance, due to its ability to integrate all stakeholders into the management process, has become a key to achieving an effective cybersecurity strategy; however, a universal governance framework has not yet been formed, and current practices still tend to focus on "management" rather than "governance", highlighting the urgency and necessity of establishing a systematic network governance mechanism [8].

In terms of cyberspace security governance models, scholars have proposed different paths to cope with the increasing severity of cyber threats [9]. Beridze and Lomidze systematically enhance organizational cybersecurity protection capabilities by integrating a hierarchical policy architecture, quantitative risk modeling and continuous monitoring mechanism; and construct a policy-centric cybersecurity governance framework by applying mathematical modeling to optimize security resource allocation, adopting a stochastic process to simulate threat dynamics and game theory to analyze adversarial behavior [10]. Hasan et al, on the other hand, suggested from the perspective of smart grids that cyberspace governance must be integrated with the needs of specific industries, and they pointed out that with the networking of critical infrastructures such as smart grids, cyberspace governance needs to be tailored to the specific needs of different domains by proposing proprietary solutions to improve the effectiveness of governance [11]. Tagarev et al. point out that in the face of increasingly complex cyber threats, the EU proposes to enhance the overall defense capability by establishing a network of cybersecurity competence centers to integrate resources and share knowledge and risks, and reveals that the core challenge of guaranteeing long-term effective collaboration of cyber organizations lies in the establishment of a scientific governance and management mechanism [12]. Yanakiev's analysis of the governance models of three typical collaborative network organizations, NATO S&T, the Gigabit European Academic Network and the Capability Technology Group of the European Defence Agency, summarizes the characteristics of the practice of highly centralized funding streams and core decision-making mechanisms in collaborative networks in the field of science and technology [13].

Collaborative governance theory originated in the 1970s, aiming at solving complex, dynamic and cross-domain problems, especially coordinating resources, information and actions among multi-interested subjects [14]. With the development of information technology, cyberspace has gradually become a complex system, and the needs of cybersecurity governance have driven the further development of collaborative governance theory. Regarding the research

on the application of collaborative governance theory in cybersecurity governance, Obioha Val found that there is a significant gap in cybersecurity governance in the education sector by analyzing the NIST Cybersecurity Framework Usage Dataset, the Global Threat Intelligence Sharing Consortium Data Repository, and the World Values Survey data and applying methods such as double-difference and logistic regression and found that the collaborative governance program can reduce the incidents of security breaches by 49.3% [15]. Albalas et al. emphasized that management concepts alone are not sufficient to deal with cyber risks, and that threats can only be effectively eliminated through comprehensive cybersecurity planning and by involving all stakeholders in a collaborative governance process [16]. Melaku proposes a concise, dynamic, and adaptive collaborative cybersecurity governance framework, which integrates often-neglected elements such as research and development mechanisms, public-private collaboration, regional and international cooperation, incident management, business continuity, disaster recovery, and regulatory compliance, and optimizes the components, processes, and activities that are missing or overlapping in the existing frameworks, and systematically solves the problem of the practical application of the existing governance models. The problem of insufficient feasibility and adaptability of existing governance models in practical application is systematically solved [17]. According to Muller, a secure and stable cyberspace is necessary for the proper functioning of economic, political, and social structures; the stability and security of cyberspace is not predestined but dynamically evolving; cyberspace is in constant flux, and in order to manage a complex set of interests, agendas, and influences, the promotion of a collaborative, multi-stakeholder model of governance among government, business, and society has become a major solution [18]. By analyzing the policy implementation loopholes and the lack of international frameworks in the current cybersecurity governance, Qudus proposes that it is necessary to build an adaptive regulatory mechanism, deepen public-private cooperation, and promote the harmonization of international standards in order to form a synergistic governance framework [19].

This study proposes a set of optimized governance frameworks for security capability enhancement in response to the cybersecurity needs of non-regulated operations. From the perspective of cybersecurity posture assessment, a GA-SVM-based cybersecurity posture assessment method is proposed, and a new fusion kernel function based on linear kernel function and Gaussian kernel function is designed by improving the kernel function of the traditional support vector machine algorithm. In order to prevent the support vector machine algorithm from falling into the local optimal solution situation during training, the improved support vector machine algorithm is considered to replace the traditional grid search method with genetic algorithm for parameter optimization. Situation prediction as the highest stage of network security situational awareness, this paper proposes a network security situation prediction method based on ARIMA. In addition, this paper examines the performance of the proposed two methods of cybersecurity posture assessment and prediction on HoneyNet and CIC-IDS-2017 datasets, respectively.

2 Cybersecurity governance framework for non-regulated operations

The cybersecurity governance framework for non-regulated operations is built on three dimensions: management, personnel and environment. In the “management” dimension, network security assessments should be carried out regularly to identify potential risks and formulate corresponding protective measures. In addition, a cybersecurity assessment mechanism should be established to cascade security responsibilities to ensure the effective

implementation of the security management system.

In the "human" dimension, it is necessary to strengthen the promotion of network security awareness and technical training to enhance the security literacy of all staff. For network security management personnel, it is necessary to carry out regular professional training to improve their technical capabilities in network security protection, threat identification and emergency response. For ordinary employees, it is necessary to carry out basic network security knowledge training to improve their sensitivity to network security events and cultivate good information protection awareness.

In the dimension of "ring", it is necessary to build a secure network environment and workplace environment to realize comprehensive protection. In order to prevent the intrusion of external threats, security facilities such as firewalls, intrusion detection systems and anti-virus software should be deployed to form a deep defense. At the same time, direct connection between internal and external networks should be prevented through a combination of physical and logical isolation to reduce the risk of attack.

Among other things, the industrial bastion machine realizes a significant improvement in the security capability of non-regulated business transactions through a series of authentication management, account management, authority management, operation audit and performance management functions.

3 Cybersecurity situational awareness

In this paper, the implementation process of the network security governance framework for non-regulated operations is centered on network security situational awareness technology to assess the network security status in real time and predict possible future security threats. Network security situational awareness is in a specific network environment, the security factors that may affect the network security posture changes extracted, the extracted security factor information understanding, visualization and other predictions of the possible development of the posture trend. Network security situational awareness is a macroscopic concept, which emphasizes the overall state of a network environment and the overall development trend. It uses data fusion technology to integrate various available security factor information to generate a holistic and comprehensive mapping of the network security posture. This allows network security personnel to enhance their understanding of the network and threat prevention. Figure 1 shows the main three-level model of holistic situational awareness.

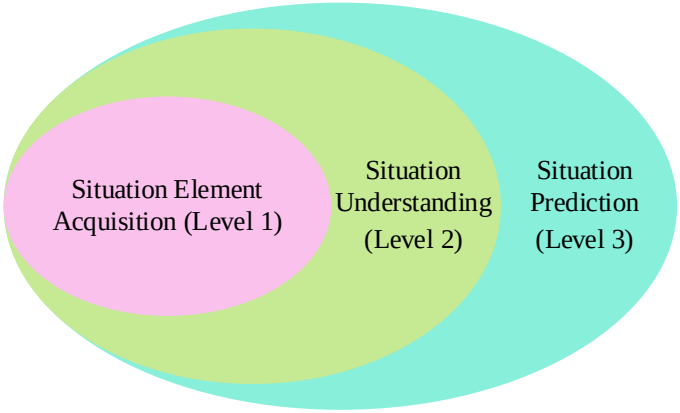


Figure 1: The three-level model of situation awareness

As mentioned above, cybersecurity situational awareness is divided into three levels of models, namely: situational element acquisition (level 1), situational understanding (level 2) and situational prediction (level 3), and the specific details of these three levels of models will be elaborated in the next section. The overall architecture of the network security situational awareness system is shown in Figure 2.

