A REVIEW ON SMART HEALTHCARE IN CYBER PHYSICAL SYSTEM

A. Kavitha[1] ,Dr R.ManickaChezian[2]

[1]Ph.D Research Scholar, Department of Computer Science, Nallamuthu Gounder Mahalingam College Pollachi, Tamil Nadu - 642001, India

[2]Associate Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College Pollachi, Tamil Nadu - 642001, India.

chezianr@gmail.com

Abstract

A smart healthcare Cyber Physical System (CPS) is a unique cyber physical system, which combines embedded software control devices, networking capabilities, and complex physiological dynamics of patients in the modern medical field. In the process of communication, device, and information system interaction of smart healthcare cyber physical system, medical cyber physical data are generated digitally, stored electronically, and accessed remotely by medical staff or patients. With the advent of the era of medical big data, a large amount of medical cyber physical data is collected, and its sharing provides great value for diagnosis, pathological analysis, epidemic tracking, pharmaceutical, insurance, and so on. The Cyber Physical System is a term describing a broad range of complex, multi-disciplinary, physically-aware next generation engineered system that integrates embedded computing technologies into the physical world. In order to define and understand CPS more precisely, this article presents a detailed survey of the related work, discussing the origin of CPS, Implementation of Smart Healthcare, CPS applications, challenges, CPS advantages, CPS disadvantages, as well as security and privacy issues.

Keywords: Cyber Physical Systems, Smart Health, Internet of Things, Sensors

1. INTRODUCTION

Cyber-physical system (CPS) is attracting a lot of attention in recent years and is being considered as an emerging technology. It combines computation and communication capabilities with the physical world. CPS relies on sensing, processing, and networking. The recent advances in wireless sensor networks, medical sensors, and Cloud Computing are making CPS a powerful candidate for healthcare applications including in-hospital and in-home patient care. These advances promise to provide CPS the ability to observe patient conditions remotely and take actions regardless of the patient's location. Considerable research is being conducted on medical sensors. These sensors are able to collect vital patient information containing health data. Collected data are sent to a gateway via the wireless communication medium. Wired sensors can also be used; however, wireless sensors provide more flexibility and comfort to both the caregiver and the patients. The data collected by the sensors can be stored in a server and made accessible to clinicians. Security is a vital concern here as patient data is confidential from legal and ethical perspectives. So, while designing CPS architecture for healthcare applications, special attentions need to be paid to ensure data security. There are also a number of other important issues to consider, for example, the requirement to store and manage the huge volume of data collected from thousands of medical sensors. Therefore, database management systems should be efficient and reliable. As medical data can provide

useful insight into actions (treatments) necessary to save a patient's life, all data should be readily available and accessible to authorized medical personnel anytime from anywhere. In addition, healthcare applications require huge computing resources for intelligent decision making based on the massive patient data. However, the networks of wireless sensors collecting the patient data are severely constrained in energy, processing, and storage capacity. A number of barriers are hindering the progress of designing, developing and deploying cyber-physical systems in healthcare as well as in other application domains. Designing CPS for healthcare is a challenging task as it involves several issues such as software reliability, system interoperability, computational intelligence, security and privacy, and context awareness. Software is an integral part of medical devices and hardware functions in close interactions with software.

Implementation of IoT in the medical area gained popularity, following modern techniques like smart cities, smart regions, and smart devices. IoT achieved immense popularity because of its data acquiring and visualizing property through sensing the objects and communication with devices through wireless networks. IoT devices are capable of sensing, visualizing, collecting, and sharing data, and communication among the devices can be done by wireless IoT protocols like Bluetooth, ZigBee, Z-Wave, WiFi, and RFID. These protocols play a vital role in the healthcare sector since they ensure ease and flexibility for data communication and data monitoring among employed devices. Data collected from these devices are used for different tasks like disease classification, designing, patient monitoring, and so on. Cloud concepts also play a vital role in smart healthcare systems. It provides firm and efficient access to data; storage can be done effectively, and the above-mentioned challenges can be overcome by employing cloud services. Deep learning (DL) techniques like Convolutional Neural Networks (CNN), Autoencoders (AE), Deep Belief Networks (DBNs), Long Short-Term Memory (LSTM), Recurrent Neural Networks (RNNs), etc. The key objective of this research paper is to provide a comprehensive survey related to Smart Health Care Cyber Physical Systems.

2. CYBER PHYSICAL SYSTEMS

Cyber-physical system (CPS) connects the virtual world with physical world. It has the ability to add more intelligence to social life. It integrates physical devices, such as sensors and cameras, with cyber components to form an analytical system that responds intelligently to dynamic changes in the real-world scenarios. CPS can have wide ranging applications, such as smart medical technology, assisted living, environmental control, and traffic management. The research on CPS in healthcare is still in the early stages. CPS in healthcare offers varied applications such as hospital, assisted living, and elderly care. System complexity largely depends on the specific application. Elements in architecture may need special organization according to the applicable area. In case of controlled environment such as intensive care unit in a hospital, the architecture may include controlled elements. On the other hand, in assisted living home, it may be required to include much automated elements in the architecture. CPS in healthcare applications can be divided into two areas: (a) assisted and (b) controlled. Assisted application includes the health monitoring without restricting independence in a person's normal living. Application in controlled environment consists of hospital and intensive care where the medical support is readily available. Security is a vital concern here as patient data is confidential from legal and ethical perspectives. So, while designing CPS architecture for healthcare applications, special attention needs to be paid to ensure data security.

