A Review Cases in Cyber Physical Systems

Girija Lakshmi L, Ashika Jadhav ,Lavanya S
(Information Science And Engineering, BMS College Of Engineering, India)
(Information Science And Engineering, BMS College Of Engineering, India)
(Information Science And Engineering, BMS College Of Engineering, India)

Abstract

The CPSs [cyber physical systems] are the communication between the two devices. That is the internet devices and the hacking devices. This system is mainly used to solve a real-world problems. This CPSs are currently becomes the main target of the hackers. And it leads highly damage to our nation. By these CPSs , valid resources, and several cases are involved in this breaches for security purpose. At the view point of the security in the digital world the fundamental and theoretical concepts are discussed worldwide. At the point of security cases in the CPSs it it still remained as less explored. In this paper a lot of securities methods are used and implemented. So here we are looking about the attacks, impacts and the intentions and incidents of the categories. This is the main thing in the cyber-physical systems.

Keywords *– cyber physical systems, threat, security, cyber ethics ,mobile phones ,network.*

I. INTRODUCTION

CPSs are the collection of all the wirelwss devices like sensors and mobility devices . these systems are become more interconnected, so it is more complex. CPS become the matter for the economic and infrastructures to every country in the world. Here types of attacks can viewed. These types of attacks can be able to provide destruction to critical infrastructures. CPSs are using in the worldwide and it is the connection oriented wireless service. And the main goal of this paper is reduce the hacking in cyber activities. This paper discusses some of the instances that is attacks on the CPSs, impacts of the CPSs, and the incidents of the CPSs. In the references the 1st paper is discussed about the biometric cancellation technique. And the 2nd reference will tells about the types of attacks happened and threats occurred. and the further refenrences will described with the more metrics and techniques. We are identifying the characteristics of the available resources here. We are developing the wireless networks management policies. Ans the problems will be solved. By the conclusion of the papers, the critical analysis for the mobility management and its related issues. At the view point of the security in the digital world the fundamental and theoretical concepts are discussed worldwide. At the point of security cases in the CPSs it it still remained as less explored. By the all conflicts we are analysed and decides to provide good better life to all internet users by the help of the CPSs. Currently running threats and attacks can be removed in this parts. So the best algorithm is used. And we are using a quantative approaches to collecting the data analysis. Finally in the last reference it will concluded the solutions for the future work.

II. LITERATURE SURVEY

WENCHENG principle [1]. In this paper we are discussing about the " securing the mobile healthcare data", that is using a " smart card based cancellable finger-vein bio-cryptosytem". This paper extracts the most systems are exiting biometric systems . the data will be stored in securely, by using the smart card information will be encrypted and stored. By using the FCS [fuzzy commitment scheme] we are going to encrypt the data. We are already know that the biometric system is very useful. So this system will provides more confidentiality in mobile healthcare.

Mohammed Nasser Al-Mhiqani1, Rabiah Ahmad1[2]. In this paper we are studying on the information about the , CPSs are largely using people's day to day life. It has some characteristics, applications and security challenges. Here it says when it is especially used by the cyber criminals against the governments. And this paper concludes that the CPSs are currently widely used in the several public industry services. Mainly the failure of the these CPSs are causes damage on the global economy. So reason is the system operation real world it can affect the physical safety or even lead to the loss of life.

Sampath Kumar Venkatachary[3] This is the paper contains the "economic impacts of cyber security in energy sector":. In this paper we are going to discuss about the , the new "digital age". It is converts the huge change in the forms. That is connections ,supplies, and the models. So cyber security is highly effects on the our economic part. And it contains more threats also, we should solving this in this paper. And providing the security. Here the electric power system comprises the both IT and electric systems infrastructures. And moreover threats can be physical, internal or external. This paper concludes

that the cyber threat is becoming the increasingly common threat.

G. Balaji[4] This is the paper aimed that is particularly concerned with major system employed in medium to the industrial enterprises. It explains the significance of the various attacks. And it concludes that the owners need to think of the threats in more global terms.The paper goal is here that everyone's responsibility here, to solve the main problem in the internet services. Paper concludes that the private information. It uses so many technologies for future references.

Mohammed Nasser Al-Mhiqani [5]. This paper proposing the different cases available in the CPSs. This is the communication between the two various channels or directions. According to the 4.0 revolution the CPSs are becoming the main of the the cyber attacks and the cyber threats. It is the big loss to our nation. By these CPSs , valid resources, and several cases are involved in this breaches for security purpose. At the view point of the security in the digital world the fundamental and theoretical concepts are discussed worldwide. At the point of security cases in the CPSs it it still remained as less explored. So as customers we should try to increase the managing and release a large amount of more security measures to the CPSs .

