International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

A Novel Framework for Early Intelligent Vulnerability Detection Algorithm for IoT Technology Environments

T Virajitha[1], Janga Rajendar[1], Mangalampalli Sesha Sai Lakshmi Lavanya[1], Kommu Anusha[2]

[1]Assistant Professor, CSE(DS) Department, CMR Engineering College, Hyderabad, Telangana, India

[1]Assistant Professor, CSE (DS) Department, CMR Engineering College, Hyderabad, Telangana, India

[1]Assistant Professor, CSE (DS) Department, CMR Engineering College, Hyderabad, Telangana, India

[2]Assistant Professor, CSE(AIML) Department, Sri Indu College of Engineering and Technology, Hyderabad, Telangana, India

Article Info

Volume 9, Issue 6

Page Number : 311-318

Publication Issue

November-December-2022

Article History

Accepted : 15 Nov 2022

Published : 02 Dec 2022

ABSTRACT

This paper specifically studies the vulnerability intelligent early warning technology withinside the IoT environment, and studies the network protection assessment method based totally definitely on the attack graph affiliation assessment of the IoT environment, and analyzes the attack graph era set of policies. Firstly, it uses the attack graph technology to installation a network protection evaluation model based totally definitely on the vulnerability affiliation assessment withinside the IoT environment. The attack graph generation algorithm policies are improved. The key attack path of the attack graph withinside the IoT environment is searched constant with the node weight value. The key attack path of the network attack graph is used to diploma the complete network protection, and the protection of the IoT environment is given. The length calculation model is used to recognize the quantitative assessment of the protection recognition of the IoT environment thru manner of way of using the attack graph. Secondly, an intelligent early warning vulnerability detection algorithm based on the dynamic stain propagation model in the IoT environment is proposed, focusing on the introduction of stains and the inspection of stains. A static detection method for early warning vulnerabilities based on the counter-example of the IoT is proposed. Through the ow detection and context sensitive detection, a possible buffer early warning vulnerability is discovered. The driver crawler realizes automatic detection, and uses function hijacking to detect the execution of the stain data. In the experimental environment, compared with the existing tools, the experimental data shows that the algorithm improves the accuracy, recall rate and efficiency of the unfiltered vulnerability of intelligent early warning detection, and proves that the proposed algorithm can effectively detect the vulnerability.

Keywords : Intelligent early warning, vulnerability mining detection, security measurement calculation model, IoT.

I. INTRODUCTION

The large-scale growth of the Internet of things (IoT) in recent years has contributed to a significant increase in fog computing, smart cities, and Industry 4.0, all of which execute the complex data processing of confidential information that must be protected against cybersecurity attacks. Cybersecurity attacks have increased rapidly in various domains, such as smart homes, healthcare, energy, agriculture, automation, and industrial processes [1]. As a result of their wide range of services, IoT device sensors generate large amounts of data that requires authentication, security, and privacy. Previously, traditional methods and frameworks were used to ensure the security of IoT. Although today's computer network defense technologies such as security anti-virus software and network firewalls are relatively mature, with the frequent occurrence of hacker attacks on network, computer network systems are exposed with more and more security vulnerabilities. Many network anti-virus software and firewalls also Incompetent and powerless. Therefore, how to effectively discover network security vulnerabilities and reduce the negative impact of hackers and computer viruses on network security, namely vulnerability exploitation and vulnerability prevention, has become a hot topic in the world of information security [1]. In response to cyberattacks, an effective method is to use a vulnerability database that is more complete, and the vulnerability database is faster to update and monitor the information assets under its jurisdiction, eliminating hidden dangers and ensuring information security [5]. Incredible developments in the routine use of electronic services and applications have led to massive advances in telecommunications networks and the emergence of the concept of the Internet of Things (IoT). The IoT is an emerging communications paradigm in which devices serve as objects or “things” that have the ability to sense their environment, connect with each other, and exchange data over the Internet [1]. By 2022, one trillion IP addresses or objects will be connected to the Internet

through IoT networks [3]. The IoT paradigm has recently been used in creating smart environments, such as smart cities and smart homes, with various application domains and related services. The goal of developing such smart environments is to make human life more productive and comfortable by solving challenges related to the living environment, energy consumption, and industrial needs [4]. This goal is directly reflected in the substantial growth in the available IoT-based services and applications across different networks. For example, the Padova Smart City in Italy is a successful example of a smart city based on an IoT system [5].