3. STRUCTURE OF CYBER PHYSICAL SYSTEMS

The Cyber-Physical Systems (CPS) are complicated networked systems which comprise of computing and communicating cyber components and interact closely with physical components, such as sensors and actuators. The most indispensable aspect of life is undeniably health. In recent years, advanced healthcare

systems have gained immense popularity due to demographic growth, and an increase in diseases which, in turn, requires enormous clinical assets and even hospital staff. Therefore, it challenges tremendous, computerized health systems providing excellent services to both patients and the hospital staff as traditional healthcare systems are incompetent to accomplish the necessity of all humans as it is not affordable and accessible to everyone. CPS is in development phase, that is it's under analysis, study and research phase. It need to be clearly specify the structure and methodology of CPS for industrial implementation. To fulfill the demand of industrial implementation of CPS, a unified system framework is designed. Collaborative algorithms and technologies at each layer are proposed for enhanced efficiency, reliability and quality of product. This collaboration can determine expected functionalities from each layer of CPS structure. Cyber physical system works as feedback system throughout application areas of CPS. The industrial implementation of CPS needs advancements in design tools, design methodologies and strong security in terms of cyber context. CPS need cyber security for physical devices or systems connected using Internet based network. The cyber security provided to devices should monitor malicious attacks, intrusion and privacy parameters of systems. CPS algorithms should be designed by considering such security concerns. Privacy of data or metadata should be maintained while performing network communication. CPS systems work as feedback systems for complete architecture. CPS may work in collaboration with humans to provide some intelligence to decision system of CPS. Based on economical efficiency and environmental results, CPS may provide feedback to central or distributed server. CPS feedbacks are based on real time monitoring and analysis of sensed data. System can be designed using adaptive or predictive algorithms for better prediction and understanding of environmental decisions.

4. APPLICATIONS OF CYBER PHYSICAL SYSTEMS

CPS is a result of advancements in technology, technology for design and fabrication at micro level and nano level, fundamental components available in required size & with required features. Some fundamental components are wireless networking devices, sensors, processors which are small in size but efficient in processing, and actuators. The developments in software design methods for complex applications, computing system software advancements like high performance computing system ,real time embedded operating systems, sensor based operations, programming languages with high level library support are also important in development of CPS. The wireless devices are feasibly connected to each other through the Internet across the world.

Some major application areas for CPS are Smart city traffic control, automobile sector, robots, aircraft for traffic control, smart power grid design, manufacturing plants for management and control of machinery, construction, medical system and many more. CPS are working in highly dynamic environment with distributed operating system, heterogeneous cyber and physical entities like software hardware, electronics devices, challenging dynamic objectives. CPS need to be adaptive for such dynamic environment. Many CPS are operated by human, which in turn require considerations of human aspects for CPS design. The considerations of human aspects need extreme advancements in theory, technology and tools for automation of CPS. The automation community has extended opportunities with this need of advancements in technology. The automation process gives opportunity to entire design process stages, which include system specification, modelling, programming language design, simulation, system validation and system components verification, parameter mapping, design of interface, analysis of performance, networking, application debugging & testing, any repairs and so on. Each of the stages or categories need more advances in technology and tools for CPS automation.

5. ADVANTAGES OF CYBER PHYSICAL SYSTEMS

Faster Response Time: CPS can provide faster response time due to faster processing and communication capability of sensors and cloud infrastructure. Fast response time can facilitate the early detection of remote failure, proper utilization of shared resources such as bandwidth.

Scalability**:** CPS is able to scale the system according to demand utilizing the properties of Cloud Computing. Users are able to acquire necessary infrastructure without investing additional resources. CPS is inherently heterogeneous as it combines physical dynamics with computational processes. The physical domain may combine mechanical motion control, chemical processes, biological processes, and human involvement. The cyber domain may combine networking infrastructure, programming tools, and software modelling. CPS can provide design methodologies and tools that support those methodologies, which scale to large designs and promote understanding of complex systems.

Dealing with Certainty: Certainty is the process of providing proof that a design is valid and trustworthy. Evidence can include formal proofs or exhaustive tests in simulations and prototypes. CPS is designed to be able to evolve and operate with new and unreliable environment. CPS is able to demonstrate unknown system behavior to study further and evolve into better system.

Network Integration: CPS has the interoperability with WSNs and Cloud Computing. This may provide the compliance with networking standards. CPS involves multiple computational platforms interacting over communication networks. CPS provides network integration characteristics such as media access control techniques and their effects on system dynamics, middleware, and software that provide coordination over networks, control over timing of network transactions, and fault tolerances.

Flexibility**:** Present systems based on CPS provide much more flexibility compared to the earlier research efforts in WSN and Cloud Computing alone.

Interaction between Human and System: Modeling and measuring situational awareness-human perception of the system and its environmental changes in parameters are critical for decision making. This is an absolute necessity for complex and dynamic systems. Some CPSs include human as an integral part of the system which makes the interaction easier because usually humans are difficult to model using standalone systems.

Better System Performance: With the close interaction of sensors and cyber infrastructure, CPS is able to provide better system performance in terms of feedback and automatic redesign. Better computational resources and cyber subsystems in CPS ensure the presence of multiple sensing entities, multiple communication mechanisms, high-level programming language, and end-user maintenance which further ensures the better system performance by CPS.

Autonomy**:** CPS can provide autonomy due to having sensor-cloud integration. Typically, CPS is a closed loop system, where sensors make measurements of physical dynamics. These measurements are processed in the cyber subsystems, which then drive actuators and applications that affect the physical processes. The control strategies in the cyber subsystems are adaptive and usually predictive.