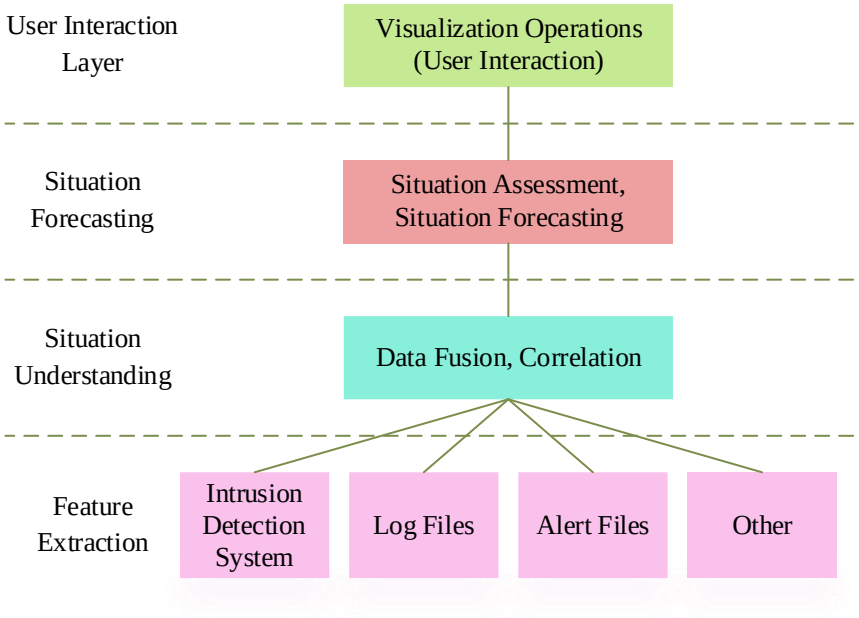


Figure 2: The overall architecture of the network security situation awareness system

(1) Acquisition of situational elements

Situational element acquisition is the basis of situational awareness, which collects network data and senses the network environment through a variety of tools and technologies. These tools include anti-virus software, vulnerability scanning, penetration testing, network scanning, password cracking tools, firewalls and intrusion detection systems. This segment realizes comprehensive network environment sensing by continuously obtaining information such as the network's operating status, event logs, traffic data, and asset lists. In addition, for the specificity of industrial control system, the sensing process also needs to focus on collecting communication data of industrial controllers (such as PLC), industrial monitoring software and industrial configuration software to ensure comprehensive monitoring of various types of equipment in the industrial control system.

(2) Situational understanding

The understanding of network security posture is in these security information elements alone, so it is necessary to integrate the processing of this information to provide effective data support to the network security posture perception analysis, so as to ensure the correctness and effectiveness of the final assessment results. This security information elements of the correlation analysis technology, is a kind of data and information fusion technology. The basis of correlation analysis is knowledge and redundant reasoning methods.

(3) Situation prediction

Situation prediction is based on the analysis and understanding of network data, using prediction algorithms to determine the development trend of network security status in advance. During the prediction process, the system will combine current security events and historical data to analyze potential attacker behavior, determine their next move, and predict the overall security status. This prediction is not only limited to the warning of a single threat, but can also

provide guidance for enterprises to develop long-term security strategies. For example, for industrial control systems, by predicting possible attack paths, weak links in the industrial control network can be hardened in advance to prevent malicious intrusions.

4 GA-SVM-based network security posture assessment model

4.1 Improvement of Support Vector Machine Algorithm

4.1.1 Construction of hybrid kernel functions

A new hybrid kernel function is constructed by choosing to combine a polynomial kernel function with a Gaussian kernel function:

$$\kappa(x_i, x_j) = \lambda(x_i^T x_j)^d + (1-\lambda)\exp\left(-\frac{\left\|x_i - x_j\right\|^2}{2\sigma^2}\right), \lambda \in [0,1] \tag{1}$$

It is necessary to prove the feasibility of the constructed mixed kernel function. A kernel function is considered feasible if it satisfies the Mercer theorem, which states that the necessary and sufficient condition for a kernel function is that its Gram matrix is semi-positive definite. Since the polynomial kernel function and the Gaussian kernel function are necessarily semi-positive definite, we denote the polynomial kernel function as K_1 and the Gaussian kernel function as K_2. The proof of the above mixed kernel function then becomes proving that $f = \alpha K_1 + \beta K_2$, where $\alpha \geq 0$ and $\beta \geq 0$ is semi-positive definite.

Suppose there exists $\{X_1, X_2\} \subseteq \overline{X} \subseteq R^n$, and by Mercer's theorem the Gram matrices $\{X_1, X_2\}$ corresponding to K_1, K_2 are semipositive definite matrices. Any chosen matrix $c \subseteq R^n$ has $c'(\alpha K_1 + \beta K_2)c = c'\alpha K_1 c + c'\beta K_2 c \geq 0$, and so it is shown that any $f = \alpha K_1 + \beta K_2$ corresponding to Gram matrices are semipositive definite matrices, so it can be proved that the constructed hybrid kernel function is an effective kernel function. The new hybrid kernel function can effectively extract the local features of the samples in the training set and consider the global features of the samples, and this hybrid kernel function to build the SVM model can effectively improve the accuracy of the cybersecurity posture assessment.

4.1.2 Improvement of Support Vector Machine Parameters

The ability to realize cybersecurity posture assessment using support vector machines is mainly determined by the penalty parameters as well as the individual parameters in the hybrid kernel function. These parameters determine the VC dimension of the feature vector in the sample space mapped to the feature space by the support vector machine and the search pattern of the algorithm for optimization.

(1) Penalty parameter C

The concept of slack variables is introduced into the support vector machine algorithm to solve the inevitable outlier problem. Addition of slack variables as well as penalty parameters form:

$$\begin{aligned} &\min\left(\frac{1}{2}\|\omega\|^2\right)+C\sum_{i=1}^{m}\xi_i \\ &s.t.\ y_i\left(\omega^T\phi(x_i)+b\right)\geq 1-\xi_i,\xi_i>0,i=1,2,\cdots,m \end{aligned} \tag{2}$$

Recalculate Eq. (2) by applying the Lagrange multiplier method to form its dual problem:

$$\begin{aligned} &\max\left(\sum_{i=1}^{m}\alpha_i-\frac{1}{2}\sum_{i,j=1}^{m}\alpha_i\alpha_j y_i y\left\langle x_i,x_j\right\rangle\right) \\ &s.t.\ 0\leq\alpha\leq C,i=1,2,\cdots,m,\sum_{i=1}^{m}\alpha_i y_i=0 \end{aligned} \tag{3}$$

$\xi_i(i=1,2,...,m)$ is the slack variable, which represents the amount of the function interval that is allowed to deviate from the corresponding sample data point x, and C is the penalty parameter that regulates the balanced weight between finding the maximum interval and the minimum slack variable in the objective classification function, but this will increase the empirical risk of the algorithm. Therefore, it is necessary to choose a better penalty parameter C, so that the support vector machine algorithm's generalization ability and empirical risk to form a balance.

(2) Hybrid kernel function parameters

The new hybrid kernel function designed in this paper has three parameters, which are the exponent d of the polynomial kernel function, the bandwidth σ within the Gaussian kernel function and the weight coefficient λ of the hybrid kernel function.

4.1.3 Genetic Algorithm for Parameter Optimization

In this paper, genetic algorithm (GA)-based cross-validation search is used for parameter optimization. Figure 3 shows the flowchart of the algorithm for optimizing the parameters of the hybrid kernel function of the support vector machine using genetic algorithm.

