A Security Situation Awareness Approach for IoT Software Chain Based on Markov Game Model

Xudong Zhu[1], Honggao Deng[2] *

[1] Wuxi Vocational Institute of Arts & Technology (China)
[2] Guilin University of Electronic Technology (China)

Received 13 December 2021 | Accepted 13 June 2022 | Published 1 August 2022

Abstract

Since Internet of Things (IoT) has been widely used in our daily life nowadays, it is regarded as a promising and popular application of the Internet, and has attracted more and more attention. However, IoT is also suffered by some security problems which seriously affect the implementation of IoT system. Similar to traditional software, IoT software is always threated by many vulnerabilities, thus how to evaluate the security situation of IoT software chain becomes a basic requirement. In this paper, A framework of security situation awareness for IoT software chain is proposed, which mainly includes two processes: IoT security situation classification based on support vector machine and security situation awareness based on Markov game model. The proposed method firstly constructs a classification model using support vector machine (IoT) to automatically evaluates the security situation of IoT software chain. Based on the situation classification, we further proposed to adopt Markov model to simulate and predict the next behaviors of participants that involved in IoT system. Additionally, we have designed and developed a security situation awareness system for IoT software chain, the developed system supports the detection of typical IoT vulnerabilities and inherits more than 20 vulnerability detection methods, which shows great potential in IoT system protection.

Keywords

Internet of Things, Markov Game Model, Security Situation Awareness, SVM, Vulnerability Detection.

DOI: 10.9781/ijimai.2022.08.002

I. Introduction

With the wide application of the Internet and the continuous development of information technology, Internet and software are heavily involved in our daily lives [1], [2]. However, simple informatization and technologies can no longer satisfy people's requirements [3], [4], [5], so that the Internet of Things (IoT) has emerged at this historic moment [6], [7].

As the extension of the Internet, IoT cannot be separated from the support of the software chain [8], [9], and with the continuous development of the software chain, its security problems have become increasingly severe [10]. In a complex environment, the software chain (refers to an IoT software system that is composed of a series of firmware, device drivers, system software and application software) has become the focus of IoT security [1], [6]. Especially in battlefield environment, the security of the IoT software chain can often affect the evolution of a war, and even determine its outcome [11], [12].

The security situation awareness [13], [14], [15] is built on an effective vulnerability classification method and some mature dynamic security enhancement technologies. Security situation awareness is regarded as a process of cognition of the system security status [13]. There are some commonly used technologies to support this process, including the fusion processing of original data measured from the system [16], the extraction of the background status and activity semantics [17], the identification of various network activities and abnormalities [18]. According to the above methods, the system's security status could be greatly learned. However, for IoT software chain, these works could not be simply implemented due to the complexity of the IoT environment [7], [19], [20]. An IoT system always accessed by many devices of different types. they may use different communication protocols, different information formats and have different behaviors. Apparently, it is very hard to summarize and analyze a large amount of collected information, so that the security situation awareness for IoT system is a challenging and worthwhile topic [21], [22], [23].

In this paper, we propose to implement Markov game model [24], [25], [26] with support vector machine (SVM) [27], [28], [29] to realize the security situation awareness of the IoT software chain, aim at analyzing and understanding the security-related elements of IoT software system, thus to perceive current security status and predict future security situation. The Markov game model is established by game theory, and has been long implemented in network security. Markov game model simulates the possible behaviors and analyze the rewards of the behaviors to address the attack defense problem, thus obtaining optimal strategy. Different as the Markov game model implementation in network security, IoT software chain contains many real device nodes. To be specific, it is to detect, extract, understand, evaluate, and predict the security elements that affect the IoT software chain. Note that the "situation" reflects the possible development tendency and complex software environments which formed by the interaction of various system conditions, rather than a certain system

* Corresponding author.
E-mail addresses: zhuxudong08@126.com (X. Zhu), 32465448@qq.com (H. Deng).

condition or phenomenon. Commonly, the situation consists of two parts, one is the "state", which refers to the overall current status quo, obtained by evaluating the information and incidents, thus determining the authenticity, type, characteristic and hazard of an attack. Another part is "tendency", which to the overall development trend. We conduct an in-depth analysis of the attack incidents within a unit of time to find out the various stages and steps of an attack. With the Markov game model, many behaviors in the IoT network could be greatly quantified, thus to select the best solution according to established rules, so that the evolution trend of both the offensive and defensive could be predicted, thereby improving the security of the IoT software chain.

The main contribution of our research is twofold:

(1) We have proposed an IoT security situation awareness method within two parts. We first utilize SVM to classify multiple security situations. And then, based on the security classification method, we have further proposed to use Markov game model to simulate three participants and predict their next behaviors in IoT system.

(2) The proposed two methods above are integrated to develop a useable system to perceive the security situation of the IoT software chain and provide guidance.

