PHS Scientific House
PHARMAHEALTHSCIENCES

International Journal of Pharma Research and Health Sciences

Available online at www.pharmahealthsciences.net

Review Article

Role of Cyber Physical Systems in Health Care and Survey on Security of Medical Data

S Nithya[1,*], M Sangeetha [2], K N Apinaya Prethi [3]

[1]Assistant Professor, Department of CSE & IT, Coimbatore Institute of Technology, India.
[2]Associate Professor, Department of CSE & IT, Coimbatore Institute of Technology, India.
[3]Assistant Professor, Department of CSE & IT, Coimbatore Institute of Technology, India.

ARTICLE INFO

Received: 08 Jan 2018
Accepted: 28 Jan 2018

ABSTRACT

Cyber Physical System (CPS) are more complex systems, with co-ordination and deep collaboration between physical and cyber space. It will involve the various perspective of social and industrial life to bring larger influence and lead computer science to the higher level. CPS may be shows a discrepancy based on where it applied such as Transport, Defense, Finance, Large scale infra-structure, Process control, Smart grid and Healthcare. This Paper attempts to summarize the role of Cyber Physical System in Healthcare/Medicine (MCPS) field , focus on architecture and key challenges for securing MCPS and examinations on how to secure a medical data to improve the life of human.

Keywords: Cyber space, Physical space, smart grid, Health care, Telemonitoring.

1. INTRODUCTION

Cyber–physical systems (CPSs) as the name reveals it fuses cyber and physical world to provide support for healthcare, automotive, cloud computing, IOT, distributed networks and the list goes on. CPS gathers information from the physical world through sensors and ensure feedbacks to the systems to process the results. Their operation needs to ensure the following metrics, which are known as S3: 1) safety2) security 3) sustainability: The embedded systems through its feedback loops makes control over the physical processes and provide computational results. Now currently many

Corresponding author *
Prof S Nithya
Department of CSE & IT, Coimbatore Institute of Technology, India
Email: snithyadr@gmail.com

researchers invest their time over this CPS and it now becoming a technology boon.

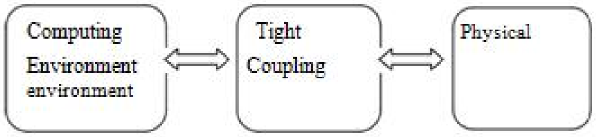

Fig 1: Cyber–physical systems, with stiff pairing between information and physical space.

SUBCATEGORY OF CPS:

CPS may be shows a discrepancy based on where it applied such as Transport, Defense, Finance, Large scale infra-structure, Process control, Smart grid and Healthcare.

Vehicular Cyber Physical Systems (VCPS) are intelligent systems in which mobile devices, smart phones and tablets communicate with the driver and assist them on driving and provide comfort. Security can be applied to the data which are transferred between server and client.

CPS plays major role in aircrafts and assist the pilot and it is major part of automatic system And CPS is also mainly used in military systems. CPS by its intelligence will ease complex tasks and also provide greater valuable efficiency and safety.

The power grid reaches lots of advancements such that it holds both power and data to the monitoring systems. These enhancements made it to perform as a smart grid with features like self-healing, adaptive protection and control over the networks. The smart grid concept has a many research areas including transmission, distribution, purchaser, markets, operations, service providers and foundational support systems. This Mechanization will lead a grid to integrated near real-time connections between advanced cyber-physical system sensors and devices. Superior communication technologies are needed to save Power, trim down costs and increase the reliability. However, cyber-physical infrastructure is the key motivating force of the expectations smart grid vision.

2. MEDICAL CYBER PHYSICAL SYSTEMS

The following section will explain the role of Cyber Physical System in health care / medical domain. (MCPS) Medical Cyber Physical Systems (MCPS) is an interconnection of medical devices and intelligent systems which helps in treatment of patients and to provide them a high availability at critical situations. MCPS is simply an embedded system for the patients controlled over the network.