Optimization**:** Present biomedical sensors and cloud infrastructure offer large optimizations for variety of applications. This capability opens the pathway for CPS to optimize the system in wide extent.

6. CYBER PHYSICAL SYSTEM CHALLENGES

Cyber-Physical Systems revolutionize our interaction with the physical world. Of course, this revolution does not come free. Since even legacy embedded systems require higher standards than general-purpose

computing, we need to pay special attention to this next generation physically-aware engineered system requirements if we really want to put our full trust in them. Therefore, we want to clarify the definitions of some common CPS system-level requirements /challenges.

Dependability - It refers to the property of a system to perform required functionalities during its operation without significant degradation in its performance and outcome. Dependability reflects the degree of trust put in the whole system. A highly dependable system should operate properly without intrusion, deliver requested services as specified and not fail during its operation. The words dependability and trustworthiness are often used interchangeably. Assuring dependability before actual system operation is a very difficult task to achieve. For example, timing uncertainties regarding sensor readings and prompt actuation may degrade dependability and lead to unanticipated consequences. Cyber and physical components of the system are inherently interdependent and those underlying components might be dynamically interconnected during the system operation, which, in return, render dependability analysis very difficult. A common language to express dependability related information across constituent systems/underlying components should be introduced in the design stage.

Maintainability - It refers to the property of a system to be repaired in case a failure occurs. A highly maintainable system should be repaired in a simple and rapid manner at the minimum expenses of supporting resources, and free from causing additional faults during the maintenance process. With the close interaction among the system components underlying CPS infrastructure, autonomous predictive /corrective diagnostic mechanisms can be proposed. Continuous monitoring and testing of the infrastructure can be performed through those mechanisms. The outcome of monitoring and testing facilities help finding which units need to be repaired. Some components, which happen to be the source of recurrent failures, can be redesigned or discarded and replaced with the ones with better quality.

Availability - It refers to the property of a system to be ready for access even when faults occur. A highly available system should isolate malfunctioning portion from itself and continue to operate without it. Malicious cyber-attacks hinder availability of the system services significantly. For example, in Cyber-Physical Medical Systems, medical data shed light on necessary actions to be taken in a timely manner to save a patient's life. Malicious attacks or system/component failure may cause services providing such data to become unavailable, hence, posing risk on the patient's life.

Safety - It refers to the property of a system to not cause any harm, hazard or risk inside or outside of it during its operation. A very safe system should comply with both general and application-specific safety regulations to a great extent and deploy safety assurance mechanisms in case something went wrong. For example, among the goals for smart manufacturing (SM), point-in-time tracking of sustainable production and real-time management of processes throughout the factory yield to improved safety. Safety of manufacturing plants can be highly optimized through automated process control using embedded control systems and data collection frameworks (including sensors) across the manufacturing enterprise. Smart networked sensors could detect operational failures/anomalies and help prevention of catastrophic incidents due to those failures/anomalies.

Reliability - It refers to the degree of correctness which a system provides to perform its function. The certification of system capabilities about how to do things correctly does not mean that they are done correctly. So a highly reliable system makes sure that it does the things right. Considering the fact that CPSs are expected to operate reliably in open, evolving, and uncertain environments, uncertainty in the knowledge, attribute, or outcome of a process in the CPS infrastructure makes it necessary to quantify uncertainties during the CPS design stage. That uncertainty analysis will yield to effective CPS reliability

characterization. Besides, the accuracy of physical and cyber components, potential errors in the design/control flow, cross-domain network connections in an ad-hoc manner limit the CPS reliability.

Robustness - It refers to the ability of a system to keep its stable configuration and withstand any failures. A highly robust system should continue to operate in the presence of any failures without fundamental changes to its original configuration and prevent those failures from hindering or stopping its operation. In addition to failures, the presence of disturbances possibly arising from sensor noises, actuator inaccuracies, faulty communication channels, potential hardware errors or software bugs may degrade overall robustness of CPS. Lack of modeling integrated system dynamics, evolved operational environment, or unforeseen events are other particular non-negligible factors, which might be unavoidable in run-time, hence the need for the robust CPS design.

Predictability - It refers to the degree of foreseeing of a system's functionality either qualitatively or quantitatively. A highly predicable system should guarantee the specified outcome of the system's behavior/functionality to a great extent every moment of time at which it is operating while meeting all system requirements. In Smart Healthcare Cyber Physical Systems, smart medical devices together with sophisticated control technologies are supposed to be well adapted to the patient's conditions, predict the patient‘s movements, and change their characteristics based on the context awareness within the surrounding environment. Many medical devices perform operations in real-time, satisfying different timing constraints and showing diverse sensitivity to timing uncertainties. However, not all components of Smart Healthcare Cyber Physical Systems are time-predictable. Therefore, in addition to new programming and networking abstractions, new policies of resource allocation and scheduling should be developed to ensure predictable end-to-end timing constraints.

Accuracy - It refers to the degree of closeness of a system's observed outcome to its calculated one. A highly accurate system should converge to the actual outcome as close as possible. High accuracy especially comes into play for CPS applications where even small imprecisions are likely to cause system failures. For example, a motion-based object tracking system under the presence of imperfect sensor conditions may take untimely control action based on incorrect object position estimation, which in return leads to the system failure.

Compositionality - It refers to the property of how well a system can be understood entirely by examining every part of it. A highly compositional system should provide great insight about the whole from derived behaviors of its constituent components. Achieving high compositionality in the CPS design is very challenging especially due to the chaotic behavior of constituent physical subsystems. Designing highly compositional CPS involves strong reasoning about the behavior of all constituent cyber and physical subsystems and devising cyber-physical methodologies for assembling CPSs from individual cyber and physical components, while requiring precise property taxonomies, formal metrics and standard test benches for their evaluation, and well-defined mathematical models of the overall system and its constituents.