The remainder of this paper is organized following: The research background and the related work of security situation awareness is presented in Section II. Section III serves to introduce the framework of the proposed method, and detail the specific process of 1) IoT security situation classification based on support vector machine and 2) security situation awareness based on Markov game model. Additionally, Section III also describes the module designs and deployment. The experiments and results are discussed in Section VI. Finally, we have the conclusion in Section V.

II. Background and Related Work

The security issues of the IoT have received extensive attention from the research community and have been resolved at different levels. Yang et al. [30] investigated the security and privacy issues of the IoT and they emphasized the limitations of applying security in IoT devices. Also, they summarized the classification of IoT attacks (such as physical attacks, remote attacks, local attacks, etc.). Moreover, they analyze different levels of IoT security issues and propose corresponding solutions. Kumar et al. [31] discussed the security issues at each layer of the IoT three-tier architecture, and investigated most of the security flaws, which are caused by various communication technologies used in wireless sensor networks. In order to ensure that only legitimate users are controlled and authorized, Kalam et al. [32] proposed an authorized access model as a security framework for IoT. However, current research on IoT security does not pay enough attention to software chain. Since IoT is more vulnerable to attacks, especially in a confrontational environment. Therefore, the security threats detection, threats addressing, and security strengthen for IoT software chain matter significantly nowadays.

The concept of cyberspace situation awareness was first proposed by Bass et al. [33], and they had pointed out that "fusion-based network situation awareness" will surely become the discovery of the development of network management. After that, Endsley et al. [34] gave a definition of the network security situation, believing that it includes acquiring, understanding and displaying of security elements which significantly influence on network situation, and future trends prediction, in a large-scale network environment. Franke et al. [35] regarded cyber security situation awareness as a subset of situation awareness, which mainly focuses on network security according to IDS alerts and vulnerability information. Network security situation awareness commonly applies some situation awareness methods to network security [36], enabling personnel to have a macro grasp of the security status of the entire network in a dynamically changing environment, and to provide decision-making support for senior managers.

Current researches [14], [37], [38] on cyber security situation awareness mainly focus on three levels, including situation perception, situation comprehension, and situation projection. Situation awareness identifies all activities in a system (including attack activities) and their features and characteristics. The related methods can be roughly classified into two categories according to whether prior knowledge is used. For situation understanding [39], it identifies attack activities and their characteristics. Additionally, by analyzing the semantics relationships of attack activities, situation understanding could infer the attacker's intentions. Currently, situation understanding mainly starts from two aspects [39], that is, attack behavior prediction and attack purpose understanding. The purpose of situation projection is to assess the hazard and the potential threats that have appeared to the managed network based on the identified attack activities. Current researches [40], [41] commonly concentrate upon knowledge-based reasoning situation projection, situation projection based on statistical analysis and gray-scale theoretical situation projection.

There are still many challenges to the network security situation awareness [42], such as the fusion of massive heterogeneous measurement data, activity identification under incomplete information conditions, semantic calculation of network activities, visualization of network situation, and network security collaboration of situation awareness etc.

III. Approach

In a complex environment, changes in the IoT software chain at any time may affect the entire security situation. In this paper, we propose an IoT security situation awareness technology based on the Markov game model with support vector machine (SVM). By assessing the current state of the IoT software chain and evaluating participants' behaviors, the proposed approach can provide useful guidance for users.

A. Framework

The framework of our method is shown in Fig. 1, includes two main procedures: IoT security situation classification based on support vector machine and security situation awareness based on Markov game model.

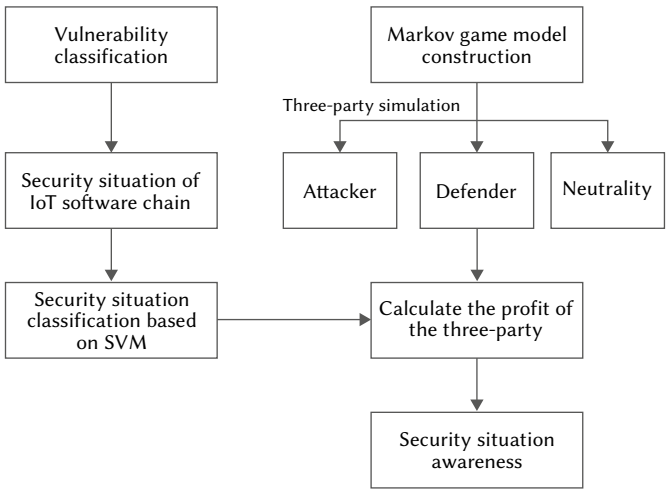

Fig. 1. Framework of the proposed method.