Telemonitoring now becomes an important service in medical domain. It helps to provide better comfort for the patients since care is given to them at the right time of critical situations. Instead patient visiting every-time to the hospital, this telemonitoring gives support in their home itself. It is more useful for elder people, pregnant ladies and for patients with critical diseases who needs continuous monitoring. These technological improvements on MCPS assures high safety for patients. But still MCPS faces few design issues that full health of the patient depend on systems which has to human intervention. If something goes run, there will no control and leads to serious problems for the patients. This had been addressed in PDeS session held on 2015 with real time scenarios.There is drastic Technology development in control systems replacing many human activity. The placed the footprints on almost all fields like industry, automotive, security, health-care and consumer products. They are the key part of cyber physical system doing complex functions like sensing, computation and communication with the physical world. Medical cyber-physical systems (MCPS) used to monitoring and treating the patient by interconnecting several medical devices. Patients are in a need of continues monitoring and treatment when they face difficult medical scenarios. Using this system will help to achieve effective, independent and efficient result.

The goal of MCPS is to provide high safety for the patients by continuous sensing monitory analysis and ensures personalized support. However traditional MCPS system faces many design challenges. These design challenges needs to be addressed in a systematic way such as verification, validation techniques. This places effective goals for researchers to work on these challenges. The primary factor of MCPS is patient safety. New MCPS must be evaluated for its risk factors before using them for patients. Every new requirements need to be fulfilled by the system. The traditional way for approval of medical devices by Food and Drug Administration (FDA) is lengthy and expensive. This process must be made easy without giving a concern for the safety measures of those devices.

The following things to be protected to prevent the patient from physical harm (i) Data from the various devices to be prevented in order to get proper action from the care giver i.e) patient data privacy must be ensured. (ii) Device used in the process should be prevented from denial of service of devices

2.1 CRUCIAL BEHAVIOUR OF MEDICAL DEVICES

In this section we have discussed about the crucial behavior of medical devices. Consider a scenario where cancer patient under gone a radiation therapy treatment. The advanced medical technologies require largest-scale medical device systems to deliver accurate doses of radiation. Cyclotron must emits the precise amount of proton in a such way that it should take up the even minor shifts in the patient’s pose. Higher exactness of the treatment, compared to predictable radiation therapy, allows higher radiation doses to be applied. This, in turn, places more strict requirements on patient safety. Control of proton beams is subject to very tight timing constraints, with much less forbearance . To get more knowledge about the problem, the same beam is applied to patient’s body in multiple locations by switching between the locations with no or less interference between beam scheduling.

In addition to scheming the proton beam, a highly serious function of software , real-time image processing to resolve the precise position of the patient and detect any patient movement. As analyzed the safety of proton therapy machines, is concentrated on a single system, the emergency shutdown. In general, appropriate analysis and validation of such large and complex systems leftovers one of the biggest challenges is there in front of the medical device industry.

2.2 ARCHITECTURE OF MCPS

Over the past few decades the capabilities of adopting new class of devices for health monitoring system have improved significantly. Medical cyber physical systems are simply embedded network system comprising of medical devices to give dosage to the patient, sensors which acquires data for monitoring of the patients. The report generated is called Electronic Health Record (EHR) which gives patient treatment report over a period of time They are capable of predicting patient health and also able to generate alert to care givers. Care giver can analyze that information and can initiate treatment, so that patient can be cured.

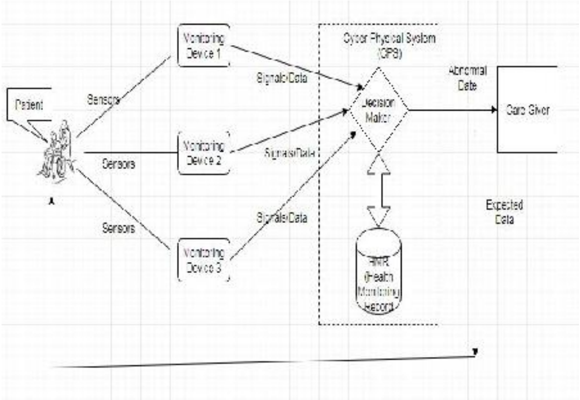

Fig 2: Role of Cyber Physical System in Health Care

2.3 APPLICATION:

Infusion Pump: A PCA is used to provide pain relievers and upon patient need it can also deliver a limited quantity of medication called bolus. These infusion pumps are primarily used for postoperative patients. Here also there is no control over the system ,if the infusion pump collapses and if some overdose is given to patient, it may lead to death also. So before using these medical devices high safety requirements must be ensured. By FDA's report more than 56,000 adverse events had occurred due to malfunctioning of infusion pumps. This clearly evident that these devices must undergo high availability tests before using for patients. This also opens a goal for researchers to work on.