Sustainability - It means being capable of enduring without compromising requirements of the system, while renewing the system's resources and using them efficiently. A highly sustainable system is a long lasting system which has self-healing and dynamic tuning capabilities under evolving circumstances. Sustainability from energy perspective is an important part of energy provision and management policies. For example, the Smart Grid facilitates energy distribution, management, and customization from the perspective of customers or service providers by incorporating green sources of energy extracted from the physical environment. However, intermittent energy supply and unknown/ill-defined load characterization

hinders the efforts to maintain long-term operation of the Smart Grid. To maintain sustainability, the Smart Grid requires planning and operation under uncertainties, use of real-time performance measurements, dynamic optimization techniques for energy usage, environment-aware duty cycling of computing units, and devising self-contained energy distribution facilities.

Adaptability - refers to the capability of a system to change its state to survive by adjusting its own configuration in response to different circumstances in the environment. A highly adaptable system should be quickly adaptable to evolving needs/circumstances. Adaptability is one of the key features in the next generation air transportation systems. Next generation capabilities enhance airspace performance with its computerized air transportation network which enables air vehicles immediately to accommodate themselves to evolving operational environment such as weather conditions, air vehicle routing and other pertinent flight trajectory patterns over satellites, air traffic congestion, and issues related to security.

Resilience - refers to the ability of a system to persevere in its operation and delivery of services in an acceptable quality in case the system is exposed to any inner or outer difficulties that do not exceed its endurance limit. A highly resilient system should be self-healing and comprise early detection and fast recovery mechanisms against failures to continue to meet the demands for services. High resilience comes into play in delivering mission-critical services. Mission-critical CPS applications are often required to operate even in case of disruptions at any level of the system. Therefore, designing highly resilient CPS requires thorough understanding of potential failures and disruptions, the resilience properties of the pertinent application, and system evolution due to the dynamically changing nature of the operational environment.

Reconfigurability - refers to the property of a system to change its configurations in case of failure or upon inner or outer requests. A highly reconfigurable system should be self-configurable, meaning able to fine-tune itself dynamically and coordinate the operation of its components at finer granularities. CPSs can be regarded as autonomously reconfigurable engineered systems. Remote monitoring and control mechanisms might be necessity in some CPS application scenarios such as international border monitoring, wildfire emergency management, gas pipeline monitoring etc. Operational needs may change for such scenarios, which call for significant reconfiguration of sensor/actuator nodes being deployed or the entire network to provide the best possible service and use of resources.

Security - It refers to the property of a system to control access to the system resources and protect sensitive information from unauthorized disclosures. A highly secure system should provide protection mechanisms against unauthorized modification of information and unauthorized withholding of resources, and must be free from disclosure of sensitive information to a great extent. CPSs are vulnerable to failures and attacks on both the physical and cyber sides, due to their scalability, complexity, and dynamic nature. Malicious attacks can be directed to the cyber infrastructure or the physical components with the intent of disrupting the system in operation or stealing sensitive information. Making use of a large-scale network, adopting insecure communication protocols, heavy use of legacy systems or rapid adoption of commercial off-the-shelf (COTS) technologies are other factors which make CPSs easily exposed to the security threats.

Integrity - It refers to the property of a system to protect itself or information within it from unauthorized manipulation or modification to preserve correctness of the information. A high integrity system should provide extensive authorization and consistency check mechanisms. High integrity is one of the important properties of a CPS. CPSs need to be developed with greater assurance by providing integrity check mechanisms on several occasions. Properties of the physical and cyber processes should be well-understood and thus can be utilized to define required integrity assurance.

Confidentiality - It refers to the property of allowing only the authorized parties to access sensitive information generated within the system. A highly confidential system should employ the most secure methods of protection from unauthorized access, disclosure, or tampering. Data confidentiality is an important issue that needs to be satisfied in most CPS applications.

Interoperability - It refers to the ability of the systems/components to work together, exchange information and use this information to provide specified services. A highly interoperable system should provide or accept services conducive to effective communication and interoperation among system components. Performing far-reaching battlefield operations and having more interconnected and potentially joint-service combat systems, Unmanned Air Vehicles call for seamless communication between each other and numerous ground vehicles in operation. The lack of interoperability standards often causes reduction in the effectiveness of complicated and critical missions. Likewise, according to changing needs, dynamic standards should be developed and tested for devices, systems, and processes used in the Smart Grid to ensure and certify the interoperability of those ones being considered for a specific Smart Grid deployment under realistic operating conditions.

Composibility - It refers to the property of several components to be merged within a system and their inter-relationships. A highly composable system should allow recombination of the system components repeatedly to satisfy specific system requirements. Composibility should be examined in different levels. Certainly, system composibility is more challenging, hence the need for well-defined composition methodologies that follow composition properties from the bottom up. Additionally, requirements and evaluations must be composable accordingly. In the future, it will probably be of paramount importance to incrementally add emerging systems to the system of systems with some predictable confidence without degrading the operation of the resulting system.

Heterogeneity - It refers to the property of a system to incorporate a set of different types of interacting and interconnected components forming a complex whole. CPSs are inherently heterogeneous due to constituent physical dynamics, computational elements, control logic, and deployment of diverse communication technologies. Therefore, CPSs necessitate heterogeneous composition of all system components. For example, incorporating heterogeneous computing and communication capabilities, future medical devices are likely to be interconnected in increasingly complex open systems with a plug-and-play fashion, which makes a heterogeneous control network and closed loop control of interconnected devices crucial. Configuration of such devices may be highly dynamic depending on patient-specific medical considerations. Enabled by the science and emerging technologies, medical systems of the future are expected to provide situation-aware component autonomy, cooperative coordination, real-time guarantee, and heterogeneous personalized configurations far more capable and complex than today's.