Commonly, there are often three objects in the game model, namely "attacker", "defender", and "user". The attacker's purpose is to attack the vulnerability of the system and cause the IoT system to malfunction or even destroy. While the defender implements reinforcement schemes to improve system security and reduce the damage caused by potential threats. For users, they are about the status of the IoT system.

We firstly construct a classifier to automatically classify the security situation based on SVM. After that, in the simulation game, we record the state of the IoT software chain at different times. At the same time, we calculate the probability of what actions the participants may take, based on the state changes caused by different behaviors. Finally, we calculate the benefits of the three parties in the game under different strategies. After completing the above steps, the Markov game model can be constructed to learn threats to the IoT systems, thus the defenders can draw up the best reinforcement scheme.

B. IoT Security Situation Classification Based on Support Vector Machine

1. Security Situation Classification

The IoT security situation classification is constructed based on vulnerabilities analysis of the IoT software chain. Specifically, we first conduct an in-depth analysis of the threats or vulnerabilities in IoT software chain, and classify them into some categories. After that, by referring to the national response plan for public emergencies, the security of the IoT software chain is classified into 5 levels according to the characteristics, hazards, and the status changes of the vulnerabilities in a IoT software chain. For convenience, the security situation of IoT software chain is quantitative described ranging from 0 to 1. The detailed classification is shown in Table I.

TABLE I. Classification of IoT Security Situation

Security score	Security level	Description
0.0~0.2	safe	The entire software chain is operating normally, no threat behavior that beyond perception, no severe vulnerabilities.
0.2~0.4	mild danger	The overall operation of the software chain is slightly affected by a few vulnerabilities, the malicious behaviors are a little active.
0.4~0.6	danger	The software chain is affected, with some security vulnerabilities in a higher threat level. And it has a high possibility that causes major damage.
0.6~0.8	severe danger	A large scale of serious attack has been found in the software chain, along with many security vulnerabilities, and the malicious behaviors are active.
0.8~1	extreme danger	The software chain has been severely damaged, malicious attacks are very active, which could cause a variety of service interruptions and endanger critical infrastructure.

2. SVM Implementation

To better realize the security situation awareness of IoT software chain, the SVM is additionally adopted in our method. In practice, we utilize SVM to classify the security level of security situations under different cases (different vulnerabilities and threats). The specific process is shown in Fig. 2.

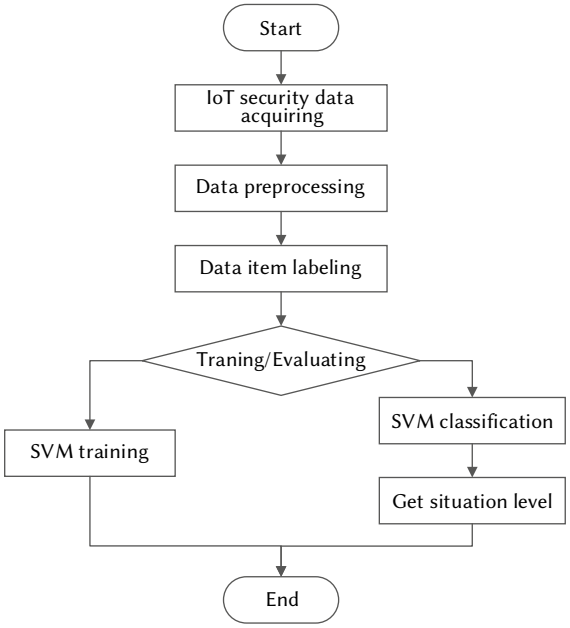

Fig. 2. The SVM implementation in IoT security situation classification.

The guided information for IoT security situation awareness is acquired from Snort's intrusion detection system, firewall and X-Scan vulnerabilities, which are detailed as follows.

Snort data item. Snort is a real-time traffic analysis tool based on libpcap, which can effectively record IP data packets. The acquired data are: activity, protocol, source, destination address, destination port, generation time of alarm and alarm level, etc.

Firewall data item. The firewall can record the network communication between internal and external networks, and effectively protecting the internal network. The acquired data are: source and destination addresses, destination ports, protocol type, duration, sent bytes, received bytes, and behavior, etc.

X-Scan data items. X-Scan mainly performs vulnerability scanning and security level assessment. The following data are acquired by scanning the specified IP, that is, the type and version of operating system, port status, port BANNER, CGI vulnerability, IIS vulnerability, and RPC vulnerability etc.

Due to the complexity of the IoT software chain, the acquired data may be complex or have diverse characteristics. Therefore, the following indexes are added below to better determine the security situation of IoT system.

