An efficient model checking based security verification technique in cyber security

[1]Prakrita K, [2]Prashanth J

[1]Student, [2]Assistant Professor
[1]Computer Science & Engineering
[1]BNM Institute of Technology, Bangalore, India

Abstract: Cybersecurity is the defense against cybercrime for systems linked to the internet, including their technology, application, and content. Enterprises generally hire cyber security specialists to safeguard their private data, preserve workers' productivity, and boost consumer faith in assets. Based on research carried out, it is noted that, a lot of attacks are taking place leading to loss of data, unauthorized access of systems, disabling of computer functions etc., that affects various organizations such as healthcare, banking, schools, etc., In order to avoid such situations, we have presented a model that provides a secure network by identifying various attacks that can take place based on the data required for the attacker. We have collected various datasets and trained them such a way as to detect an attack based on its features. We have also utilized malware detection using machine learning to classify attacks into malware and non-malware data.

***Index Terms*— Cyber-security, Assaults, Malware, Non-malware.**

I. INTRODUCTION

Data protection is the basic goal of cyber security. To secure the data from cyberattacks, a triangle of three interconnected principles is offered by the security industry. The CIA trio is the name given to this idea. The information security infrastructure of an organization should be governed by policies that follow the CIA model. Either of these rules have been broken whenever a security flaw is discovered. Confidentiality, Integrity, and Availability are the three components of the CIA model. In reality, it is a security paradigm that facilitates discussion of numerous aspects of IT security. A criminal act intended to exploit the vulnerabilities, hack a system, or otherwise interfere with digital world poses a serious threat in the context of cybersecurity. Cyber-physical systems(CPS) combine physical infrastructure and equipment to the net and to one another by integrating detection, cognition, controlling, and connectivity into them. Applications of cyber-physical systems include smart technology, autonomous vehicles, clinical diagnosis, automated manufacturing infrastructures, and many other CPS. A security integration methodology incorporates security protocols with cyber defense technologies to protect the distributed system and restrict access to confidential information. Malicious software, also known as malware, is the most popular approach of assault. An attacker or malicious hackers uses it to harm or interfere with an authorized user's PC.

However, for successful hacking, a hacker needs domain knowledge of operational-technology of the system. Operational technology (OT) consists of hardware and software that directly examines, regulates, and alters machineries, resources, operations, and occurrences. Hence, understanding a CPS's inadequacies is essential. To ensure a secure network, we present a model that provides a secure network, using model-checking based on UPPAAL model, which is an integrated framework that is used for security validation of various attacks. Every attack has variety of features based on which the attacks are classified. Keeping variety of security constraints in mind, the model is trained such that it detects various assaults such as man-in-the-middle assault, phishing assault, birthday assault, password assault, SQL-injection assault, drive-by attack, crosstie-scripting assault, teardrop attack and eavesdropping attack. Based on the data, we can thus identify the type of assault and hence carry out the model-checking analysis which indicates the attack type, network traffic position and the number of records. The data entered can be visualized in graphical form indicating the number of attacks happened in a particular year. Hence, this research was carried out to see how a network can be secured, by identifying attacks in the earlier stages.

II. RELATED WORK

J. Yang et al., [1], Two obfuscated code injection assaults were created, one for the feedback path and the other for the forward path of a control system. Each have a variable parameter that influences the rate of deprivation. The cautious strategy for reversing a linear forward attack was created using the least squares or minimal method of mean square. The common Kalman filter is looked into as defense mechanism against a sound injection assault on the feedback-path. A noise injection attack (NIA) is anticipated in the feedback-path to introduce noisy data to increase the variance of the parameter variation, while a linear forward attack (LFA) is proposed in the forward path to linearly transform a monitoring incoming to minimize the effectiveness of a control system with linear quadratic Gaussian (LQG) regulation.