DOA Monitoring: Monitoring the depth of anesthesia clinical surgery which ensures accurate amount of drug dosage to the patients. DOA is based on the analysis of the EEG or mid-latency auditory-evoked potentials. These examinations helps to give precise drugs to the patients . Anesthesia is a balance between the amount of anesthetic drug(s) administered and the state of arousal of the patient. Given that the intensity of surgical stimulation varies throughout surgery, and the haemodynamic effects of the anesthetic drugs may limit the amount that can be given safely, it is not uncommon for there to be critical imbalances between anesthetic requirement and anesthetic drug administration.

3. ISSUES AND CHALLENGES in MCPS

i) SAFETY:

Implementation of high technologies and sensors in MCPS reveals the truth that embedding these systems on human beings how much is it safe, that it won't cause any uncertain effects to them. Malfunctioning of these devices may cause hazardous impacts on them and even lead to death. In a survey conducted by U.S. FDA MAUDE in 2010-2013 it states that (88.3%) of the cases were failed only because of malfunctioning of the medical devices. Prior testing has and proper guidance of usage should be carried away before using them for health measurements.

ii) SECURITY AND PRIVACY:

Wireless sensors gather and send information to the monitoring systems. These monitoring systems diagnose huge amount of data and give analysis results to the care-givers. A high protected environment should be there to prevent attack and interference. Unauthorized access should be potentially handled with encryption standards. Disclosure of patient's data may lead to alteration and may cause severe effects to that person.so patients personal details should be privatized and stored under secure.

iii) RELIABILITY:

The care-givers rely on the devices for diagnosing patient's health status. Dislocation of machines, weather conditions, and some hardware issues may cause erroneous results. But it should not be the case as suspected. They directly influence patient next level of treatment. So the data from these devices should be more accurate and promising as per patient's health. Since these devices measure more complex and dynamic data there should be persistent maintenance and frequent performance analysis. Though the medical devices inspect patient more precisely, at all cases its not be possible to trust on systems. Manual check at last staging is necessary.

iv) CONNECTIVITY:

Medical cyber physical system is composite sensor network system. Recent advancements in MCPS potentially enabled to observe patient remotely and shoot appropriate actions regardless of the location. The data are sent to centralized server and doctors and care givers have access to the servers monitor them accordingly. However high persistent network should be established to carry away this method of inspection. All the sensors, monitoring systems and servers should be closely connected. If there is any miscellaneous happened in the network, it would generate false alarms and give wrong results. Hence Connectivity among the systems should be maintained.

v) CLOSED LOOP NETWORK:

A closed loop network enclose patients, sensors, monitoring devices, care-givers and doctors. If the care-giver doesn't monitor due to emergency are by carelessness, and unfortunately if some critical event occurs for the patient, then the report will have a huge impact. Physiological closed-loop systems have been proposed to solve this problem as shown in figure.

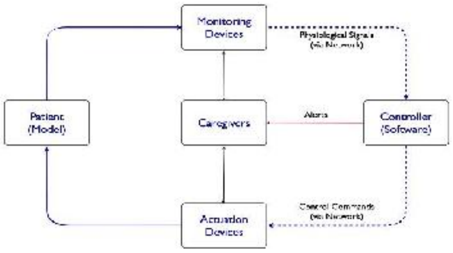

Fig 3: Closed loop system

This closed loop system builds a safe and effective control over the patient monitoring. All things must be under coordination to achieve best objective out of MCPS.

4. A SURVEY ON SECURITY

Security Mechanism usually connected with cryptography, access control, anomaly detection, authentication and many other solutions in wider field. Those mechanisms are very important in securing information and ensure the secure communication among the cyber physical systems. Weakness of security will lead the cyber

physical system into a unimaginable consequences. This section explores the existing anomaly detection method to ensure the security in CPS. Anomaly in the CPS will lead whole system into severe time delay and serious degradation of performance.

Anomaly detection is performed with the patient records which are made public .These data have anomalies due to the following reasons 1)Patient abnormality.2) Patient movements 3) Device Malfunctions and 4) Transferring errors.

Austin Jones [3] et al proposal was to develop an unsupervised learning algorithm. The main idea in this proposal is signal temporal logic (STL) formula which gives the behavior of the patient If the measurements doesn't coincide with STL formula measurements are in human readable format so that even patients will also have knowledge about the treatment. STL formulae can be used for early prediction and provide treatment to the patient in a proactive way.

