Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Research on network security protection model of multimedia fusion technology based on fuzzy inference algorithm in Internet of Things environment

Xuewei Liu[1], Bingfu Hu[2,✉], Ruiwei Duan[2]

[1] *Science and Technology Division, Weifang Engineering Vocational College, Weifang, Shandong, 262500, China*

[2] *Department of Information Engineering, Weifang Engineering Vocational College, Weifang, Shandong, 262500, China*

ABSTRACT

With the explosive growth of the variety and quantity of multimedia information in the Internet of Things (IoT) environment, its security problem is becoming more and more prominent. Therefore, this paper constructs APODAC dynamic access control model. The information processing of massive data of IoT is carried out through the fusion technology of multiple media features. Based on the real-time access behavior sequence of IoT, a fuzzy reasoner is used to analyze the degree of risk and assess the network security posture. Based on the degree of risk, IoT access rights are dynamically adjusted. The simulation experiment results show that the fuzzy reasoning method in this paper has a 4.4% higher risk detection rate for IoT network and a 10.5% decrease in false alarm rate compared to the traditional SVM method. In risk behavior oriented dynamic access control, the APODAC model proposed in this paper still outperforms the other 2 models in terms of response time for both higher number of access requests and smaller amount of access request data.

Keywords: multimedia information, Internet of Things, APODAC model, network security, risk level

1. Introduction

As a kind of intelligent physical device network, the Internet of Things (IoT), which uses Internet technology to collect and transmit information data in large quantities, can realize a certain connection between items and objects, thus providing convenient services for the majority of users [1-3]. For example, IoT technology is used in scenarios such as bike sharing, automatic vehicle driving, and smart home control [4]. However, while IoT technology contributes to the modern society, the security risks it has become more and more serious.

In order to ensure the security and availability of IoT data, people need to take relevant technical means for data protection measures, i.e., computer network security protection in the IoT environment [5]. The security protection technology in the IoT environment mainly focuses on the

✉ Corresponding author.
E-mail address: lidandan891@126.com (B. Hu).
Received 15 January 2024; Revised 20 February 2024; Accepted 30 November 2024; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-357

secure access of devices, the secure transmission of data and the all-round protection of privacy. Secure access of devices is the first line of defense for IoT security protection, which ensures that only legitimate devices can access the IoT platform through authentication and authorization management of devices [6-7]. Data transmission security, on the other hand, focuses on the encrypted transmission and integrity verification of data in the IoT environment to prevent data tampering and theft [8]. Privacy protection is one of the important goals of IoT security protection, which reduces the risk of user privacy leakage by desensitizing and encrypting sensitive information [9-10]. At the same time, perfect privacy protection policies and regulatory mechanisms need to be focused on to ensure that users' privacy rights and interests are safeguarded [11]. However, if the computer network security technology is not guaranteed to a certain extent, a large amount of transmitted information in the Internet of Things will be subject to the risk of leakage, or even destruction and tampering [12-13]. In the era of Internet of Things, if you want to manage data security, you need to combine advanced network security technology to develop protective measures to minimize security risks and losses, so that the computer network can be in a stable and stable state [14-17].

Aiming at the growing information explosion and network security problems of the Internet of Things, this paper constructs APODAC dynamic access control model based on fuzzy inference algorithm. The multimedia fusion analysis technology is embedded in the IoT system, and the massive information data are fused and processed. Real-time access behavior sequence and access activity state are constructed based on these information data. A fuzzy reasoner is used to perform fuzzy inference on the fuzzy variables of the access sequence that has been obtained, and the risk level is evaluated to obtain the fuzzy risk level. Based on the obtained fuzzy risk level, the access rights of IOT network are dynamically adjusted to realize the information security protection of IOT network. Finally, the real IOT network environment is simulated to verify the advantages of the model.

2. Network security protection technology in the Internet of Things environment

2.1. Security Threats to IoT Development

The concept of “Internet of Things” is a network technology concept based on the “Internet concept”, which extends its user side to any different things to communicate and exchange between them. It is based on the Internet and extends and expands the network on this basis [18]. The Internet of Things (IoT), through intelligent sensing and identification technologies, enables the networking of things and the correlation of things, allowing a large number of previously stand-alone, independent work, different forms of sensing devices, multimedia devices to access the network, and the addition of new devices to make the types and quantities of multimedia information generated and involved in the transmission of interactions to be exponentially increased. In the IoT network, every object can be addressed, communicated with and controlled, and connectivity is enhanced from “any time, any place” to “any object, any time, any place”. The Internet of Things (IoT) is widely used in the convergence of networks through intelligent sensing and identification technologies, and is considered to be the pillar of future Internet development. As the application of IoT technology in various industries continues to deepen, its security issues are becoming more and more prominent. IoT systems face a variety of security threats at the network level, including malware attacks and phishing attacks. Malware, such as viruses, worms and Trojan horses, can spread through the network and infect computers or servers in the control system, leading to data loss or system paralysis. Phishing attacks, on the other hand, trick users into disclosing sensitive information, such as login credentials and configuration details, by disguising themselves as legitimate requests, allowing attackers to illegally control or steal data.