High Assurance Software: Software plays an increasingly important role in medical devices. Many functions traditionally implemented in hardware – including safety interlocks – are now being implemented in software. Thus high-confidence software development is critical to assure the safety and effectiveness of Smart Healthcare Cyber Physical Systems.

Context-Awareness: Patient information exchanged during device inter-operation can not only provide a better understanding of the general health of the patient, but also enable early detection of ailments and generation of effective alarms in the event of emergencies. Given the complexity of the human body and variations of physiological parameters over patient population, developing such computational intelligence is a non-trivial task.

Autonomy: The computational intelligence that Smart Healthcare Cyber Physical Systems possess can be used for increasing the autonomy of the system by enabling actuation of therapies based on the patient's current health state. Closing-the-loop in this manner must be done safely and effectively.

Certifiability: The complex and safety-critical nature of Smart Healthcare Cyber Physical Systems requires a cost-effective way to demonstrate medical device software dependability. Certification of medical devices provides a way of achieving this goal. Certifiability is therefore an essential requirement for the eventual viability of Smart Healthcare Cyber Physical Systems and an important challenge to be addressed.

7. SMART HEALTH CARE APPLICATIONS

Smart healthcare applications are software's implemented to generate, gather, maintain, and data related to both patients and health organizations. This data is utilized for performing different tasks like remote patient health monitoring, generating patient records, planning treatment, disease detection, sensing patient conditions, and so on. Smart healthcare systems benefit patients, physicians, guardians, healthcare centers, and insurance organizations. Smart Healthcare System is a healthcare service and maintenance system that works with integrated technologies like IoT, wearable devices, Internet for the exchange of information, and it binds the patients, medical staff, healthcare institutions, guardians, and data intelligently into a common platform to assist remotely. It is an aggregate of various areas viz, patient monitoring and management, detection of diseases, prevention, and diagnosis, decision making systems, virtual assistance, drug discovery, health center management, and assisting drug and medical research.

A package of distinct technologies viz, IoT, artificial intelligence, cloud computing, fog computing, edge computing, big data, the Internet, sensors, wearable devices, applied sciences, and nanotechnology collectively embodies "smart healthcare". The Smart Healthcare System will facilitate connection among all concerned bodies and acknowledge that all the associates receive the necessary services. Concisely Smart Healthcare System can be defined as the medical information structure of the top level.

Personal Health Monitoring: Personal health monitoring is mainly reflected in the family monitoring of the elderly, children, pregnant women and disabled patients, emergency warnings, and so on. According to a report released by the United Nations, the proportion of people aged 60 and above to the total population is expected to double between 2007 and 2050, reaching two billion by 2050. The monitoring of the personal health environment will promote the development of smart homes. The term "smart home" refers to a special type of home or residence, equipped with sensors and actuators, integrated into the residential infrastructure, which aims to monitor the environment of residents and improve the personal experience at home. The monitoring system is an indispensable part. Privacy is the main problem that hinders the adoption and use of home monitoring technology, for example, the possible privacy violation caused by the use of cameras.

Hospital Monitoring System: The hospital monitoring system is the focus of managers of laboratory, testing and radiation departments, doctors' consulting rooms, wards, nurse's offices, and emergency departments. The demand of a hospital for a monitoring system is very large, and almost all medical occasions need monitoring equipment to collect data, so as to record the medical information and facilitate the hospital's macro understanding of patients, people flow, department needs, and other aspects.

Smart Medical System: Medical management departments have a great demand for timely prevention and detection of epidemic situations, prevention of epidemic situations, and supervision of disease. The health management department can call the remote monitoring system to understand the real-time situation of each hospital and analyze the monitoring medical data to understand the latest disease situation. For drug

management departments, monitoring data can not only provide the data of the disease and patients but also extract the price data of drugs, the use of medical devices, the detection results of hospital disinfection, and the current situation of infectious disease control and prevention. Without Smart Healthcare Cyber Physical Systems, medical institutions belong to the information island, with massive medical data resources, but cannot establish effective contact with the outside world. Insurance, pharmaceutical enterprises, scientific research institutions, and other peripheral institutions in urgent need of data support are unable to obtain medical data conveniently and quickly. It is very difficult and costly for enterprises participating in medical insurance to obtain data, which restricts the development of the industry.

8. 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 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. The following figure 1 shows the various technologies in healthcare cyber physical systems.