Xin Sun [4] et all present a thoughts on the design of a novel hybrid system for detecting anomalous traffic in large-scale and policy-rich data networks. This approach combines static configuration analysis and dynamic traffic analytics. Initially develop the abstractions and mathematical models to properly model the network and security configurations to statically check for violation of network-wide invariants, which are potential security vulnerabilities. Then develop dynamic data analytic techniques to analyze traffic in real-time and detect anomalous traffic patterns that may be exploiting the security vulnerabilities. The results of static analysis will be used to support and guide the dynamic traffic analytics to optimize resource allocation and minimize false positives.

Vishal Sharma [5] et al proposal is based on a method called Cross Platform behavior. Users share their private data on Social networks. These data can be easily captured and used by the fraudulent. Such fraudulent are called anomalies To prevent this anomalies , cognitive tokens based solution were tried, It is an intelligent sensing model for anomalies detection (ISMA) . purposefully injecting false data to arrest the strange users.

To identify the attacks in the smart grid field a machine learning based method was proposed by Shubhalaxmi Kher [6] et al. ensuring the security and stability of the smart grid systems can be done using this method. Communication between each tower can be established in the smart gird by using cluster topology and the local information about individual towers can be collected then its processed by the linear chain topology to connect to the base station. Notification can be enabled if there is any anomalous event in WSN.

Federico Simmross-Wattenberg [7] et all method was to detect anomalies in network traffic. It based on alpha-stable first-order model and statistical hypothesis. The main concept of this paper to detect two anomaly typesfloods and flash-crowds anomalies. Receiver Operating Characteristic (ROC) curves can be used to measure the performance.

Junho Hong [8] et al proposed an integrated Anomaly Detection System (ADS) which contains host- and network-based anomaly detection. Temporal anomalies in the substation are the key factor in host-based anomaly detection. Then the automated multicast message will be generated in substation if there is any malicious activity.

Ronghua Shi et al [9] present an inarticulate traffic datasets were strictly tested by matrix-based visualization system to project the well analyzed forensics report. Which contains tri-Collaborative aspect. they are i) timeline ii) matrix vector iii) Historical view. Timeline view is used to wrap the active feature and independent dispersion which depends on information entropies. Network structure and supply of IP address should be stabilized by lend hands with matrix vector. Dynamically time slot should be compared with forthcoming slots to identify the changes in network, which can be done by using historical view.

To detect the network attack by using One-class SVM were approached by Ming Zhang et al [10].In this approach the well trained dataset are bind as secured or safety network unit. The new or upcoming event's behavior is not matches with secured unit will be kicked off and declared as unsafe network unit. This should be monitored to get out of unit attack.

Anomalies can be captured during IP traffic, to do that an Entropy-Mahalano bisbased method was initiated by J. Santiago-Paz et al [11]. In this kind of approach the feature of source IP and Destination IP were keenly observed by using balanced estimator II to build a intrinsic feature. The Ellipse were described with the hand of Mahalanobis distance which is used to find the Entropy from a group of connected devices. Through this we can analyze the time slot is either falls under normal region or abnormal regions.

An Assumption method was proposed by Yuan Chen et all [12]. Which contains 3 Assumptions? First for each information pattern should be provided with the necessary and enough tight condition for an attacker which should be untraceable. Second classify the attack based on its sustainability which means find the attack which is not traced by any attacker for long period of time. Finally construct the "Zero State attack" from the classified attack that remains dynamically untraceable nevertheless of information available to attacker.

5. CONCLUSION

In this Article, a role of cyber physical system in healthcare has been discussed and also a small survey on security of medical data has been presented. The challenges faced by Medical cyber Physical system are huge, but still it’s a vast area to research with immediate impact, some of the major issues are identified and discussed. lots of opportunities are there for Research & Development community people, if they start to solve these kind of challenges.