As the extension and extension of the Internet [10], the IoT (IoT) mainly realizes the information collection, transmission and processing of objects through various existing transmission means, and truly realizes the connection of objects and the exchange of information between people and things. Are active vulnerability, that is, malicious data embedded in a page, immediately follows the request and is immediately returned from the server to the browser.

The object method and attribute of the dynamic update page cause the security vulnerability attack [6]. Another important feature of the security vulnerability is that the malicious code does not echo back in the return page source, but runs directly. When viewing the source code of the page, the original page script is seen. This attack script may not appear inWet. page of the HTML source code [2]. Therefore, security vulnerabilities [3 cannot be detected by the method of feature matching for the above two XSS vulnerabilities, which brings challenges to automated vulnerability detection. In view of the above problems, this paper firstly uses the attack graph technology to establish a network security assessment model based on vulnerability correlation analysis. The attack graph generation algorithm is improved.

II. RELATEE WORK

This paper studies the existing IoT security assessment methods. The traditional network security assessments are mostly the superposition of vulnerability risk quantification, and lack of correlation analysis of vulnerabilities in the whole network. This paper studies the existing IoT security assessment methods. The traditional network security assessments are mostly the superposition of vulnerability risk quantification, and lack of correlation analysis of vulnerabilities in the whole network. This paper studies the network security assessment method based on the attack graph association analysis of the IoT environment, and analyzes the attack graph generation algorithm.

III. VULNERABILITY MINING DETECTION KEY TECHNOLOGY

Intelligent early warning detection technology provides network security management personnel with specific information about system vulnerabilities, and helps to formulate corresponding security policies, which can effectively prevent loopholes from being exploited by malicious attackers and causing system damage. With the development of network technology and the emergence of new types of vulnerabilities, vulnerability detection technology has also exposed various shortcomings. The existing vulnerability detection tools mostly detect the vulnerability in batches, and do not find the relationship between the vulnerabilities. The simple vulnerability risk overlay does not reflect the security status of the entire network.

In addition, the vulnerability detection only detected the known vulnerability, and did not pay attention to the unknown vulnerability. Vulnerability risk awareness warning mainly relies on vulnerability scanning technology. Vulnerability scanning technology can be generally divided into host-based security vulnerability scanning, network-based vulnerability scanning, target-based vulnerability scanning and application-based vulnerability scanning, among which host-based security vulnerability scanning and network-based vulnerability scanning is the most common vulnerability scanning technology [6]. Host-based security vulnerability scanning technology refers to the use of an agent running in a computer host system for vulnerability scanning. The technology consists of a vulnerability scanning server and a vulnerability detection agent. Host-based vulnerability scanning technology has the advantages of communication process encryption, high scanning accuracy and easy management.

The network-based security vulnerability scanning technology is mainly applied to the enterprise environment. It uses different types and characteristics of security vulnerabilities. It uses network servers to generate network data packets and transmits them to multiple targets in the network in various forms of propagation. Whether are the specified vulnerability exists. The detection process of network-based vulnerability scanning is similar to the ``bottoming'' work before the actual attack by the hacker on the attacking site. The security administrator or network administrator actively implements the security vulnerability scanning to detect and analyze the security threats or security existing in the computer system [7].

(1) The statistics device vulnerability scanning engine actively probes the goal host or community connection tool, and collects associated statistics and operating status.