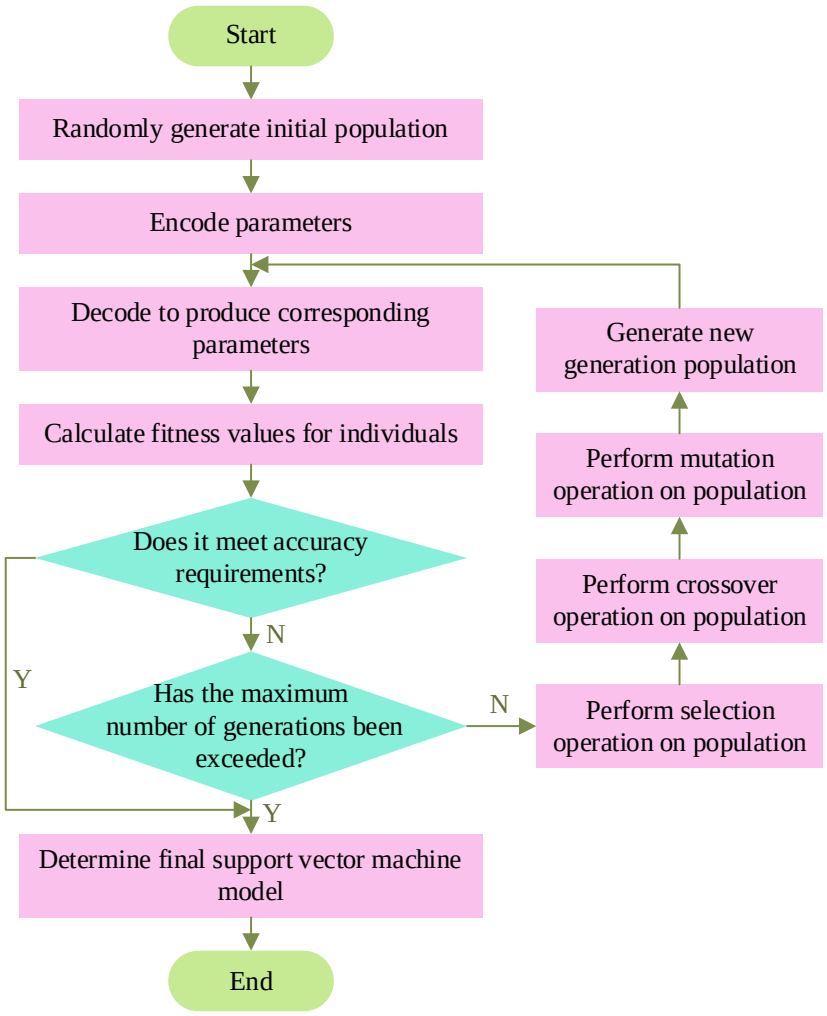


Figure 3: Genetic algorithm process

The specific steps are as follows:

(1) Randomly generate an initial population. Set the initial population size to N and the maximum number of evolutionary generations to G.

(2) Encoding parameters. And encode the penalty parameter C, the index d, the bandwidth σ and the weighting coefficient λ using binary to get the individual gene coding string.

(3) Decoding to generate support vector machine parameters. The individual gene coding string is decoded into corresponding parameters, which are passed as inputs to the support vector machine for training.

(4) Calculate the fitness value of each individual in the population with the fitness function.

(5) Determine whether the optimal individual fitness value is less than the set threshold, if so, find the optimal parameters of the support vector machine algorithm and terminate the algorithm. Otherwise, continue to execute the following steps.

(6) Determine whether the current evolutionary generation exceeds the set maximum generation G, if so, terminate the algorithm. Otherwise, continue the following steps.

(7) Evolve the population with the above selection, crossover and mutation operations respectively to produce a new generation of population, jump to step (3) to continue the cycle.

4.2 Network Security Posture Assessment Indicator System

4.2.1 Selection of indicators

This paper comprehensively analyzes the network security posture from different levels, and divides the network security posture into four sub-postures, which are vulnerability sub-posture, disaster-tolerance sub-posture, threat sub-posture, and stability sub-posture, and describes them specifically by establishing the corresponding secondary indexes, and the specific constructed system of network security posture assessment indexes is shown in Table 1.

Table 1: Network security situation assessment index system

First-level indicator	Secondary indicators
Fragile temperament and posture	Network vulnerability level, number of safety equipment, total amount of equipment open port and kernel state of equipment system
Disaster recovery nature situation	Network bandwidth, equipment access net station frequency, network topology, server concurrent thread number
Threatening posture	The number of alarms, the severity of the attack, the frequency of the security event history and the distribution of different protocol packets
Maintain a stable state of mind	The average survival time of the equipment, the rate of the subnet flow, the total amount of the subnet traffic, the average time of failure

4.2.2 Classification of cybersecurity assessment levels

In this paper, the network security assessment level is divided into five levels: excellent, good, medium, poor and critical, and in order to facilitate a more intuitive analysis of the results of the situational assessment, these five security levels are numerically characterized as the situational index, and the network security assessment level is divided as shown in Table 2.

Table 2: Classification of cybersecurity assessment levels

Safety level	Trend Index e	Description of network operation status
Excellence	[0-0.2]	The network is operating normally
Good	(0.2-0.4]	The network operation is slightly affected
Medium	(0.4-0.6]	The network operation has been affected to a certain extent
Bad	(0.6-0.8]	The network operation has been significantly affected
Danger	(0.8-1]	The network runs a serious safety accident

4.3 Cybersecurity posture assessment models

This paper divides the cybersecurity situation into sub-situations based on the macroscopic nature of cybersecurity, and then selects the corresponding sub-situations as secondary indicators according to the different characteristics of cybersecurity data. Next, the original data collected by the data collector is quantified into situation indicator values according to the situation indicator system designed in this paper. Finally, the cybersecurity situation assessment is realized through the improved GA-SVM algorithm. The cybersecurity situation assessment based on GA-SVM is shown in Figure 4.

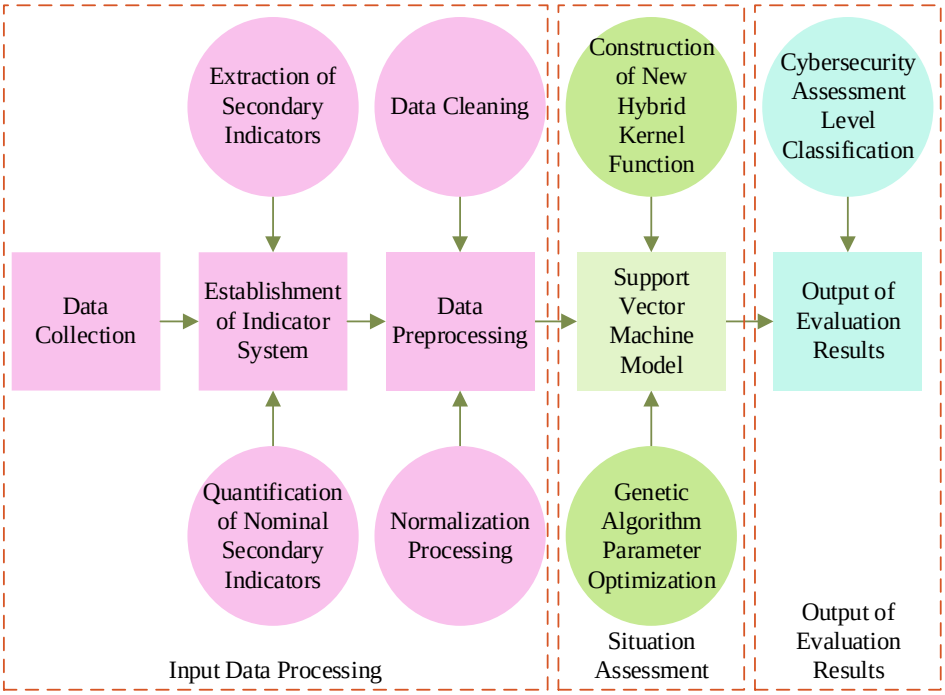


Figure 4: Network Security Situation Assessment Based on GA-SVM

(1) Model input data processing

Firstly, according to the different levels of analysis of network security posture, four sub-postures are divided according to the nature of network security, and then the corresponding second-level sub-postures are selected for the four sub-postures according to different characteristics. Then the collected data are categorized and labeled according to the above posture indicator system, and the data set of the assessment model is produced using the second-level sub-posture as a sample feature. Finally, the data are preprocessed, including quantifying the non-numerical posture indicators and transforming them into numerical features, followed by cleaning and normalizing the data.

(2) Situation assessment

According to the above improved support vector machine algorithm, a posture evaluator is constructed, and for the multi-classification problem of posture evaluation in this paper, a binary tree support vector machine is used to realize the classification of K security levels. For a problem with N security levels, N-1 posture evaluators need to be constructed, and the binomial tree support vector machine model is shown in Fig. 5.

