2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

Cyber Physical Systems- Implications and Challenges

Vaishali Sharma
Amity Institute of Information Technology
Amity University,
Noida, Uttar Pradesh, India
vaishalisharma11@outlook.com

Ajay Vikram Singh
Amity Institute of Information Technology
Amity University,
Noida, Uttar Pradesh, India
avsingh1@amity.edu

Ajay Rana
Amity Institute of Information Technology
Amity University,
Noida, Uttar Pradesh, India
ajay_rana@amity.edu

***Abstract*- Cyber physical systems are a topic of utmost interest and curiosity in the recent days. But at the same time the security threats and safety concerns are also being highlighted. Underway progresses which are being made on a regular basis in the field of science and technology improves relationship between physical and computational elements by using intellectual ways which increase the efficiency, reliability, adaptability, functionality, safety, usability and autonomy of the cyber physical systems drastically. The process of remodeling physical system into a cyber physical system is an ongoing thing which is completed by imbibing intelligence into the physical systems. This transformation can be considerably used for the welfare of the environment and the society by revamping the quality of life, convenience and comfort of the humans, even for minimizing depletion of environmental assets and bringing down ecological impacts. With all the fast paced advancements being made in this field, the security and safety are a huge concern. In this paper, we talk about the implications of cyber physical systems and its smart utilities as well as discuss the challenges and the security threats faced in cyber physical systems.**

Keywords- Cyber Physical Systems, Cyber Computing, Smart City, Safety Critical Systems, Embedded Systems Security

I. INTRODUCTION

Many contemporary computing systems display an amalgamation of cyber and physical components of a system, which are developed openly. Cyber computing is being effectively used to manage physical systems capably. An essential transformation in these systems is enabling automatic and efficient management of the nation-wide physical system infrastructure [1] including public utility service infrastructure, mobile health management, transportation, disaster management. Internet-Of-Things [2] and Cloud Computing [3] technologies are being merged with cyber-computing to maintain and manage enormous scale physical system infrastructure.

We can say that this will be deployed at a larger scale in the major cities of India. Off lately, the Government of India presented an investment of millions that will aide in building 100 smart cities with massive focus on automation of utility functions, development of urban systems that monitor and break down the personal satisfaction of individuals living in these urban communities. Furthermore, smart systems will be made for the betterment of the environment, monitoring energy usage, providing personalized health services, ensuring complete public security and safety through integrated transportation systems while focusing on conservation and treatment of water. Any failure in the functionality or a threat to the security to such physical infrastructure may give rise to physical infrastructure malfunction, service disruption, decimation to national assets and death toll.

CPS is an amazingly unique research field, and the mix of distinguishing, control, figuring, correspondence and coordination in CPS, for instance, present day planes, power network, transportation and human services device frameworks, presents epic challenges because of their complexities. A collection of issues ought to be comprehended at different layers of the designing and from different pieces of structure setup to encourage the blend of the physical and computerized universes[17]. Right now, some research difficulties are outlined from different perspectives in Table (1).In this paper, we understand the cyber- physical security systems, their implementations and various security threats and challenges associated with them.

TABLE I. DIFFERENT PERSPECTIVES ON CHALLENGES FACED

No.	Challenge	Perspective
1.	Real Time Performance	Hardware related issues and wireless sensor connectivity to the internet can affect the real-time execution of CPS
2.	Sensors and Mobile Networks	An autonomous system needs better connectivity to the mobile network for data transmission which becomes difficult to track as humungous amount of raw data is generated from it
3.	Reliability, Robustness and Security	These three elements become essential for some random CPS considering security break in the framework.
4.	Abstractions	These incorporate embedded systems or sensors for real time correspondence. This element needs to guarantee that the framework is issue tolerant, versatile and improved. New appropriated embedded systems and real time correspondence just as calculation technique are required.
5.	Validation	Better algorithms are needed to validate software details and verify other information at an initial stage.