(2) The statistics device vulnerability scanning engine opens the community port detection module, collects and organizes the operating community connection

tool port or the goal host device to paintings in a sunny state, and obtains community statistics in actual time.

(3) The statistics device vulnerability scanning engine makes use of the vulnerability detection era to open the protection vulnerability detection statistics to the goal community tool or the host device and await and obtain remarks from the goal device.

(4) If the statistics device vulnerability scanning engine gets the remarks from the goal host and compares it with the statistics withinside the vulnerability database, if the matching is successful, it is able to affirm that the goal device has a protection hole.

(5) The statistics device vulnerability scanning engine sends the detection end result and the disposal notion to the vulnerability situation-conscious early caution device after the crowning glory of the detection, and the device matches the guided asset library to understand the vulnerability detection alarm and situational focus caution of the statistics device.

Security directors can use the vulnerability-conscious early caution device to find out open ports and services, device configuration statistics, recognized protection vulnerabilities, and associated protocols withinside the goal host device or community device to efficiently discover capacity protection risks withinside the goal host device. Security scanning era generally gives customers with the capacity to find out the existing protection breaches, however it can not save you hackers from exploiting unknown vulnerabilities. Therefore, protection scanning era desires to cooperate with vulnerability assessment device to offer organizations with systems. The capacity of vulnerability assessment, despite the fact that now no longer absolutely fixing the hassle of protection vulnerabilities, can sell the generation of latest protection patches to a sure extent.

IV. ATTACK GRAPH GENERATION ALGORITHM

From the perspective of security vulnerabilities, security issues caused by protocols can be classified into many types, including denial of service vulnerabilities, buffer warning vulnerabilities, cross-site scripting vulnerabilities, information disclosure vulnerabilities, code injection vulnerabilities, encryption problems, boundary condition vulnerabilities, and so on. How to effectively exploit these vulnerabilities and take corresponding remedial measures against these vulnerabilities is one of the important means to ensure the security of communication protocols and data security. The detection process of intelligent communication early warning security vulnerabilities based on the IoT.

1) Enter the assault node and initialize the assault queue.

2) Take a bunch because the assault initiation node, use the forward seek set of rules to look for adjoining assault nodes, and find the assault path. Each time a node that could successfully in alternate is found, the node is introduced to the cutting-edge assault collection.

3) If the assault collection reaches the goal node or the variety of assault hops exceeds the set most fee, the collection is searched backwards to eliminate redundant nodes and extraneous nodes, and the cutting-edge assault collection is reduced.

4) If the goal node isn't reached and the variety of assault hops is much less than the set most fee, loop 2 is performed till all nodes withinside the assault queue whole the seek. Calculate the PR stage fee of the cutting-edge web site, calculate the PR fee of every web page pointing to the cutting-edge web site, and decide the burden of the cutting-edge web page by the get right of entry to hyperlink weight and the get right of entry to hyperlink. The extra the hyperlink

get right of entry to or the get right of entry to web site the better the PR rating, the extra critical the cutting-edge net web page and the better the PR rating.

