Wireless Personal Communications (2022) 122:1413–1433
https://doi.org/10.1007/s11277-021-08955-6

Smart City Healthcare Cyber Physical System: Characteristics, Technologies and Challenges

Rupali Verma[1]

Accepted: 9 August 2021 / Published online: 26 August 2021

Abstract
The recent pandemic has demanded a strong and smart healthcare system which can monitor the patients efficiently and handle the situation that arises from the outbreak of the disease. Smart healthcare cyber physical systems are the future systems as they integrate the physical and cyber world for efficient functioning of medical processes and treatment through external monitoring and control of patients, medical devices and equipment for continuous communication and information exchange of physiological data. Technologies like Internet of Things, Machine learning and Artificial Intelligence have given birth to smart cyber physical systems like Smart Healthcare Systems, Smart Homes, Smart Vehicular Systems and Smart Grid. Such systems are interdisciplinary in nature with multitude of technologies contributing to its effective working. This paper presents a case study on healthcare cyber physical systems presenting its characteristics, role of various technologies in its growth and major challenges in successful implementation of cyber physical medication systems.

Keywords Artificial intelligence · Healthcare cyber physical systems · Symbiotic cyber physical systems · Security

1 Introduction

In the current pandemic, a strong healthcare system is a backbone for any smart city. Effective and efficient monitoring of patients together with regular supply of necessary medicines and treatment with aid of medical devices is possible when a system can meet the demand and supply situation. Such a scenario is possible with a predictive mechanism which forecasts the healthcare situation and works smartly for handling the medical emergency.

Smart Healthcare Cyber Physical Systems (SHCPS) are the future systems capable of supporting the medical fraternity in handling the pandemic situation effectively. Such systems comprise of physical world of patients, medical devices and equipment; externally controlled and monitored medical treatment, connected with cyber world through

✉ Rupali Verma
rupali@pec.edu.in

[1] Computer Science and Engineering, Punjab Engineering College, Chandigarh, India

communication networks for data transfer and information exchange of physiological data which are analysed for feedback and control signals. Such systems improve the quality of medical care by providing efficient and smart services [1].

The design and development of healthcare cyber physical systems have brought some open issues for discussion like autonomy level, security and reliability which are vital for healthcare cyber physical systems.

1.1 Autonomy Level

Cyber physical systems can be classified from low to high level of autonomy based on the tasks performed by the humans in the loop. Technologies like machine learning and artificial intelligence play a major role in shifting the control from human to machine and artificial distributed networks [2].

Various factors that are crucial in defining the autonomy level in healthcare cyber physical systems (HCPS) are broadly categorized into two domains.

- *Equipment based* Factors like the medical device type, interaction type and duration with the patient are deciding factors for autonomy level. Medical robots for serving food and medicines to coronavirus patients can work autonomously for assisting the Medicare systems. The team of researchers from Hong Kong have created a humanoid robot called 'Grace' for interacting with isolated coronavirus patients and provides services like temperature recording and responsiveness through the thermal camera fitted in the chest. The robot will also socially interact with the coronavirus patients in order to prevent the stress arising from isolation [3].
- *Patient related* Patient related factors include the disease type and patient risk level. Communicable diseases like coronavirus necessitate high level of autonomous Medicare cyber physical systems whereas high patient risk level require continuous medical expert support along with the autonomous Medicare systems.

1.2 Security Mechanisms

A number of technologies play a vital role in the cyber physical system which can be classified into distinctive areas ranging from data collection with sensor technology and IOT; handling big data and its storage with Cloud computing; data analytics and decision making using artificial intelligence; control and coordination signals to smart machines and actuators thus leading to the commencement of new era termed by Industry 4.0 [4] and specifically Healthcare 4 for medical applications. A comprehensive security mechanism for authenticated, confidential and secure communication between cyber and physical world forms an integral part of framework during the design and development of cyber physical systems. The criticality of healthcare applications with high levels of autonomy demands a preventive approach for defence against cyber-attacks [5] and thus the Healthcare Cyber physical systems must incorporate the following in their security mechanism:

- Identification of cyber-attacks on sensors.
- Lightweight cryptography for transmitting physiological data.
- Encryption mechanisms and Blockchain technology for secure storage on cloud-based systems.
- Encrypted feedback signals to actuators.

The data transmitted from patients to medical expert is vulnerable to attacks and hence requires encryption techniques at the client end. Many cryptographic techniques exist in literature, the broad classification is symmetric cryptography and asymmetric cryptography. Biological cryptographic approach based on amino acid codes [6] is used for transmitting the data from patients to healthcare experts in telemonitoring healthcare system.

1.3 Reliability

Reliability is an important metric for cyber physical systems and of utmost significance to healthcare industry. Figure 1 shows the reliability of healthcare cyber physical systems (HCPS) which is dependent on hardware units like health sensors and actuators, software reliability on software systems computing patient's health status, and network reliability determined by communication networks for transfer of patient data.

The commencement of cyber physical systems requires optimization of resources and self-adaptive behaviour for efficient, reliable and improved services [7]. The autonomous systems must be able to identify the failure of different components in the closed loop system and take corrective measures in terms of handling the tasks. Self-adaptive components of cyber physical systems learn from the past data and behave in the current scenario. Smart machines like healthcare robots can self-organize to dynamic environment to meet the challenge of service quality.

This paper highlights the following:

(i) Characteristics of healthcare cyber physical systems
(ii) Amalgamation of technologies that have contributed to the growth and implementation of healthcare cyber physical systems.
(iii) Real time challenges which prompt the researchers, healthcare and manufacturing sector to retrospect and consider during design and effective execution of healthcare cyber physical systems.