II. CYBER PHYSICAL SYSTEMS AND INTERNET-OF-THINGS (IOT)

The conventional mechanism of Cyber Physical System has the accompanying significant advances:

A. Monitoring

- Estimate and deliver feedback on past actions.
- Basic functionality of Cyber Physical System.
- Guarantee appropriate working on upcoming actions.

B. Networking

- Handles historic and summarized data
- Simultaneous interaction of various applications is enabled by network communication.

C. Computing

- Data being generated during monitoring is analyzed.
- Guarantees that the physical processes meet previously fixed benchmarks. In case the benchmarks are not met, alternatives are suggested and implemented.

D. Actuation

- Implements actions decided in the computing phase.
- Stimulate various actions like rectifying the Cyber behavior of Cyber Physical Systems and replacing the physical process.

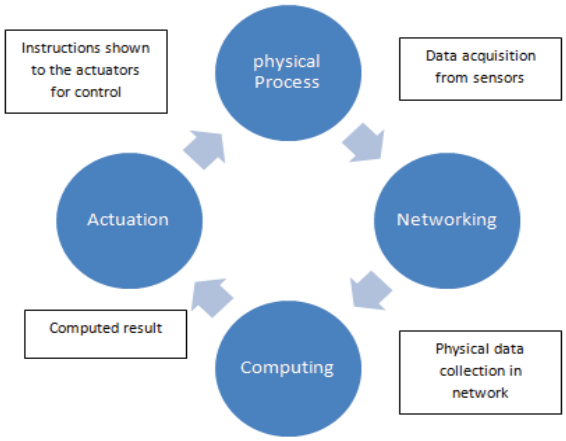

Fig. 1. Workflow of Cyber Physical Systems

The stream of progression in IoT is associated—anyway not undefined nor fundamental—to CPS. For IoT applications, a continuous analysis command of physical strategies may not be significant. Or maybe, various IoT system structures make adaptable applications or cloud applications as unequivocal organizations, using the joining of keen sensors, remote systems, web access, and cloud stages with bleeding edge data assessment. Then again, the last organizations in CPS are physical systems per-encircling constant control endeavors in the physical world.[17]

Some IoT applications give splendid actuator headings from consistent sensor readings. Nevertheless, these exercises are once in a while limited to the commencement of information limits (eg, message appear, sound admonitions) for observation, collaborations, and watching.

These essential exercises are confined to information care, while not completing a physical strategy autonomous from any other person. Or maybe, CPS performs control exercises to such an extent that changes the new state of the sensor readings and subsequently the states in the control hover by actuator headings with physical aftermaths. Principally, some CPS applications are related with the Internet to use data finding in a good paced organizations. Right now, develop an order of CPS-IoT from the intersection purpose of this field, to be explicit, those CPS that recall Internet relationship for their framework plans.

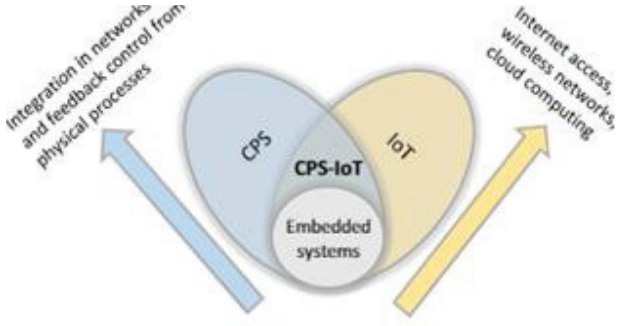

Fig. 2. Relationship between CPS and IoT

Here we demonstrate a sample CPS which can be used in an industrial setting for bulk production. This CPS has two PLCs (Programmable Logic Units) which are interconnected to each other via a bus network connected to certain workstations. This is known as the Primary Bus.[11]. Moving down the PLCs are the secondary bus connections terminating at devices like- boilers, packing units, assembly lines, electronic lighting etc. (field devices). This network operates on IP packets and has links which are serial where the current can be controlled to run devices. There are no communication based standard protocols like TCP/IP. This is the Physical component of CPS.