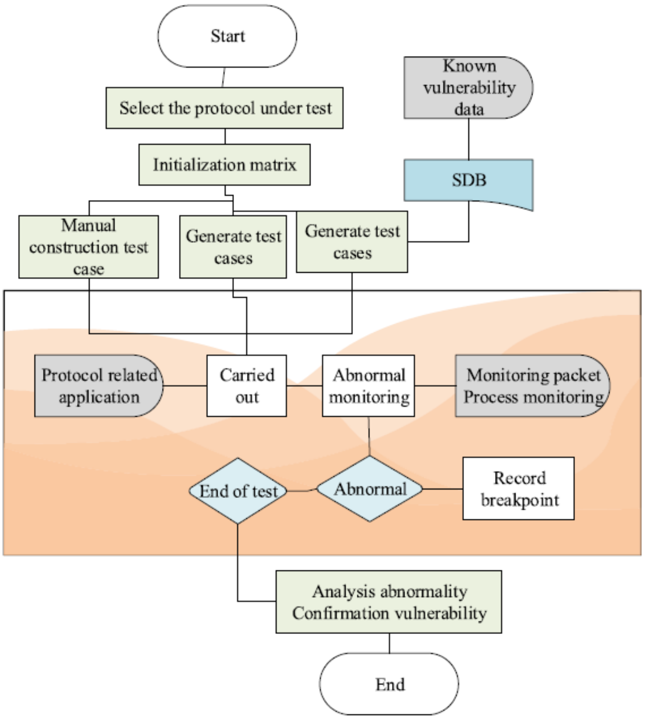

Start
Select the protocol under test
Known vulnerability data
Initialization matrix
SDB
Manual construction test case
Generate test cases
Generate test cases
Protocol related application
Carried out
Abnormal monitoring
Monitoring packet Process monitoring
End of test
Abnormal
Record breakpoint
Analysis abnormality Confirmation vulnerability
End

Fig 1. Architecture of the work

$$PR(W)\ \mathrm{D}\ (1-d) = N\mathrm{C} + d^{*}(PR(W1) = C(W1) + \ldots\ldots. \\ PR(Wn) = C(Wn))$$

The calculation model is applied to the attack graph state node weight calculation, and the calculation formula is as
Follows

$$R(S)\ \mathrm{D}\ (1-d) = N\mathrm{C} + d^{*}\ (R(S1) = C(S1) \\ +\ldots..\mathrm{C}R(Sn)) = C(Sn))$$

where: N is the number of all state nodes in the attack graph R(S) represents the weight of the attack graph state node S R(Si) indicates that the degree arc points to the S of the state node S, and the weight of the node C(Si) represents the state node S, the number of exit arcs. d is the damping coefficient,

$$0 < d < 1, \text{ generally } 0.85.$$

The risk assessment of critical attack paths calculates the average loss of the critical attack path. Let the probability that the state node *Si* penetrates into the next state node *Sj*C1 is *Pi;j*C1, then the probability of successful attack from the initial state node to the state node *Si.*

V. ALGORITHM FLOW

One of the conditions for an intelligent early warning vulnerability attack in the IoT environment is that the page is in an unsafe way to obtain data from the object (or any other object that the attacker can modify), and the object that the attacker can inject the taint data is the input point. Correspondingly, the DOM object method and attribute of the taint data entering the dynamic update page is another condition of the DOM XSS vulnerability attack.

The DOM object method and attribute of the dynamic update page are called output points, including directly modifying the DOM by writing the original HTML function. The function directly executes the script function. If the path from the input point to the output point exists and the taint data is not filtered, the taint data can be executed as an instruction, which proves that the intelligent early warning vulnerability exists. Based on the above analysis, this paper proposes an intelligent communication early warning vulnerability detection algorithm based on dynamic stain propagation model in the IoT.

Algorithm: ***Intelligent Early Warning Vulnerability Detection***

Algorithm Based on Dynamic Stain Propagation Model in IoT Environment

Input: Website

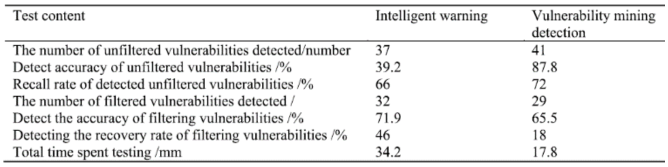
Output: A website page with a smart alert vulnerability and a successfully executed vulnerability test script.

a) Crawl the target site's page with input and output points.

b) Injecting taint data into pages containing input and output points.
c) Monitor the output point.
d) If the taint data is executed or an exception occurs, report the intelligent early warning vulnerability, output the website page with the intelligent early warning vulnerability and the
script successfully executed, and perform step f); otherwise, perform step e).
e) Judge whether all the taint data has been tested, if yes, perform step f; otherwise, select the next smear data generated by fuzzing, and perform step b).
f) Determine whether all the pages containing the input point and the output point of the target website are tested.
If yes, the algorithm ends; otherwise, find the next undetected page and perform step b).

