International Journal for Housing Science and Its Applications
Publish August 4, 2025. Volume 46, Issue 3 Pages 2568-2578

https://doi.org/10.70517/ijhsa463215

Network Security Emergency Response Mechanism and Data Protection Strategy for Downward Multi-Level Protection in Cloud Computing Environment

Xibao Wang[1], Hengming Yuan[1], Yueyue Bu[2], Wenhui Chu[1], Chengcheng Gao[1] and Lei Wang[1,*]
[1] Industrial Internet Business Division, Yunding Technology Co., Ltd., Jinan, Shandong, 250000, China
[2] Integrated Machine Parts Department, Yankuang Energy Group Co., Ltd., Material Supply Center, Jining, Shandong, 250000, China
Corresponding authors: (e-mail: 15254106762@163.com).

Abstract The wide application of cloud computing technology makes network security challenges increasingly complex, and traditional single-layer protection strategies are difficult to cope with diverse network attacks. This study proposes a network security emergency response mechanism and data protection strategy based on multi-layer protection for the increasingly complex network security threats in cloud computing environment. Methodologically, a Partially Observable Markov Decision Process (POMDP) model is constructed, combined with an attack defense tree for security strategy decision-making, and the defense strategy benefit is quantified by fuzzy hierarchical analysis. The experiments are validated using real cloud platform data, and the results show that: in the analysis of the attack gain matrix, the maximum attack gain value under the high-risk state reaches 14.12; after the implementation of the optimal defense strategy, the defense gain matrix shows that the maximum defense gain can reach 54.8, which is significantly higher than the attack gain; and the experiment of the temporal strategy proves that, when the defense period (3DT) is smaller than the attack period (5AT), the percentage of infected nodes accounts for ratio is only up to 34.75%, and the network system quickly tends to the steady state at t=29s. The conclusion shows that the multilevel protection mechanism proposed in this study can effectively identify the optimal defense strategy and improve the network security level in cloud computing environment, which provides theoretical basis and technical support for practical application.

Index Terms cloud computing environment, network security, emergency response mechanism, multilevel protection, POMDP model, defense gain

I. Introduction

Cloud computing, as an emerging computing paradigm, has been widely used in a variety of fields, including finance, healthcare, and education [1], [2]. However, since the services involved in cloud computing, such as information processing as well as data storage, are realized based on the Internet, security has been one of the biggest obstacles in its development [3], [4]. In a cloud computing environment, users' data are stored on the servers of cloud service providers, so it is important to ensure that the data stored in the cloud are not illegally accessed and stolen, and that the cloud computing network is protected from malicious attacks and hacking [5]-[8]. In order to ensure the security of cloud computing network, it is essential to adopt network security emergency response mechanism with data protection strategy [9], [10]. Network security emergency response mechanism is a kind of emergency handling mechanism for network security threats and events, which aims to respond to network security events in a timely and effective manner, and prevent or mitigate their damage to network systems and data [11]-[13]. Cybersecurity emergency response mechanisms usually include incident discovery and confirmation, incident classification and level assessment, emergency response process, information sharing and notification, and after-action summarization and improvement [14], [15]. The establishment and improvement of cybersecurity emergency response mechanisms are crucial to guarantee the safe operation of network systems and data security [16]. Organizations and enterprises should formulate relevant emergency response strategies and organize regular emergency drills and training to improve the ability and level of responding to cybersecurity events and ensure that network security is effectively protected [17]-[19]. And data protection strategy is a very important work in cloud computing environment, data protection not only refers to data security, but also includes data backup and recovery and other aspects of the work [20]-[22]. For data security, strict access control, encrypted storage and other strategies are needed to protect users' data from illegal tampering and theft [23], [24].

The rapid development of computer technology and the Internet has promoted the process of global informatization, and cloud computing, as a new computing model, has been widely used in governments,

enterprises and individual users. Cloud computing environment is characterized by resource sharing, on-demand service and scalability to provide users with convenient services, but it also faces unprecedented network security challenges. Cybersecurity issues in cloud computing environments not only include traditional information security threats, but also involve new types of security issues such as virtualization security, multi-tenant security and data privacy protection. Once a cybersecurity incident occurs, it may lead to sensitive data leakage, business interruption or even cause huge economic loss and reputation damage. International Data Corporation (IDC) survey shows that more than 70% of the world's enterprises have suffered from varying degrees of network security attacks, of which cloud platform-related security events accounted for nearly 40%, and is a year-on-year upward trend. The traditional single protection method has been unable to meet the complex and changing network security needs, the establishment of an all-round, multi-level network security protection system and efficient emergency response mechanism has become the focus of the current research direction. Existing research mainly focuses on static defense strategies and single attack models, lacking in-depth analysis of the attack and defense game process in the dynamic network environment, making it difficult to adapt to the complexity and variability of network attacks in the cloud computing environment. How to formulate optimal defense strategies and maximize network security protection under limited resources is a key problem to be solved in the current network security field. In this study, firstly, we analyze the challenges and threats of network security in cloud computing environment, and clarify the necessity of multi-level protection; secondly, we construct a security strategy decision model based on Partially Observable Markov Decision Process (POMDP), and portray the interactions between attack and defense through attack-defense tree; and then, we introduce Fuzzy Hierarchical Analysis to calculate the benefit of the defense strategy, and comprehensively consider the cost and effect of defense in order to find the optimal defense strategy. Then, the fuzzy hierarchical analysis is introduced to calculate the benefit of the defense strategy, taking into account the defense cost and the defense effect, in order to obtain the optimal defense strategy; finally, the experimental validation is carried out through the data of the real cloud platform to analyze the evolution law of the network node state in the process of the attack-defense game and evaluate the effectiveness of the proposed method. This study combines theoretical analysis and experimental verification to explore new ideas and methods for network security protection in cloud computing environment, and provides theoretical support and technical guidance for improving network security level in cloud computing environment.