S. Baldoni et al., [2], The focus of this contribution is on metadata that has been altered and injected into a transmission medium with the intention of altering the state of the physical system. By coding the output of the measuring equipment and building a secure control system that can spot the insertion of modified data, the risk is mitigated. The design of the permutation matrices used in the method described here is based on a distinctive pattern discovered using Fibonacci p sequences. The perceptual technique respects the significant delay restrictions imposed by a Cyber Physical Systems. By spotting deceptive attack patterns, a strategy is offered for securing Internet - of - things based CPS. The suggested technique flips and rotates the output vector by structuring the outcome employing marked permutations matrix. A two-key security system is produced by choosing the suitable permutation matrix using the Fibonacci p-sequences. The evaluation's findings imply that the suggested tactic is effective.

D. Levshun et al., [3], The work investigates a novel distributed and secure formal verification approach for microcontroller-based security systems. The fundamental idea behind this methodology is to identify most economical means of enhancing cyber-physical systems while accounting for the fact of primary requirements, semi-requirements, and compliance and security constraints. Additionally, a verification process is used to confirm each solution's security and dependability in terms of duration and suitability. By using a virtually complete version of a railway line to improve the accuracy of the design and analysis strategy for safe and dependable cyber-physical systems, the methodology's significance is confirmed. Utilizing verification techniques and broadening the modelling strategy for safe cyber physical systems increased the strategy's efficacy. Verification algorithms employ the model to evaluate the system's scope, its components, and their interdependencies, whereas verification algorithms use the model to investigate the elemental composition and nesting (hierarchy) of individual CPS elements.

X. Zhang et al., [4], A flexible safety governing system centered on trusted computing is described. It is based on the technical elements of existing survival mechanisms and the stated potential vulnerabilities of a control system for industry. The planning entails a discrepancy identity verification technique between an Internet security solutions of industrial physical-cyber systems, inner fire control walls, and anomaly perception and prevention systems, and trusted connection server of an Industrial Automation System. Multiple network security devices can transmit information, enhancing the entire defense the industrial automation system's capacity, because the hardware encrypted data, memory, and control integrity modes are also employed by the trusted computing module. It accomplishes the objective of greatly enhancing the control systems safety by resolving issue of easy breakage brought on by conventional repairing procedures based solely on software.

S. Hopkins et al., [5], The whole survey outlines the requirements for a signalized intersection, creates a highly secured basis, analyses & designs mechanism assaults, and follows the norms for implementation, validity, and assessment at each phase of the design. The program development effort used an agile approach life-cycle for the STCB's ongoing improvement. The Project Initiation Review's first stage is considered its professional turning point (PIR). PIR's engineering milestone is to distribute a practical reference point in the direction of a designated baseline. A realistic boundary condition is established by the providing targeted NIST 800-53 TSEC and ISO-5408, and it is then expanded to an STCB employing descriptive survey and prior work in a secure framework.

K. Chen, et al., [6], The dynamic network theories is being utilized for the research to investigate the vulnerabilities of the physical-cyber controllers. The implications of strong neural network on cybersecurity vulnerabilities is investigated using complex dynamic analysis. To properly describe the power system's features, the interconnect distribution is described. The dissemination of the broad range and proximity of such energy grid like a strategic model is examined employing case studies of power systems. The morphological modelling of the cyber-physical model is described, and parametric analysis is used to assess the structural vulnerabilities of the cyber-physical machine. The IEEE 302 bus simulation model is used to validate the model.

P. S. Sarker et al., [7], The military micro grid is described in this report as a test - bed for both computer security and cyber survivability. The upcoming IEEE 2030.5 protocol for DERs and micro grids is the foundation upon which the cyber model and interface are developed. The REST interface is used to build a framework for integrating the protocol with free software for design and simulation. OpenDSS has been brought up in conversation. The protocol's probable flaws are looked into, and vital components like the fight micro-grid are rated. For examination, a sizable Miramar military micro-grid system template is used. The simulated outcomes were displayed that highlight practical applications, such as operating circumstances and cyber-physical resilience management. It is shown & explored how to measure the resilience of a micro - grid.