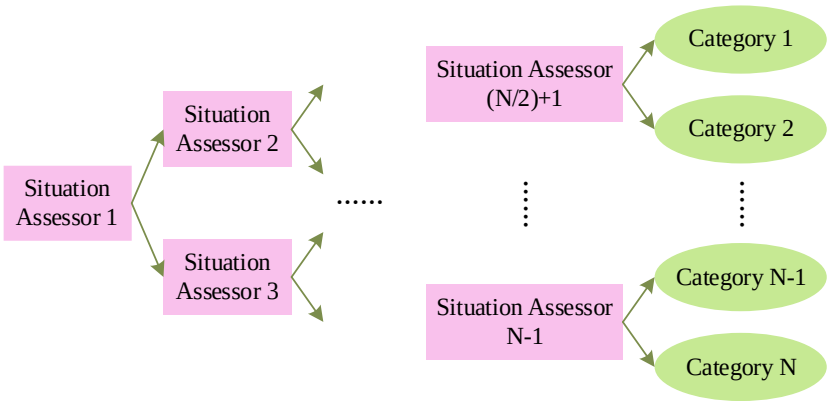


Figure 5: Binary tree support vector machine model

K-fold cross-validation method is used in the training process, which utilizes the no-repeat sampling technique and can effectively improve the generalization ability of the model. The idea is to divide the dataset into k disjoint subsets, select one from these subsets without repetition as the validation set each time, and train the remaining k-1 as the training set, repeat the training k times, and the evaluation accuracy of each training will be used as the adaptation function.

(3) Output evaluation results

According to the above security level table of posture values, the evaluation is performed for the input test set to give the evaluation results of all the samples in the test set.

5 ARIMA-based cybersecurity posture prediction model

The values of the posture are obtained based on different moment points, the cybersecurity posture can be regarded as a sequence of time, and to make a prediction of the posture is to make a prediction of the indicators that characterize the posture. In this study, we chose to use ARIMA model to do a prediction study on cyber security posture.

5.1 ARIMA model

The Autoregressive Moving Average (ARIMA) model is based on the lag and stochastic nature of time series and is fitted using a mathematical model so as to predict the trend of the series. The model parameters and significance are shown in Table 3, the ARIMA model involves three parameters p, d, q, p is the lagged order of the original data itself, d is the order of the difference operation that needs to be carried out when the network data is transformed into the smooth data, and q is the lagged order of the model's prediction error. $ARIMA(p,d,q)$ includes the autoregressive model $AR(p)$, the sliding average model $MA(q)$, the autoregressive-sliding average hybrid model $ARMA(p,q)$, and the autoregressive moving average model $ARIMA(p,d,q)$.

Table 3: Parameters and significance of the ARIMA model

Parameter	Parameter significance
p	Self-regression
d	Difference number
q	Moving average
$AR(p)$	Self-regression model
$MA(q)$	Moving average model

The autoregressive model $AR(p)$ applies only to phenomena associated with a moment in its own pre-existing period, with the following expression:

$$x_t = \sum_{i=1}^{p} u_i x_{t-i} + \varepsilon_t \tag{4}$$

where x_t is the current value, u_i is the autocorrelation coefficient, ε_t is the white noise sequence, p is the order, and $AR(p)$ reflects the linear relationship that exists between the current value at the moment of t and the previous p values, ie:

$$x_t \sim u_1 x_{t-1} + u_2 x_{t-2} + \cdots + u_p x_{t-p} \tag{5}$$

The moving average model $MA(q)$ expresses the accumulation of the error term in the autoregressive model with the following expression:

$$x_t = \sum_{i=1}^{q} \theta_i \varepsilon_{t-i} + \varepsilon_t \tag{6}$$

where x_t is the current value, θ_i is the autoregressive coefficient, ε_t is the white noise sequence, q is the order, and $MA(q)$ reflects the linear relationship that exists between the current value at the moment of t and the previous q values of the error, namely

$$x_t \sim \theta_1 \varepsilon_{t-1} + \theta_2 \varepsilon_{t-2} + \cdots + \theta_q \varepsilon_{t-q} \tag{7}$$

The ARMA model is a combination of autoregressive and moving average with the following expression:

$$x_t = \sum_{i=1}^{p} u_i x_{t-i} + \sum_{i=1}^{q} \theta_i \varepsilon_{t-i} + \varepsilon_t \tag{8}$$

When the time series is an unsteady time series, the series is differenced before being input into the ARMA model, i.e., the ARIMA model.

5.2 Modeling Steps for ARIMA Models

The modeling idea of ARIMA modeling is as follows: first of all, the original data should be judged to determine whether the sequence is a smooth sequence or not, and for the non-smooth sequence, the original sequence should be smoothed by the difference method first. Then the sequence is modeled. The modeling steps are shown in Figure 6.

Step1: Obtain the original sequence.

Step2: Obtain the timing diagram of the original sequence, if the sequence is a non-smooth sequence, then go forward to Step3, if it is a smooth sequence, go forward to Step4.

Step3: Perform first-order difference on the non-smooth sequence to make it smooth.

Step4: make a time series plot for the difference sequence. If it is not smooth, go back to Step3. If it is smooth, go forward to Step5.

Step5: Model identification (IDENTIFY), determine the delay order p, q by calculating the autocorrelation function and partial correlation function, drawing ACF and PACF, and selecting the appropriate model according to the model identification rules shown in Table 4.

Step6: Parameter Estimation and Model Diagnostic Test (EST1-MATE), p, q are determined using AIC, BIC minimum criteria.

Step7: Forecasting (FORECAST).

Step8: Make time series plot of true and predicted values and end.

Table 4: Model recognition rules

	AR (p) model	MA (q) model	ARMA (p, q)
ACF	Trailing	Truncate after phase q	Trailing
PACF	Truncate after phase p	Trailing	Trailing

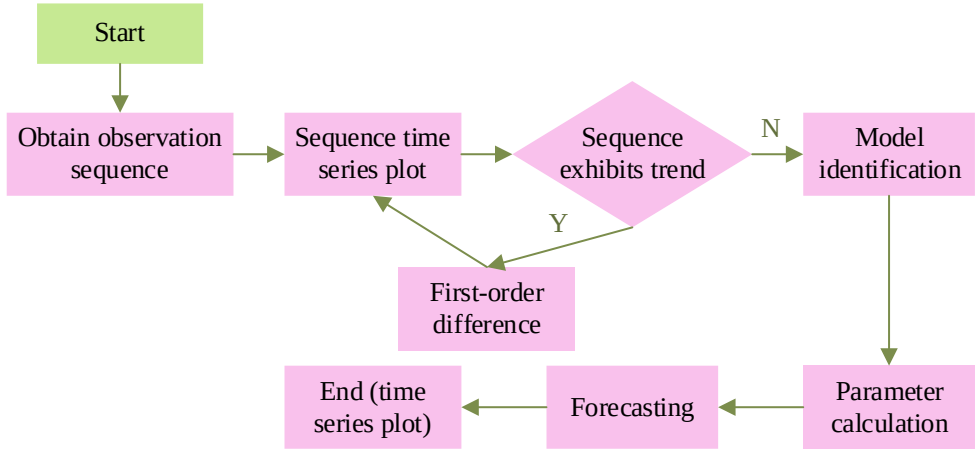


Figure 6: ARIMA modeling steps

6 Experiments and results

6.1 Security posture assessment experiment

6.1.1 Objects of study

In order to analyze the performance of the cybersecurity posture assessment model for non-regulated operations, the HoneyNet dataset is selected as the research object, and a total of 1,000 data are collected, and the change curves are shown in Fig. 7, and the last 200 data are used as the validation data, and the others are used as the training data.