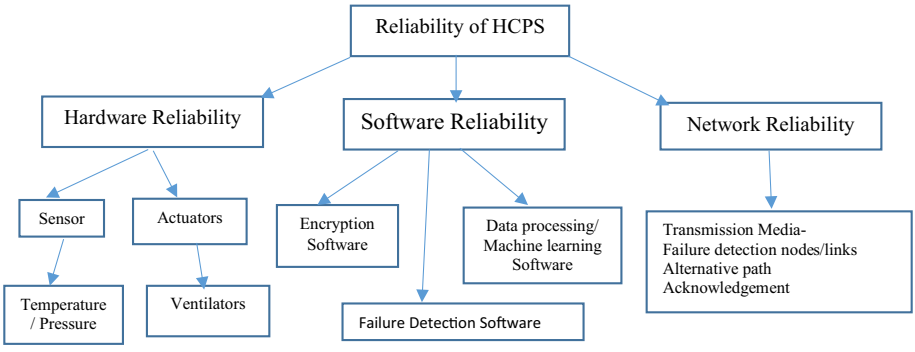


Fig. 1 Reliability of HCPS

2 Cyber Physical Systems

The need for continuous communication, control and collaboration for efficient and effective systems for quality of service has brought a new era called Industry 4.0 that introduces cyber physical systems. The term cyber physical system was first coined by Helen Gill at NSF in US in the year 2006. A cyber physical system integrates cyber and physical world with sensors, which act like data collectors to gather information like temperature, pressure or speed/activity time for transmission to cyber world for storage in servers. This data is further processed and analysed to act as stimuli for control and coordination signals to actuators thus forming a closed loop system as shown in Fig. 2.

The systematic design and modelling of cyber physical systems play a key role in defining the architecture of the system with various software and hardware components, the functional roles of each component; and the communication and control mechanism between cyber and physical space. Thereafter, the simulation of the design with well tested and validation strategies are applied for final adoption of the model in the real time setup [8]. Unlike the conventional approach to design and deployment, the authors in [9] suggest a shift from design to runtime and implementation phase for critical decisions, which depend on real time inputs and environment. Table 1 presents the various CPS simulation software and their characteristics, which can be used to test various concepts of modularity, scalability and complexity of cyber physical systems in the application domain.

Some systems have a symbiotic relationship between physical world and virtual world giving rise to a new term "symbiotic cyber physical systems" [14]. The term symbiotic relationship has arisen from biology where two organisms benefit from each other and such a relationship is symbiotic in nature. Smart Grid is a perfect example of symbiotic cyber physical system where technology drives to generate energy smartly and the energy is the source of power for the technology elements in the cyber physical system. The smart healthcare cyber physical systems are symbiotic to various autonomous systems as shown in Fig. 3. Smart grid, smart home, smart vehicular systems, smart hospitals and smart manufacturing units provide services for a smart city healthcare system. In turn, the smart city healthcare system provides healthcare to its inhabitants. These inhabitants or humans are working in various organizations and manufacturing units, thus providing their service or role in various autonomous units. To define the precise role of humans in the autonomous CPS systems is a big and challenging task. An effective approach in this direction is to

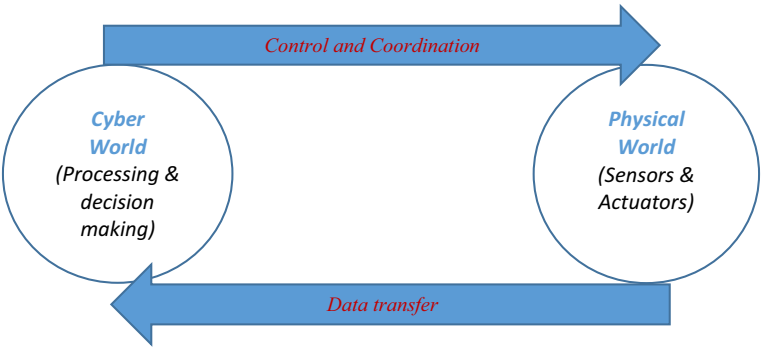


Fig. 2 Cyber physical world with closed loop

Table 1 Simulators for modelling cyber physical systems

Refs.	Simulator	Characteristics	Application in healthcare domain (CPS for coronavirus)
[10]	COSSIM	Open-Source Framework, Ultra-Fast Simulations, simulates software (multicore processors) and hardware components (FPGA devices), Integrate with network and power simulators, more accurate power estimations	The simulation software can model and estimate the power of various medical devices used in coronavirus treatment
[11, 12]	Modelica	Open-source software, Modelica language to model complex CPS and equation modelling for physical elements, real time simulation with event-based triggers, task scheduling based on fixed priority and deadline-based policies, represent network communication with real time issues like noise and delay	It can model the treatment process of patients with identification of equipment need for patients based on their health parameters, Model the clusters of people based on their location tapped through mobile phones for study of transmission rate
[13]	Hybrid	Dymola or MATLAB-Simulink for model and simulation of plant process, Open-source environments like NS-3 or commercial environments like OPNET for simulation of communication network and event-based control in Colored Petri Net	Simulation of communication networks for estimating network reliability and efficient delivery of health status from patients at remote site

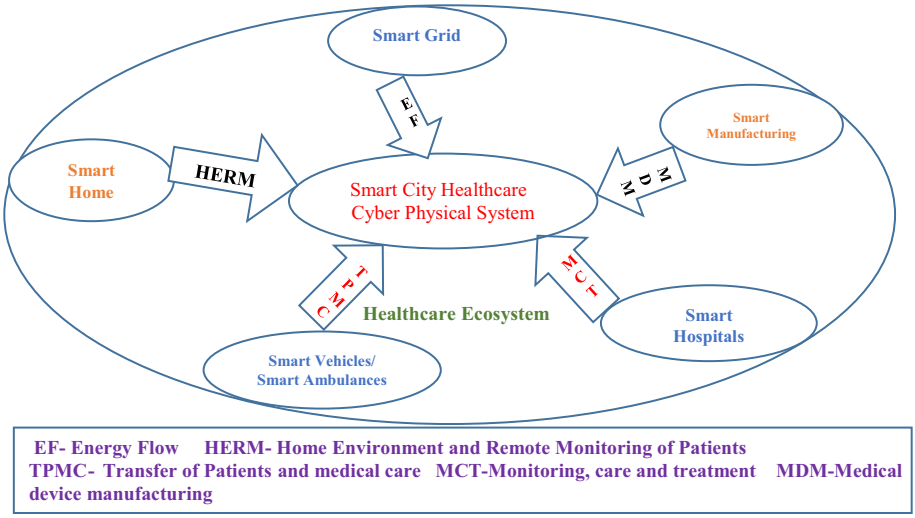


Fig. 3 Smart city healthcare cyber physical system

identify the control strategies and interactions of humans in the closed loop CPS at early stages of software development and thereafter, validate through fast prototyping techniques [15].