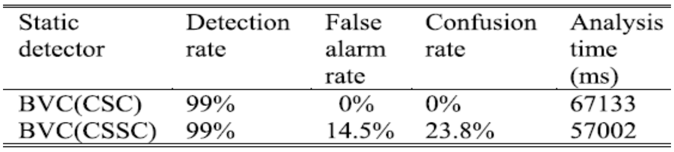
In order to enhance the detection efficiency of the set of rules, the level of acquiring the enter factor and the output factor through the hybrid pressure detection adopts the protocol-pushed mode. Since the clever early caution is a connectionless and stateless object-orientated protocol, most effective the static content of the website is obtained, which is easy and flexible. Features are consequently extra efficient. After injecting the stain statistics into the web page, the screen output factor always calls for the gadget to name the parsing engine to pay attention to the unique feature withinside the take a look at script, and the dynamic execution of the web page always ends in a lower in efficiency. Analysis indicates that this hybrid pressure detection approach is extra efficient than the usage of a unmarried event-pushed detection.

The early caution vulnerability detection approach primarily based totally on the counter-instance of the IoT firstly detects the possible early caution vulnerabilities and their name stacks thru the ow touchy context touchy detection, after which plays the direction touchy context touchy detection below the steering of the speedy detection effects, disposing of the short Detect fake alarms and factor the person to a counterexample that can motive a buffer caution. Since the correct detection is completed below the steering of the speedy detection end result, the set of rules can concurrently gain excessive detection accuracy and detection efficiency.



Test content	Intelligent warning	Vulnerability mining detection
The number of unfiltered vulnerabilities detected/number	37	41
Detect accuracy of unfiltered vulnerabilities /%	39.2	87.8
Recall rate of detected unfiltered vulnerabilities /%	66	72
The number of filtered vulnerabilities detected /	32	29
Detect the accuracy of filtering vulnerabilities /%	71.9	65.5
Detecting the recovery rate of filtering vulnerabilities /%	46	18
Total time spent testing /mm	34.2	17.8

Table 1. Work results comparison.



Static detector	Detection rate	False alarm rate	Confusion rate	Analysis time (ms)
BVC(CSC)	99%	0%	0%	67133
BVC(CSSC)	99%	14.5%	23.8%	57002

Table 2. Static warning results of early warning vulnerabilities using different constraint state security check methods.

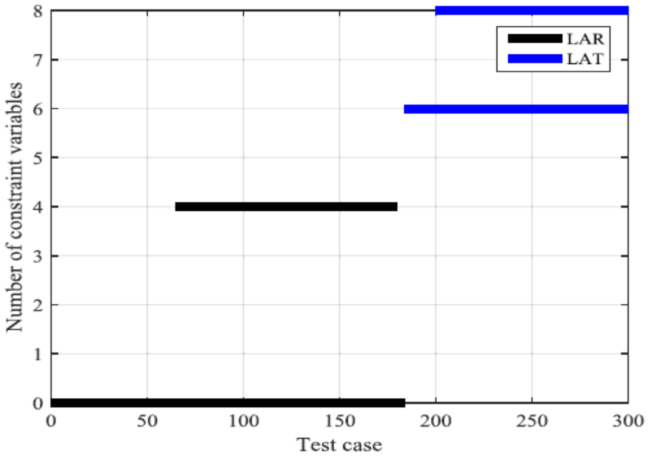


Figure 3. Lar Results are more Precise than the Lat Results.