II. Cybersecurity and emergency response

II. A. Network information security

The progress of computer technology and the rapid development of the Internet have given people's work, study and lifestyle a great convenience, and the communication between people is more convenient and wider in scope than before. However, along with the popularization of people's life and informatization, the network security problem has become increasingly serious, and has gradually become a major factor hindering the development of information [25].

Generally speaking, network security is divided into two parts: information security and control security. The so-called information security means: “the integrity, availability, confidentiality and reliability of information”. While control security refers to authentication, non-repudiation, authorization and access control.

The Internet has the characteristics of openness, interactivity and decentralization, which makes the network able to meet people's needs for information sharing, openness, flexibility and speed, thus creating conditions for information sharing, information exchange and information services, and providing a great impetus to the progress of human society. However, it is due to the above characteristics of the Internet that many security problems have arisen.

(1) Information leakage, information pollution, information is not easy to control. For example, unauthorized use of resources, system denial or denial of information flow.

(2)Some people due to special purposes, information destruction, information leakage, information infringement and information infiltration, and even political subversion behavior, seriously endangering the legitimate rights and interests of the state, society and all kinds of subjects.

(3)Due to the extensive nature of the network, it often results in the dispersion of control management, and due to the divergence of interests and goals of various individuals, it often results in the disconnection of the management and maintenance of information resources, thus triggering a wide range of information security problems.

(4) Accompanied by the trend towards the electronicization of the offices of the relevant State agencies, network security incidents can bring about serious security problems for the relevant agencies, thus causing a great deal of negative impact.

II. A. 1) Cyber information security objectives

The attributes of network information security are shown in Figure 1.

The goal of network information security is to ensure the security of the global network and system integrity; for security issues, event detection can be summarized and synthesized to the monitoring center, to ensure that the traceability is the entire system traceability. Therefore a secure computer network system should support the following security objectives.

(1) Confidentiality: to prevent information or system processes leaked out. There is a risk of direct leakage when information is transmitted over a communication link or recorded on a computer storage device.

(2) Integrity: Ensuring that data has not been maliciously altered or corrupted.

(3)Availability: The ability of authorized users to access and use resources for a valid period of time.

(4)Non-repudiation: Avoiding the non-recognition of all or part of the act of communication by the entities involved in a communication.

(5) Controllability: mainly in the global monitoring, early warning capabilities and emergency response capabilities. The so-called global warning is to establish a global security status collection system, for new security vulnerabilities and attack methods to understand in a timely manner, to respond to security incursions and so on. From the above, it can be seen that in a network security system, to realize the above security goals, it is crucial to establish a fast and effective emergency response system.

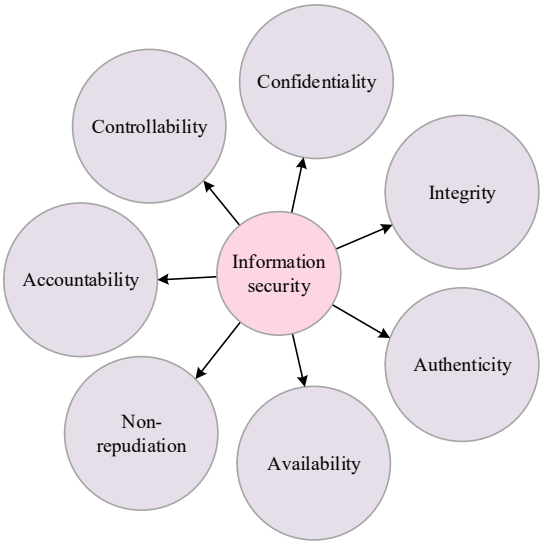


Figure 1: Seven Attributes of Information Security

II. A. 2) Network information security model

The research and understanding of network security architecture has gone through the process of: Communication Confidentiality (COMSEC), Information Security (INFOSEC) and Communication Assurance. Among them, academics have further divided information security assurance into four segments, namely PDRR. p refers to protection, D refers to detection, the first R refers to reaction, and the second R refers to recovery. On the basis of the original PDRR model, the WPDRRC model has been formed, which constitutes the framework of the macro information network security assurance system structure through the six links of WPDRRC (warning, protection, detection, reaction, recovery, counterattack) and the three major elements of people, policy (including laws, regulations, systems, management) and technology. This framework gives a performance index of information security guarantee system, namely: early warning capability, protection capability, detection capability, response capability, recovery capability and counterattack capability. The interrelationship is shown in Figure 2.