2.2. APODAC Dynamic Access Control Model

2.2.1. IoT information processing technologies. From the "terminal network" connected by machines in the former Web era to the platform as a carrier, or to provide information, or to provide services, or to help users extend the relationship to achieve the explicit connection, to the data-based big data era, intelligent personalized recommendations for people to build implicit connection, more and more people, things, information, effective It will effectively connect more and more people, things and information, and realize the benign circulation of information.

As a core technology of information processing, the multimedia convergence analysis system should be able to access or embedded into other Internet of Things systems to provide information processing capabilities based on multimedia data content. The establishment of the architecture of the multimedia fusion analysis system is a sign of the maturity of the research on multimedia fusion analysis, and here we make some preliminary discussions about it [19]. The fusion of multiple media features can improve the performance of semantic analysis of multiple composite media with different forms and reduce the uncertainty caused by processing only a single media. There are many approaches that can be used for fusion processing of multiple media features, but they are basically based on the following schemes i.e., serial structure for fusion of multiple media features, parallel structure, and multilevel as shown in Fig. 1.

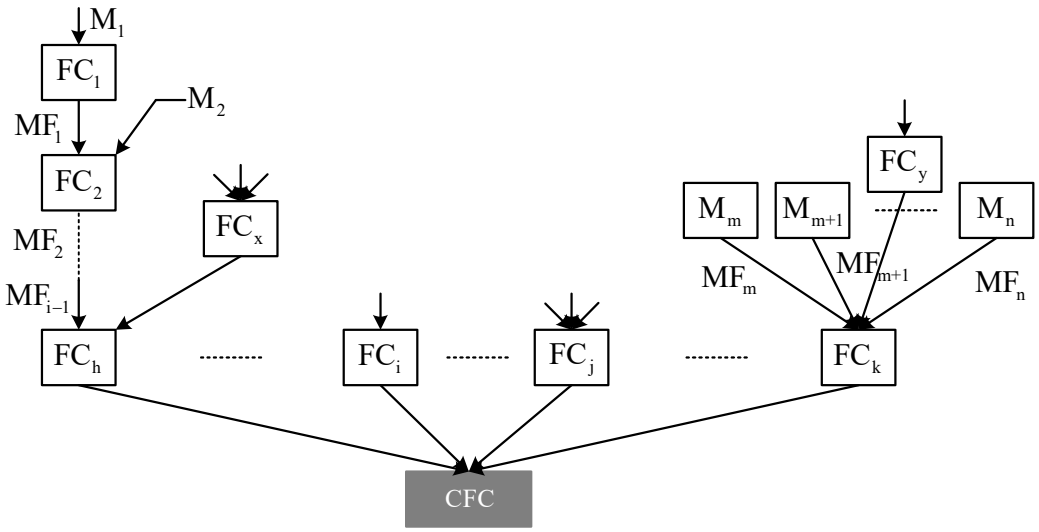

Fig. 1. Multi-stage step-by-step fusion scheme

2.2.2. Definition of basic elements of the APODAC model. In order to realize the dynamic adjustment of user's authority in the process of accessing the IOT network, this paper improves the APODAC model based on the RBAC model to obtain the APODAC model, and the specific relationship of the APODAC model is shown in Fig. 2. The fuzzy S_r sequence satisfaction degree (FS), fuzzy S_T deviation degree (FD), and fuzzy S_F consistency degree (FC) are inputted into the fuzzy reasoner to infer the fuzzy IoT risk level, and then the system dynamically adjusts the user's privileges according to the fuzzy risk level, and the upper limit of privilege adjustment is the user's role-based all the permissions acquired by the user based on the role [20].

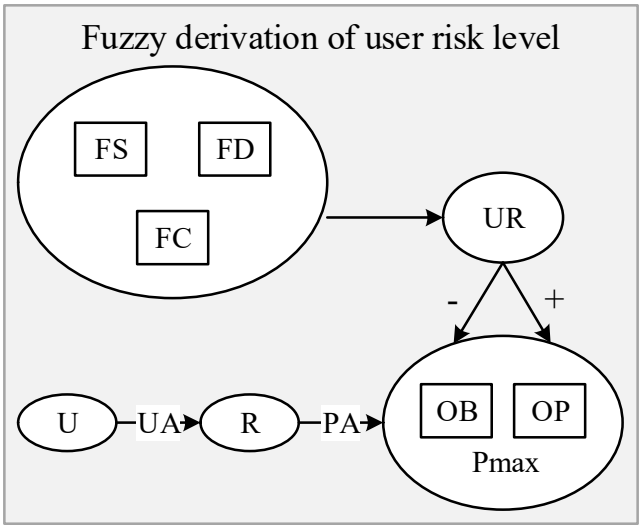

Fig. 2. APODAC model

Access control techniques are one of the information security strategies to address network risks.