A. Aigner et al., [8], Security metrics and security evaluation frameworks can be used to quantitatively portray security based on various measurements and rules. However, current security scoring techniques may not be able to generate trustworthy security scores for CPS due to insufficient consideration of typical CPS characteristics, such as the communication of heterogeneous systems in the physical- and cyber-space domain in an unpredictable way. As a result, the research offers Security Qualification Matrix as a framework for security analysis (SQM). The SQM has the ability to interpret several threats concurrently at the System-of-Systems stage. This method allows for the quick identification and evaluation of interdependence, potential risks, as well as the effectiveness of countermeasures. In order to quantitatively represent assurance depending on multiple measurements and regulations, it is possible to employ security metrics and security evaluation frameworks. Furthermore, current security scoring systems may not be able to generate trustworthy security scores for CPS due to insufficient consideration of typical CPS characteristics, such as the communications of heterogeneous networks in the physical- and cyber-space domain in an unusual manner. As a result, the research offers Security Qualification Matrix as a framework for security analysis (SQM). The SQM has the ability to interpret several threats concurrently at the System-of-Systems stage. This method allows for the quick identification and evaluation of interdependence, potential risks, as well as the effectiveness of countermeasures.

A. Kovačević et al., [9], A study is being conducted to thoroughly examining awareness of cyber security and to try to understand what various factors, including socio-demographics, cyber defense perspectives, past cyber security breaches, IT usage, and knowledge, may have an impact on cyber security behavior either individually or collectively. Since students are the group in society that uses technology the most, research was done on them to demonstrate this. Although students are digital natives, we found that knowledge was the key to understanding cyber security awareness. Despite this, students do not feel safer online, will not behave appropriately, and lack the information necessary to defend oneself. As an illustration, IT awareness and use appeared as crucial elements of smartphone-related behavior, showing that the effects of cyber security attitudes, knowledge, and behaviors are greater than the impacts of psychological risk factors for smart phones.

F. H. Sohime et al., [10], This investigation's goal is to prepare students for the job market for cyber security, determine all necessary skill sets and create a hierarchical system for data security competencies. The job title is information security analyst being studied since, based on the literature analysis, that is the highest position for cyber security. The technical and interpersonal skills, plus numerous types of professional security certifications, are assessed. All of the talents for a job as an information security analyst are compared. Using the analytical hierarchy technique, the study created a structured model for cyber security expertise

(AHT). The AHT technique is used to define and rank the criteria of cyber security skillsets in order to prepare learners for the cyber security job market and construct a hierarchy structure for cyber security competency. Because of the demand for specialists in the sector of cyber security, it is vital to assess the necessary skills and abilities. According to the study, the following criteria should be prioritized in order of importance: (1) Conversational Skills, (2) IT Infrastructure Navigation, (3) Hazard Identification, (4) Business Development, & (5) Skills in analysis. The survey's learning found which abilities are highly crucial for young grads to have when applying for jobs as information security analysts.

III. METHODOLOGY

As shown in the below *Figure 1*, the proposed model shows how a system can be verified using model-checking relying on various attacks. The *Figure 1*, thus indicates a CPS, where initially security constraints is considered based on which, a security verification model is established. Once the model is established, model- checking is carried out which relies on the attack tree to detect various assaults. Once the assault is detected, we check for the safety of the network and analyze whether the attack detection is successful or not. If it fails to do so, we will check for other vulnerabilities to further improve the model.