II. B.Emergency response

This section first discusses the basic concepts of emergency response from three perspectives, and then briefly describes and analyzes the current state of emergency response and explores the possibilities for its improvement, setting the stage for the entry of the paradigm-based reasoning (CBR) technique below. Emergency response, usually refers to the preparations made by an organization to cope with the occurrence of various sudden and unexpected events as well as the measures and actions taken after the events [26].

For computer system and network security, from a micro perspective, a security event is the confidentiality of data and information on computer systems and networks, integrity and availability of information, applications, services

and networks, etc. From a macro perspective, more and more security events are emerging with the development of the Internet, such as e-fraud in e-commerce and malicious scanning of networks.

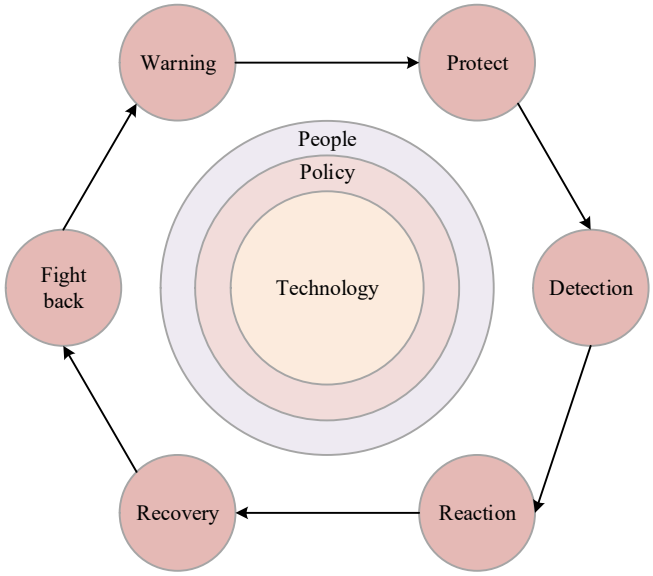


Figure 2: Schematic diagram of the Information Assurance Model WPDRRC

The content of emergency response is actually incident response. By incident response, we mean the measures and actions taken after a security incident occurs. These measures and actions are usually used to organize the development and expansion of the event and to reduce the negative impact of the event.

It is impossible to guarantee the absolute safety of the network with prior warning, and there are security risks in any network, which fundamentally determines the importance of the emergency response system for network security.

III. Network security strategy based on multi-layered protection

III. A. Methodological Framework for Security Strategy Decision Making

The field layer security policy decision-making method proposed in this paper mainly consists of two modules: security policy decision-making and defense policy benefit quantification. The security policy decision module is the process of constructing a POMDP model for the security policy decision process at the field layer, and solving the POMDP model based on real-time attack evidence to obtain the optimal security policy. For the construction of POMDP model, first analyze the system structure and protection knowledge, set the state space and observation space; then summarize the experience to get the observation function by analyzing the historical operation data; and then design the security state transfer probability by the system vulnerability utilization rate. Finally, the action space and benefit function are obtained by using the defense strategy benefit quantification module, so as to construct the POMDP decision model [27].

III. B. Quantifying Defense Strategy Benefits

III. B. 1) Attack defense tree construction

Attack tree model is a model that uses a tree structure to describe the security threats faced by a system and the multiple attacks to which the system may be subjected, and is often used to analyze the attack paths present in a system, vulnerability assessment, risk assessment etc. Attack trees provide a formal and organized way to describe the security of a system under different attacks.The tree structure is used to describe the possible ways of attacking a system.The root node is the final attack goal and the different attacks to achieve that goal are the leaf nodes. Each node is a sub-goal and the children of that node are the methods to achieve that sub-goal. The branches of the attack tree represent the various attack paths that can be taken to achieve the attack goal. An obvious limitation of the attack tree is its inability to capture the interaction between the attacks performed on the system and the defenses deployed, which also limits the accuracy of analyzing the best defense strategy, which can be overcome by introducing defense strategies. The Attack Defense Tree extends the attack tree with a graph that represents the

possible attacks that an attacker can take and the defenses that a defender can use, i.e., the graph contains two opposite types of nodes:attack nodes and defense nodes.

III. B. 2) Calculation of Defense Strategy Benefits

Fuzzy hierarchical analysis is introduced in the attack and defense layers of the attack-defense tree to calculate the defense strategy gains, respectively. In the attack layer, the attack node benefit is calculated by considering the attack cost of the attack node and the severity caused by the attack, and the risk value caused by the attack node is used as the attack node benefit. Calculate the defense node revenue in the defense layer, taking into account the defense cost and defense effect of the defense node, and the defense effect is the mitigated risk value which is the attack node revenue. The steps for calculating the defense strategy gain are as follows:

(1) Calculate the risk-based attack node gain

The system risk value depends on the probability of occurrence of risk in the system and the consequences of occurrence of risk [28]. So the risk value can be obtained from the product of the probability of occurrence of an attack event and the damage caused:

$$risk(A_i) = p(A_i) \times q(A_i) \tag{1}$$

where $p(A_i)$ denotes the probability that the attack event A_i occurs, and $q(A_i)$ denotes the loss of assets due to A_i.