The basic elements of APODAC model are defined as follows:

Definition 1: A user is an authorized legitimate user. The set of legitimate users is denoted as U, and the U set element is denoted by u.

Definition 2: A role is a categorization of a user based on the characteristics of the user's need for a system application or function. The set of user roles is denoted as R, the elements of the R set are denoted by the letters r, and R and U are in a many-to-many mapping relationship.

Definition 3: An object is an object to which the system has access control, such as an application or a function. The set of objects is denoted as OB and the OB set element is denoted by ob.

Definition 4: An operation is an action that occurs by U on an OB, the set of operations is denoted as OP, and the elements of the OP set are denoted by op.

Definition 5: A privilege is the right of a legitimate user to use a specific system resource, which can be expressed as OB × OP, i.e., it is expressed as a binary relationship between an object and an operation. The set of permissions is denoted as P and the elements in the P set are denoted by p.

Definition 6: User risk level refers to a parameter derived from the evaluation of user behavior. The set of user risk levels is denoted by UR(userrisk) and the elements in the UR set are denoted by ur.

Definition 7: Fuzzy S_r Sequence Satisfaction (FS) refers to the degree to which a user's real-time access sequence fits the user's base sequence.

Definition 8: Fuzzy S_T Deviation Degree (FD) is the degree of deviation between a new sequence consisting of the longest element extracted from the user's real-time sequence and a new sequence consisting of the longest element extracted from the user's base sequence.

Definition 9: The degree of fuzzy S_F -consistency (FC) is the degree of consistency between the new sequence consisting of the elements with the highest frequency of occurrence extracted from the user's real-time sequence and the new sequence consisting of the elements with the highest frequency of occurrence extracted from the user's base sequence.

2.2.3. APODAC model constraints. Constraints in the APODAC model are crucial, through which the dynamic authorization capability of the model can be improved and the usability of the model can be enhanced. The model can dynamically adjust the user's privileges only within the range allowed by the constraints, if the constraints are not satisfied, the dynamic adjustment of privileges by the model is prohibited [21]. The APODAC model defines two constraints, Privilege Dependency Constraints (PDCs) and Maximum Privilege Constraints (MPCs).

Definition 10: Permission Dependency Constraint (PDC) means that the granting or disabling of one permission in the APODAC model must be contingent on the granting or disabling of another permission. PDC can be expressed as a ternary (P_1, P_2, PDC), $\exists P_1 \in P, \exists P_2 \in P, \exists P_2 \in P$, P_1 depends on P_2, then the PDC constraint can be expressed as:

$$(P_1, P_2) \in PDC \wedge (P_1 = Authorised) \Rightarrow P_2 = Authorised \tag{1}$$

Or:

$$(P_1, P_2) \in PDC \wedge (P_1 = Disabled) \Rightarrow P_2 = Disabled \tag{2}$$

Definition 11: Maximum Privilege Constraint (MPC) means that U cannot increment more than P_{Max} in the APODAC model. Where P_{Max} is the set of all permissions granted to a legitimate user on a role-based basis. the MPC can be expressed as a triple (p, num, P_{Max}), where p denotes the permissions granted, num denotes the number of permissions granted, and P_{Max} denotes the maximum number of permissions that U can have. $\exists p \in P$, then the MPC constraint can be expressed as:

$$P.num \le P_{Max} \subseteq P \Rightarrow P = Authorised \tag{3}$$

2.2.4. User behavior sequences . A user behavior rule base based on roles and business logic needs to be established before assessing the risk level of users [22]. The specific steps are as follows:
1) Mark each application or function.
2) Give the user base behavior sequence based on user role and business logic.
3) Record the real-time sequences that grow up to a set threshold when accessing the application or function in the order of user access.
4) Extract the element with the longest access time in the real-time sequence to form a new sequence.
5) Extract an element with the highest access frequency in the real-time sequence to compose a new sequence.
6) Get the user's behavior sequence.

2.2.5. User risk level assessment. The APODAC model is realized by a fuzzy reasoner to assess the user's risk level. The fuzzy inference system has the property of being able to approximate any nonlinear continuous function in the tight branching set, which can overcome the difficulties encountered by linear combinatorial prediction methods in solving the problem of non-equilibrium time series combinatorial modeling. Theoretical analyses and a large number of example predictions show that: the method has a strong learning and generalization ability, and it is very useful in dealing with nonlinear system combinatorial modeling and prediction methods such as the time series correlation, which has a certain degree of uncertainty. Prediction methods have good applications.