The cyber physical systems differ in terms of their characteristics like autonomy level which determine the tasks controlled and operated by humans, scale which depends on the number of devices connected and risk management which depends on the critical environment of the system. Table 2 presents the various applications areas, characteristic features, technologies and services provided by the CPS in different domains in face of the various security risks and challenges.

3 Characteristics of Smart City Healthcare Cyber Physical System

Healthcare Cyber Physical Systems can be divided into various levels:

- Unit level HCPS
- Integration level HCPS
- System level HCPS
- Acceptance level HCPS
- Evolutionary level HCPS

Unit level HCPS are basic or the first level of healthcare cyber physical systems which provide monitoring and control of patients in intensive care units or at the hospital level. At this level it continuously monitors the physiological parameters like temperature, pressure, heart rate etc. of the patients and feed the data to the intelligent systems which analyse and control the health actuators connected to the patient. Also, the health staff is in the HCPS loop for support and information to health experts for immediate healthcare aid to the patients.

Table 2 Cyber physical systems

Application area	Characteristics	Technologies	Services	Security/risks/challenges
Healthcare 4.0 [4]	Wearable devices, IOT of medical devices	Data analytics on patient's data	Telemedicine, Robotic surgery, Mobile health	The accuracy of sensors and other monitoring devices is a big challenge as it determines the medication level
Manufacturing unit [4, 16–18]	Smart machines like robots, Smart product	Machine to machine communication	Autonomous machines in production process, Self-organizing capability of smart machines, Detection and management of industrial hazards, Node failure detection through similarity ie pattern matching	Delays above some threshold value lead to disruption of manufacturing cycle Malfunctioning of nodes
Smart home [19–21]	Cameras, temperature sensors Smart televisions, smart locks, smart lights, smart switches and smart meters	Remote controlling of home devices	Reduce power consumption, Detect and classify safety hazards, Remote health management and emergency services	Attack on privacy of residents by gathering data like user initiated and device actions Local network attacks by bringing devices close to vicinity of home
Smart vehicles Autonomous [22, 23]	Cameras, sensors, Vehicle states	Sensing technology for obstacle detection, Navigation trajectory under control of software, Prediction mechanism to determine motion of other vehicles, Proactive mechanisms for fault detection and management	Stable vehicle movement with continuous monitoring of vehicle health, Lane detection and emission control mechanisms	Software defects Difficulty in integration of diagnostic tools in framework

Table 2 (continued)

Application area	Characteristics	Technologies	Services	Security/risks/challenges
Smart grid [24]	Power line, Communication line, Sensors, Actuators, Smart meters	Remote control and monitoring of electrical components in grid, Distributed energy resources act as microgeneration units, Distributed renewable energy generation Big data analytics on power generated and usage, Prediction and recommendation using machine learning techniques	Reliable delivery of power with energy storage at large scale, Energy conservation with reduced loss and greenhouse emissions	Vulnerable to cyberattacks affecting public life due to dependency on power for running of appliances at home and equipment in professional sector

Integration level HCPS are the second stage of HCPS where the hospitals integrate with smart homes to provide remote monitoring and remote healthcare service to the patients. In case of transfer of high-risk patients in ambulances to hospitals, the latter can integrate with smart ambulances to continuously monitor the patient's health status and make necessary emergency services in hospital like availability of bed, ventilator support etc.

System level HCPS are the third stage of HCPS where different autonomous systems support the HCPS to form a Smart City Healthcare Cyber Physical System. The smart grid, the powerhouse of energy and backbone for various cyber physical system together with smart home, smart ambulances, smart hospital manufacturing units and smart hospitals form a healthcare ecosystem providing quality of healthcare service to the patients.

Acceptance level HCPS is the level of HCPS where the researchers, technologists, engineers, health experts, academicians coordinate to make the healthcare system effective with policies and standards oriented towards successful implementation of the healthcare ecosystem.

Evolutionary level HCPS is the ideal future HCPS systems which have properties of self-adaptability and self-management. Self-adaptive components of cyber physical systems learn from the past data and behave in the current scenario. Hence, the role of evolutionary behaviour is critical and of significance for the dynamic environment of cyber physical systems.

The Cyber Physical System has physical components and processes which can be represented by a **state diagram and different states**: healthy, unhealthy, critical and non-working state as shown in Fig. 4. The overall health of the CPS depends on the working conditions of different components in the closed loop system [25].

The nature of devices in CPS is **heterogeneous** which range from sensors, actuators to physical machines controlled by external inputs like mobile devices at dew layer and systems at cyber level. The input and output of data of various devices differ in the data formats, which may be structured/unstructured in nature, which necessitate the conversion of formats through interfaces [16]. The healthcare cyber physical systems are application

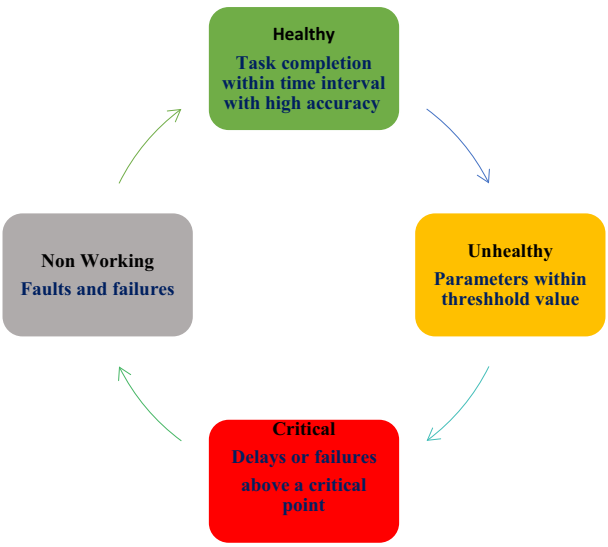


Fig. 4 State diagram of cyber physical system

domain where time is a critical factor in determining the performance and reliability of the system. A delay in seconds or microseconds in medication to patients can reduce the effectiveness and dependability of the system.