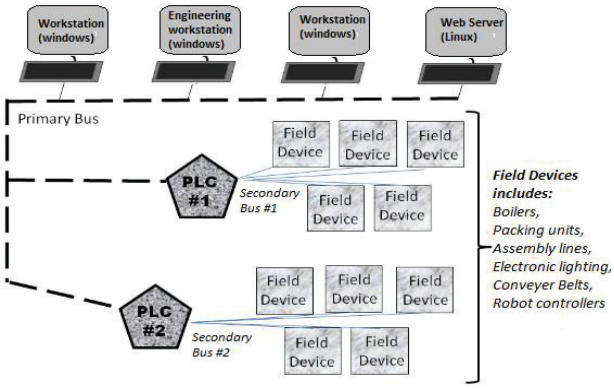

Fig. 3. A sample simple CPS

III. APPLICATION AREAS OF CYBER PHYSICAL SYSTEMS

Because of their remarkable highlights, cyber physical system configuration approach has been utilized in numerous spaces. In what follows, we outline a couple of these application areas where Cyber Physical Systems are being put to complete use.

A. Transportation Systems

Present day vehicles are cyber-physical systems, which give improved information, entertainment, displays, deal with the movement and energy utilization of the vehicles. Improvement of an automotive system includes system prerequisites specification, system investigation and execution [7]. The cyber security systems in this case have separate modules which execute the task of Operating system

and software components specification to process a communication model. The Cyber physical systems also takes certain factors related to humans into account while engaging safety applications which will aide the human drivers.

B. Healthcare and Medical Systems

The point of Cyber Physical Systems is to give a system to safe entomb network of medical devices. The intuitive CPS watches the movement and exercises of day by day living of the clients. In view of this, the CPS gives the administrations to the client at the ideal area. These administrations incorporate helping the client to remember critical and significant exercises, for example, taking drug and help with shopping.

C. Smart Homes and Buildings

The digital physical frameworks make a home a brilliant organized home. In shrewd homes, the sensors and actuators are configured to such a degree, that they can be controlled remotely through the web. Through this, the activities of the customers can be checked. Shrewd social order takes brilliant homes further by using organizing among a get-together of savvy homes. The individual homes are exhibited as multi utilitarian sensors and at whatever point basic, modified or human-controlled physical analysis is given to improve system prosperity, social protection quality and home security. The makers moreover talk about the correspondence and systems administration in the shrewd network.

D. Gaming

The consolidation of digital physical frameworks into diversion can acquire a progressive change. For instance, a computer game with CPS upgrades the physical contributions to the game utilizing sensors. This consequently can improve clients' venture and give better comprehension of credibility. The clients wear various sensors on their body and the data gained from these sensors is shared continuously. To play this game, a client wears diverse inertial sensor center points which sense the bearing and development of the user[10]. This information is continued to the game controller which makes suitable move.

E. Energy Systems and Electrical Power Grids

A planned power and transportation foundation is utilized for propelling usage of sustainable power sources. In an electric system, computerized vulnerabilities may happen due to misguided advantages an entrance controls, powerless firewall rules, cryptographic issues, nonappearance of data acknowledgment and so forth. Resulting to perceiving these, the physical impact of ambush on control applications can be settled using transient and suffering state multiplications [11]. In perspective on this, the danger mitigation steps can be settled. Digital Physical Systems address the issue of distinguishing the smallest course of action of exposed meters in a power structure, which when attacked, lead to network being un-operational.

IV. SECURITY AND POTENTIAL THREATS TO CPS

The objectives of Cyber Physical Security Systems are as follows:

A. Availability

High availability of a Cyber Physical System refers to continuous offering of services by resisting controls and processing because of failure of equipment, upgradation of systems and blackout of controls.