Fuzzy inference is a kind of fuzzy implicit relationship, which is a mapping process to establish an input-output relationship based on fuzzy logic. The process of fuzzy logic decision-making consists of three parts: fuzzification, fuzzy reasoning, and clarification. The fuzzification is done through the affiliation function. The basic structure of a fuzzy inference system consists of four main parts: the fuzzifier, the rule base, the reasoner and the antifuzzifier.
1) Fuzzy ware. A fuzzifier is a fuzzy set that maps the exact point in the input space $x = (x1, x2, ..., xp) \in x$ is mapped into a fuzzy set A' in x. Here x is the vector. A fuzzifier is a built-in front-end machine with prefiltering.
2) Rule base. Fuzzy rule base consists of a collection of if-then rules. In the general case rule R can be expressed as follows:
$R^t : if\ u_1$ is A_1^l and u_2 is A_2^l and. and u_p is A_p^l, then v is G^l.

where: l=1, 2,.... , m is the number of rules, A_p and G^l are the fuzzy sets in $Xi \subset R$ and $Y \subset R$ respectively. $u = (ul, u2, ..., up)T \in X1 \times X2 \times ... \times XP$ and $\upsilon \in Y$. Their values are $x \in X, y \in Y$. Multiple premises (more than two) and multiple rules are expressed in Eq.

3) Reasoner. The reasoner in a fuzzy inference system is the set of fuzzy if-then rules in the fuzzy rule base that maps the set of fuzzy inputs in $X = X1 \times X2 \times ... \times XP$ to the set of output fuzzy in Y , utilizing the aforementioned principle. Order:

$$A \hat{=} A_1^l \times A_2^l \times \cdots \times A_p^l, B \hat{=} G^l \tag{4}$$

Then:

$$R^l : A \square A_1^l \times A_2^l \times \cdots \times A_p^l, \rightarrow G = A \rightarrow^l B \tag{5}$$

Here the reasoner is treated as a system that maps one fuzzy set into another fuzzy set using $\mu_{A \rightarrow B}(x, y)$. Since the rule has more than one premise, here x is a vector.

Unlike traditional reasoning systems, fuzzy reasoning systems are closer to human thinking and reasoning, and they provide access to imprecise or approximate knowledge from real cybersecurity environments. Fuzzy inference systems have precise inputs and outputs, which complete the nonlinear mapping from the input space to the output space, partially realizing some human intelligence. In fact, in complex large-scale network security applications, the presence of uncertainty or imprecision in the system, such as false alarms, makes fuzzy reasoning better than conventional reasoning. Therefore this reasoning method is more suitable for analyzing and researching cyber security risks.

3. Experiments and results

3.1. Risk assessment of analog simulation IoT

Firstly, we use the Honeynet dataset, which simulates the real IoT network environment to verify the validity of the model. Because Honeynet is not announced to the outside world when it connects to the Internet and does not induce hacker attacks, the data it captures is able to reflect the actual network environment.

In order to mine the risk of network attacks and complex attack correlations, the raw data were processed with data filtering, format standardization, normalization and correlation analysis. In this experiment, the thresholds for the number of alarms and vulnerabilities are set to b1 and b2.

The experiment firstly focuses on detecting the correct detection rate and false alarm rate of this design method for network attacks, and also provides statistics on the success rate of some correlation attack detection; secondly, the experiment also selects two machine learning methods, SVM and NaiveBayes, to carry out the detection comparison on the same experimental data, and the experimental results are shown in Table 1. From the experimental results in the table, it can be seen that APODAC adopting multimedia fusion technology and fuzzy reasoning can well discover the risk of IoT network attack under reasonable parameter settings. Under the condition of setting b1=5 and b2=6, the detection rate of this detection method increases from 86.4% to 90.8% and the false alarm rate decreases from 26.8% to 16.3% compared with the traditional SVM method.

