Internet of Things and Cyber-Physical Systems 1 (2021) 22–33

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems

# Cyber Physical Systems: Analyses, challenges and possible solutions

Amit Kumar Tyagi [a,b,*], N. Sreenath [c]

[a] Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India
[b] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India
[c] Department of Computer Science and Engineering, Puducherry Technological University, Puducherry 605014, India

ARTICLE INFO

*Keywords:*
Cyber-physical systems
Internet of things
Internet of everything
Challenges
Security, and privacy

ABSTRACT

It is becoming more difficult to protect the authentication of our data in today's world of smart living. On the one hand, we are able to live in smart homes and smart cities with ease. Even if we use the most complicated passwords, we can't be sure that the Internet of Things and the Internet of Everything are safe. One way to make sure people and things are safe is to use Multi-Factor Authentication. Also, a big and complicated system needs more efficient and robust solutions for real, and strong, security, so this is important. There are a lot of smart ways to solve problems today. For this reason, the internet of things is being used in every possible field or application. This new ecosystem, which is called Cyber Physical Systems, was built by IoTs. 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. We have a big problem with the security of CPS because the basic blocks used to make them are very different. Even if we're talking about natural gas systems or transportation systems or other automated systems, they all have something to do with CPS, no matter what. These days, CPSs systems are used for energy, transportation, the environment, and health care, among other things. This article talks about a number of problems that need to be solved by researchers and scientists (working related to respective area, i.e., CPS). As a result, this article also talks about a partial survey of important research issues, and an overview of several research projects that have been done in the last decade by a number of different people to improve CPS.

## 1. Introduction

It's very important to be safe in today's world of smart devices and smart environments, where almost all of the devices are connected to the internet. People who make their devices more secure also make them more efficient. It doesn't matter if researchers work for an organisation or work on their own personal data; security is important to all of us. Governments all over the world are passing new laws like the General Data Protection Regulation (GDPR) [1] to stop people from doing illegal things and to help people protect their own information. But, to keep data safe over a control system or a smart device, we need effective cryptographic methods. To be honest, we have to admit that there is no best way to protect ourselves. Even though encryption is a better way to keep communications safe, it requires that both the encryption key and the decryption key be kept in a safe place. Multi Factor Authentication (MFA) [2] is becoming more and more common as a way to protect their data from hackers. The best way to avoid an attack is to figure out how to predict when one is going to happen. CPS is an intelligent computerised system that uses controlled mechanisms and different algorithms to connect software and hardware parts so that it can work and show a variety of ways and approaches.

This is how it works now: CPS is used in a lot of different things like medical devices or transportation, and it's becoming more important as time goes on. Security is the main problem with the CPS system. To come up with a way to make these systems more secure in an efficient way is the biggest problem (but not rigid, fixed to one form of system). In Refs. [3,] many works have been done to make cyber-physical systems more secure. An authentication framework for a machine-to-machine communication in CPS has been talked about in Ref. [4]. Identity-based encryption and the AES (Advanced Encryption Standard) have been mixed together in this framework of encryption. There are more computer attacks on critical infrastructures and industrial control systems, and the core of these systems, known as CPS, is becoming more vulnerable to these. In this article, we talked about a lot of things that

* Corresponding author. Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India.
*E-mail addresses:* amitkrtyagi025@gmail.com (A.K. Tyagi), nsreenath@pec.edu (N. Sreenath).

https://doi.org/10.1016/j.iotcps.2021.12.002
Received 27 July 2021; Received in revised form 11 December 2021; Accepted 21 December 2021
Available online 23 December 2021

people are worried about when it comes to the security of CPS. So, in the organisation part, we talked about how this work would go and how it would be done (in the last of this section). This isn't all: There are a lot of different types of CPSs that we use in our daily lives, like in the following:

- Industrial Control System Cyber-Physical Systems (CPS)
- Smart Grid CPS
- Medical CPS
- Smart Vehicles/Automotive CPS
- Household CPS
- Aerospace CPS
- Defence CPS

### 1.1. Medical Cyber-Physical Systems

Medical Cyber Physical System (MCPS) 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. These tools can have a big effect on a patient's health if they're not used correctly. It's very important to make sure that all of the interactions are safe and accurate, but it can be very hard to do because of how complicated they are. Modeling and efficient simulation of the patient's body will play a big role in designing and testing Medical CPS as well as in designing and testing customised treatment plans. Then, in [5,6] we show that simulation speeds can be achieved in real time (for complex spatial patterns that could be linked to heart arrhythmias) with a standard desktop with GPU technology. Soon, hospitals will be able to run real-time simulations of organs. This will help people use model-based clinical diagnostics and treatment planning without needing supercomputers.