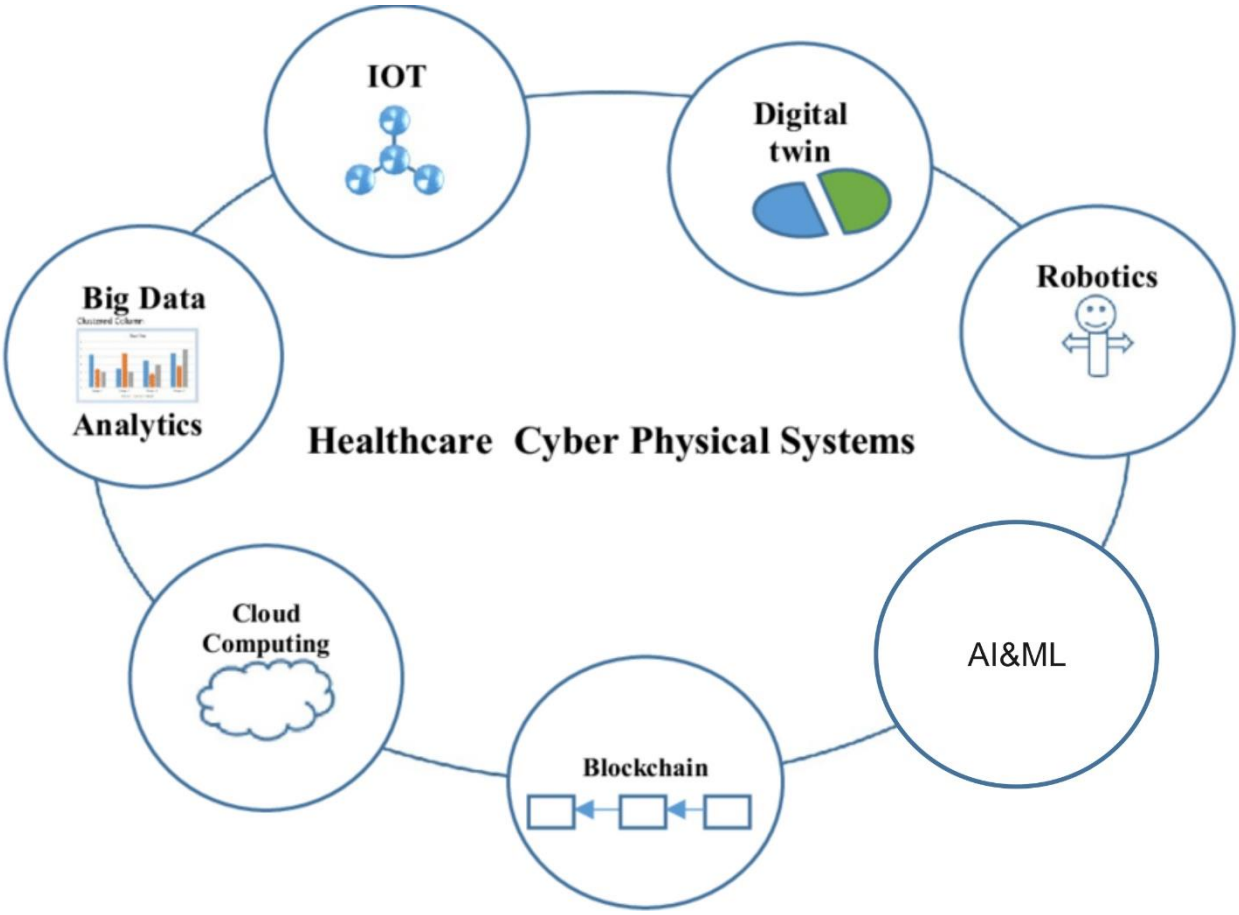

Figure 1: Technologies in Healthcare Cyber Physical Systems

Digital Twin: Digital twin 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. Digital twin for Smart Healthcare Cyber Physical System is basically a simulation model for medical devices and equipment, and for behavioral analysis of patient treatment process to assist the health care experts to study, analyze 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. 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.

Internet of Things (IOT): The Internet of Things brought a new era of machine-to-machine communication 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 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.

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.

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. 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.

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. The Dew computing layer is very useful for providing services in healthcare domain 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; 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.

Blockchain: Blockchain technology provides a decentralized and distributed database for secure and authentic access to electronic health records maintained by cloud servers. It provides a decentralized platform for maintaining untampered records of events for various medical transactions that may be at device level or vaccines; and events at patient level. 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.

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.

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.

9. DATA SECURITY AND PRIVACY PROTECTION

9.1 Threats and Requirements

The possible threats in three layers of Smart Healthcare Cyber Physical Systems are given as follows;

1) Sensing/Execution Layer: The sensing/execution layer contains various sensing devices and diagnostic devices. Therefore, it is most vulnerable to physical attacks at this layer. The common threats are node capture, illegal substitution, exhaustion attack, insider leak, and so on.

2) Network Layer: For the network layer, attackers may launch attacks during the data transmission phase to capture and tamper with data or break the transmission channel. The attacks that an attacker may launch are selective forwarding attacks, sinkholes, wormholes, flooding, jamming, and so on.

3) Application Layer: The application layer of Smart Healthcare Cyber Physical Systems will process a large amount of sensitive medical data. Therefore, the attacks in this layer will threaten data security and privacy. The possible attacks on the application layer are buffer overflow, identity theft, and so on.

9.2 Requirements

The security and privacy of patient-related data cannot be ignored. Data security means the complete storage and transmission of medical data to ensure its integrity, effectiveness, and authenticity. Data privacy protection means that only legitimate users can access the medical data of patients. The requirements for data security and privacy protection are given as follows.

1) Data Integrity: It means that all data values stored in the database are in the correct state. It includes four categories, such as entity integrity, domain integrity, referential integrity, and user-defined integrity. The database uses many methods to ensure data integrity, including foreign keys, constraints, rules, and triggers. The system well deals with the relationship between the four, uses different methods according to different specific situations, and complements each other.

2) Data Availability: It is to ensure that authorized users can use data or data systems. Medical big data not only bring huge benefits but also face huge challenges, such as unreliable or inaccurate data. In addition, unauthorized access leading to data loss or destruction will affect the availability of data.

3) Data Audit: It is the compliance management of fine grained audit of database operation, warning the risk behavior of database, and blocking the attack behavior. It is an effective means to monitor the use of medical resources. In addition, cloud service providers who store medical data have a great responsibility and need reasonable audit methods. Audit content usually includes users, cloud service providers, access, and operation process.