Table 1. Experiment results of situation assessment

Method	Threshold and frequency	Test rate/%	False rate/%	For the success rate of associated attack detection/%
SVM	N/A	86.4	26.8	3.3
NaiveBayes	N/A	87.5	28.2	14.2
Methods of this	b1=5, b2=6	90.8	16.3	63.4

article				
	b1=10, b2=4	89.6	12.7	54.8
	b1=20, b2=4	88.4	5.8	50.2

Here a dataset from the Honeynet organization for the month of November 2024 is taken, which records the logs of the attacks suffered by 9 hosts (with consecutive IPs ranging from 172.16.1.101 to 172.16.1.109) in an IoT LAN in that month. On a daily basis, indicators are extracted from the dataset and the security risk of each host is evaluated using the CDRAC model constructed based on the fuzzy inference technique to obtain the security risk value of that host for that day. The security risk value of all hosts in one day is summed up to get the network security risk value of that day. Since Honeynet's dataset does not contain the vulnerability information of the hosts, here we need to assume that each attack recorded in the dataset is a valid attack, i.e., the vulnerability of the host corresponding to the attack exists and the host does not have other vulnerabilities also need to assume that the weight of the 9 hosts is the same. Through the assessment, we can get the macro risk assessment value of network security of 9 hosts and the whole network in 30 days, and the daily security risk value of each host and network is shown in Table 2.

Table 2. The daily security status of the Internet of things

Date	101	102	103	104	105	106	107	108	109	Internet
1	0	0	0	1	0	0	1	0	1	3
2	1	0	0	0	1	0	55.23	0	0	57.23
3	0	0	1	1	0	1	18.05	0	1	22.05
4	3.025	3.025	3.025	3.025	3.025	3.025	3.025	3.025	3.025	27.225
5	1.126	0	1	0	1.144	0	1	0	0.144	4.414
6	6.024	5.892	5.892	5.892	5.892	3.025	1721	5.892	5.892	1765.401
7	3.845	0	0	1.144	0	1	33.56	0	0	39.549
8	0	0	1	0	0	0	1	0	0	2
9	1	0	0	0	0	1	0	0	0	2
10	0	0	0	0	0	1	1	0	0	2
11	0	0	1	0	0	0	67.45	0	1	69.45
12	0	0	0	0	0	0	1	1	0	2
13	0	0	0	1	0	0	3.025	1	0	5.025
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	1	0	0	1
16	0	0	0	1	0	0	0	0	0	1
17	0	0	0	0	0	0	0	0	0	0
18	3.025	0	0	0	0	0	1	0	0	4.025
19	3.025	0	1	0	0	1	3.025	0	0	8.05
20	3.654	0	0	0	0	0	12.23	0	0	15.884
21	3.025	0	0	0	0	0	82.15	0	0	85.175
22	0	0	0	0	0	0	21.26	0	0	21.26
23	3.271	3.025	3.025	3.025	3.025	3.025	9.084	3.025	0	30.505
24	0	0	0	0	0	0	0	0	0	0
25	1.522	0.687	0.687	0.687	0.687	0.295	1.522	0.687	0	6.774
26	0.295	0	0	0	0	0	0	0	0	0.295
27	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0
29	3.025	3.025	3.025	3.025	3.025	3.025	3.025	3.025	3.025	27.225
30	0	0	0.295	6.123	0	0	0	0	0	6.418

1) Analysis of host security risk assessment results. Two hosts that have suffered more attacks are selected for comparison, i.e., hosts with IPs 101 and 107, respectively, and their security risk curves during the month are generated as shown in Figure 3. As can be seen from the figure, it is obvious that the attack suffered by host 107 is stronger than host 101. Checking the number of attacks on the two hosts in a month against the Honeynet logs, the total number of attacks on host 101 is 26 and the total number of attacks on host 107 is 335.