B. Authenticity

It becomes necessary to ensure that the communication and computation process enables legitimate exchange of information as well as the parties involved in the communication process is authentic. In Cyber Physical System, the authenticity expects acknowledgment of confirmation of all processes like detection, interchange, etc.[13]

C. Integrity

Integrity of a cyber physical system makes sure that the data or assets cannot be changed without approval. When an invader alters or erases information unintentionally or with malicious desire, it leads to a breach in the integrity. This breach can lead to incorrect information being sent[12].

D. Confidentiality

Preventing unauthorized parties from accessing the information is referred to as the confidentiality

Some Threats to a CPS are as follows:

1) Man-in-the-middle Attack

In this assault the communication between two parties can be monitored and altered by an unauthorized party. It can lead to an unrequited actions being performed or the required action not being performed[14].

2) Eavesdropping

This is a passive attack where the information being transmitted is intercepted by the attacker. A Cyber Physical System is extremely prone to eavesdropping. User’s privacy is hampered by eavesdropping.

3) Denial-of-service Attack

Now and again legitimate solicitations made by the framework to get to the system assets are halted from being handled. This assault can be Denial-of-service attack. It involves transmission of large amount of data to keep the system pre occupied and over burdened [15].

This leads to irregular and uneven transmission of data which can lead to loss of critical information.

V. CPS SECURITY MODELS

There are 4 most popular classes of models for risk evaluation and administration for Cyber Physical Systems:

A. Expert Elicited Models

These models remembers computational models to review chance ward for expert elicited distinctive evidence and depiction of cyber system characteristics, for instance, network data streams and the estimation of the weakness of those benefits and data streams to different sorts of deal. This procedure has basic interest for certain, applications, including cases including tangled networks for which little structure information is immediately available and cases in which a decently quick examination is required. One critical impediment of this strategy is nonappearance of completeness.

B. Game Theoretic Models

This model undeniably addresses the resemblance of assailants and shields. The compositions are fundamentally

increasingly moved and the strategy is altogether less made than the expert evoked. A distorted cyber experience between an attacker and a protector (security engineer) can be depicted by a problem between two players who both have total data about the cyber system and their foe. The sound moves of the two players are all around depicted by saddle-points once the expenses and grants are portrayed over each game technique [16].

C. Attack Graphs

This method advocates advancement of attack trees or graphs, either by hand or through modernized interrogation of a plan of interest. This procedure has various inclinations. Central is a light information need. Compositions in this class don't endure exactness or consistent quality weaknesses since they are become direct from system information without reflection or accumulation [16]. Additional incredible circumstance of this strategy is flexibility.

D. Stochastic Games

This system fuses stochastic games on different frameworks, making an altogether progressively unbelievable and besides troublesome methodology [16]. This model impels subject to strikes diverging from the framework screen measures dislodge abuse unequivocal advances.

Security frameworks are valuable for evaluating danger. Measurements are depicted as measurable quantities of a structure that assess what sum central purposes of the framework are penetrated. Measurements can outfit mechanized defenders of this system with central encounters concerning the structure. Measurements are generally snatched by breaking down material qualities of that particular system.

VI. FUTURE SCOPE

CPS is revamping the way humans interconnect with physical systems which is very identical to the way internet has altered the way humans communicate to one another. Many countries have started taking an initiative to aide the use of CPS by incorporating them into industries like, Aerospace, Healthcare, Manufacturing and Agriculture. All these operations require advanced data processing capabilities which are provided by technologies like Internet-of-Things and Big Data Analytics [18]. IoT aims to give, a tether-free and related data the officials organize with real-time spilling and dealing with limits. Such framework gives capability to a CPS to put in use Big Data Analytics to a good use for the evolution of data.

In the subsequent times, resilient compatible CPS designs are needed. These systems should enable smooth integration of the hardware and software features which can be refurbished or moulded as per the new advancements in the CPS. Since reliability and security are two crucial threats to CPSs, we require all these elements to be more complex with better tools, frameworks and algorithms to ensure no breach.