The three attributes of attack cost, attack difficulty and probability of attack being detected are chosen as the evaluation metrics of the attacking node. Then the formula for the risk probability value of the attacking node is as follows:

$$p(Ai) = w_{\cos t} \times u_{\cos t} + w_{diff} \times u_{diff} + w_{possi} \times u_{possi} \tag{2}$$

where w denotes the weight of each evaluation metric of the attacking node, which is calculated from equation (2). u denotes the utility value of each evaluation metric of the attack node, which can be obtained by the inverse of its rank score.

Since the attack node in the attack defense tree is the attack event and its parent node is the attacked field device, the asset loss due to the attack event is expressed in terms of the security importance of the field device, and the actual value is determined by the demand.

(2) Calculate the defense node gain

The defense node gain should consider the cost of the defense strategy itself and the mitigated system risk, which can be obtained by subtracting the cost of the defense node from the gain of the attack node:

$$U(D_i) = \sum_{j=1}^{m} \varepsilon_j \times risk(A_j) - \cos t(D_i) \tag{3}$$

where ε_j denotes whether the defense node D_i successfully defends the attack event A_j or not, and the success of the defense is 1, otherwise it is 0. $risk(A_j)$ denotes the value of the risk of the attack event A_j, and $\cos t(D_i)$ denotes the cost of the defense node D_i.

Three attributes of the defense strategy, namely, consuming time, occupying resources and the degree of impact on the system, are chosen as the evaluation indexes of the defense node, and the defense cost of the defense node is calculated by the following formula:

$$\cos t(Di) = w_{time} \times time + w_{resour} \times resource + w_{effect} \times effect \tag{4}$$

where w denotes the weight of each defense attribute, which is calculated by equation (4).

III. C. Optimal Defense Strategy Solving

The POMDP model is an extension of the Markov Decision Making (MDP) model.The MDP model is modeled with complete knowledge of the state of the system, and its solution process is a state-to-action mapping: $\pi(s) \to a$, s is the state of safety in which the system is located, and a is the action chosen by the policy π [29]. The optimal policy can be computed iteratively by the Bellman equation:

$$Q(s,a) = R(s,a) + \gamma \max_{a} \sum_{s \in s'} T(s,a,s')Q(s',a') \tag{5}$$

$$\pi^* = \arg\max_a Q(s,a) \tag{6}$$

where the Q-value function $Q(s,a)$ is the gain value of executing the action a in the current security state, and π^* is the optimal policy at the maximum gain value.

But the POMDP model is modeled under uncertainty about the state of the system, and the intelligent body can only obtain observation information from the environment as a reference to the state, so it has to be based on all the observations and the historical sequence of executing actions $\{a_0, z_1, ..., a_{t-1}, z_t\}$ to make a decision about the next action a_t. Over time, this history sequence can become long, and Astrom proposes that it can be summarized by a belief distribution, where b is a vector representing the probability distribution over states, as follows:

$$b_t(s) = P(s_t = s \mid z_t, a_{t-1}, z_{t-1}, ..., a_0) \tag{7}$$

The belief point b_t at the moment of Eq. t can be updated according to Bayes' rule, which involves only the belief state b_{t-1} of the previous step, the action taken a_{t-1}, and the observation obtained z_t as follows:

$$b_t(s') = \tau(b_{t-1}, a_{t-1}, z_t) = \frac{O(s', a_{t-1}, z_t)\sum_s T(s, a_{t-1}, s')b_{t-1}(s)}{P(z_t \mid b_{t-1}, a_{t-1})} \tag{8}$$

$$P(z_t \mid b_{t-1}, a_{t-1}) = \sum_{s'} O(s', a_{t-1}, z_t)\sum_s T(s, a_{t-1}, s')b_{t-1}(s) \tag{9}$$

Thus the process of solving the POMDP model can be viewed as a mapping of belief states to actions: $\pi(b) \to a$, b is the belief distribution, and a is the action chosen by the strategy π. A Bellman equation similar to solving the MDP model can then be obtained:

$$Q_{t+1}(b,a) = \sum_s b(s)R(s,a) + \gamma \sum_z P(z \mid b,a)V_t^*(\tau(b,a,z)) \tag{10}$$

$$V_{t+1}^*(b) = \max_a Q_{t+1}(b,a) \tag{11}$$

$$\pi_{t+1}^*(b) = \arg\max_a Q_{t+1}(b,a) \tag{12}$$

where the Q-value function $Q_{t+1}(b,a)$ is the value of the gain from executing a at the current belief point b within the t-step horizon, $V_{t+1}^*(b)$ is the value of the maximal gain achieved by the choice of the action $Q_{t+1}(b,a)$, and $\pi_{t+1}'(b)$ is the optimal at the time of maximum gain value. Strategy.