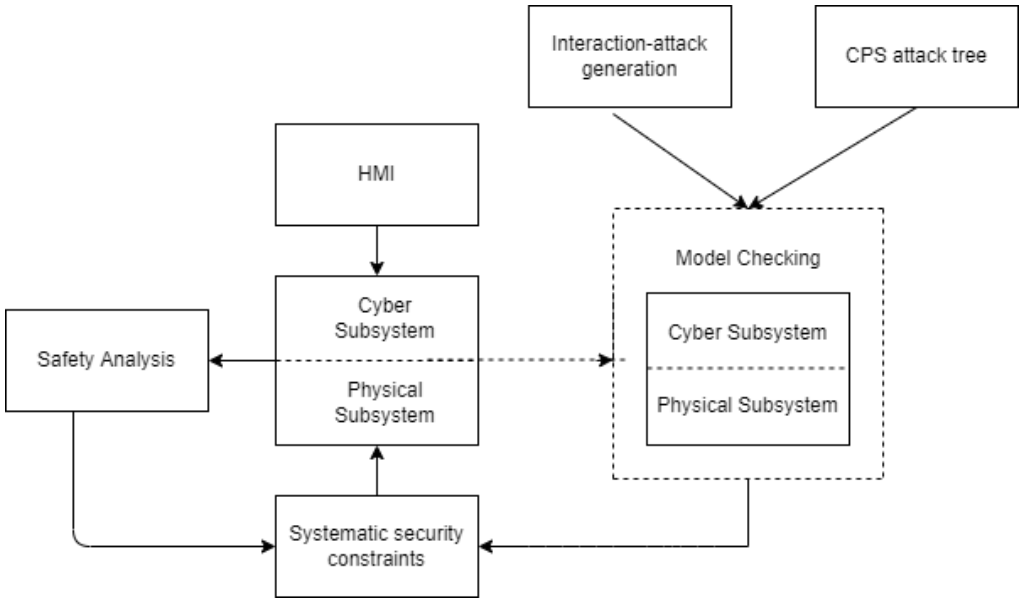


Figure 1: Model for security verification

Dataset

The dataset is collected on breaches data where it contains attributes such as the state of the attack, number of records lost, the year of attack, method of leak of the data, etc., The datasets collected is thus pre-processed removing unwanted data, and features are extracted based on different types of attacks. Based on the data collected from the dataset, considering the unsafe situations of the security system, we generate constraints for the attack, based on which we detect the various attacks.

Units

Due to missing values and inconsistent data, the dataset cannot be handled in the classification process. Since they were the same for each individual, a number of factors were eliminated. For categorization, the random Forest algorithm is employed. To obtain the important characteristics for this work, random forest is used. All of the data in the dataset should be eliminated because there may be numerous duplicates or incorrect values in the data. Therefore, using the random forest, we will exclude the undesirable values and produce a new dataset called reduced features that can store the entire dataset.

To generate p classifiers:

for i=1 to p **do**

Randomly sample the training data T with replacement to produce T_i

Create a root node, R_i containing T_i

Call ConstructTree(R_i)

end for

ConstructTree(R):

if R contains instances of only one class **then**

return

else

Randomly select y% of the possible splitting features in R

Select the feature F with the highest information gain to split on

Create f child nodes of R, R_1, ….., R_f, where F has f possible values (F_1, ….., F_f)

for i=1 to f **do**

Set the contents of R_i to T_i, where T_i, is all instances in R that match F_i

Call ConstructTree(R_i)

end for

end if

Models

Heading 1

UPPAL MODEL – UPPAAL is an integrated framework that is mainly used for the verification of security based on the features of various attacks. As shown in the below *Figure 2*, we have added an extra model to the normal UPPAAL module, known as the assault module. In a specific threat paradigm, the Assault Module imitates disruption in communications, application, and devices, comprising values discrepancies, logical mistakes, file transfer faults, device breakdown, and electrical breach engagement.