Continuous alarm time. Suppose that at time t the alarm is alerted, and suspended until $t+n$ time, the continuous alarm time is defined as Equation(1):

$$\mathrm{IP\_}n = \sum_{i=1}^{n} D_i^S \cup D_i^f \cup D_i^x \tag{1}$$

where n is a continuous time interval, D_i^S is the alarm information captured by Snort at time i, D_i^f represents the operational alarm behavior captured by the firewall at time i, and D_i^x is the vulnerability

alarm information captured by X-Scan at time *i*. The addressing range of *n* is [0, +∞], if on alarm is captured, *n* is set as 0.

Vulnerability risk value. Suppose that in a fixed time period *s*, the sequence of vulnerabilities captured from the detection is $L = \{L_1, L_2, L_3, \dots, L_n\}$, and the risk that the vulnerability may be exploited in *s* is $T = \{T_1, T_2, T_3, \dots, T_n\}$, then the vulnerability risk value is defined as:

$$\mathrm{T_n} = \sum_{i=1}^{m} L_n | W_i \tag{2}$$

where m is the amount of network data captured, and W_i is the damage level of vulnerability form L_n in the captured network data.

For convenience, we normalize all the above training data to [0,1], using the following formula:

$$\mathrm{F}(i) = \begin{cases} \frac{D_i}{100}, D_i < 100 \\ 1, D_i \geq 100 \end{cases} \tag{3}$$

where D_i is the captured data.

Based on the preprocessed data, the SVM can be easily adopted to realize the IoT security situation classification with gaussian kernel function. But a simple two class model cannot meet our requirement because the security situation level is classified into 5 levels in our approach. Hence, we adopt a one-against-one strategy for the implementation. To be specific, we utilize multiple two-class SVM classifiers for every two levels respectively and get the corresponding score. Finally, the level of IoT security situation will be classified according to the sum score.

In summary, the classification of IoT security situation with SVM mainly includes three procedures: security data acquiring, data preprocessing and the training and classification of SVM. The algorithm description is given as Algorithm 1.

Algorithm 1. IoT security situation classification with SVM

Inputs. IoT security data

Output. The level of IoT security situation.

1. Acquire the security data from IoT software chain;
2. Preprocess the acquired data;
3. Obtain the needed data item and index value;
4. *Classify the IoT security situation using SVM;*
5. Output the security level of IoT system.

C. Security Situation Awareness Based on Markov Game Model

1. Construction of the Markov Game Model

The Markov game model is built on the game theory and Markov decision process (MDP). The former refers to the theory of how to make decisions under the interaction of multiple participants, while the latter is to make decision from the available behavior set based on the observed information (or state). Although the next state may be random, but the state transition is traceable according to Markov probability. Simply, the next state is only related to the current moment. In our approach, we have fully considered the impact of the behaviors of both attackers and defenders, and adopted the two-role Markov game analysis for security assessment, so that the potential threats can be dynamically analyzed.

Here, we list the basic components of Markov game model as following:

Participants. Participants are classified into three camps, that is, attacker, defender and user. The attacker conducts malicious attacks to make the IoT software chain disabled, while the defender implements security reinforcement solutions to reduce the vulnerability of the system, thereby improving the security of the IoT software chain. The user only uses the equipment, but does not care about the security issues.

Situation space. All possible situations in the IoT software chain constitute the situation space.

Behavior space. The behavior space is constituted by all the possible behaviors of the three participants.

Transition probability. With the evolution (caused by participants' behaviors) of IoT system, the situation is constantly changing. According to the transitions and the security evaluation of the IoT system, all participants may choose corresponding behaviors from the behavior space, with a probability.

Reward function. It refers the gains of all participants. Since the purpose of the attacker is to cause maximum damage to the system, its reward is expressed in terms of damage to the system; The purpose of the defender is to enhance the security of IoT system, the reward is expressed by the damage that the administrator can reduce after taking security actions; For users, their requirement is to get sufficient network resources, so the reward is expressed by the degree of utilization of system services.

2. The Markov Game Process

The game process means that all participants select a behavior from the behavior space according to the current state of the system, and then the system transfers to a new state. Subsequently, the participants need to make decisions based on the new state. This process is repeated until the preset condition is satisfied. In other words, at any time, for a certain threat, the three participants choose the corresponding behavior and get their rewards.

At a given moment and for a certain threat *t*, the three participants choose their own behavior strategy, and get their rewards, respectively. In our method, the reward that each part will obtain is described as a reward function. The purpose of each participant is to maximize the reward function, this process is quantitatively described as:

$$\mathrm{TPN}(t, k) = \{S_i(k), e_j(k)\} \tag{4}$$

where $S_i(k)$ is the state of the *i*-th propagation node at time *k*; $e_j(k)$ is the state of the *j*-th propagation path at time *k*. Simply, TPN(*t*, *k*+1) is the system state at time *k*+1, and the state change of the system follows the Markov rule. For attackers, they need to analyze which type of *t* belongs and consider that how to utilize this threat could get the most reward. Then, they could adopt some malicious behaviors. For the defensive side, the administrator's implementation of security measures on node *i* will bring about two impacts: 1) reducing the damage of threats *t* that affect the IoT software chain. 2) reducing the impact on system availability, that is, the impact of security plan on the availability of node *i*, which is described as:

$$V_s(S_i(k)) = \Delta\rho_{ai} \cdot value_{ai} \tag{5}$$

where $\Delta\rho_{ai}$ is the number of changes in node utilization performance, measured by the node utilization value before the security enhancement is implemented and the after value; and $value_{ai}$ represents the availability of node *i*. For users, their reward is measured by the sum of the use ratio of *N* nodes and the amount of *M* utilization path.