4) Information Privacy: Patient information records can be divided into two categories. One is general records, which refers to records that can be publicly accessed. The other is sensitive records, including the patient's personal identity information and some medical diagnosis information. The access of sensitive records needs reasonable access control policies.

10. CHALLENGES OF CPS IN HEALTHCARE

Software Reliability. Software is an integral part of medical devices. Device functionality and multiple functions are ensured via software. Software also ensures the proper cooperation between medical devices and the patients. So, the safety and efficiency of the system rely on the proper software design, development, and management.

Medical Device Interoperability. Multiple medical devices may have different communication interfaces. A well-maintained management system should be there to integrate heterogeneous medical devices in a safe, secured, and certified manner.

Data Extraction. Medical devices collect multiple physiological parameters from the patients. These parameters are widely varied in nature and capable of providing not only general information about patients but also early prediction of future illness, possible nullification of emergency situation. However, it is a

challenging task to design such system that can seamlessly extract complex physiological parameters from patients.

System Feedback. Development of feedback system is a challenging task for CPS in healthcare because the design stability will be void without feedback system or patient care improvement. CPS in healthcare scenario depicts a perfect feedback system via smart alarm system. Alarm system is of paramount importance to notify the caregiver for any possible illness or emergency situation.

Complex Query Processing. Due to the presence of heterogeneous biosensors, sometimes wireless battery operated sensors present a few challenges such as low energy consumption and limited processing capability which hinders the pavement for complex query processing. Complex query processing can help reduce the amount of transmission and context aware predictions. These functionalities can reduce the energy consumptions in a limited energy network. Complex queries can utilize the access to multiple physiological parameters, thus predicting possible illness. However, this approach requires complex design and computational skill sets.

Lack of Prototype Architecture in CPS for Healthcare. At present, there is a lack of secure and trustworthy prototype architecture for testing, evaluation, and system developments which includes healthcare devices. For the very reason, there is inability to ensure the correctness of CPS in healthcare architecture in the uncertain environmental scenario.

High Assurance Software: Medical devices use technology to automate some features, like hardware and other things. But it is well known that software development is too important to keep Smart Healthcare Cyber Physical Systems safe.

Context awareness: In addition to giving a better sense of the patient's general health, information about the patient that is shared during system contact can also help detect disease early and raise alarms in emergencies, as well.

Autonomy: The analytical knowledge that Smart Healthcare Cyber Physical Systems has can be used to make the device more flexible by allowing it to be used to treat patients in a way that is best for them at that time. In this way, the loop must be closed safely and quickly.

Certifiability: Smart Healthcare Cyber Physical Systems needs a cost-effective way to show that medical device software is reliable and safe, like by getting medical device certification.

Executable clinical workflows: Today, more and more medical devices connect with each other and work together so that they can build and deploy Smart Healthcare Cyber Physical Systems quickly to provide efficient clinical services to a patient. Patients' safety is the biggest problem with putting Smart Healthcare Cyber Physical Systems on the market. As a result, we need to make sure that patients are safe in these unique situations by using valid, workable clinical workflows.

Model-based Development: It will be easier to figure out how safe a scenario is for patients before we build a software system, and it will help us write specifications for safe devices that can be used in the scenario and its connections. Then, during deployment, these specifications can be checked to make sure that the implementation is safe. Notice how scenario analysis is done with the help of Smart Healthcare Cyber Physical Systems model-based growth, which is how it is done. The most difficult thing is to figure out how static and dynamic security checks work together.

Physiological close-loop control: There are a lot of things that people don't like about using automatic control in medical care, like controlling an application to a certain point, doing multiple treatments at the same time that could affect a lot of different body systems in complicated patients, and so on. Keep in mind that each person's treatment may be different.

Patient Modelling and Simulation: It's important to have models of patients so that we can look at how different situations and closed loop control work. One of the things being talked about here is the need to figure out how the drug is absorbed and pay attention to important things like the heart and respiratory rates of the patient in closed loop situations. We need more simple methods to help us solve the problem of designing and analyzing things. These methods could make some comprehensive models less complicated.

Adaptive Patient and smart alarms: This is the fourth thing that we're going to talk about in this text. Most of the medical equipment is made to work for groups of patients. Patients may have a very different reaction to treatment, which could cause a lot of confusion and waste time in Smart Healthcare Cyber Physical Systems. For example, if a potentially dangerous condition is found, most medical devices may sound an alarm at the same time. It is also possible for medical devices to send out false alarms. Caretakers don't have these kinds of things happen to them. Today, medical devices are building a strong network connection so that they can provide an efficient solution to patients and collect data that can be used to make Electronic Health Records.

User Centered Design: The caregiver may make mistakes because they are overworked or stressed, or because they have trouble operating a device. So, medical devices might have to be made with the needs of the people who will use them in mind, like having a user-friendly interface, interactive ways to learn how to use the device if they get stuck, and ways to fix mistakes so that people will be happy with how the device works.

Infrastructure for Medical-Device Integration and Interoperability: At the moment, only one company is developing distributed Smart Healthcare Cyber Physical Systems that use a proprietary communication. There are many open standards that are the norm when it comes to Smart Healthcare Cyber Physical Systems. Still, these standards need to be more effective if they can be used on platforms that are easy to make and use. Manufacturers of medical devices have to follow certain rules when they make their products in order to make them work together and integrate with each other to get the most out of them.