VII. CONCLUSION

Cyber Physical Systems provide synchronization between physical and computational resources in a technology based environment and therefore they're supposed to contribute in an vital manner in the planning, progress and success of the smart homes, smart grids, autonomous vehicles etc. the objective of this paper is to instill knowledge about the Cyber Physical Systems by discussing its working mechanism, the application areas and the security challenges that come into the picture with the implementation of the cyber physical systems. The implications of the cyber physical systems in the field of Smart Grid Utilities and Enterprise Cloud have been discussed in detail. We have also discussed some security models that are currently being used to overcome the security threats to the cyber physical systems. Overall this paper help in development of infrastructure support needed for developing the mechanism of Cyber Security. Additionally this paper will help in understanding the capabilities and challenges of a Cyber Physical System and help in arriving at solutions that address the possible dangers to the Cyber Physical Systems.

REFERENCES

[1] N Bott and et al, "Cloud Computing Architectures for the Underserved: Public Health Cyber infrastructures through a Network of Health ATMs," in the proceedings of 43rd Hawaii International Conference on System Sciences (HICSS), Hawaii, USA, Jan 2010, pp.1-10

[2] Jayavardhana Gubb and et al: " Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", Future Generation Computer System 29(7): 1645-1660 (2013)

[3] Olson, M., Chandy, K.M., "Performance Issues in Cloud Computing for Cyber-physical Applications ", *IEEE International Conference on Cloud Computing (CLOUD), 2011*

[4] E. Amoroso, " Practical Methods for Securing the Cloud," *IEEE cloud computing, May, 2014, pp. 28-38*

[5] Lincoln D. Stein, " The Electronic Medical Record: Promises and Threats", *Web Journal, Volume 2, Issue 3*

[6] M. A. Faisal, Z. Aung, J. R.Williams and A. Sanchez, "Securing Advanced Metering Infrastructure using Intrusion Detection System with Data Stream Mining", *PAISI 2012, Springer Verlag Kualalumpur, Malaysia, May 2012, pp. 96-111*

[7] Nidhi Chandra, Sunil Kumar Khatri, Subhranil Som, (2018) "Cyberbullying Detection using Recursive Neural Network through Offline Repository", 7th International Conference on "Reliability, Infocom Technologies and Optimizations (Trends and Future Directions) ICRITO 2018, Published **IEEE Xplore:** 01 July 2019, **DOI:** 10.1109/ICRITO.2018.8748570, 29-31 August 2018, IEEE Conference, Amity University, Noida, India.

[8] Ye Yan et al. " A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges", Communications Surveys & Tutorials, *IEEE, Volume 15, Issue 1*

[9] Vaibhav, Sunil Kumar Khatri, Subhranil Som, (2018) "Intrusion Detection System Providing Security with Machine Learning Technique", 7th International Conference on "Reliability, Infocom Technologies and Optimizations (Trends and Future Directions) ICRITO 2018, Presented, 29-31 August 2018, IEEE Conference, Amity University, Noida, India.

[10] Huang, He, Yan Lindsay Sun, Qiang Yang, Fan Zhang, Xiaorong Zhang, Yuhong Liu, Jin Ren and Fabian Sierra "Integrating neuromuscular and cyber systems for neural control of artificial legs" ICCPS (2010)

[11] Kottarathil Eashy, Mary Reena, Abraham Theckethil Mathew, and Lillykutty Jacob, "An Occupancy Based Cyber-Physical System Design for Intelligent Building Automation," *Mathematical Problems in Engineering, vol. 2015, Article ID 132182, 15 pages, 2015*

[12] C. Wu et al "multi screen cyber physical video game: an integration with body-area inertial sensor networks", PERCOM,2010

[13] M. Ilic et al., "Modeling future cyber-physical energy systems," *PES-GM,2008, pp. 1–9*

[14] JB.McMillin, et al, "Environmental Obuscation of a Cyber Physical System - Vehicle Example", Computer Software and Applications Conference, 2010.