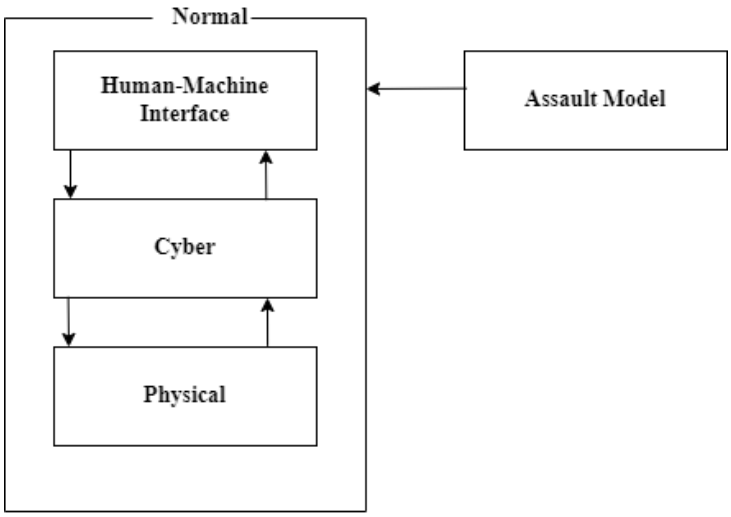


Figure 2: The UPPAAL Model

Heading 2

ASSAULT MODEL - Based on the security vulnerability under consideration, the Assault Module can vary the inputs & outputs in the Normal Module, anticipating destructive cyber-attacks on physical devices, application processes, or communications that lead to erroneous data.

Malware Detection Using Machine Learning

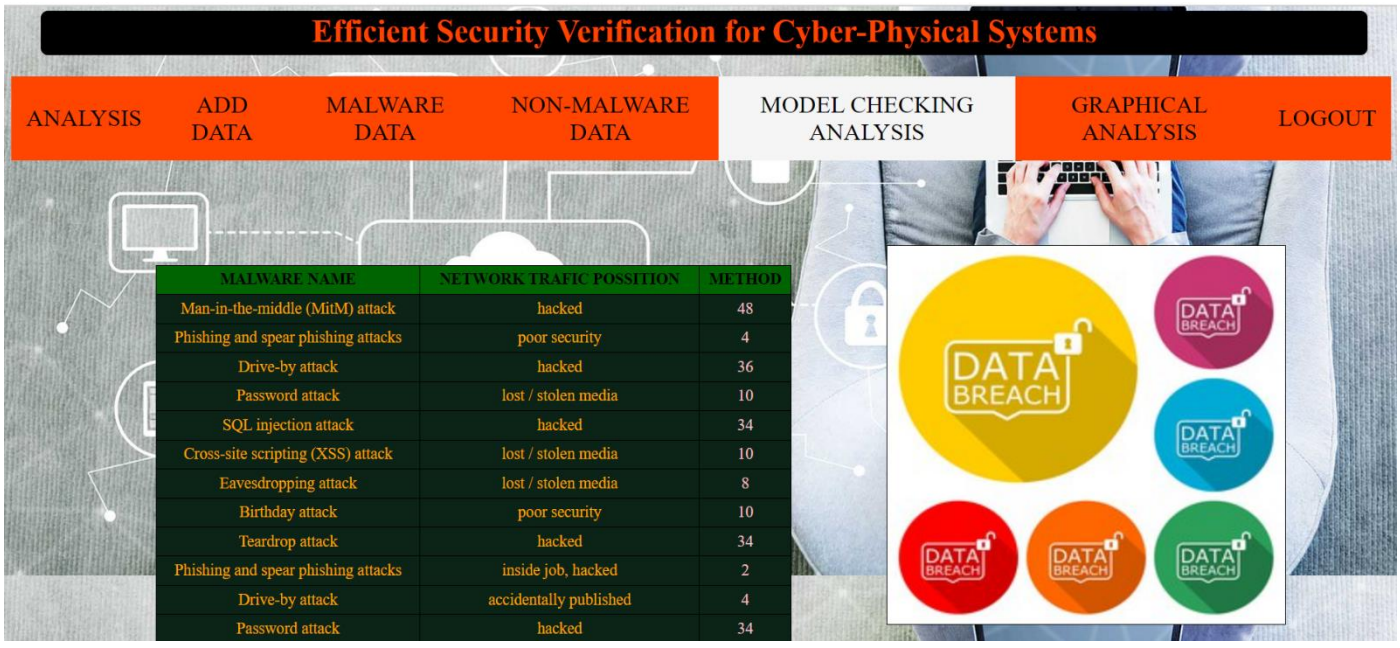
A ransomware prediction module based on various attacks such as man-in-the-middle(MitM) attack, phishing attack, birthday attack, password attack, eavesdropping attack, etc., are used where, based on features of each attack, it detects the type of attack that has taken place in a cyber-physical system. The malicious executables are trained that forms the prediction model in the training phase. However, in the developed stage, the prediction model assesses the unknown executable to determine whether the attack is malware or non-malware data.