Compositionality: Techniques like temporal induction can help keep Smart Healthcare Cyber Physical Systems safe by making it easier to think about how devices that are connected to each other interact with each other in a certain way. The most difficult thing to do in this situation is to figure out how medical devices might interact in a way that isn't expected. Radio interference may happen between medical devices that are giving different treatments to the same person because they are close together.

Security and Privacy: In general, when medical devices connect to the internet, they have some networking abilities that could lead to security and privacy breaches when they are used together. Patients could be hurt or even killed if someone hacks into the Smart Healthcare Cyber Physical Systems network. Extremely, we can limit the functionality of devices that can be called up through the network interface but not accept any commands from the network, which is what we can do now. It's hard to keep the right balance between being able to move around and being safe for Smart Healthcare Cyber Physical Systems. We need to come up with some effective ways to deal with problems in electronic health records.

Verification, Validation and Certification: Before verification and certification are done, they are done when the design is finished. This is how it is now. The “design for verification approach” can be used to

make scaling for verification easier and easier to get the proof of the verification process. iii) Another method called model-based generative techniques allows verification to be done in the early stages of design, which increases the guarantees that can be provided by verification. Note that medical devices can be made into run-time parts.

11. CONCLUSION

Smart Healthcare Cyber Physical System refers to advanced medical technologies that use sophisticated embedded systems and network communication to monitor and control the physical dynamics of patient bodies, such as proton therapy machines, electro-anatomic mapping and intervention, bio-compatible and implantable devices, and robotic prosthetics. These technologies can be used to monitor and control the physical dynamics of patients. Modeling and efficient simulation of the patient's body will play a big role in designing and testing Smart Healthcare Cyber Physical Systems as well as in designing and testing customized treatment plans. Cyber-Physical Systems use computing, communication, and control to make new technology or the next generation of engineered systems. In the last decade, there has been a lot of work done on cyber physical systems that we didn't expect. There have been a lot of threats, challenges, and important issues in the last decade. These days, CPSs systems are used for energy, transportation and Industries among other things. This article made a comprehensive review about Cyber Physical Systems applications especially about Smart HealthCare.

References

[1] Ahmad Alzahrani, Mohammed Alshehri et al., "Improved Wireless Medical Cyber-Physical System (IWMCPS) Based on Machine Learning", Healthcare 2023, 11, 384. https://doi.org/10.3390/healthcare11030384.

[2] Amine Rghioui, Jaime Lloret et al., "Big Data Classification and Internet of Things in Healthcare", International Journal of E-Health and Medical Communications, Volume 11, Issue 2, April-June 2020, doi: 10.4018/IJEHMC.2020040102.

[3] Amit Kumar Tyagi, N. Sreenath, "Cyber Physical Systems: Analyses, challenges and possible solutions", Internet of Things and Cyber-Physical Systems 1 (2021) 22–33, https://doi.org/10.1016/j.iotcps.2021.12.002.

[4] Antonio Puliafito, Giuseppe Tricomi et al.," Smart Cities of the Future as Cyber Physical Systems: Challenges and Enabling Technologies", Sensors 2021, 21, 3349. https://doi.org/10.3390/s21103349.

[5] Fulong Chen, Yuqing Tang et al., "Medical Cyber–Physical Systems: A Solution to Smart Health and the State of the Art", IEEE Transactions on Computational Social Systems, Vol. 9, No. 5, October 2022, doi: 10.1109/TCSS.2021.3122807.

[6] Furqan Alam, Rashid Mehmood et al., "Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT)", Elsevier, Procedia Computer Science 98 (2016) 437 – 442.

[7] Rupa Ch, Gautam Srivastava et al., "Robust Cyber-Physical System Enabled Smart Healthcare Unit Using Blockchain Technology", MDPI, Electronics 2022, 11, 3070. https://doi.org/10.3390/electronics11193070.

[8] Rupali Verma, "Smart City Healthcare Cyber Physical System: Characteristics, Technologies and Challenges", Wireless Personal Communications, Springer, 26 August 2021, https://doi.org/10.1007/s11277-021-08955-6.

[9] S. K. Lakshmanaprabu, K. Shankar et al., "Random forest for big data classification in the internet of things using optimal features", Springer, International Journal of Machine Learning and Cybernetics, 4 January 2019, https://doi.org/10.1007/s13042-018-00916-z.

[10] Shah Ahsanul Haque, Syed Mahfuzul Aziz et al., "Review of Cyber-Physical System in Healthcare", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2014, Article ID 217415, 20 pages, http://dx.doi.org/10.1155/2014/217415.

[11] Suraj Kurde, Jayant Shimpi et al., "Cyber Physical Systems (CPS) and Design Automation for healthcare System: A new Era of Cyber Computation for Healthcare System", International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 12, Dec 2019, e-ISSN: 2395-0056, p-ISSN: 2395-0072.

[12] Syed Saba Raoof and M. A. Saleem Durai, "A Comprehensive Review on Smart Health Care: Applications, Paradigms, and Challenges with Case Studies", Hindawi, Contrast Media & Molecular Imaging, Volume 2022, Article ID 4822235, 18 pages, https://doi.org/10.1155/2022/4822235.

[13] Tejal Shah, Ali Yavari, et al., "Remote health care cyber-physical system: quality of service (QoS) challenges and opportunities", IET Cyber-Physical Systems: Theory & Applications, 2016, Vol. 1, Iss. 1, pp. 40–48, ISSN 2398-3396, doi: 10.1049/iet-cps.2016.0023.

[14] Volkan Gunes, Steffen Peter et al., "A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems", KSII Transactions on Internet and Information Systems Vol. 8, No. 12, Dec. 2014.