Since the belief space is continuous, the POMDP model solution cannot be solved directly and iteratively as in MDP, in order to solve the POMDP model, Smallwood showed that the value function on any finite horizon t can be represented by a set of vectors: $\Gamma t = \{\alpha_0, \alpha_1, ..., \alpha_m\}$, with each α vector denoting a $|S|$-dimensional hyperplane and defining the value function on the belief bounded region:

$$Vt(b) = \max_{\alpha \in \Gamma_t} \sum_s \alpha(s)b(s) \tag{13}$$

Many approximate POMDP solutions utilize specific or a small number of belief points to update the gain values and gain computational advantage by increasing the number of iterations to ensure that the algorithm works.

IV. Analysis of experimental simulation results

IV. A. Experimental data

In this paper, some real network data of a cloud platform is collected and stored using neo4j as shown in Fig. 3. Where the orange nodes indicate the attack conditions, as the necessary prerequisites of the attack action. The blue node indicates the attack action, the process of the attacker to implement the attack, the goal is to obtain a certain attack state. The red node indicates the attack state, which is obtained after the attacker executes the attack action. Gray nodes denote defensive actions, for which there may be multiple defensive actions for a certain attack action, and a single defensive action may apply to multiple attack actions. The relationships include four kinds:

trigger, obtain, further, and defense. The relationship between orange node-blue node is trigger, i.e., a specific attack action can be triggered by satisfying certain attack conditions. The relationship between blue node-red node is obtaining, i.e., another state can be reached after unfolding a certain attack action. The relationship between red node-blue node is further, i.e., the attacker can further launch other attack actions in a certain state. The relationship between gray node-blue node is defense, which is the effective defense action corresponding to a certain attack action.

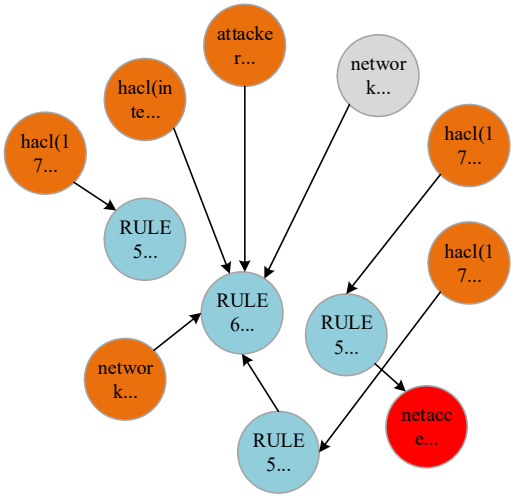


Figure 3: Experimental attack and defense diagram

IV. B. Optimal Strategy Simulation

For the above experimental environment, the information needed for the game is extracted from it, including the information of each state, the information of attack action and the information of defense action, and the overall attack graph and the single-point defense graph are established, based on which the above optimal strategy selection algorithm is implemented using Python. For each attribute of defense action, set dk={name, probability, profit, cost}={defense_id, 0.46, 30.8, 1.4}. For the attack action attributes, they are obtained from the neo4j database, and all the data in the second tuple are obtained from the database. The attack and defense gains for each state are calculated and the attack gain matrix for each state is obtained as shown in Table 1.

Table 1: State/attack income matrix

	S1	S3	S6	S8	S13	S15	S32	S37
a2	0	2.79	0	0	0	0	0	0
a4	0	0	10.41	0	0	0	0	0
a7	0	0	0	9.14	0	0	0	0
a9	0	0	5.78	0	0	0	0	0
a11	0	0	0	0	5.74	0	0	0
a14	0	0	0	0	0	14.12	0	0
a16	0	0	3.72	0	0	0	0	0
a18	0	0	0	0	3.69	0	0	0
a20	13	0	0	0	0	0	0	0
a22	0	0	0	0	0	0	0	0
a27	5.72	0	0	0	0	0	0	0
a31	0	0	0	0	5.28	0	11.78	0

The defense domain benefit matrix is shown in Table 2.

Based on the gain matrix, the variation of the curve for calculating the sum of attack/defense gains for each state is shown in Fig. 4, where the horizontal coordinates represent the cloud platform in eight different states with unique state numbers, and the vertical coordinates represent the gains of the attacker and the defender.

Table 2: State/attack income matrix

	S1	S3	S6	S8	S13	S15	S32	S37
a2	0	12.22	0	0	0	0	0	0
a4	0	0	13.85	0	0	0	0	0
a7	0	0	0	20.03	0	0	0	0
a9	0	0	8.02	0	0	0	0	0
a11	0	0	0	0	8.14	54.8	0	0
a14	0	0	0	0	0	0	0	0
a16	0	0	0	0	0	0	0	0
a18	0	0	0	0	0	0	0	0
a20	16.28	0	0	0	0	0	0	0
a22	0	0	0	0	0	0	0	0
a27	7.89	0	0	0	0	0	0	0
a31	0	0	0	0	0	0	8	0