This detection can be taken place in different ways:

- Data is recognition about something like a file which can be accessed without even being run during the pre-execution period. This might comprise, among other things, the high points of the executable file type, program interprets, bit values stats, word documents, and metadata that code interpreters have extracted.
- Metadata is used in the post-execution cycle to shed light upon system behavior or situations brought on by process activities.

IV. EXPERIMENTAL RESULTS

Figure 3 below shows the analysis the model performed using the user's inputted data. Based on malware detection, network traffic position, as well as number of records, the model analyses data. The model checking analysis shows an insight depending on the sample provided by the users as to what assaults are occurring for a specific data, what losses have been sustained, and how many attacks of that sort have occurred. Assessing the different attack types that can occur in a network and the damages that can result from each form of assault is made easier with the help of the model presented. A safe network is created as a result of safety evaluation, which is conducted using the paradigm to validate the attack based on the cyber-physical system's security limitations. We can therefore offer new security restrictions and consider looking at the attack tree if the security is unable to evaluate the networks.



MALWARE NAME	NETWORK TRAFIC POSSITION	METHOD
Man-in-the-middle (MitM) attack	hacked	48
Phishing and spear phishing attacks	poor security	4
Drive-by attack	hacked	36
Password attack	lost / stolen media	10
SQL injection attack	hacked	34
Cross-site scripting (XSS) attack	lost / stolen media	10
Eavesdropping attack	lost / stolen media	8
Birthday attack	poor security	10
Teardrop attack	hacked	34
Phishing and spear phishing attacks	inside job, hacked	2
Drive-by attack	accidentally published	4
Password attack	hacked	34

Figure 3: Model-analysis

The column chart in *Figure 4* below demonstrates the amount of assaults that occur in a certain period. The x-axis in this graph denotes the recordings, and the y-axis the year. The graph above provides a proportion of the number of assaults that occur yearly based upon the information that users have submitted.