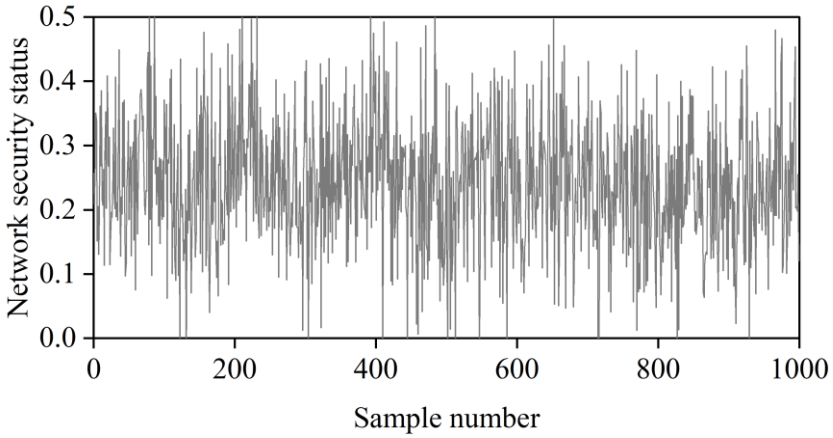


Figure 7: Sample data of network security situational assessment

The variation of delay time and embedding dimension of the sample data for cyber security posture assessment in Fig. 7 are shown in Fig. 8 and Fig. 9 respectively. The optimal delay time = 7 and embedding dimension = 7 for the sample data of cyber security posture assessment, based on which the learning sample dataset for cyber security posture assessment is generated.

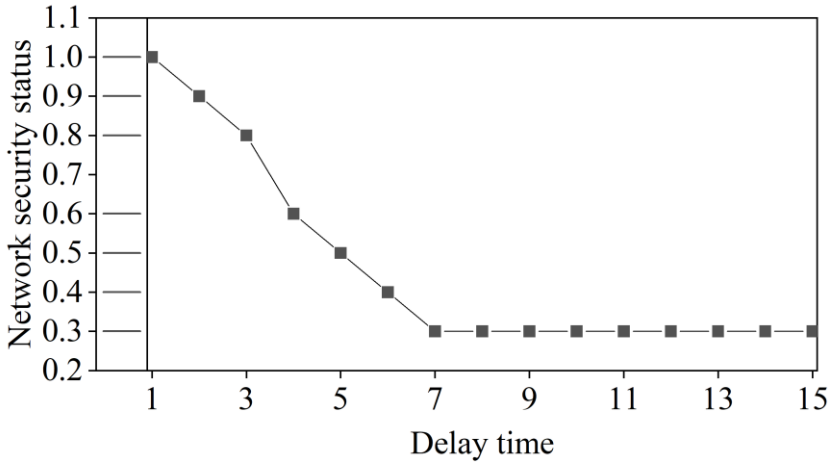


Figure 8: Sample delay time for cybersecurity situation assessment

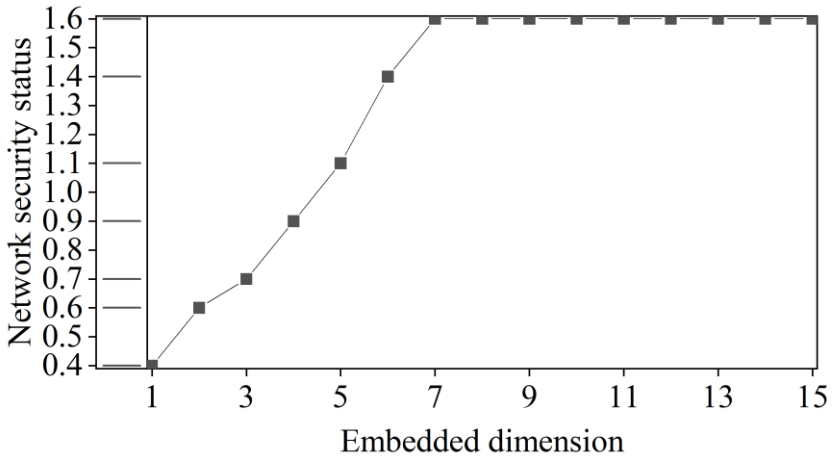


Figure 9: Dimension estimation of sample embedding

6.1.2 Optimization results of SVM algorithm parameters

The optimization sequence of the GA-SVM algorithm is shown in Table 5, and only part of the data is shown due to space limitation. With the increase in the number of iterations, it can be seen that the corresponding parameters such as the penalty factor are constantly updated iteratively, and when the coefficient of determination gradually tends to stabilize, the best parameters can be obtained. After iteration of the GA-SVM algorithm, the optimal kernel function parameters are finally obtained as 9.56499, the input dimension is 7, and the penalty factor is 26.60554.

Table 5: The optimization sequence of the GA-SVM algorithm

Serial Number	Coefficient of determination e	Penalty factor	Kernel function parameters	Input the dimension
1	0.8762	49.39912	11.66847	7
2	0.8986	41.8402	9.44292	7
3	0.9077	26.37053	9.63351	7
4	0.9128	26.34944	9.63409	7
5	0.9246	26.64059	9.53488	7
6	0.9266	26.60554	9.56499	7

Figure 10 refers to the comparison between the predicted and true values of the GA-SVM network security posture prediction model under the time series from 0 to 200. The true value and the predicted value have a completely consistent in some time periods, but in some time periods there is an opposite trend of change, and the coefficient of determination of the predicted sequence of the GA-SVM model is calculated to be 0.91486. Therefore, the model has a very high goodness of fit and good prediction effect. The closer the coefficient of determination is to 1, the higher the degree of fit is, and with the stabilization of the coefficient of determination, the corresponding optimal parameters can be obtained.

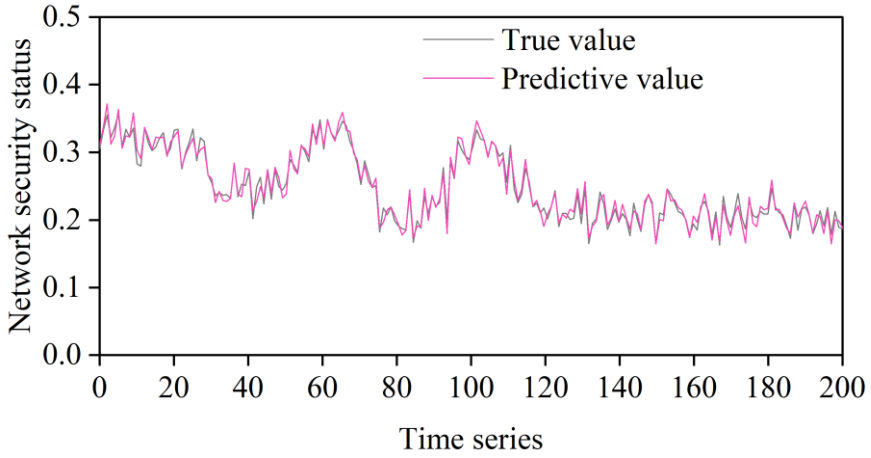


Figure 10: Shows the comparison diagram

6.1.3 Results of the cybersecurity assessment

Figure 11 shows the comparison between the predicted and true values of the 3 models, GA-SVM, RBF, and PSO-SVM. It can be seen that all three prediction models have very high performance, and the network security posture values are stable between 30 and 50 under the time series of 0 to 200. The parameters of SVM are optimized by particle swarm algorithm PSO, and the coefficient of determination of the corresponding prediction model is obtained as 0.90352. However, because the particle swarm algorithm is prone to be trapped in the local minimum solution, the global search ability obtained is relatively weaker than that of GA-SVM. Radial basis neural network is RBF is a new type of neural network algorithm at present, which can greatly reduce the training time, has strong generalization ability, and the coefficient of determination of its prediction model can reach 0.90229, but it is very difficult to construct the model. In summary, the GA-SVM model proposed in this paper is the better model. The experiment further compares the performance of the 3 prediction models and the results of their accuracy, AUC value, and F1 value are shown in Table 6. In terms of accuracy, the values of the 3 models GA-SVM, RBF and PSO-SVM are 89.47%, 79.05% and 78.61% respectively. From the variation of AUC value, the GA-SVM prediction model has the highest value of 0.8792.The F1 value of the 3 models GA-SVM, RBF, PSO-SVM are 0.8644, 0.7413, 0.7396 in that order.In summary, the GA-SVM model has the best performance.