Cyber physical systems are monitored and controlled continuously for effective operation and hence this gives rise to a new term called health-monitoring system (HMS) for CPS [25]. HMS can perform dual function: to check the status of each physical component in CPS and to apply pre-emptive approach in determining probabilistic health of CPS. Study of behavioural models of physical components is a passive monitoring approach where as a stimulus-based response is an active strategy to determine for anomaly detection [25].

Based on the above characteristics, the unit and the integration level of HCPS are analysed in terms of characteristics of CPS in Table 3.

Section 4, presents the role of various technologies in seamless monitoring the time critical domain with heterogeneous devices in cyber physical systems where each state is defined by a set of variables. The technologies play a crucial role in defining the health of the system.

4 Technologies in Healthcare Cyber Physical Systems

The recent pandemic has put an unprecedented pressure on the healthcare system of any city in the world and long working hours of medical experts and health workers. Hence, the future healthcare systems demand Smart City Healthcare Cyber Physical Systems where technology plays a significant role in its successful implementation. Cyber Physical Systems is an application domain where there is integration of plethora of technologies for smart and efficient working of interconnected devices. Internet is the backbone for communication in cyber physical systems and is primarily the most crucial technology and enabler for other technologies like IOT, cloud computing and blockchain [4]. This section presents the role of various technologies like digital twin, IOT, big data, cloud computing, blockchain, artificial intelligence, machine learning and robotics in the field of healthcare cyber physical systems as shown in Fig. 5.

4.1 Digital Twin

Digital twin as shown in Fig. 6 is a virtual twin for a physical object or a process. In smart healthcare systems, the digital twin creates virtual assets in cyberspace so that the digital information of resources can be used for planning, control and coordination [27]. Digital twin for SHCPS is basically a simulation model for medical devices and equipment, and for behavioural analysis of patient treatment process to assist the health care experts to study, analyse and predict the health status of patients.

The digital twin maintains a resource graph for various medical equipment which is stored as a three-tuple vector represented by {resource id, allocation status, patient id}. The allocation status be busy or idle and expected reallocation may depend upon the patient health. The patient treatment process can be represented by a graph where the nodes represent the health status at different intervals of time and the edges represent the transition based on change in physiological parameters. These graphs can be used for machine learning for computation and classification of patient's health status.

Table 3 Characteristics of unit and integrated level of HCPS

Level of health CPS	Characteristics			
	State transition & state diagram	Heterogeneous devices/data formats	Time critical applications	Seamless monitoring & control
Unit level	Healthy working state of all sensors and actuators in smart hospitals as patients are in risk zone Therefore, early replacement of faulty medical devices	Medical application interfaces to deal with heterogeneous data	Time critical and requires efficient decision making	Regular monitoring and control in Smart hospitals
Integration level [26]	Healthy state depicts good working condition, Smart ambulances periodically checked for working condition of its medical devices and connectivity, Coordination and communication for integration of different autonomous systems for healthy working state, Requires continuous monitoring for failure detection of nodes and links	Audio, image and video (behavioural) analysis, Different autonomous systems connected require medical API's to deal with heterogeneous data sets	Home monitoring is not time critical whereas monitoring of patients during transit from home to hospital in smart ambulance is time critical	Monitoring and control of elderly patients Reminder systems Wearable sensors

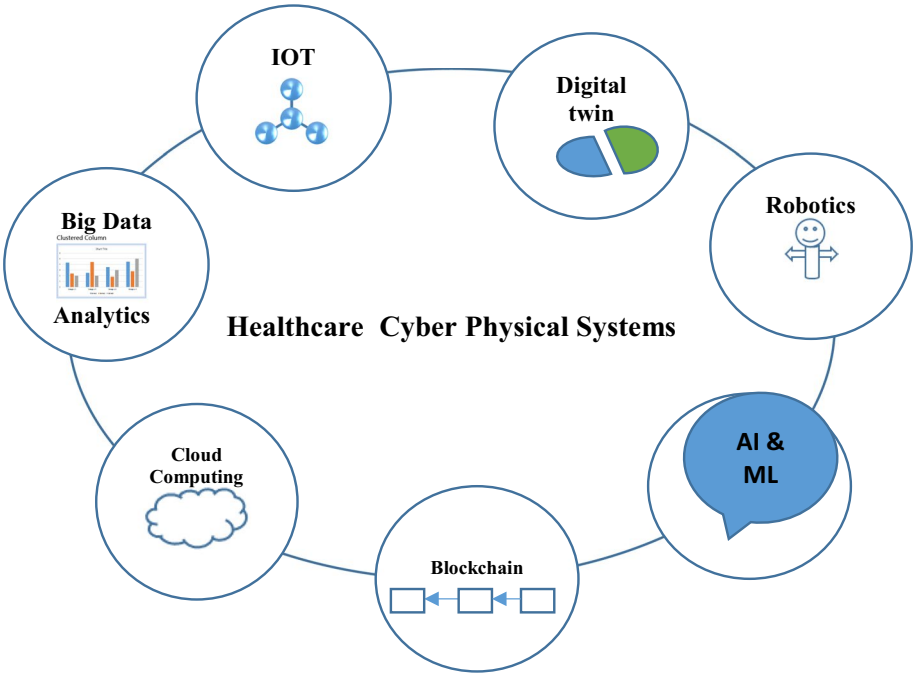


Fig. 5 Technologies in healthcare cyber physical systems

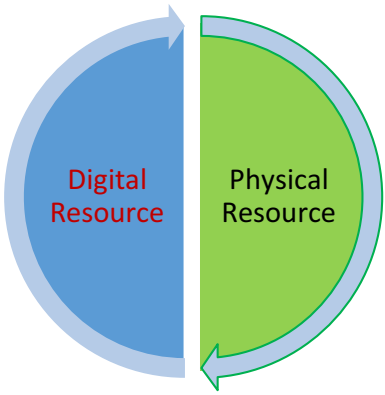


Fig. 6 Digital twin-virtualization in cyber space

4.2 Internet of Things (IOT)

The Internet of Things brought a new era of machine-to-machine communication [4] which can be through wireless networks, Bluetooth and other technologies like Near Field Communication, radio communication etc. The IOT enables in integration level smart healthcare cyber physical systems where the sensor networks generate high volumes of data which are then transmitted to remote servers for analysis and control operations. Since some devices in Medical IOT are resource constrained in terms of processing power and memory therefore lightweight authentication and lightweight cryptographic schemes are

essential for integrity and confidentiality of data and information exchange. The Medical IOT has helped in recent pandemic in remote monitoring of patients [28, 29] through smart wearables like smart watch and smart band to collect patients heart rate and blood pressure; and smart thermometers to measure body temperature. These devices are connected to smart phones, which ultimately send the data to the cloud servers for health analytics.