In order to triumph over the limitations of the static detection approach for early caution vulnerabilities the usage of statistics move evaluation or constraint evaluation, the vulnerability detection set of rules primarily based totally at the counterexample combines the effects of statistics move evaluation with the effects of constraint evaluation to mutually whole the early caution vulnerability detection. If the enter parameters of the modern-day technique are referenced withinside the constraint state, the end result of the test may be ``undefined''. To this end, it's miles important to continuously set up the constraint courting among the actual parameters of the calling factor and the known as feature parameter thru the bottom-to-technique inter-technique question technique, thereby progressively disposing of the constraint information because of the shortage of technique parameters, ensuing withinside the detection end result. Determine the situation.

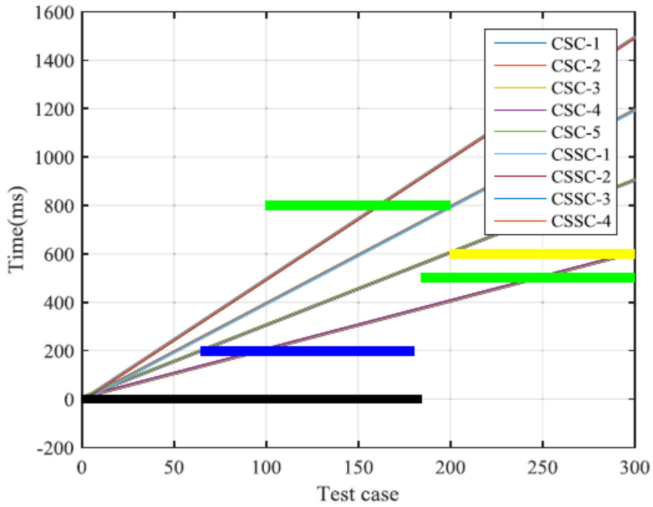


Figure 3. Smart alert Vulnerability Map using CSC.

Accurate, that is, LAR improves the evaluation accuracy of the constraint variable by greater than 50%. In order to check the detection impact of various constraint technology methods, we put into effect constraint country safety checkers, one is the constraint country safety checker whose variety constraint and manage constraint are mutually improved, and the alternative is a easy constraint country safety checker, constraints The country safety checkers are denoted as CSC and CSSC, respectively. In the following experiments, the relaxation of the BVC remained unchanged, except that they had been examined the use of extraordinary constraint country safety checkers. In particular, the static detection technique primarily based totally at the counter-example buffer caution vulnerability can attain excessive detection accuracy without person comments. The detection efficiency has reached the goal.

VI. CONCLUSION

This paper studies the existing IoT security assessment methods. The conventional community safety tests are mostly the superposition of vulnerability chance quantification, and loss of correlation evaluation of vulnerabilities withinside the whole community. This paper research the community safety evaluation technique primarily based totally at the assault graph affiliation evaluation of the IoT environment, and analyzes the assault graph technology set of rules. The weight calculation version is delivered and the technique of the use of the node weight to find the important thing assault course is proposed. Finally, the technique is proposed. The critical assault course is used to degree the safety reputation of the IoT, and a quantitative assessment plan is given for the safety reputation of the IoT. This paper analyzes the formation precept of sensible verbal exchange early caution vulnerability mining detection of the IoT, and proposes a dynamic pollutants propagation version primarily based totally at the dynamic pollutant's propagation version for the sensible verbal exchange early caution vulnerability exploitation of the IoT. Static detection technique for early caution vulnerabilities primarily based totally at the counterexample of IoT. As a hierarchical evaluation technique, this technique detects feasible buffer early caution vulnerabilities thru stream-sensing and context-touchy fast detection, after which plays course-touchy and context-touchy accurate detection of the steerage of fast detection results, doing away with fast detection. The delivered fake positives set up a specific course which can cause buffer warnings. The sensible verbal exchange early caution vulnerability mining detection set of rules finds the enter factor and output factor web page level to apply the protocol to power the crawler. The script injection level makes use of the event-pushed crawler to evaluate the test with the present detection gear withinside the experimental environment, and the experimentally proves the proposed set of rules. It can correctly locate the sensible verbal exchange early caution vulnerability mining detection of the IoT. In the subsequent step, the proposed scheme is carried out to the experimental community environment. The topology layout and experimental records evaluation of the experimental community are given, and the safety metric calculation is completed at the experimental community.