### 1.2. Cyber physical systems – in general

For the physical environment to work correctly and better, it is important to keep an eye on the behaviour of physical processes and take actions that could change their behaviour, which is why CPS was built. There are two main parts to CPS: one is the physical process and the other is the cyber system, both of which work together. With more interaction between these two parts, the impact of security threats in the cyber system on the physical system also rises, which makes it more important to keep them safe. In CPS, many attacks have been stopped over the last decade. There was a lot of damage done to Iran's nuclear facilities by the Stuxnet worm attack in 2010 [18]. Also in the last few years, some attackers or hackers have tried to make the systems of the United States, like air traffic control mission-support systems, useless. ‘Carshark’ was a name for a piece of software that some hackers used to be able to kill a car's engine from afar in 2010. It could also stop the car from stopping. If the ECUs communicate with each other, it could make the measuring instruments give out false readings. For example, it could look at how the ECUs communicate with each other and make false data packets so that hackers could do bad things. Also in the past, attackers/hackers have made changes to Siemen's plant-control system with a virus, worm, or patch. Some hackers are now able to get into medical devices that are implanted in people's bodies and work with wireless communications or Android apps. Several types of security flaws are found in most cyber-physical systems, such as digital power grids, smart transportation systems, medical systems, and defence systems.

Future CPSs don't just have physical parts. They also have chemical and biological parts, where information can be found in different substances and forms (information exists on multiple spatial and time scales). Multi-Scale Informatics (MSI) is thought to be able to get information from these subsystems. It can also figure out how information moves, and then connect subsystems together in a physical, syntactic, semantic, and operative way, so that they can work together better. MSI could be an important part of information theory, but it still needs a lot of people to use it and a lot of research. Complexity of technology makes it more difficult to keep new systems (technology) safe, but it also makes it more important to keep them safe. Privacy isn't a concern here (or large networking). It takes a lot of devices to make something complicated like a CPS or the Internet of Things. They connect together and change their structure often. As long as anyone can use the system and then leave the system after they've used it, new systems could be added to these types of systems. But, when users communicate with each other in CPSs, security is a must-have thing to have. So, the security architecture must be able to change with these kinds of changes and be able to give users safe and secure services.

Thus, the rest of this paper is organised as shown in Fig. 1: Section 2 starts with background work, which is a list of all the work that has been done by different researchers and scientists over the last decade to improve CPS (industrial, control systems, medical devices, smart Vehicles etc.). Section 3 has also talked about security components, requirements, or parameters. This is where they are explained. Section 4 talks about a number of critical threats that have been found in CPSs. Many problems with CPSs (like industrial, control systems, medical devices and smart cars) are also talked about in the fifth section of the text. Section 6 is the best part of this article because it talks about challenges and opportunities in medical cyber physical systems. Some more efficient solutions have been suggested, and more about them in Section 7. Section 8 talks about (lists) a number of open issues that have been found in CPSs that need to be addressed soon. Section 9 gives future researchers in CPSs a chance to work on a number of important issues and problems (raised in CPSs). In the end, this work comes to an end in section 10 with a short summary. In the end, Table 1 tells about the list of abbreviations used in this work.

## 2. Background

Cyber Physical Systems (CPSs) are those IT systems which are introduced in the applications of physical world. In these systems, sensors and actuators are already ingrained. The progress in ICTs results into more communication among cyber world and physical world which in turn increases the inter communication among physical processes.