4.3 Big Data Analytics

In healthcare cyber physical systems with IOT of Medical devices, machine to machine communication among heterogeneous nodes and sensors capturing data continuously lead to large data sets which may be structured, unstructured or semi structured and hence require storage, processing and analysis for medical advice. The big challenge is to deal with unstructured data, complexity and veracity issues. The new computing paradigms with high processing power and big data technologies enable to extract hidden patterns and relationships in large amount of data which are gathered from various sources in healthcare cyber physical systems.

The pandemic has led to regular check-up of physiological parameters like temperature, pressure, heart rate so that the symptoms could be easily predicted. The different type of data generated related to coronavirus are the human physiological parameters like temperature, pressure, heart rate; the hospital data which include current corona patient intake, patient health status, facilities available like number of beds, ventilators; the city data like the number of residents currently corona infected, number of patients healthy, number of corona deaths, number of residents vaccinated. The researchers and analysts are interested in survey of spread and predictive analysis for future effect. High end computing devices and deep learning models enable to work on large datasets and identify these hidden patterns. These hidden patterns can be unlocked using statistical, machine learning and deep learning techniques.

The complexity and uncertainty of real world data generated in real time systems like healthcare CPS can also be dealt by methodology based on computational intelligence which includes fuzzy logic approach based on approximation techniques and fuzzy rules for decision making and inferences; evolutionary algorithms like genetic programming and swarm intelligence for natural selection; and artificial neural networks which have many hidden layers with neurons, mimic human brain and trained on large data sets to set the learning parameters for pattern recognition, prediction and classification of data sets [30].

4.4 Cloud Computing

Healthcare data silos are medical information of patients at discrete locations which may be redundant or non-coherent based on data management strategies. Cloud computing is a computing paradigm that provides infrastructure, resources and services to end users on pay per use basis where the cloud servers provide data storage and computing power to users. In healthcare cyber physical systems, the Electronic Health Records can be digitally stored in encrypted format at the cloud server so that it can be shared and accessed by the different entities like patients, hospital management, insurance companies and banks [31]. The challenging issue is to ensure safety of patient records which depends on the security framework adopted for safeguarding the key generation centre that maintains private keys of all authentic users [31].

Besides the storage of encrypted data in cloud servers, industry 4.0 standards have defined new service models for cloud manufacturing like control as a service, machinery as a service and industry automation as a service [4]. These new cloud-based models can be applied for hard real tasks with fog computing resulting in service closed to end users with efficient real time communication in information transfer and control between the healthcare level and controllers.

4.5 Dew Computing

The cloud architecture provides services which can be enhanced by edge/fog computing paradigm, a distributed service architecture which improves the efficiency of cyber physical systems by reducing the transmission delay of services provided by cloud model. Dew computing further reduces the delay and provides energy efficiency by introducing another level with smart interfaces or smart devices closer in network to IOT devices as compared to edge devices. These smart systems provide processing capabilities, work on data from physical components, control the actuators and have additional technology benefits of scalability and resilience [32]. The Dew computing layer is very useful for providing services in healthcare domain [33] where the patients can be monitored more effectively by providing processing and analytic services close to monitored area. A dew computing architecture with IOT devices; sensors and actuators in first layer; smart devices like smart phones and tablets in second layer called the dew computing layer; storage systems and network equipment in edge device layer; cloudlets and servers at fourth layer called edge server layer which represents the edge or fog computing distributed service and finally the fifth layer with cloud servers providing various infrastructure and software based services[32]; can be very time efficient for healthcare domains. The lightweight applications on tablets and smart phones in Dew computing paradigms can share patient information and are interoperable which helps in collaboration with other systems to be a part of healthcare cyber physical system of systems.

4.6 Blockchain

Blockchain technology provides a decentralised and distributed database for secure and authentic access to electronic health records maintained by cloud servers [31]. It provides a decentralised platform for maintaining untampered records of events [4] for various medical transactions that may be at device level or vaccines; and events at patient level. The blockchain is defined by a chain of blocks, each with a number of transactions or communications which are hashed and structured by a Merkle tree. Each block is identified by a hash value and contains the hash of previous block with the exception that the first block is called genesis and has no parent hash value stored in it. Such a link with parent block gives an immutable structure which cannot be tampered.

Such immutable structures can store the transactions of different medical devices and vaccines; and information related to patients. Hence, this technology can have different blockchains for healthcare: Blockchain of medical devices, Blockchain of coronavirus infected patients, Blockchain of vaccines in a hospital. The IBM blockchain [34] helps in transparent distribution of coronavirus vaccine, by maintaining the transactions safe and traceable. QuillTrace [35] is a blockchain based technology that helps in tracking

medicines in supply chain and identification of fake medicines with help of QR code on medicines.

4.7 Artificial Intelligence and Machine Learning

AI and machine learning can be applied at various aspects of healthcare which include medicines, medical equipment, patient and disease. The researchers, academicians and healthcare experts are working together to extract useful information, the hidden patterns from large databases of patient data. These large databases are also used to train machine learning models which are used to classify the patients and help in automatic disease detection and thus support medical experts. The recent pandemic has seen the urgent need of study of drug discovery for coronavirus, the high demand of ventilators which have become the life saving device for the high-risk coronavirus patients, the study of patients with high risk levels and the effect of disease on other organs of the body.