VII. REFERENCES

[1]. X. Jiang and M. Diao, "A new type double-threshold signal detection algorithm for satellite communication systems based on stochastic resonance technology," Wireless Netw., vol. 10, pp. 134-145, May 2019.

[2]. S.Wen, Q. Meng, C. Feng, and C. Tang, "Protocol vulnerability detection based on network traffic analysis and binary reverse engineering," PLoS ONE, vol. 12, no. 10, Oct. 2017, Art. no. e0186188.

[3]. S. M. Darwish and A. G. El-Shnawy, "An intelligent database proactive cache replacement policy for mobile communication system based on genetic programming," Int. J. Commun. Syst., vol. 31, no. 2, May 2018, Art. no. e3536.

[4]. H. Xu, "Intelligent modulation algorithm of WMSN communication channel," J. Discrete Math. Sci. Cryptogr., vol. 20, nos. 6-7, pp. 1477-1481, 2017.

[5]. J. Haitao, Y. Guo, H. Chen, J. Guo, C. Zhou, and J. Xu, "Unauthorized access vulnerability detection method based on finite state machines for mobile applications," J. Nanjing Univ. Sci. Technol., vol. 41, no. 4, pp. 434-441, 2017.

[6]. Q.-Y. Zhang, S.-B. Qiao, Y.-B. Huang, and T. Zhang, "A high-performance speech perceptual hashing authentication algorithm based on discrete wavelet transform and measurement matrix," Multimedia Tools Appl., vol. 77, no. 16, pp. 21653-21669, 2018.

[7]. J. J. Anaya, A. Ponz, F. García, and E. Talavera, "Motorcycle detection for ADAS through camera and V2V Communication, a comparative analysis of two modern technologies," Expert Syst. Appl., vol. 77, pp. 148-159, Jul. 2017.

[8]. A. Pinto,W. R. Schwartz, H. Pedrini, and A. Rocha, "Using visual rhythms for detecting video-based facial spoof attacks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 5, pp. 1025-1038, May 2015.

[9]. W. Xu and J. Leng, "Simulation of potential vulnerability spillover detection under network active protection," Comput. Simul., vol. 183, no. 993, pp. 190-202, Mar. 2018.

[10].M.Yasinzadeh and M. Akhbari, "Detection of PMU snooping in power grid based on phasor measurement analysis," IET Gener. Transmiss. Distrib., vol. 12, no. 9, pp. 1980-1987, May 2018.

[11].M. Kumar and A. Sharma, "An integrated framework for software vulnerability detection, analysis and mitigation: An autonomic system," S adhan a, vol. 42, no. 9, pp. 14811493, 2017.

[12].M.-C. Chen, S.-Q. Lu, and Q.-L. Liu, "Global regularity for a 2D model of electro-kinetic fluid in a bounded domain," Acta Mathematicae Applicatae Sinica-English, vol. 34, no. 2, pp. 398-403, 2018.

[13].W.Wei, J. Su, H. Song, H.Wang, and X. Fan, "CDMA-based anti-collision algorithm for EPC global C1 Gen2 systems," Telecommun. Syst., vol. 67, no. 1, pp. 63-71, 2017.

Cite this article as :

T Virajitha, Janga Rajendar, Mangalampalli Sesha Sai Lakshmi Lavanya, Kommu Anusha, "A Novel Framework for Early Intelligent Vulnerability Detection Algorithm for IoT Technology Environments", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 6, pp. 311-318, November-December 2022.
Journal URL : https://ijsrst.com/IJSRST229645