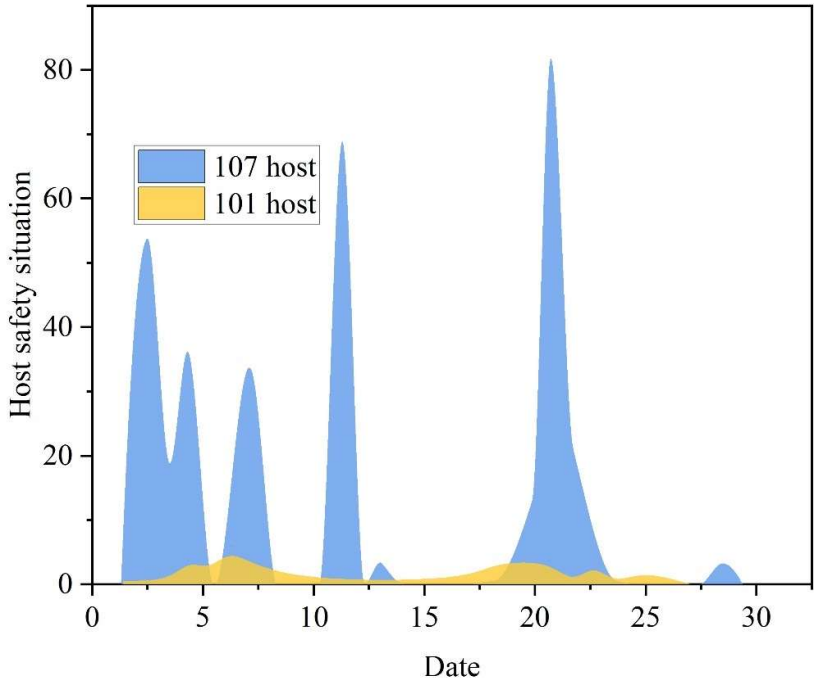

Fig. 3. The security posture diagram of the host 101 and 107

The peak of the risk value for host with IP 107 occurs on the 20th, and we see from the Honeynet logs that host 107 was attacked from the 20th to the 23rd as shown in Table 3, and it is clear that the order of intensity of the attacks on host 107 is 21st>22nd>23rd>20th, which also matches with the trend of the risk shown in the graph.

Table 3. The number of attacks of 107 and four days

Date	Weak attack	Moderate attack	Strength attack
20	0	5	0
21	1	20	1
22	0	8	0
23	1	4	1

2) Analysis of network security risk assessment results. The analysis of the network security risk assessment results is shown in Figure 4, assuming that the IP from 101 to 109 of this host has the same weight, so the security risk value of the 9 hosts is added up to obtain the security risk value of the entire network as the blue area in the figure. The yellow area in the figure is the sum of the number of attacks on all hosts in a day, with roughly the same ups and downs when compared to the security risk line. The combined Honeynet dataset analyzes this, and although there were only 2 attacks on the 7th day, the intensity of the attacks was high, so the security risk value would be much higher than the number of attacks. on the 25th day, there were almost 20 attacks in total, but the intensity of the attacks was low, and the threat was limited, which is why the security risk curve for that day is lower than the curve for the number of attacks. In general, 4 attacks with high intensity will cause more harm than nearly 20 attacks with low intensity, which shows that the model used in this experiment is good for security. Comprehensive analysis results in this section can be seen that the CDRAC model constructed by the fuzzy inference algorithm can be a good fusion of indicators, and the assessment results can correctly reflect the security status of hosts and networks from a macroscopic point of view, presenting the changing trend of network security.

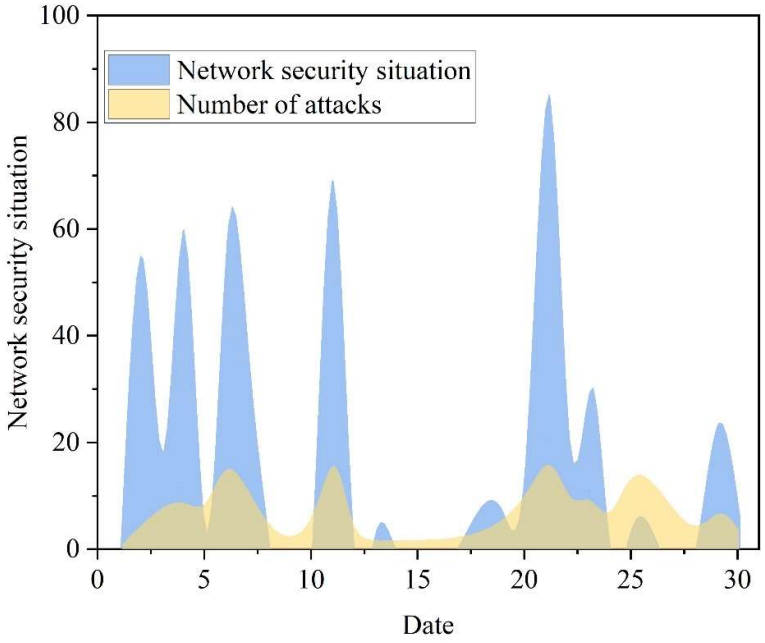

Fig. 4. Network security situation

3.2. Dynamic Risk Protection Model Effectiveness Study

The experimental dataset consists of different access requests, each of which contains four main attributes: subject, object, access activity, and access occurrence time, each of which consists of different sub-attributes, which consist of corresponding members. Training set: (1) (I, M, V)1 and DRM module evaluation results P1 for the first 1500 access requests of rs1; (2) (I, M, V)2 and DRM module evaluation results P2 for the first 150,000 access requests of rs2. The test sets are all (I, M, V) and DRM module evaluation results Ptest for the last 50 access requests, which consists of normal access requests (P =0) and malicious access request (P=1) intervals.