Based on the risk level, the coronavirus patients can be divided into low risk level and highrisk level. At the first stage the patients can be isolated in their homes and the various physiological parameters like their temperature, pressure and heart rate at discrete time points can be sent to medical experts for predicting symptoms based on machine learning techniques and healthcare can be provided through telemonitoring. The next stage demands hospitalization of patients with continuous medical support, care and monitoring. AI and machine learning algorithms have been used to predict the mortality rate of high-risk patients [36] by training the model with balanced dataset; and features are chosen based on wrapper and filter-based approaches. These features include symptoms, pre-health status and demographic factors which significantly contribute to the disease status of the patient.

4.8 Robots

Robots are autonomous machines which are programmed to perform a particular task with precision and accuracy. They are cognitive models based on artificial intelligence with capabilities to continuously capture the environment data with sensors to work in complex environments and perform pre-defined actions with high frequency. Robots have a vast role to play in cyber physical systems like medical robots to assist in surgery and patient care, industrial robots to perform manufacturing tasks and surveillance robots for security and safety.

The recent pandemic has seen rising number of coronavirus cases which resulted in patient overload in hospitals. The healthcare robots have found a key role in patient care providing services from patient testing to patient service by delivering regular medicines, food etc. Robots like Moxi perform various services like delivering PPE kits, covid 19 tests and provides pick/drop service to patients [37]. The robot Mitra assists health staff by taking temperature readings of patients and helps patients in connecting with their relatives through video conferencing [38].

Industrial robots help in manufacturing products like covid testing kits and ventilators with high frequency and precision; and short development life cycle. Industrial cyber physical working environments with human robot collaboration aim for agile product development and demand for context awareness in robots which identify human working zones and adjust their area and speed [39]. Unlike machines, human behaviour is flexible and requires constant reminders in the form of audio-visual messages for maintaining a safe distance

during collaborative work with high-speed autonomous machines. Therefore, high precision algorithms are required for depth estimation to send control signals to robots and other autonomous machines to avoid accidents due to erroneous computations and movements.

Security robots can help in detecting adherence to covid protocols like wearing of masks, social distancing etc. They capture images, identify objects, generates reports and communicate using multimodal technologies through audio, video and textual data.

Figure 7 presents the various technologies at various domains and the benefits which helps in automation, resource control and intelligence-based decision making based on big data analytics. Though, various technologies have contributed to the growth of modern cyber physical systems which have led to an evolutionary process resulting in smart, self-aware and self-healing systems but still the present day cyber physical systems face many challenges which have an adverse impact on the health of cyber physical systems affecting its devices, their communication and collaboration resulting in human intervention for reinstating the working state of system.

Section 5, presents some challenges for a smart city healthcare cyber physical system like energy flow in CPS, integration of diverse devices/levels, the delay or latency which can affect the closed loop system and the cyber-attacks which have surfaced for information theft and disruption of devices.

5 Challenges in Smart City Healthcare Cyber Physical System

There are numerous challenges for a successful implementation of HCPS like energy flow, integration of heterogeneous devices and at various levels of HCPS, minimum acceptable delay for time critical operations and security risks in healthcare cyber physical systems as shown in Fig. 8.

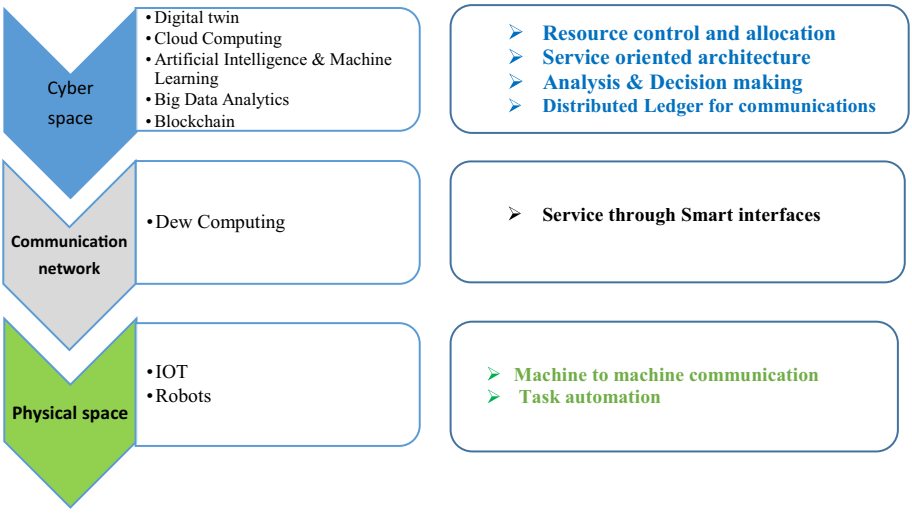
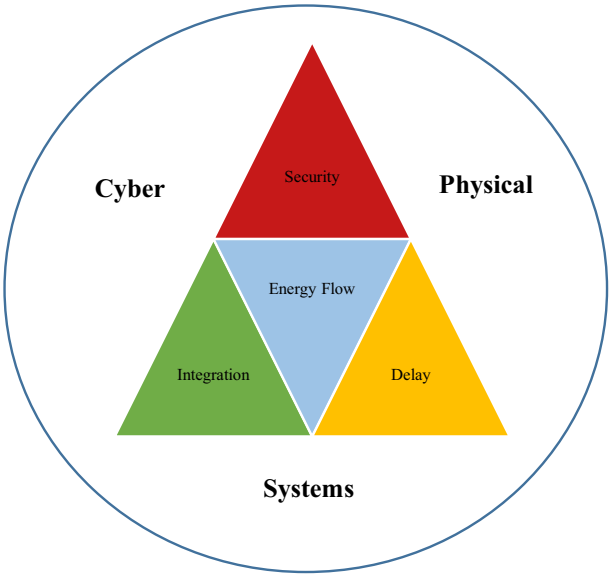


Fig. 7 Technological benefits for cyber physical systems

Fig. 8 Challenges in HCPS



5.1 Energy Flow in Cyber Physical Components

The autonomy of cyber physical systems and their applications in critical domain like healthcare demand a continuous flow of energy either from high-powered batteries or from direct power supply. During the system design and modelling of HCPS it becomes imperative to estimate the various components and their energy requirement so that a continuous flow of energy is maintained for smooth functioning of the healthcare cyber physical system. Resource constraint devices with limited battery power is a challenging issue and various energy saving mechanisms exist to manage energy efficiently like the smart sensors [20] within these devices adapt to the need of environment and change the working mode accordingly but gives a ripple effect on energy quality trade-off. The successful implementation of CPS and its integration to form a smart city healthcare CPS depends primarily on the Smart Grid which is a backbone of energy to the cyber physical systems. The smart home, smart hospitals and smart manufacturing units can aid the Smart grid by installing solar panels and contribute as energy production units in order to meet the energy requirements which have increased exponentially in cyber physical systems.