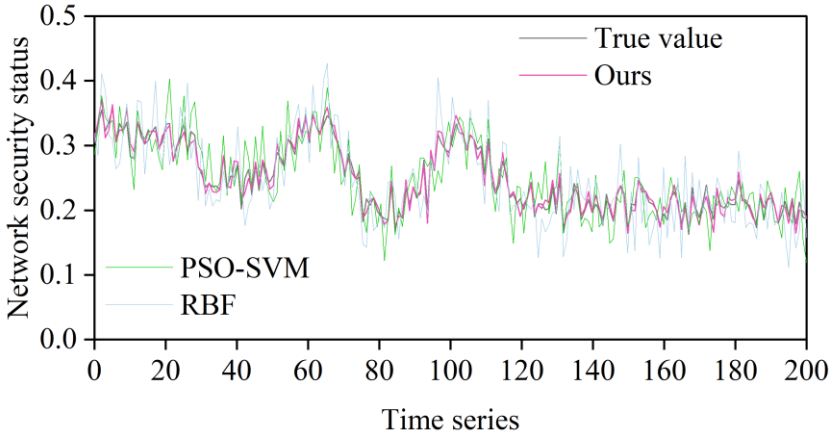


Figure 11: Algorithms dynamic contrast

Table 6: Shows the accuracy rate, AUC value and F1 value of the model

	Accuracy rate	AUC	*F*1
GA-SVM	89.47%	0.8792	0.8644
RBF	79.05%	0.7623	0.7413
PSO-SVM	78.61%	0.7315	0.7396

6.2 Security posture prediction experiment

6.2.1 Data preparation

This section additionally selects the CIC-IDS-2017 dataset, which is a dataset for network intrusion detection released by the Cybersecurity Research Team at the University of Ontario Institute of Technology in Canada in 2017. The dataset contains network traffic data in a real network environment and consists of multiple attack types. The attack traffic includes DoS/DDoS attacks, scans, malware, brute force exploits, botnets, and many other types. The dataset also provides traffic PCAP files from Monday to Friday, which is not conducive to constructing experimental data as the individual PCAP files are very large. Therefore, in this paper, we use Editcap tool to split the daily generated PCAP files, and the splitting strategy is as follows: at the duration of the traffic, split every 5 minutes. The specific splitting is shown in Table 7.

Table 7: CIC-IDS-2017 Dataset and splitting

Date	Description of Pacp load	Total number of PACPs after splitting -
Monday	Benign	92
Tuesday	FTP-Patator, SSH-Patator	91
Wednesday	DoS, Hearbleed Attacks, Slowhttptest, slowloris, Hulk and GoldenEye	90
Thursday	Web and Infiltration Attacks, Web BForce, XSS, Sql Inject, Infiltration Dropbox, Download, Cook disk	93
Friday	Botnet ARES DDoS LOIT, PortScans	91

A total of 457 PCAP files are split out, and after splitting, by modifying the target IP of the attacking machine in the traffic packet as the host asset in the constructed posture evaluation system, and replaying the traffic to the posture evaluation system constructed in this paper through Tcpreplay, the network posture results generated in the system are collected as experimental data. The network security posture generated in 5 days is plotted as a line graph, which can be obtained as a network security posture timing diagram, and the network security posture timing diagram is shown in Figure 12.

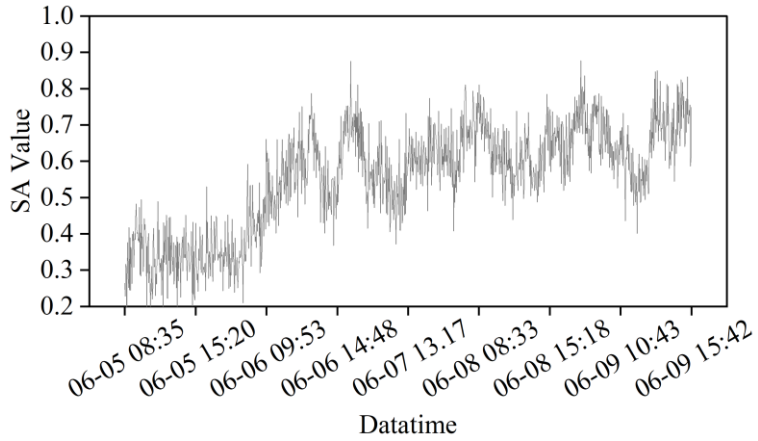


Figure 12: Network security situation sequence

As can be seen from the graph, the posture values fluctuated in a lower range until 18:00 on June 5, due to the fact that the day was a Monday and the replayed packets were normal traffic. After that time, there was a period of high momentum in the morning and afternoon of Tuesday, and a comparison of the attacks shows that the network was subjected to FTP and SSH bursts during these two periods, respectively. Similarly, there was a spike in the morning of Wednesday, and a review of the packets shows that the network was hit by a DoS attack, and on Thursday, the network was mainly hit by Web bursting, XSS and SQL injection attacks, which led to a spike in the network posture in the corresponding time period. The network was hit by a DDoS attack on Friday from 1:38 p.m. to 3:21 p.m., resulting in the highest cybersecurity posture value for that time period. In addition, the Heartbleed attack that occurred between 12:22 and 12:48 p.m. on Wednesday did not cause a significant change in the posture value because Heartbleed was a security vulnerability that appeared in a lower version of the cryptographic library OpenSSL, and the corresponding version in the experimental setup was not in the affected range and did not cause serious harm. Similar attacks include Cool Disk for MACs and Dropbox Download for the application Dropbox. From the above posture value curves and analysis results, it can be further proved that the cyber security posture assessment model proposed in this study is effective. Further, the posture assessment results obtained from this dataset can be utilized as dataset A as additional data for predicting future posture values.

6.2.2 Stability treatment

Smoothness is an important property of time-series data, which describes the stability of statistical characteristics (e.g., mean, variance) possessed by time-series data at different moments, and ARIMA is built on the assumption of data smoothness. The first 400 data in dataset A are training data, and the network security time series graph is obtained as shown in Fig. 13. The trend of increasing and decreasing phases can be found, which belongs to the unsteady time series.

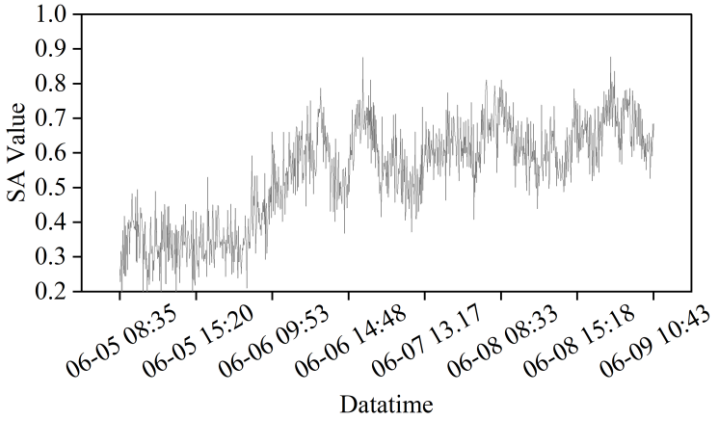
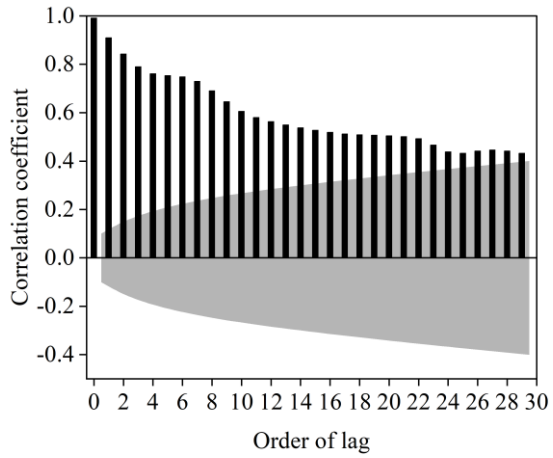