For example, suppose that there are 4 nodes in the IoT software chain, and the threat's propagation path is shown in Fig. 3. Initially, at time *k*, only node 1 detects the threat, and the system situation danger level reaches mild danger. Subsequently, at *k*+1 time, the threat spreads to node 3. So that the defender implements a reinforcement plan for node 3 according to the transmission route. If the reinforcement fails, node 3 is successfully infected and the system situation level reaches general danger. Otherwise, node 3 is not infected, and the system

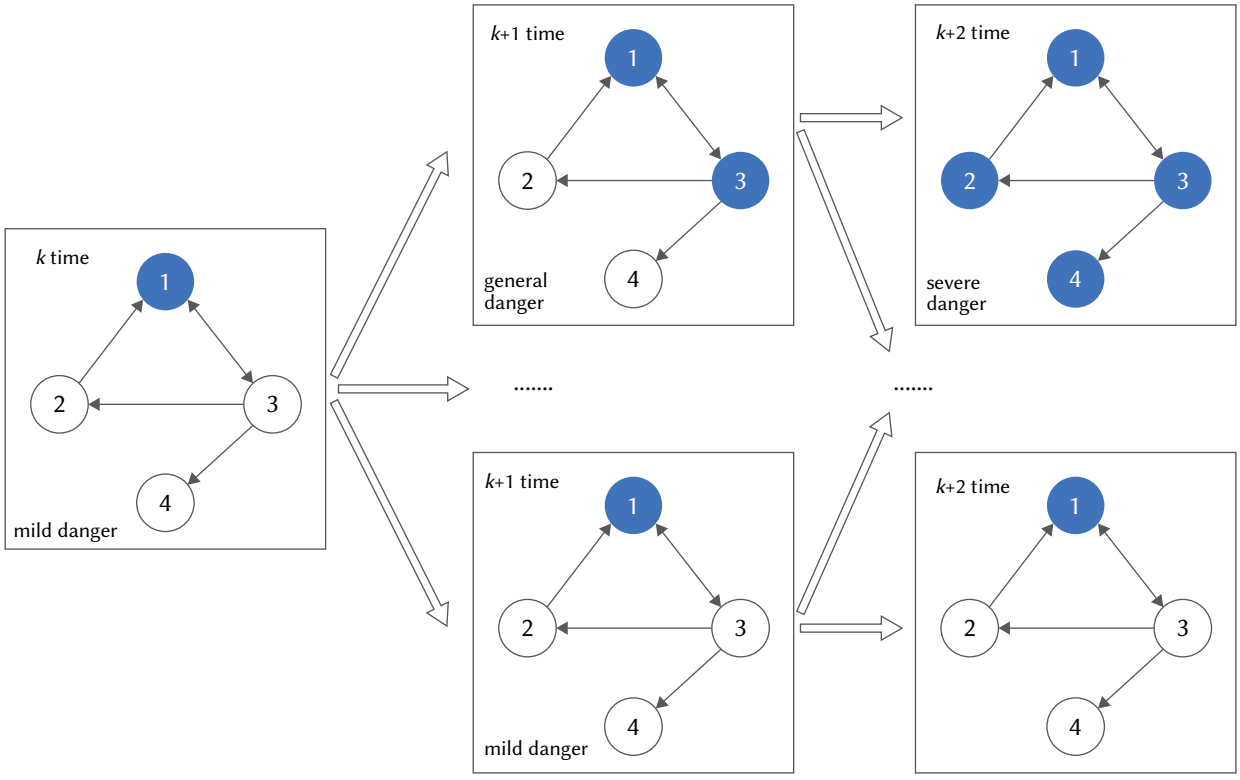

Fig. 3. The Markov game process.

situation level is still in mild danger. At k+2 time, under the case that node 3 is successfully infected, the threat continues to spread to nodes 2 and 4. At this time, if the defender chooses to reinforce node 1 but the reinforcement fails, the entire IoT software chain is completely infected, with a severely dangerous system situation. The defender needs to consider whether to turn off the system. If node 3 is safe, the defender only needs to implement reinforcement plan on node 1. If it succeeds, the entire system is in a safe condition.