5.2 Integration of Heterogeneous Devices/Levels of HCPS

The smart city healthcare ecosystem requires the integration of cyber physical systems which depends on third party service providers for communication service and third-party cloud service providers for safe data storage which can be accessed by medical experts, insurance companies, patients and researchers. At the internal level, each cyber physical system has heterogeneous nature of devices with different data formats which requires integration and encapsulation of the devices for efficient and effective environment. The major

challenge in a heterogeneous environment will be the need of interfaces to communicating devices with different technology level in terms of hardware and software resources. The integration and higher levels of HCPS require data sharing and collaborative functionality which demands system level planning, design and prototype testing [26].

5.3 Delay/Latency

Low latency is a critical requirement for real time applications like healthcare. The delays above a threshold value in transmission of patient data are unacceptable and lead to disrupting the telemonitoring cycle of cyber physical systems affecting timely medication and care to the patients. Also, it is significant in real time applications like healthcare that the fault latency which is a measure of time delay between the occurrence of fault and its recognition must be a small value so that its timely management could enhance the reliability of the system [23].

5.4 Security

Security of healthcare cyber physical systems is a critical issue and needs to be addressed in view of the different types of attacks like denial of service, replay, false data injection and deception attacks. The authors in [40] have proposed a tree-based attack model for cyber physical systems where the branches categorise the attacks in various sub domains like fault signal injection and hardware tampering of sensors, packet replay attack and information theft in communication channels of closed loop with sensors, controllers and actuators; equipment failure and software malfunctioning in computing resources. Critical infrastructures like smart healthcare systems require cyber security systems, which monitor continuously for identifying fault injections in system that lead to incorrect working of equipment and faulty readings [24].

Smart healthcare cyber physical systems are future digital systems which must be forensic ready to deal and counter with cyber security attacks [19, 41]. Artificial intelligence or machine intelligence have wide role in autonomous systems performing tasks like abnormal behaviour detection due to faults or cyber-attacks [42]. Malware detection is an important task for smooth and efficient working of cyber physical systems. Many machine learning approaches based on system calls, operation codes and energy consumption patterns are used to identify the malwares [43].

Along with challenges related to digital world, the healthcare systems are facing the major physical challenge of smart waste management. The hospitals are generating the waste at an alarming rate which needs effective management strategies including its collection at generation sites, transportation and handling techniques for maintaining the health of city environment. The recent pandemic has seen the rise of PPE kits and use of disposable masks which needs smart waste management plan.

The Healthcare Cyber Physical systems are currently working at unit or integration level, with continuous growth of technologies they will evolve into higher level CPS. Smart manufacturing systems that produce vaccines or medical equipment are advanced level CPS with subsystems having characteristics of self-awareness and self-management, and can set to self-configuration mode to optimize the various real time production processes [20].

6 Conclusion

The pandemic has taught us that healthcare systems are the lungs of every society and a smart healthcare cyber physical system provides an ecosystem which merges the two wheels cyber world and the physical world connected by a closed loop and steered by various technologies like digital twin, IOT, cloud computing, artificial intelligence, machine learning and big data analytics which play a major role in its effective functioning. The working and implementation in physical world controlled by cyber space face many challenges like heterogeneous nature of physical components, incompatible data formats exchanged between components, resource constraint devices and vulnerability of devices to attacks. Apart from the digital challenges, the physical challenge of waste management still holds its critical place. Though, the birth of new technologies contributes to smart interconnected systems but the challenges of physical and virtual world must be addressed for its growth, efficiency and effectiveness.

Authors' Contributions Conceptualization, organization, writing, analysis and editing.

Declarations

Conflict of interest The author declares that they have no conflict of interest.

References

1. https://www.nist.gov/el/cyber-physical-systems. Accessed on July 20 2019
2. CarrerasGuzman, N. H., Wied, M., Kozine, I., & Lundteigen, M. A. (2020). Conceptualizing the key features of cyberphysical systems in a multi-layered representation for safety and security analysis. *Systems Engineering., 23*, 189–210. https://doi.org/10.1002/sys.21509
3. https://www.reuters.com/business/healthcare-pharmaceuticals/meet-grace-healthcare-robot-covid-19-created-2021-06-09/. Accessed on June 14 2021
4. Aceto, G., Persico, V., & Pescape, A. (2019). A survey on information and communication technologies for industry 4.0: state of the art, taxonomies, perspectives, and challenges. *IEEE Communications Surveys & Tutorials, 21*(4), 3467–3501. https://doi.org/10.1109/COMST.2019.2938259
5. Dibaji, S. M., Pirani, M., Flamholz, D. B., Annaswamy, A. M., Johansson, K. H., & Chakrabortty, A. (2019). A systems and control perspective of CPS security. *Annual Reviews in Control, 47*, 394–411.
6. Dey, J., & Mukherjee, S. (2021). Wireless COVID-19 telehealth: Leukocytes encryption guided by amino acid matrix. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-021-08534-9
7. Caesar, B., Grigoleit, F., & Unverdorben, S. (2019). (Self-)adaptiveness for manufacturing systems: challenges and approaches. *SICS Software-Intensity. Cyber-Physical Systems, 34*, 191–200. https://doi.org/10.1007/s00450-019-00423-8
8. Oks, S. J., Jalowski, M., Fritzsche, A., & Moslein, K. M. (2019). Cyber-physical modelling and simulation: A reference architecture for designing demonstrators for industrial cyber-physical systems. *29th CIRP Design, 2019*, 257–264.
9. Bellman, K., Landauer, C., Dutt, N., Esterle, L., Herkersdorf, A., Jantsch, A., TaheriNejad, N., Lewis, P. R., Platzner, M., & Tammemae, K. (2020). Self-aware cyber-physical systems. *ACM Transactions on Cyber-Physical Systems, 4*(4), Article 38. https://doi.org/10.1145/3375716
10. https://cossim.org/. Accessed on June 18 2020.
11. Henriksson, D., Elmqvist H. (2011). Cyber-physical systems modeling and simulation with modelica. In *Proceedings 8th Modelica Conference, Dresden, Germany*, pp 502–509.
12. https://www.modelica.org/. Accessed on July 5 2020.
13. Neema H., Sztipanovits J., Steinbrink C., Raub T., Cornelsen B., and Lehnhoff, S. (2019). Simulation integration platforms for cyber-physical systems. In *Design Automation for CPS and IoT (DESTION*