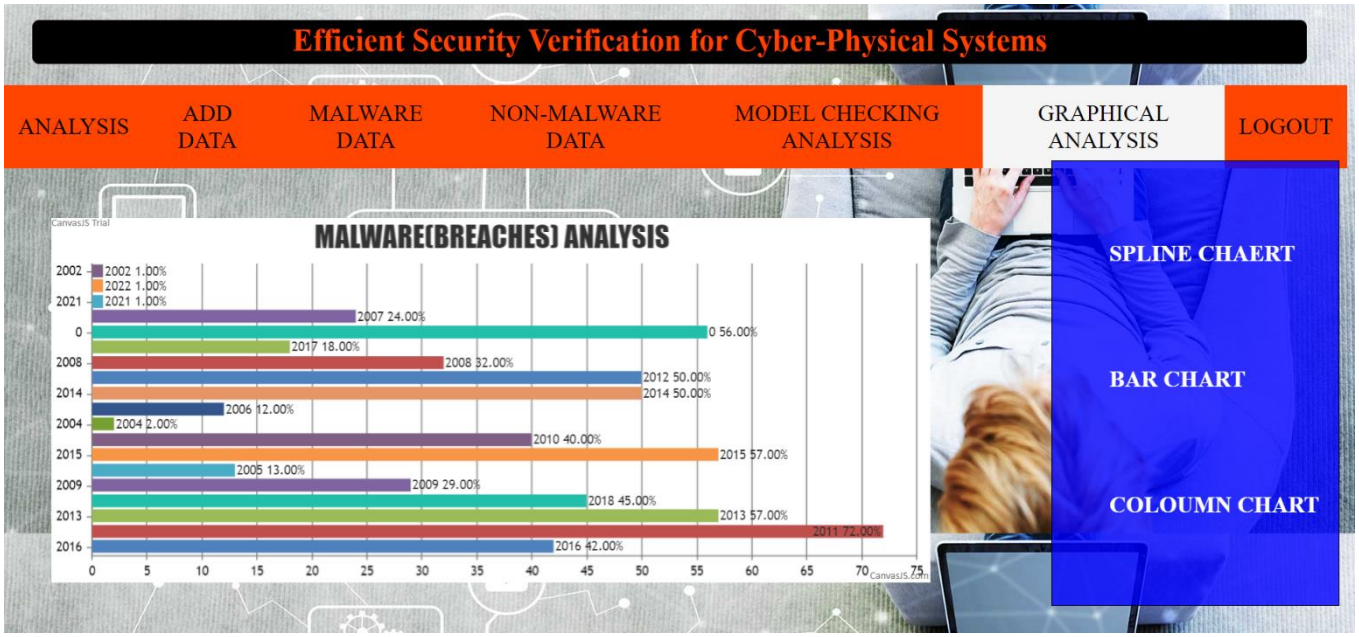


Figure 4: Column Chart

V. CONCLUSION

Cybersecurity for a CPS is essential. By thwarting attacks during the design stage and spotting them during the runtime stage through constraint monitoring, we can guarantee the protection of a CPS. Cybersecurity is crucial because it can be challenging to identify a CPS's weaknesses. Model checking enhances security verification as a result, and data and networks are shielded from unauthorized access. In addition, it helps to improve global defense. The research helps to identify different types of attacks dependent on restrictions, that improves the system safety. Researchers can construct numerous limitations to identify an intrusion by taking into account the unfavorable conditions of a network.

REFERENCES

1. J. Yang, "A Controllable False Data Injection Attack for a Cyber Physical System," in IEEE Access, vol. 9, pp. 6721-6728, 2021, doi: 10.1109/ACCESS.2021.3049228.
2. S. Baldoni, F. Battisti, M. Carli and F. Pascucci, "On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems," in IEEE Access, vol. 9, pp. 41787-41798, 2021, doi: 10.1109/ACCESS.2021.3065228.
3. D. Levshun, A. Chechulin, I. Kotenko and Y. Chevalier, "Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems," 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2019, pp. 1-5, doi: 10.1109/NTMS.2019.8763814.
4. X. Zhang, X. Cai, C. Wang, K. Han and S. Zhang, "A Dynamic Security Control Architecture for Industrial Cyber-Physical System," 2019 IEEE International Conference on Industrial Internet (ICII), 2019, pp. 148-151, doi: 10.1109/ICII.2019.00038.
5. S. Hopkins, C. Henry, S. Bagui, A. Mishra, E. Kalaimannan and C. S. John, "Applying a Verified Trusted Computing Base to Cyber Protect a Vulnerable Traffic Control Cyber-Physical System," 2020 SoutheastCon, 2020, pp. 1-8, doi: 10.1109/SoutheastCon44009.2020.9249758.
6. K. Chen, N. Zheng, Q. Cai, Y. Li, C. Lin and Y. Li, "Cyber-Physical Power System Vulnerability Analysis Based on Complex Network Theory," 2021 6th Asia Conference on Power and Electrical Engineering (ACPEE), 2021, pp. 482-486, doi: 10.1109/ACPEE51499.2021.9436982.
7. P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn and B. Miller, "Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5," 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, 2020, pp. 1-6, doi: 10.1109/MSCPES49613.2020.9133689.
8. A. Aigner and A. Khelil, "A Security Qualification Matrix to Efficiently Measure Security in Cyber-Physical Systems," 2020 32nd International Conference on Microelectronics (ICM), 2020, pp. 1-4, doi: 10.1109/ICM50269.2020.9331797.
9. A. Kovačević, N. Putnik and O. Tošković, "Factors Related to Cyber Security Behavior," in IEEE Access, vol. 8, pp. 125140-125148, 2020, doi: 10.1109/ACCESS.2020.3007867.
10. F. H. Sohime, R. Ramli, F. A. Rahim and A. A. Bakar, "Exploration Study of Skillsets Needed in Cyber Security Field," 2020 8th International Conference on Information Technology and Multimedia (ICIMU), 2020, pp. 68-72, doi: 10.1109/ICIMU49871.2020.9243448.