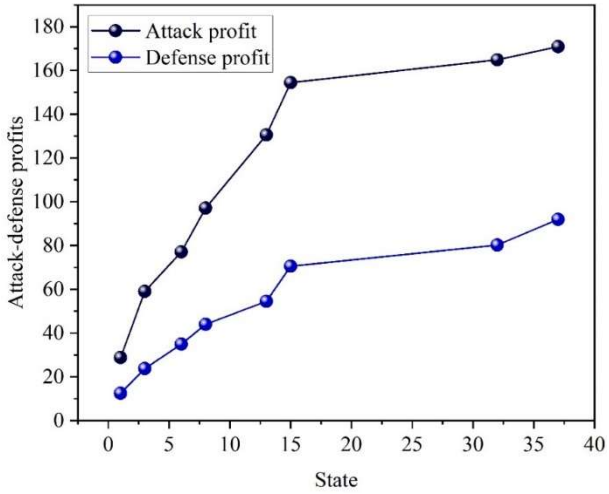


Figure 4: Defense and benefit

Based on the attack/defense gain matrix, the optimal attack/defense strategy for each state is calculated as shown in Fig. 5. Where the horizontal coordinates are still the eight states of the cloud platform, the points of the attack strategy correspond to the predicted optimal attack action chosen by the attacker in a certain state, and the points of the defense strategy correspond to the optimal defense action taken in a certain state.

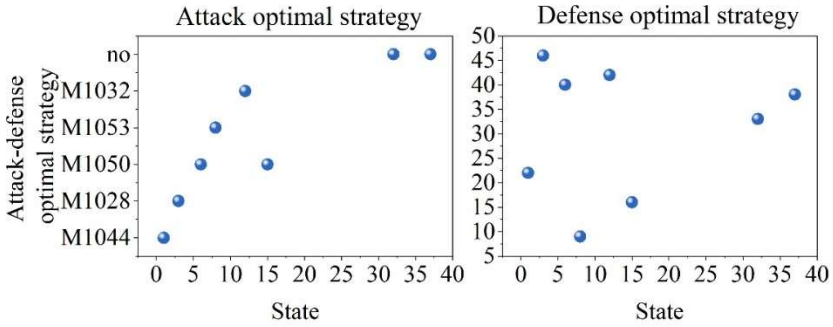


Figure 5: Optimal attack/defensive action

In addition, according to the way the algorithm is designed to calculate the attack/defense success rate, the attack/defense success rate is obtained as shown in Figure 6.

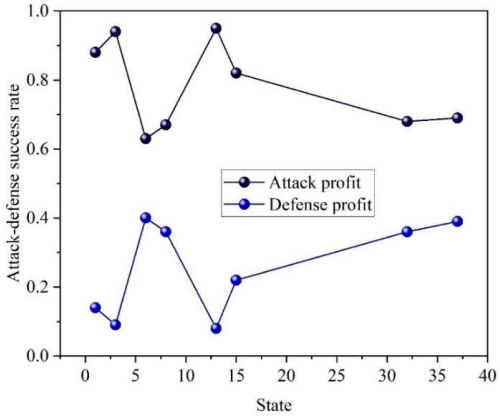


Figure 6: Attack/defense success rate

IV. C. Numerical experiments and analysis

In this chapter, the MATLAB tool is used as the experimental platform, and the corresponding experimental parameters are set to simulate the network attack and defense scenarios in different initial states in order to verify the validity and scientificity of the model. First, initialize the experimental parameters, set the proportion of the number of three kinds of network nodes in the system, namely, the normal working state S, the attack-infection state I and the defense-repair state R, as 0.10:0.3:0, respectively, the recovery rate of the network nodes = 0.6, and the time range of the attack-defense game is set to [0, 100s].

Without considering the time strategy, when the attacker and the defender select only the behavioral strategy for the game, the network node state evolution of a single behavioral strategy is shown in Fig. 7. The state of the network node changes in real time with the result of the behavioral confrontation between the attacker and the defender. As can be seen from the figure, when the initial t=0s, the main goal of the attacker is to scan the system for vulnerabilities, and the selected attack strategy is low-intensity, at the same time, the system implements passive defense measures, so that the internal potential infected nodes are gradually transformed into repair state nodes, and then restored to normal working nodes. When t=5s, the attacker successfully invades the Web server, and then immediately adopts a high-intensity attack strategy to expand the damage. Due to the fast and covert attack action, the low-intensity defense strategy cannot respond effectively in time, which leads to a sharp decrease in the percentage of network nodes in normal working state, and the corresponding percentage of infected network nodes rises rapidly, and the attack efficiency is highest when t=12s. When the attacker reaches the established goal with the high-intensity attack in a short period of time, the low-intensity attack strategy is used to ensure the efficiency ratio, while the defense system detects the attack behavior within the system, and immediately adopts the high-intensity defense strategy to quickly repair the infected nodes. With the interactive confrontation between the attacker and the defender, the nodes in the three states tend to be stabilized when t=50s, at which time the proportion of nodes working normally is more than 90%, and gradually tends to be closer to 1, and finally reaches a stable state.