Experimental base environment: Dell PowerEdge R210 II with 4G RAM, 500G disk, Inter Xeon CPUE3-1220 V2@3.10GHz. Configure the master node master in the mainframe, virtualize 3 VMs using KVM (kernel based virtualmachine), and configure slave nodes respectively salves1, salves2 and salves3, each virtual machine is configured with 1G memory space and 50G disk space. The host uses ubuntu-16.04 operating system, and each virtual machine uses centos7 (kernel-3.10.0-327.e17.x86_64) operating system. Experimental running environment: Hadoop platform was deployed on Dell servers, platform version Hadoop-2.7.3; database and MATLAB were deployed on Windows7 64-bit operating system, database version MySql-5.7.17, MATLAB version R2016a.

Comparison of dynamic access control elapsed time for 80 to 20,480 access requests is shown in Fig. 5, comparing the response time of APODAC, DRAC and ABAC models as the number of access requests increases, but the response time of APODAC for access requests is less than that of DRAC and ABAC models. Since DRAC and ABAC models take more time to match the rules while this paper's model scales down the number of rules, the APODAC model proposed in this paper is more advantageous in terms of response time as compared to the other 2 models when the number of access requests is high.

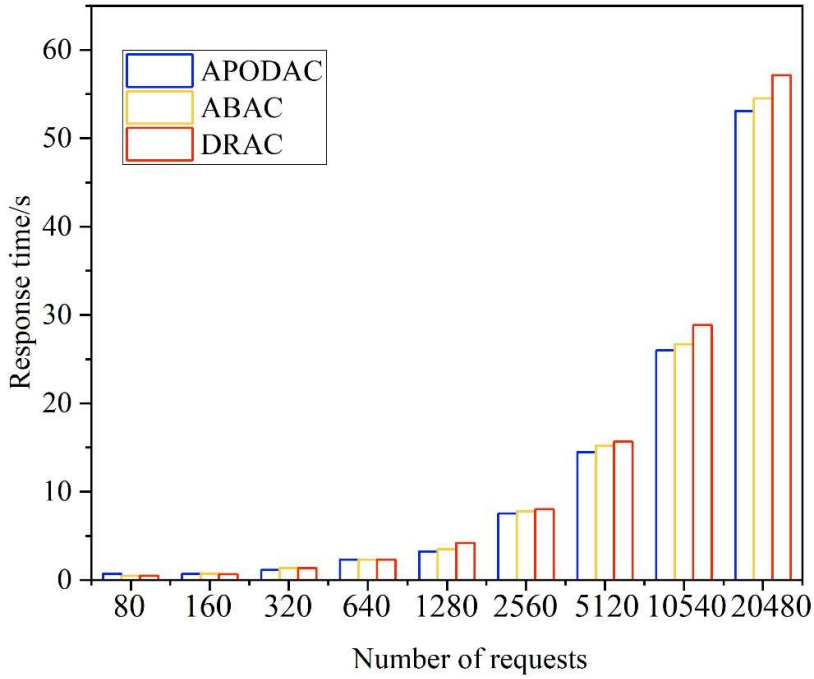

Fig. 5. The 80~ 20480 line access request evaluates the time

150~650 access requests evaluation time consuming comparison is shown in Figure 6, the highest difference between the response time of APODAC model and DRAC model for access requests reaches 100ms, and the highest difference between the response time of APODAC model and ABAC model for access requests is 150ms, so for the access requests with small amount of data the difference between the response time of APODAC model and the other 2 models is not much, but still better than the other 2 models.