Figure 13: Training data situation curve in dataset 2

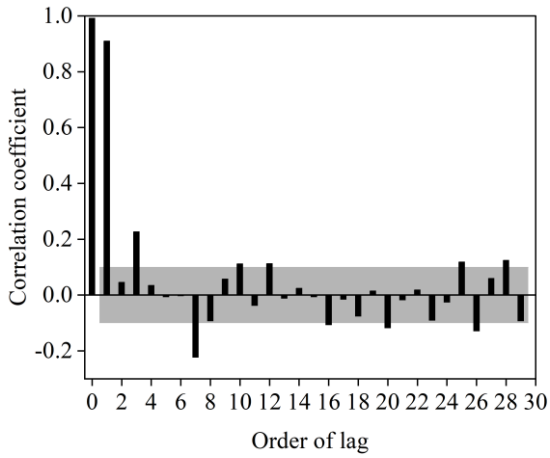
The autocorrelation function and non-autocorrelation function of the original data are plotted in Fig. 14 (a) and (b), and the autocorrelation function is converging to zero but never falls into the confidence interval, which verifies the unsteady nature of the security posture. The original series is first-order differenced, and the autocorrelation function and non-autocorrelation function after differencing are shown in Fig. 14(c) and (d), respectively, and the autocorrelation function and the partial correlation function decay to 0 after lagging 1 and 2 periods, in addition to ADF smoothness test by statsmodels in Python, and the results of the ADF test of the smoothing process of the time-series data are shown in Table 8 results. In the original data p is greater than the significant level and Test Statistic Value cannot reject the original hypothesis at 5% confidence level. These two conditions are reached after the 1st order differencing, so the time series data only meets the smoothness requirement after the 1st order differencing.

Table 8: ADF test results of time series data stabilization process

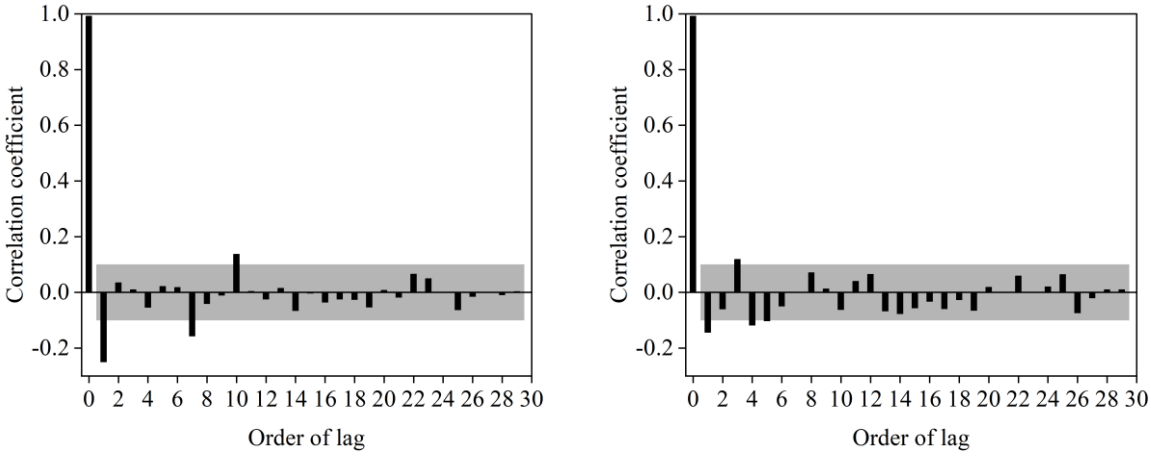
Parameter	Original data	First-order difference
Test Statistic Value	-2.6936	-7.1743
p-value	-0.0639	1.5694e-10
Critical Value (1%)	-3.4276	-3.4276
Critical Value (5%)	-2.7664	-2.7664
Critical Value (10%)	-2.3932	-2.3932



(a) Raw data ACF



(b) Raw data PACF



(c) After difference ACF (d) After difference PACF

Figure 14: ACF and PACF before and after differential

6.2.3 Model identification and ordering

The main work of model identification and order determination is to determine the parameters of ARIMA. Since the autocorrelation and partial correlation functions basically fall within the confidence interval after the 1st order differencing, the sequence meets the smoothness requirement, and d=1 in ARIMA(p, d, q) can be determined. d=1 in ARIMA(p, d, q) can be assumed to be 1 from the fact that the partial correlation function is truncated in the 1st order after differencing in Fig. 14(c) and (d), and the autocorrelation function is gradually decaying to zero in the 1st order, and it can be assumed that the parameter p is 1, and the autocorrelation function truncated in the 2nd and 3rd order can be assumed to have q=2 or q=3, i.e., there are alternative models ARIMA(1,1,2), ARIMA(1,2,3), etc. Further, expanding the range of p, q for screening, the Akaike Information Criterion (AIC) criterion takes into account the fit and complexity of the model, which can be used to identify the model to determine the parameters, and the smaller the value of AIC is the better the model. The optimal ARIMA model can be obtained from the results of the grid parameter search, i.e., ARIMA(1, 1, 3), and the generated AIC matrix of the grid search is shown in Table 9, at which time the AIC value is -1228.73.

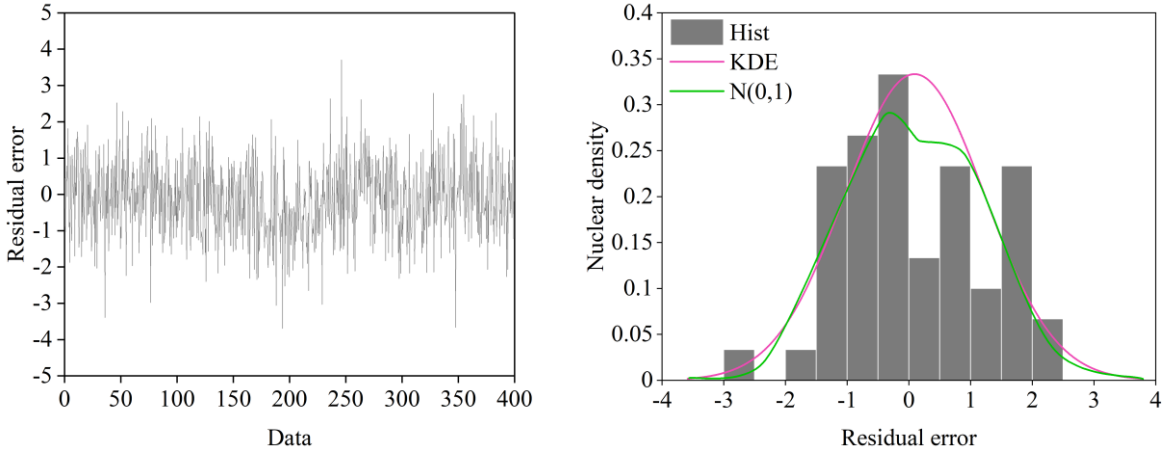
Table 9: AIC matrix

AR(p) / MA(q)	0	1	2	3
3	-1217.60	-1223.79	-1224.67	-1216.96
2	-1208.72	-1221.80	-1205.63	-1223.53
1	-1207.23	-1221.11	-1224.07	-1228.73
0	-1178.53	-1210.12	-1218.61	-1225.98