JALAL AL-MUHTADI[6]. The author says in this paper , "related issues of the wireless sensor networks in the CPSs". It describes the what are the different types of problems may arises and how to solve those problems. So this paper talks about the techniques, that will be used in the sensor networks in the CPSs. Disadvantages also available in the wireless networks discussed in this paper. Finally , this paper finalizes the ways to analyze the management and its problems.

QIANMU LI[7]. The main of the paper is to introduce and analyze the structure CPSs.This is the topic about " safety risk monitoring of cyber physical algorithm". Here the processing mechanism can be train the networks features protocols. This is for design an abnormal detection framework based on big data mining. Here we introduces the [EPABT] algorithm . This paper is for the future work of the detect the safety mechanism. The algorithm is better and powerful.

YU WANG1, BIN SONG1[8]] In this paper to propose feature of algorithm rule to satisfy the rate between image classification. They fuse large pre trained neural network options by genetic algorithm. The gaps can be increased between various centers by dynamically weight assignment for different categories .Next to propose a methodology to do accurate time which can improve flexibility and efficiency of image classification in CPSs.

un-Sheng Wang and Guang-Hong principle [9] In this paper it aims to get rid of some assumptions and provides methodology called sneaky attack for closed loop cycles. Using TCIP management underneath second measure un know a benchmark platform and TCIP based networked ad hoc used for testing sneaky attack built in different data driven ways. The inspiration formed for eavesdropping data for TCIP. Different approaches made to interference and injecting false detector is explored .Sneaky attack data driven is obtained by above results.

GEORGE LOUKAS[10] This paper is about detecting cyber attacks against vehicles. Vehicles has rule based or light weight machine learning techniques .And inflated resources is accessible during permit access manner to additional advanced technique .Case study for victimization a little simple machine tend to demonstrate usefulness task of intrusion detection for deep learning. In this paper they proposed an approach which achieves high efficiency and accuracy more systematic way .It relate to each cyber processes in time period that feeds to neural spec. It also proves for learning various attacks .some are denial of services ,command injection and malware as example. There is additional reliable network is reducing detecting latency achieved.

ZHIHONG TIAN[11] In this paper its new and exciting analysis of technology for users to improve in field like teaching ,analysis, learning especially in role of cybersecurity .Cyber is virtualization platform consisting networks, computers on real-world threats .This paper supports work vary with C2RS method .This method is lustiness and scalable for tasks. Main aim is to reduce memory usage and raise performance.

IVO FRIEDBERG1[12] Associated with a physical process CPSs have dependability requirements. CPS always deviates from the operation hence it is very important to look over it. .Evidential networks are referred it to as the solution to these problems in this paper .In this paper it describes the ways to integrate of different types of sensors which are low level through evaluating the CPS systems. The results say that the accuracy of the system can also be identified by the networks through approaches which use the Bayesian method.

G.NIKHITA REDDY[13] In this paper the author has said that this domain plays an important role in IT field . Gaining the knowledge is the biggest challenges now a days .The moment we think we think about this domain the word that is related to it is cyber crimes which are increasing rapidly .Government has taken measures in order to prevent

the cyber crimes that are emerging today .Even though many measures had been taken this domain is given a very big importance to take care of. This paper mainly gives focus on threats ,problems faced by this domain on the latest developed applications ,ethics and trends which changes the face of the cyber security.

Martin Husák[14] In this paper the author provides a survey conducted of forecasting and prediction used .There are 4 main tasks involved in this discussed are attack projection ,in which there is need to know about the next move of the attacker , intrusion prediction of the threats and attacks .In this paper we discuss about many approaches and methods which are based on many other networks ,graphs and and series according to the time which are been tested and compared .

Basit Shahzad[15] Social media has enabled a way sharing information among people around the world without financial crisis and time crisis .The mode of communication is been carried out through mobile by most of the people and hence the sharing of the information or the data through voice or message or mail has changed the view towards the sharing information .Now a days with development of many fast growing applications the privacy of the information should be compromised if the proper measures are not been taken .Author also has described about the importance of the health care facility through online since it very important during emergency times and also about the health care system application .In this application the individuals or customers who use this app are guaranteed with privacy of their details and also safe and secured when the communication is done through the help of cloud environment which is multiple across the network through social media .

III. ADVANTAGES AND DISADVANTAGES

A. ADVANTAGES

a) Network integration

CPSs involve multiple process platforms once interacting over communication networks. Network integration characteristics provided by Hz, like media access management techniques and their effectiveness on system dynamics, middleware, and computer code.

b) Interaction between systems and human

Cyber Physical Systems include humans beings as an important part of the systems, thereby leading to simple interaction as humans square measure tough to model employing a standalone system.

c) Improved system performance

Cyber Physical Systems will get good performance in terms of automatics designs and feedback for an concepted interaction between cyber systems and sensors. Cyber process resources and subsystems in Cyber Physical Systems guarantees multiple mechanisms of high level programming languages, communication and user maintenance thus the system performance is good

d) Scalability

Cyber Physical Systems measures heterogeneously as they mix processes with dynamics of physical systems .Physical domains will mix up with motion managements ,mechanical process, chemical process, human activities, and biological involvement. Cyber domains will mix up computer codes ,modeling, programming tools and network infrastructures.

e) Optimization

The usage of medical facility cloud infrastructure and sensor and will change huge optimization for more applications. This system allows optimizing cyber physical systems in huge extent.