[15] D. Work, A. Bayen and Q. Jacobson, "Automotive Cyber Physical Systems in the Context of Human Mobility", *National Workshop on High- Confidence Automotive Cyber-Physical Systems, Troy, MI, 2008*

[16] R. Saltzman, A .Sharabani, "Active Man in the Middle Attacks, A Security Advisory", A whitepaper from IBM Rational Application Security Group, February 27, 2009

[17] K. Pelechrinis , M. Iliofotou , "Denial of Service Attacks in Wireless Networks: The case of Jammers", UC Riverside Department of Computer Science and Engineering, 2006

[18] E. Colbert ., "Security of Cyber-Physical Systems", Journal of Cyber Security and Information Systems, Volume: 5, Number: 1, Cyber Science & Technology at the Army Research Laboratory (ARL)

[19] M. A. Lundteigen et al, "Conceptualizing the key features of cyber physical systems in a multi-layered representation for safety and security analysis," Systems Engineering, 2019

[20] Dev Bhatnagar, Subhranil Som, Sunil Kumar Khatri (2019) "Advance Persistant Threat and Cyber Spying - The Big Picture, Its Tools, Attack Vectors and Countermeasures", Amity International Conference on Artificial Intelligence (AICAI'2019); February 04-06, 2019, Published IEEE Xplore: 29 April 2019, DOI: 10.1109/AICAI.2019.8701329, Amity University Dubai, UAE.

[21] Celiktas,et al. "Overview of Cyber Physical Systems In Future Production". Conference: Ulusal Mühendislik Araştırmaları Sempozyumu (UMAS'15), At Duzce (2015)

[22] Walia, H., Rana, A., Kansal, V., "Word sense disambiguation using unsupervised approach applied on Punjabi language" in International Journal of Advanced Science and Technology, Vol 28, No 20, pp 183-192 (2019).

[23] P. Chawla, I. Chana, A. Rana, "Framework for cloud-based software test data generation service" in Software - Practice and Experience, Vol. 49, Issue 8, pp 1307-1328 (2019).

[24] M. Bhardwaj, A. Rana, N. K. Sharma, "How software size influence productivity and project duration" in International Journal of Electrical and Computer Engineering , Vol. 9, Isuue 3, pp 2006-2017 (2019).

[25] N. Tyagi, A. Rana, V. Kansal, "Creating Elasticity with Enhanced Weighted Optimization Load Balancing Algorithm in Cloud Computing", in Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019, pp 600-604 (2019).

[26] M. Nagaraju, P. Chawla, A. Rana, " A Practitioner's Approach to Assess the WCAG 2.0 Website Accessibility Challenges" in Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019, pp 958-966 (2019).

[27] H. Walia, A. Rana, V. Kansal, "Case Based Construal using Minimal Features to Decipher Ambiguity in Punjabi Language" in Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019, pp 977-980 (2019).

[28] N. Agarwal, A. Rana, J.P. Pandey, " Guarded dual authentication based DRM with resurgence dynamic encryption techniques" in Enterprise Information Systems , Vol 13, Issue 3, pp 257-280 (2019).

[29] S. Ghosh, A. Rana, V. Kansal, "A Novel Model Based on Nonlinear Manifold Detection for Software Defect Prediction" in Proceedings of the 2nd International Conference on Intelligent Computing and Control Systems, ICICCS 2018, pp 140-145 (2019).

[30] S. Ghosh, A. Rana, V. Kansal, "Statistical assessment of nonlinear manifold detection-based software defect prediction techniques" in International Journal of Intelligent Systems Technologies and Applications, Vol. 18, Issue 6, pp579-605 (2019).

[31] H. Walia, A. Rana, V. Kansal, "Case based interpretation model for word sense disambiguation in Gurmukhi ", in Proceedings of the 9th International Conference On Cloud Computing, Data Science and Engineering, Confluence 2019, pp 359-364 (2019).