Finally, the system constantly evolutes as the above process. For a finite-step (K-step) game process, from time k to time k+K, the states in different times forms a tree structure, and each path from the root node to the leaf node is a possible evolution, with the total rewards of all participants.

In summary, the IoT security situation awareness mainly includes three procedures: data processing, threat propagation network construction and IoT security evaluation based on Markov game model. The process is given as Algorithm 2.

Algorithm 2. IoT security situation awareness based on Markov game model.

Inputs. IoT security data

Output. The IoT security situation.

1. Preprocess the IoT security data;
2. Construct the threat propagation network for each threat t based on the security information;
3. According to the threat propagation network, construct a Markov game model for t, and the security situation of t is calculated;
4. Analyze the best reinforcement plan for the defender to deal with the threat of t;
5. Sum up the damage of all threats, and evaluate the overall security situation of the IoT software chain based on different requirements.

D. Module Designs and Deployment

1. Framework

In this paper, we design a practical system of the security situation awareness for IoT software chain as shown in Fig. 4. The system consists of a database, an interface for users and 5 main modules, including data acquisition module, situation analysis module, situation assessment module, security enhancement module and situation prediction module. We will detail these main modules below.

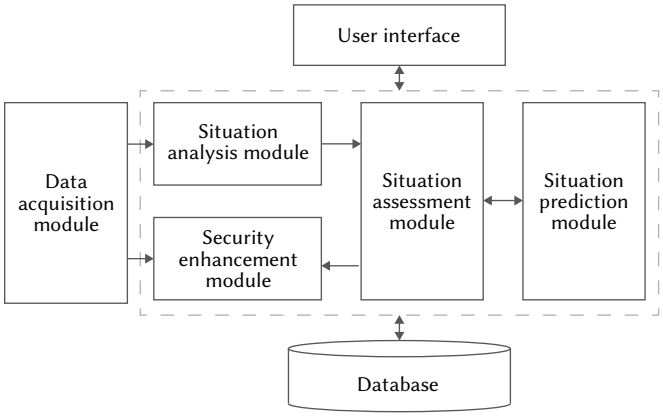

Fig. 4. Framework of the proposed system.

2. Data Acquisition Module

The data acquisition module obtains various data such as the status of the IoT system, the security threats faced and other security-related data through some automatic tools in the IoT software chain. These data will be stored in the database, and the invalid data will be cleaned up regularly.

3. Situation Analysis Module

The situation analysis module is actually a process of analyzing and standardizing the collected data. This is because the obtained data from the data acquisition module cannot be directly used as the input of subsequent modules. This module uses such as standardized analysis, redundancy detection, and conflict detection methods to analyze the original data, thus obtaining a standardized data set.

4. Situation Assessment Module

After getting standardized data, these data will be input to our proposed SVM-based security situation classification method to conduct security situation assessment by 1) analyzing the data from the situation analysis module 2) and the security situation awareness technology based on the Markov game model. Therefore, the security situation of the IoT system can be quantitatively described.

5. Situation Prediction Module

The situation prediction module adopts a situation prediction algorithm, based on the current security situation and the threats faced from the IoT system. Then it analyzes the law of changes in the situation, thus to predicts the tendency of the security situation of the IoT software chain.

6. Security Enhancement Module

The purpose of security enhancement module is to generate the reasonable security reinforcement plan for users. According to the predicted security situation tendency, and analyzing the weakest node of the IoT software chain, this module finally provides a reinforcement plan to advice the administrator to improve the security of the system.

IV. Implementation and Results

A. Running Environment

We have deployed our system with two proposed methods on a computer equipped with i7 CPU in 3.8GHz, RAM 32-GB, the used operation system is Window 11 Home.

B. Results and Analysis

Based on the above proposed methods, we have developed a security situation awareness system for IoT software chain. To evaluate the effectiveness of our approach, we deployed the system on a complex project and monitor the attacks on the IoT software chain of the target project. The detailed security information is shown in Table II.

In practice, our system supports the detection of typical IoT vulnerabilities and inherits more than 20 vulnerability detection methods, so that it can effectively detect various vulnerabilities and realize the security situation awareness.

C. Threat to Validity

At present, the proposed security situation awareness system for IoT software chain is still in preliminary exploration. Here, we discuss the threat to validity to our work.

Since the acquired security data are from different ways, we have normalized these data into a suitable format that can be used by SVM. But this process involves manual effort, which means, it may bring in some risks of human mistakes.

The second threat is that we need to choose a kernel function for SVM classification, different kernel function may produce different outcomes. We still need to learn how to reasonably choose a suitable kernel function.

Additionally, in our experiment, the used data set is too small, which directly affects the experimental outcomes and maybe not sufficient to provide convincing evaluation. We will look for some large-scale data set and conduct corresponding evaluations in the future.