'19), April 15, 2019, Montreal, QC, Canada. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3313151.3313169.
14. Skowroński, R. (2019). The open blockchain-aided multi-agent symbiotic cyber–physical systems. *Future Generation Computer Systems., 94*, 430–443.
15. Gil, M., Albert, M., Fons, J., & Pelechano, V. (2020). Engineering human-in-the-loop interactions in cyber-physical systems. *Information and Software Technology, 126*(106349), 1–21.
16. Napoleone, A., Macchi, M., & Pozzetti, A. (2020). A review on the characteristics of cyber-physical systems for the future smart factories. *Journal of Manufacturing Systems, 54*, 305–335.
17. Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters, 3*, 18–23.
18. Sinha, D., & Roy, R. (2020). Reviewing cyber-physical system as a part of smart factory in industry 4.0. *IEEE Engineering Management Review, 48*(2), 103–117.
19. Do, Q., Martini, B., & Choo, K. K. R. (2018). Cyber-physical systems information gathering: A smart home case study. *Computer Networks., 138*, 1–12.
20. Delicato, F. C., Al-Anbuky, A., & Wang, K.I.-K. (2019). Editorial: Smart cyber-physical systems: Towards pervasive intelligence systems. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2019.06.031
21. Seiger, R., Huber, S., & Schlegel, T. (2018). Toward an execution system for self-healing workflows in cyber-physical systems. *Software & Systems Modeling, 17*, 551–572.
22. https://waymo.com/tech/. Accessed on June 25 2020.
23. Dowdeswell, B., Sinha, R., & MacDonell, S. G. (2020). Finding faults: A scoping study of fault diagnostics for Industrial cyber-physical systems. *The Journal of Systems & Software, 168*, 1–16.
24. Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks, 169*, 1–14.
25. Shangguan, L., & Gopalswamy, S. (2020). Health monitoring for cyber physical systems. *IEEE Systems Journal, 14*(1), 1457–1467.
26. Mosterman, P. J., & Zander, J. (2016). Industry 4.0 as a cyber-physical system study. *Software & Systems Modeling, 15*(1), 17–29. https://doi.org/10.1007/s10270-015-0493-x
27. Lu, Y., & Xu, X. (2018). Resource virtualization: A core technology for developing cyber-physical production systems. *Journal of Manufacturing Systems, 47*, 128–140.
28. Ates, H. C., Yetisen, A. K., Güder, F., et al. (2021). Wearable devices for the detection of COVID-19. *Nat Electron, 4*, 13–14. https://doi.org/10.1038/s41928-020-00533-1
29. Nasajpour, M., Pouriyeh, S., Parizi, R. M., et al. (2020). Internet of things for current COVID-19 and future pandemics: An exploratory study. *Journal of Healthcare Informatics Research, 4*, 325–364. https://doi.org/10.1007/s41666-020-00080-6
30. Iqbal, R., Doctor, F., More, B., Mahmud, S., & Yousuf, U. (2020). Big data analytics and computational intelligence for cyber-physical systems: Recent trends and state of the art applications. *Future Generation Computer Systems, 105*, 766–778.
31. Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet of Things Journal, 6*(5), 8770–8781.
32. Gushev, M. (2020). Dew computing architecture for cyber-physical systems and IoT. *Internet of Things*. https://doi.org/10.1016/j.iot.2020.100186
33. Manocha, A., Bhatia, M., & Kumar, G. (2021). Dew computing-inspired health-meteorological factor analysis for early prediction of bronchial asthma. *Journal of Network and Computer Applications, 179*, 102995. https://doi.org/10.1016/j.jnca.2021.102995
34. https://www.ibm.com/blockchain/solutions/vaccine-distribution. Accessed on July 14 2021.
35. https://trace.quillhash.com/tracepharma. Accessed on July 15 2020.
36. Pourhomayoun, M., & Shakibi, M. (2021). Predicting mortality risk in patients with COVID-19 using machine learning to help medical decision-making. *SmartHealth*. https://doi.org/10.1016/j.smhl.2020.100178
37. https://www.forbes.com/sites/saibala/2021/01/26/robots-have-become-an-essential-part-of-the-war-against-covid-19/?sh=7aaf7bd25ef3. Accessed on July 10 2020.
38. https://edition.cnn.com/2020/11/11/tech/robots-india-covid-spc-intl/index.html. Accessed on July 11 2021.
39. Nikolakis, N., Maratos, V., & Makris, S. (2019). A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace. *Robotics and Computer Integrated Manufacturing, 56*, 233–243.
40. Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry, 100*, 212–223.

41. Lu, Y. (2017). Cyber physical system (cps)-based industry 4.0: A survey. *Journal of Industrial Integration and Management*. https://doi.org/10.1142/S2424862217500142
42. Farivar, F., Haghighi, M. S., Jolfaei, A., & Alazab, M. (2020). Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. *IEEE Transactions on Industrial Infromatics, 16*(4), 2716–2725.
43. HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep recurrent neural network based approach for internet of things malware threat hunting. *Future Generation Computer Systems, 85*, 88–96.

Rupali Verma received B. Tech in Computer Science from Panjab Technical University, India in 2001; ME in Computer Science (IT) from Panjab University in 2005, and PhD in Computer Science from Panjab University in 2016. She is currently working as Assistant Professor in Computer Science and Engineering, Punjab Engineering College, Chandigarh, India. Her research interests are Cryptography, Algorithms and Data Analytics.