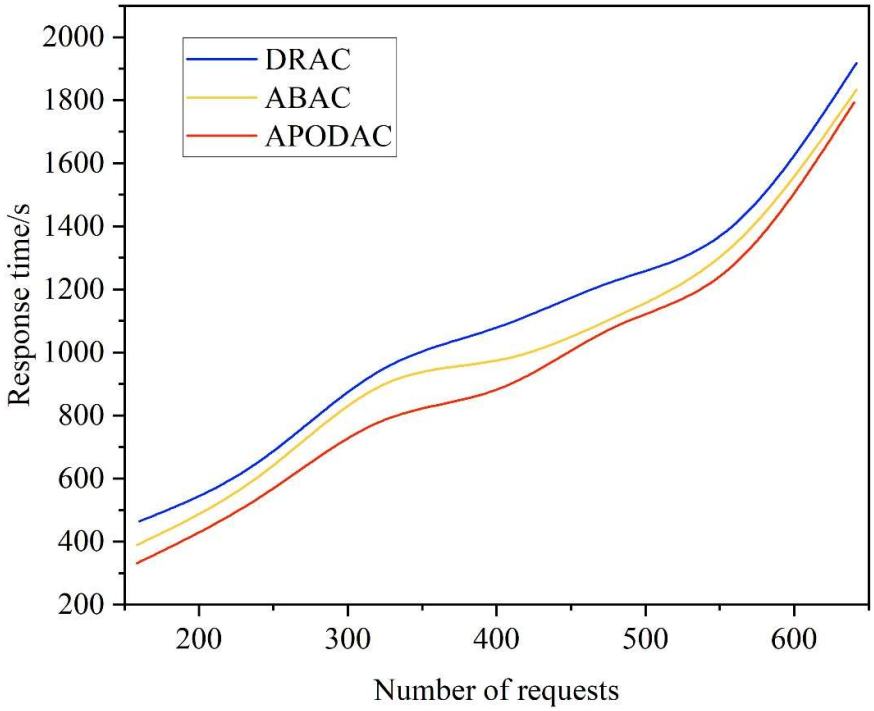

Fig. 6. 150~ 650 requests to evaluate time

4. Conclusion

In this paper, a dynamic access control model for IoT network security problems is proposed based on fuzzy inference algorithm and multimedia fusion technology, which adds a strong barrier for information security. The main work of this paper is as follows.

1) Using Honeynet as a dataset, we simulate a real IoT network environment to detect the correct detection rate and false alarm rate of this paper's model for IoT network attacks. It can be found that compared with the SVM method, the detection rate of APODAC model is improved and the false alarm rate is reduced. It can also correctly reflect the security status of hosts and networks.

2) By comparing the time consumed for 80-20480 and 150-650 access requests, the APODAC model dynamic access control response time has a large advantage. Therefore, the APODAC model realizes the dynamic control of privileges in the access process and provides new ideas for network security protection.

References

[1] Taherdoost, H. (2023). Security and internet of things: benefits, challenges, and future perspectives. Electronics, 12(8), 1901.

[2] Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. Information security journal: A global perspective, 27(3), 162-182.

[3] Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. SN Computer Science, 1, 1-19.

[4] Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2019). Internet of Things applications: A systematic review. Computer Networks, 148, 241-261.

[5] Miloslavskaya, N., & Tolstoy, A. (2019). Internet of Things: information security challenges and solutions. Cluster Computing, 22, 103-119.

[6] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88.

[7] Hou, J., Qu, L., & Shi, W. (2019). A survey on internet of things security from data perspectives. Computer Networks, 148, 295-306.

[8] Zhang, J. (2021). Distributed network security framework of energy internet based on internet of things. Sustainable Energy Technologies and Assessments, 44, 101051.

[9] Kanade, A., Ranganthan, C. S., Babu, A. J., Ramachandran, G., Kusuma, A. K., Anand, M., & Reddy, L. D. V. (2024). Analysis of wireless network security in internet of things and its applications. Indian Journal of Engineering, 21(55), 1-12.

[10] Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnostopoulos, M., Spathoulas, G., Giannoutakis, K. M., ... & Nijdam, N. A. (2019, September). From internet of threats to internet of things: A cyber security architecture for smart homes. In 2019 ieee 24th international workshop on computer aided modeling and design of communication links and networks (camad) (pp. 1-6). IEEE.

[11] Bagay, D. (2020). Information security of Internet things. Procedia Computer Science, 169, 179-182.

[12] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. IEEE access, 7, 124379-124389.

[13] Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of things, 5, 41-70.

[14] Chen, H., Hu, M., Yan, H., & Yu, P. (2019, September). Research on industrial internet of things security architecture and protection strategy. In 2019 International conference on virtual reality and intelligent systems (ICVRIS) (pp. 365-368). IEEE.

[15] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54, 101728.

[16] Liu, Y., & Zhang, S. (2020). Information security and storage of Internet of Things based on block chains. Future Generation Computer Systems, 106, 296-303.

[17] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[18] Yu Zhang,Ping Tu,Zhiyuan Zhao & Xuan Yan Chen. (2025) .Incorporating prior knowledge of collision risk into deep learning networks for ship trajectory prediction in the maritime Internet of Things industry. Engineering Applications of Artificial Intelligence,146,110311-110311.

[19] Su Yongjuan. (2024) .The Integration of Digital Media Technology and Film and Animation Production under the Multimedia Environment. Journal of New Media and Economics,1(3).

[20] Eyecioglu Onder,Kayisli Korhan & Beken Murat. (2024) .Strain Energy Prediction of Single Wall Carbon Nanotubes Using General Regression Neural Network and Adaptive Neuro – Fuzzy Inference System. Electric Power Components and Systems,52(8),1437-1447.

[21] Aparna Singh & Geetanjali Rathee. (2024) .Smart contract empowered dynamic consent: decentralized storage and access control for healthcare applications. Peer-to-Peer Networking and Applications,18(1),1-16.

[22] Yang Guodong,Li Kuangyu,Zhang Yunfan & Feng Qindi. (2024). End-to-End Modeling and Long Short-Term Memory Application in Time Series Modeling: Modeling and Prediction of Electronic Commerce User Behavior. Journal of Organizational and End User Computing (JOEUC),36(1),1-27.