6. REFERENCES

1. Insup Lee, Oleg Sokolsky, Sanjian Chen, John Hatcliff, Eunkyoung Jee,” Challenges and Research Directions in Medical Cyber Physical Systems”, 1-2012.
2. Nutjahan, Farhana Nizam, Shudarshon Chaki, Shamim Al Mamun, M. Shamim Kaiser, “Attack Detection and Prevention in the CyberPhysical System”, (Ieee] - 2016), Jan. 07 - 09,2016.
3. Austin Jones, Zhaodan Kong, Calin Belta, ‘Anomaly Detection in Cyber-Physical Systems: A Formal Methods Approach, IEEE Conference on Decision and Control December 15-17, 2014.
4. Xin Sun, Fu-Shing Sun, “A Hybrid Approach to Detect Traffic Anomalies in Large-Scale Data Networks”, Conference on Computational Science and Computational Intelligence, 2016.
5. Vishal Sharma, Ilsun You, Ravinder Kumar,” ISMA: Intelligent Sensing Model for Anomalies Detection in Cross Platform OSNs With a Case Study on IoT”, Intelligent Sensing On Mobile And Social Media Analytics,2017
6. Shubhalaxmi Kher, Victor Nutt, Dipankar Dasgupta, Hasan Ali, Paul Mixon, “ A Prediction Model for Anomalies in Smart Gri withSensor Network”, ACM 978-1-4503-1687-3.
7. Federico Simmross-Wattenberg, Juan Ignacio Asensio-Pe´ rez, Pablo Casaseca-de-la-Higuera,Marcos Martı´n-Ferna´ndez, Ioannis A. Dimitriadis, ”Anomaly Detection in Network Traffic Based on Statistical Inference and _-Stable Modeling”, IEEE Transactions On Dependable And Secure Computing, VOL. 8, NO. 4, JULY/AUGUST 2011.
8. Junho Hong,Chen-Ching Liu, Manimaran Govindarasu, “Integrated Anomaly Detection for Cyber Security of the Substations” , IEEE Transactions On Smart Grid, VOL. 5, NO. 4, JULY 2014
9. Ronghua Shi, Mengjie Yang, Ying Zhao, Fangfang Zhou, Wei Huang, and Sheng Zhang, “A Matrix-Based Visualization System for Network Traffic Forensics”, IEEE Systems Journal, VOL. 10, NO. 4, DECEMBER 2016
10. Yuan Chen, Soummya Kar, and Jos´e M. F. Moura,” Dynamic Attack Detection in Cyber-Physical Systems with Side Initial State Information”, IEEE Transactions on Automatic Control.
11. Emeritus Professor Ioan Dumitrache,” Cyber-Physical Systems in Healthcare Networks”, The 5th IEEE International Conference on E-Health and Bioengineering ,EHB 2015
12. Ovunc Kocabas, Tolga Soyata, and Mehmet K. Aktas,” Emerging Security Mechanisms for Medical Cyber Physical Systems”, Ieee/Acm Transactions On Computational Biologyand Bioinformatics, VOL. 13, NO. 3, MAY/JUNE 2016.
13. Tingshan Huang, Harish Sethu and Nagarajan Kandasamy,”A Fast Algorithm for Detecting Anomalous Changes in Network Traffic”.
14. J. Santiago-Paz, D.Torres-Rom´an and P. Velarde-Alvarado,” Detecting Anomalies in Network Traffic Using Entropy and Mahalanobis distance”.
15. Robert Mitchell, Ing-Ray Chen,” Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical CyberPhysical Systems”, Member, IEEE.
16. Manasi Kadam, Bhagyashree Patle,” Survey on Secure Medical Cyber Physical System Based on Behavior Rule Specification”.
17. Paul Bogdan, , Rahul Mangharam, ,” Cyber-Physical Systems for Medical Applications”, IEEE Design Special Issue, Publication September/October 2015.& Test date:
18. LuFeng, Andrew L. King Sanjian Chen Anaheed Ayoub Junkil Park ” A Safety Argument Strategy for PCA Closed- LoopSystems: A Preliminary Proposal”.
19. Jonathan Goh, Sridhar Adepu, Marcus Tan and Lee Zi Shan,” Anomaly Detection in Cyber Physical Systems using Recurrent Neural Networks”, 2017 IEEE 18th

International Symposium on High Assurance Systems Engineering (HASE).

20. Arnab Ray, Rance Cleaveland," Security Assurance CasesforMedicalCyber–Physical Systems".
21. Riham altawy and amr m. Youssef," Security Tradeoffs in Cyber Physical Systems:A Case Study Survey on ImplantableMedical Devices", IEEE ACCESS,2016

Conflict of Interest: None
Source of Funding: Nil