IV. DISADVANTAGES

A. Isolation Assumption: The dominant feature in most of all is the trend of "security" if not all ,since their initial style. Since the protection has not been a of good importance the main aim of this has been to plan reliable , secured and safe systems.

B. accumulated Connectivity: Hz square measure a lot of connection than had before ever .Makers have put faith in Wire less technologies and open net works to improve Hz services by adding services in them.

C. Heterogeneity: Heterogeneous COTS are measured by Hz elements, third party ,to make Hz a application proprietary elements square measure integrated. The multivendor systems are usually always measured by CPS and every product has its own security issues.

D. Cyber Vulnerabilities

a) ICS Vulnerabilities

b) Smart Grids Vulnerabilities

c) SG V2, computer code vulnerabilities

d) Medical Devices Vulnerabilities

V. CONCLUSION

CPSs area unit presently wide utilized in many public and business services. Failure of CPSs will cause vital injury on the worldwide economy and important business missions. the explanation is that system operation within the planet will have an effect on the physical safety or perhaps result in the loss of the life. As the unit area of the CPs during this analysis the safety ,the threats ,the challenges, advantages, features and application area are mentioned. In the past similar studies are executed and conducted , but the organizations and researches will utilize the tools and theories to know the kinds of recent threats, security challenges, and also the effects every threat is the reason to lack the space in CPSs systems .The mechanisms of Hz for detecting ,preventing, and convalescent from attacks are going to be examined in future. The tools especially which will be accustomed to stop hacklers from gaining access to the systems to those which are going to be explored .To cut back the impact of the attacks , particularly in those of oil industries or alternative utility services recovery systems will be improved mainly.

REFERENCES

[1] Yang, Wencheng , et al. "*Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem*." IEEE Access 6 (2018): 36939-36947.

[2] Al-Mhiqani, Mohammed Nasser, et al. "*Investigation study of Cyber-Physical Systems: Characteristics, application domains, and security challenges.*" ARPN Journal of Engineering and Applied Sciences 12.22 (2017): 6557-6567.

[3] Venkatachary,Sampath Kumar,Jagdish Prasad,and Ravi Samikannu. "*Economic impacts of cyber security in energy sector: a review.*" International Journal of Energy Economics and Policy 7.5 (2017): 250-262.

[4] Vidyasagar, K., G. Balaji, and K. Narendra Reddy. "*RFID-GSM imparted School children Security System*." Communications on Applied Electronics (CAE). Vol. 2. No. 2. Foundation of Computer Science FCS, 2015.

[5] Al-Mhiqani, Mohammed Nasser, et al. "*Cyber-security incidents: a review cases in cyber-physical systems*." International Journal of Advanced Computer Science and Applications 9.1 (2018): 499-508.

[6] Al-Muhtadi, Jalal, et al. "*A critical analysis of mobility management related issues of wireless sensor networks in cyber physical systems*." IEEE Access 6 (2018): 16363-16376.

[7] Li, Qianmu, et al. "*Safety risk monitoring of cyber-physical power systems based on ensemble learning algorithm*." IEEE Access 7 (2019): 24788-24805.

[8] Wang, Yu, et al. "*A fast feature fusion algorithm in image classification for cyber physical systems.*" IEEE Access 5 (2017): 9089-9098.

[9] Wang, Jun-Sheng, and Guang-Hong Yang. "*Data-driven methods for stealthy attacks on TCP/IP-based networked control systems equipped with attack detectors*." IEEE transactions on cybernetics 49.8 (2018): 3020-3031.

[10] Loukas, George, et al. "*Cloud-based cyber-physical intrusion detection for vehicles using deep learning.*" Ieee Access 6 (2017): 3491-3508.

[11] Tian, Zhihong, et al. "*A real-time correlation of host-level events in cyber range service for smart campus*." IEEE Access 6 (2018): 35355-35364.

[12] Friedberg, Ivo, et al. "*Evidential network modeling for cyber-physical system state inference.*" IEEE Access 5 (2017): 17149-17164.

[13] Reddy, G. Nikhita, and G. J. Reddy. "*A Study of Cyber Security Challenges and its emerging trends on latest technologies*." arXiv preprint arXiv:*1402.1842* (2014).

[14] Husák, Martin, et al. "*Survey of attack projection, prediction, and forecasting in cyber security.*" IEEE Communications Surveys & Tutorials 21.1 (2018): 640-660.

[15] Al-Muhtadi, Jalal, et al. "*Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment.*" Health informatics journal 25.2 (2019): 315-329.