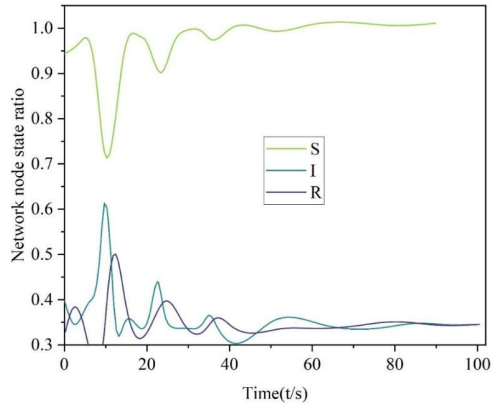
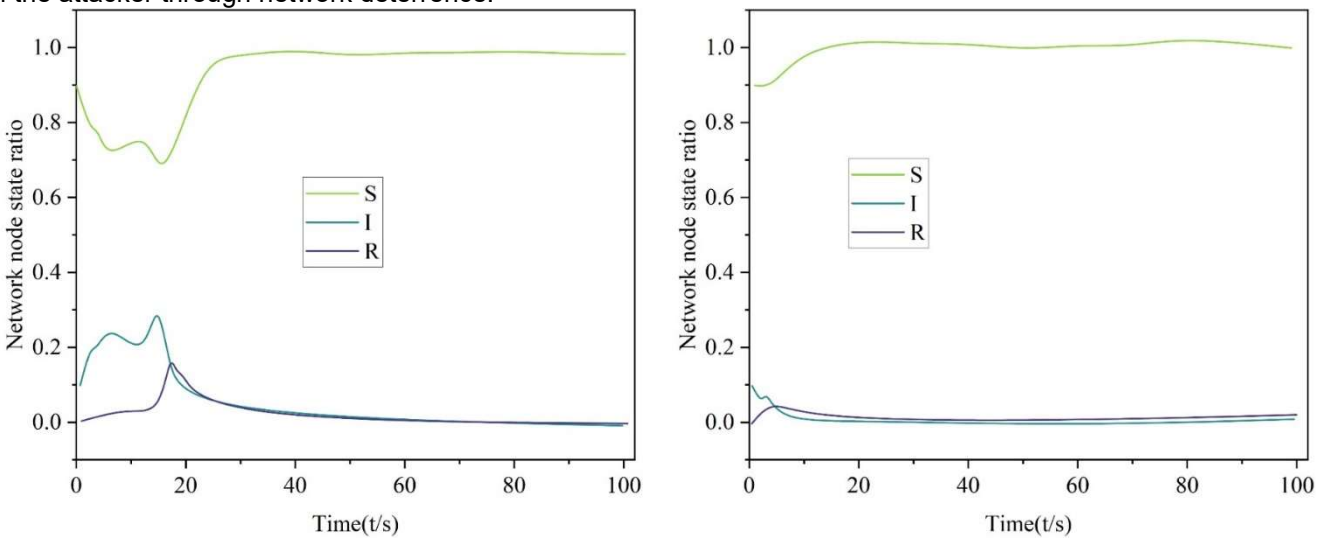


Figure 7: The network node state evolution of a single behavior strategy

The attacker and the defender select behavioral strategies in conjunction with the time policy, and when the defense period is smaller than the attack period, the state evolution of the network nodes is shown in Fig. 8.

The time strategy is introduced mainly to solve the problems of how long the attacker should launch the next attack and how often the defender should defend the system. Comparing the graphs, after both sides add the time policy, since the system adopts a fixed-period defense strategy and the internal system carries out regular detections, even in the face of sudden hidden blitzkrieg-type attack behaviors, the system can ensure that it can effectively defend itself against cyber-attacks and mitigate the proliferation of cyber-attacks. When t=15s, the attack efficiency reaches the highest, at which time the proportion of infected nodes is 34.75%, and when t=29s, the state of network nodes tends to be in steady state. The state of network nodes tends to steady state. In the two experiments, the time for the state of the nodes to tend to the steady state is shortened accordingly, which shows that the time strategy is an important influencing factor for the change of the security state of the network system. When the period strategy of the defense side is determined, the influence of different attack period strategies on the change of node security state is analyzed. In this paper, the defense period is fixed as =3DT, and the attack periods =4AT and =5AT are taken as examples to analyze the change of the network node security state when the defense period is smaller than the attack period. Due to DATT, it indicates that the action frequency of system defense is higher, and the network nodes spend more time in the defense state, so when the time strategy of the defender is fixed, the larger the action cycle of the attacker is, the smaller the fluctuation of the attack and defense confrontation is, the smaller the number of network node state transformations are, and the time of transforming from infected nodes to repair state nodes and restoring to normal nodes is shortened accordingly. The experimental results show that while strengthening the network security defense capability, it is also crucial to improve the network deterrence capability, and it is more conducive to ensure the security of the network system by reducing the action frequency of the attacker through network deterrence.