TABLE II. Security Information Under Evaluation

Type of vulnerability	Attack description	CWE ID	Number of test cases
Time-related vulnerability	Race condition attack	366	38
	Competitive hazard attack	364	20
Environment-related vulnerability	Usage after memory is released	416	522
	Type obfuscation attack	400	904
	Uninitialized conditions	176	83
	Buffer overflow	457	981
	Other types	121	909
Security designing flaw	Other types	464	80
Hardware vulnerabilities	Other types	506	160
Memory-related vulnerability	Integer overflow	369	904
Logical-related vulnerabilities	Other types	404	626
Digital-related vulnerability	Uninitialized conditions	459	38
	Buffer overflow	122	920
Trigger vulnerability	Other types	510	72
	Type obfuscation attack	681	56
	Uninitialized conditions	665	316
	Buffer overflow	680	938

V. Conclusion and Future Work

The security of the IoT software chain no doubt affects the activities of the entire IoT system, especially in a complex environment. To provide more useful information for administrators and enhance the security of IoT system, in this paper, we have proposed a security situation awareness method for IoT software chain, and construct a Markov game model to simulate behaviors of attackers, defensives and users in the complex IoT application environment. Then the obtained security information is used to calculate the gains and losses of the three participants in the game, thus to evaluate the current security situation IoT system and predict the security situation in next stage. In order to improve the practical effect of the proposed security situation awareness, the SVM is adopted to pre-classify the security situation of the IoT system. Additionally, we have designed and implemented an IoT security situation awareness system that integrates 5 modules with different functions.

In fact, the current work still needs to be expanded. For example, we use SVM to classify the security situation, at this stage, introducing other more advanced models (such as neural network) can improve the classification accuracy and further improving the effectiveness of the proposed method.

References

[1] Perera C , Zaslavsky A , Christen P , et al. "Context Aware Computing for The Internet of Things: A Survey," *IEEE Communications Surveys & Tutorials*, 2014, 16(1):414-454.

[2] Heath T , Bizer C . "Linked Data: Evolving the Web into a Global Data Space," *Molecular Ecology*, 2011, 11(2):670–684.

[3] Malaiya R K, Kwon D, Kim J, et al. "An empirical evaluation of deep learning for network anomaly detection," *International Conference on Computing, Networking and Communications (ICNC). IEEE*, 2018: 893-898.

[4] Chen X Z , Zheng Q H , Guan X H , et al. "Quantitative Hierarchical Threat Evaluation Model for Network Security," *Journal of Software*, 2006, 17(4):885-897.

[5] Macqueen J . "Some Methods for Classification and Analysis of MultiVariate Observations," *Proc of Berkeley Symposium on Mathematical Statistics & Probability*. 1965.

[6] Li S , Xu L D , Zhao S . "Applications of Internet of Things: A Survey," *Information Systems Frontiers*, 2015, 17(2):243-259.

[7] D Miorandi, Sicari S , Pellegrini F D , et al. "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, 2012, 10(7):1497-1516.

[8] Wang X , Liu W . "Research on Air Traffic Control Automatic System Software Reliability Based on Markov Chain," *Physics Procedia*, 2012, 24:1601-1606.

[9] Wang L Z , Zhang S S , Tao Q K . "A software-reuse-oriented agile supply chain model based on software agent," *Journal of Computer Research and Development*, 2002, 39(2):153-158.

[10] Cui J , Wang L , X Zhao, et al. "Towards predictive analysis of android vulnerability using statistical codes and machine learning for IoT applications," *Computer Communications*, 2020, 155(Apr.):125-131.

[11] Zanella A , Bui N , Castellani A , et al. "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, 2014, 1(1):22-32.

[12] Granjal J , Monteiro E , Silva J S . "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials*, 2015, 17(3):1294-1312.

[13] Sanchez-Arias G , Garcia C G , G-Bustelo B . "Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things," *Future Generation Computer Systems*, 2017, 74(SEP.):444-466..

[14] Webb J , Ahmad A , Maynard S B , et al. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security*, 2014, 44(2):1-15.

[15] Zhang D , He Q . "Security Situation Awareness Method for Smart Grid," *International Core Journal of Engineering*, 2020, 6(5):49-55.

[16] Lei Z , Wu X . Wu, X.: "An edge-guided image interpolation algorithm via directional filtering and data fusion," *IEEE Transactions on Image Processing*, 2006, 15(8):2226-2238.

[17] Dey A , Mohammad F , Ahmed S , et al. "Anomaly Detection in Crowded Scene by Pedestrians Behaviour Extraction using Long Short Term Method: A Comprehensive Study," *International Journal of Education and Management Engineering*, 2019, 9(1):51-63.