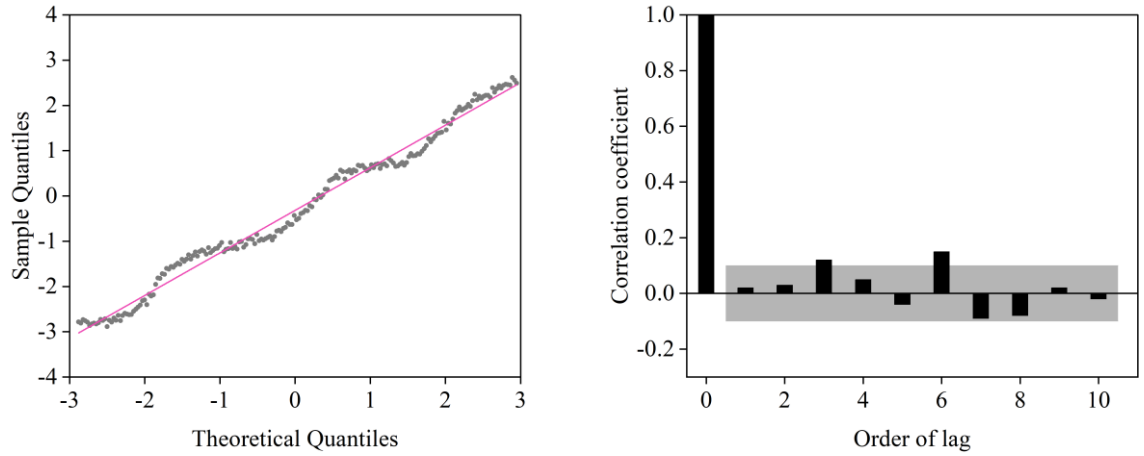
6.2.4 Residual tests

The residuals test determines whether the ARIMA model is able to capture all the information in the data. If the model has structures or patterns in the data that are not captured, then the residuals will show some patterns or regularities. The optimal model ARIMA(1, 1, 3), identified through the above steps, is tested as shown in Fig. 15, with (a) standardized residual distribution, (b) histogram estimation of the residuals, (c) quantile-quantile plots, and (d) standardized autocorrelation plots of the residuals.

It can be observed that subplot (a) fluctuates above and below 0, with a trend consistent with a mean of 0 and a constant variance. The orange curve in subfigure (b) is the kernel density estimate obtained from the histogram, the red curve represents the standardized normal distribution, and the green curve is adjacent to the red curve, indicating that the residuals of the model roughly conform to the normal distribution. Subfigure (c) is almost a straight line except at the head and tail, indicating that the samples largely conform to a normal distribution. In subfigure (d), the horizontal axis indicates the order of the lag, the vertical axis indicates the size of the correlation coefficient, and the shaded part represents the range in which the standard deviation is 2 times; after order 0, the autocorrelation coefficient hardly exceeds the range in which it is 2 times the standard deviation, which indicates that there is a low correlation between the residuals and the lagged values. In summary, the model can be considered to have passed the test and can be used for prediction.



(a) Standardized residual difference cloth (b) Histogram plus estimated density



(c) Normal Q-Q (d) Correlogram

Figure 15: Results of model diagnosis

6.2.5 Model predictions

The model passes the residual test, and the prediction result can be obtained by ARIMA(1, 1, 3), and the prediction graph is shown in Fig. 16, and the indicators MAE, MSE, and R^2 of the ARIMA(1, 1, 3) model are 0.0265, 0.0010, and 0.9672, respectively. It can be seen that the model's prediction result is fitted well.

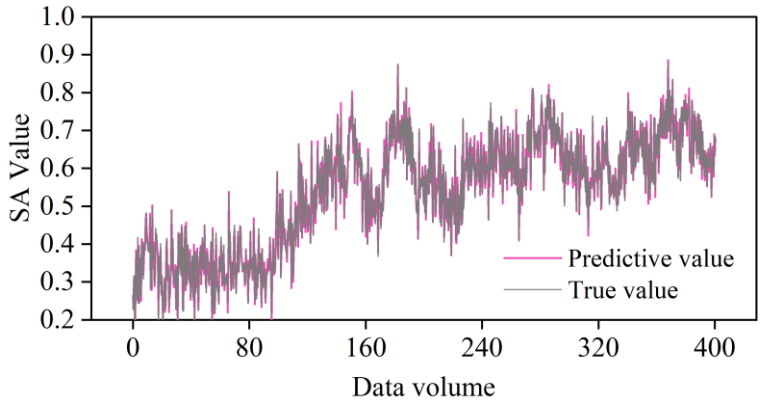


Figure 16: Predict diagram of ARIMA(1,1,3) model

7 Conclusion

Cyberspace is facing increasingly diversified and complex threats and attacks, and maintaining cybersecurity has become a top priority. In this paper, through an in-depth study of network security posture assessment and prediction, managers can understand the current actual non-regulatory business network security situation and master its development law, so as to be able to deal with network security events in a targeted manner, deploy defense measures correctly, and cope with the possible arrival of network security events in advance. Accurate situational identification and prediction through the GA-SVM-based network security posture assessment model and ARIMA-based network security posture prediction method can help enhance the proactivity of non-regulatory business network defense, so as to maintain stronger protection capability in the face of complex and changing network threats. In terms of cybersecurity situational identification, the GA-SVM model has a coefficient of determination of 0.91486, an optimal kernel function parameter of 9.56499, an input dimension of 7, and a penalty factor of 26.60554.Compared with RBF and PSO-SVM, the GA-SVM model has the best performance advantage. The prediction experimental results on CIC-IDS-2017 posture data show that the ARIMA-based cybersecurity posture prediction method has high prediction accuracy and strong generalization ability.

Funding

This research was supported by the Research on Management Optimization of Network Security Capability Improvement for Non-regulated Business (GZKJXM20232261).

About the Author

Qijing Zhang (1989-1), female, Han ethnicity, native of Liupanshui, Guizhou Province, holds a bachelor's degree and works as an engineer. Her research focuses on cybersecurity in the ubiquitous power Internet of Things (IoT).

Renmeng Lu (1980-1), male, Bouyei ethnic group, from Zhenning, Guizhou Province, holds a bachelor's degree and is a senior engineer. His research focuses on ubiquitous networks and information security, information infrastructure, as well as information operation, maintenance, and services.

Yu Lu (1976-12), female, Han ethnicity, from Guiyang, Guizhou Province, holds a bachelor's degree and is a senior engineer specializing in innovative development of ubiquitous power Internet of Things (IoT).

References

[1] Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. Chinese Political Science Review, 1(1), 81-93.

[2] Van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Digital Policy, Regulation and Governance, 19(6), 429-448.

[3] Liaropoulos, A. N. (2017). Cyberspace governance and state sovereignty. In Democracy and an open-economy world order (pp. 25-35). Cham: Springer International Publishing.

[4] Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. Security Studies, 26(3), 452-481.

[5] Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. Edpacs, 63(6), 1-22.

[6] Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. Journal of applied security research, 16(4), 490-513.

[7] Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of cyber policy, 3(2), 258-283.

[8] Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7-34.

[9] Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering, 5(5), 67.

[10] Beridze, T., & Lomidze, G. (2024). A Policy-Centered Framework for Cybersecurity Management: Ensuring Information Assurance Through Governance and Oversight. International Journal of Advanced Computational Methodologies and Emerging Technologies, 14(8), 1-13.

[11] Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of network and computer applications, 209, 103540.

[12] Tagarev, T., Davis, B. A., & Cooke, M. (2022). Business, Organisational and governance modalities of collaborative cybersecurity networks. Multimedia Tools and Applications, 81(7), 9431-9443.

[13] Yanakiev, Y. (2020). A Governance Model of a Collaborative Networked Organization for Cybersecurity Research. Information & Security, 46(1).

[14] Gash, A. (2022). Collaborative governance. In Handbook on theories of governance (pp. 497-509). Edward Elgar Publishing.

[15] Obioha-Val, O. A. (2025). Bridging gaps in cybersecurity governance: Leveraging collaborative digital solutions. Asian Journal of Research in Computer Science, 18(2), 82-100.

[16] Albalas, T., Modjtahedi, A., & Abdi, R. (2022). Cybersecurity governance: A scoping review. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 7(4), 9.

[17] Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy, 3(3), 327-350.

[18] Muller, L. P. (2016). Power dynamics in cyberspace: how do we produce cybersecurity?. INTERNASJONAL POLITIKK, 74(4).

[19] Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. International Journal of Science and Research Archive, 14(1), 1146-1163.