(a) Defense cycle=3,Attack cycle=4 (b) Defense cycle=3,Attack cycle=5

Figure 8: Network node state evolution

V. Conclusion

Multi-level protection network security policy shows significant defense effect in cloud computing environment. The experimental data show that using the POMDP model for security policy decision-making can accurately identify attack behaviors and formulate optimal defense measures. In the attack and defense gain matrix analysis, the maximum defense gain when the cloud platform is in the S15 state reaches 54.8, which is much higher than other states, indicating that the implementation of key protection for key nodes has obvious advantages. The experimental results of the time strategy show that when the defense period is fixed at 3DT and smaller than the attack period (5AT), the system reaches the steady state at t=29s, and the highest percentage of infected nodes is only 34.75%, which is significantly lower than that in the case of no time strategy. The multi-level protection mechanism effectively quantifies the defense strategy gains by integrating the attack defense tree and fuzzy hierarchical analysis, which provides a scientific basis for resource allocation optimization. Validation based on real cloud platform data shows that the method can not only cope with known attack types, but also predict and prevent unknown threats. Future work will further explore the application of deep reinforcement learning in dynamic attack and defense environments to improve the adaptive capability of defense strategies and extend it to more complex cloud environments and

hybrid cloud architectures, laying the foundation for building a more robust cloud computing security protection system.

References

[1] Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: state-of-art. International Journal of Big Data Intelligence, 4(2), 81-107.

[2] Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings, 51, 2172-2175.

[3] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[4] Khan, M. A. (2016). A survey of security issues for cloud computing. Journal of network and computer applications, 71, 11-29.

[5] Akbar, H., Zubair, M., & Malik, M. S. (2023). The security issues and challenges in cloud computing. International Journal for Electronic Crime Investigation, 7(1), 13-32.

[6] Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. Procedia Computer Science, 48, 204-209.

[7] Markandey, A., Dhamdhere, P., & Gajmal, Y. (2018, September). Data access security in cloud computing: A review. In 2018 International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 633-636). IEEE.

[8] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.

[9] Alnajrani, H. M., & Norman, A. A. (2020). The effects of applying privacy by design to preserve privacy and personal data protection in mobile cloud computing: An exploratory study. Symmetry, 12(12), 2039.

[10] Mathew, A. J. (2024). Unscripted practices for uncertain events: Organizational problems in cybersecurity incident management. Science, Technology, & Human Values, 49(4), 827-850.

[11] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering, 29(1), 223-246.

[12] Dsouza, Z. (2017). Are cyber security incident response teams (CSIRTs) redundant or can they be relevant to international cyber security. Fed. Comm. LJ, 69, 201.

[13] Korn, E. B., Fletcher, D. M., Mitchell, E. M., Pyke, A. A., & Whitham, S. M. (2021). Jack pandemus–cyber incident and emergency response during a pandemic. Information Security Journal: A Global Perspective, 30(5), 294-307.

[14] Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and privacy, 3(6), e126.

[15] Oriola, O., Adeyemo, A. B., Papadaki, M., & Kotzé, E. (2021). A collaborative approach for national cybersecurity incident management. Information & Computer Security, 29(3), 457-484.

[16] Lin, Y. (2023). Construction of Computer Network Security System in the Era of Big Data. Advances in Computer and Communication, 4(3).

[17] Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on services computing, 9(1), 138-151.

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

[19] Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1), tyy002.

[20] Ramaswamy, Y., Sankaran, V. N., & Sundar, B. K. M. (2024). Advanced Cybersecurity Strategies in Cloud Computing: Techniques for Data Protection and Privacy. Library of Progress-Library Science, Information Technology & Computer, 44(3).

[21] Wei, Y., & Zhang, Y. (2018). Cloud computing data security protection strategy. In Cloud Computing and Security: 4th International Conference, ICCCS 2018, Haikou, China, June 8-10, 2018, Revised Selected Papers, Part I 4 (pp. 376-386). Springer International Publishing.

[22] Jones, K. I., & Suchithra, R. (2023). Information security: A coordinated strategy to guarantee data security in cloud computing. International Journal of Data Informatics and Intelligent Computing, 2(1), 11-31.

[23] Julakanti, S. R., Sattiraju, N. S. K., & Julakanti, R. (2022). Securing the Cloud: Strategies for Data and Application Protection. NeuroQuantology, 20(9), 8062-8073.

[24] Kumar, G. (2019). A review on data protection of cloud computing security, benefits, risks and suggestions. United International Journal for Research & Technology, 1(2), 26-34.

[25] Yu Zhong & Xingguo Li. (2025). Network information security protection method based on additive Gaussian noise and mutual information neural network in cloud computing background. Egyptian Informatics Journal,30,100673-100673.

[26] Li Yongkui,Liu Yan,Wang Siyuan & Han Yilong. (2025). Stress-Testing the Functionality of Healthcare Infrastructure Systems: Percolation Analysis on Network Flows. Journal of Management in Engineering,41(4),

[27] Thomas K.Waring,Vera L. J.Somers,Michael A.McCarthy & Christopher M.Baker. (2024). When to monitor or control: Informed invasive species management using a partially observable Markov decision process (POMDP) framework. Methods in Ecology and Evolution,15(9),1667-1676.

[28] Liang Tian,Chenquan Gan,Jiabin Lin,Fengjun Shang & Qingyi Zhu. (2025). Analysis of attack-defense game for advanced malware propagation control in cloud. Computer Communications,237,108148-108148.

[29] Xinyuan Liu & Ping Luo. (2025). Design of Dynamic Load Balancing Optimization Model Based on Improved Weights in Dempster–Shafer Evidence Algorithm for Cloud Computing Environments. Journal of Circuits, Systems and Computers,(prepublish),