[18] Wilks P , English M J . "A system for rapid identification of respiratory abnormalities using a neural network," *Medical Engineering & Physics*, 1995, 17(7):551-555.

[19] He W , Yan G , Xu L D . "Developing Vehicular Data Cloud Services in the IoT Environment," *IEEE Transactions on Industrial Informatics*, 2014, 10(2):1587-1595.

[20] Park N , Kim M , Bang H C . "Symmetric Key-Based Authentication and the Session Key Agreement Scheme in IoT Environment," *Lecture Notes in Electrical Engineering*, 2015, 330:379-384

[21] Weber R H . "Internet of Things – New security and privacy challenges," *Computer Law & Security Review the International Journal of Technology & Practice*, 2010, 26(1):23-30.

[22] D Guinard, Trifa V , Karnouskos S , et al. "Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services," *IEEE Transactions on Services Computing*, 2010, 3(3):223-235.

[23] Sicari S , Rizzardi A , Grieco L A , et al. "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, 2015, 76(jan.15):146-164.

[24] Jia R , Ding Y . "Nonzero-sum non-stationary discounted Markov game model," *Mathematical Methods of Operations Research*, 2000, 52(2):265-270.

[25] Lei C , Zhang H Q , Wan L M , et al. "Incomplete Information Markov Game Theoretic Approach to Strategy Generation for Moving Target Defense," *Computer Communications*, 2018, 116(JAN.):184-199.

[26] Hu H , Hu C , Yao S . Decision Model of Optimal Active Response for Network Security Using Partial Observable Markov Game[J]. *Hsi-An Chiao Tung Ta Hsueh/Journal of Xi'an Jiaotong University*, 2011, 45(4):18-24.

[27] Cauwenberghs G , Poggio T . "Incremental and Decremental Support Vector Machine Learning," *Advances in neural information processing systems*, 2001, 13(5):409-412.

[28] Amari S , Wu S . "Improving support vector machine classifiers by modifying kernel functions," *Neural Networks*, 1999, 12(6):783-789.

[29] Zien A , G Rätsch, Mika S , et al. "Engineering support vector machine kernels that recognize translation initiation sites," *Bioinformatics*, 2000, 16(9):799-807.

[30] Yang Y , Wu L , Yin G , et al. "A Survey on Security and Privacy Issues in Internet-of-Things," *Internet of Things Journal, IEEE*, 2017, 4(5):1250-1258.

[31] Sathishkumar J , Patel D R . "A Survey on Internet of Things: Security and Privacy Issues," *International Journal of Computer Applications*, 2014, 90(11):20-26.

[32] Bouij-Pasquier I , Kalam A , Ouahman A A , et al. "A Security Framework for Internet of Things," *Springer, Cham*, 2015.

[33] Bass T . "Intrusion Detection Systems & Multisensor Data Fusion: Creating Cyberspace Situation Awareness," *CiteSeer*, 2000.

[34] Endsley, Mica R . "Measurement of Situation Awareness in Dynamic Systems," *Human Factors*, 1995, 37(1):65-84.

[35] Franke N , Hippel E V . "The Case of Apache Security Software," *Social Science Electronic Publishing*.

[36] Kou G , Wang S , Tang G . "Research on Key Technologies of Network Security Situation Awareness for Attack Tracking Prediction," *Chinese Journal of Electronics*, 2019, 28(001):162-171.

[37] Zhylin A , Hudyncev M , Litvinov M . "Functional model of cybersecurity situation center," *Collection Information technology and security*, 2018, 6(2):51-67.

[38] Lakhno V , Akhmetov B , Korchenko A , et al. "Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity," *Journal of Theoretical and Applied Information Technology*, 2018, 96(14):4530-4540.

[39] Chen S , Jian Z , Huang Y , et al. "Autonomous driving: cognitive construction and situation understanding," *Science China Information Sciences*, 2019, 62(008):1-27.

[40] Kourti T . "Abnormal situation detection and projection methods—industrial applications. October 28–29, 2003. Hamilton, Ontario, Canada," *Chemometrics & Intelligent Laboratory Systems*, 2005, 76(2):215-220.

[41] Lewis L , Jakobson G , Buford J . "Enabling cyber situation awareness, impact assessment, and situation projection," *Military Communications Conference. IEEE*, 2008.

[42] Lin P , Chen Y . "Network Security Situation Assessment Based on Text SimHash in Big Data Environment," *International Journal of Network Security*, 2019, 21(4):699-708.

Xudong Zhu

Xudong Zhu is currently working as an Associate Professor for the Wuxi Vocational Institute of Arts & Technology, Wuxi, China. His research interests include software engineering and Internet of things.

Honggao Deng

Honggao Deng is currently working as a researcher for the Guilin University of Electronic Technology, Guilin, China. His research interests include software engineering and communication and Information System.