### 2.1. Cyber physical systems – in real world

CPSs are used as the new generation of embedded control system that can monitor and control the physical world. Many applications like energy, transportation and healthcare are being increasingly dependent on CPSs. It depends on the technology being used as a very relevant and symbolic CPS is the Supervisory Control and Data Acquisition system [9] (SCADA) (used in CIs such as smart grids and ICSs), wearable and Implantable Medical Devices (IMDs) (used in medical care). Hence, it will be a herculean task to list out all the variations of CPSs, but in this work we are providing four representative applications of CPS and important details of these four applications are discussed in brief as:

a) Industrial Control Systems (ICS): ICS (or SCADA or distributed control systems) is the control system that enhances the control and production while monitoring different industries such as the nuclear plants, water and sewage systems, and irrigation systems. In ICS, we have different controllers such as PLC (Programmable Logic Controller). This device has variety of capabilities that can collaborate to reach a number of desired results. Sensors and actuators are being used to connect this device to the physical world. Both the wireless and wired communication capacities are configured in this system that can be used based on the nature of surroundings. Further, it can monitor and control the operations in a control centre by connecting it to PC systems.

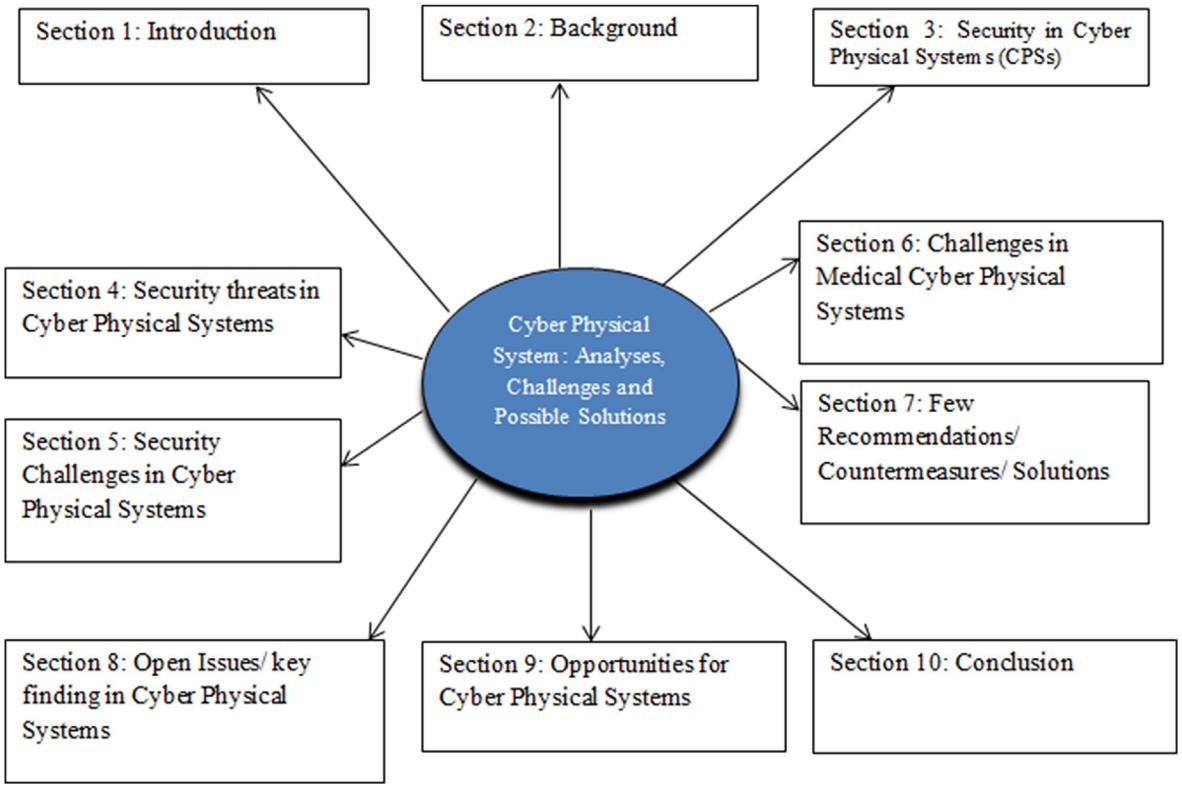


**Fig. 1.** Key organisation of the Work.

**Table 1**
List of abbreviations used.

| Short forms | List of Abbreviations |
|---|---|
| CPS | Cyber Physical System |
| SCADA | Supervisory Control and Data Acquisition |
| AES | Advanced Encryption Standard |
| MCPS | Medical Cyber Physical System |
| GPU | Graphics processing unit |
| ECU | Engine control unit |
| ICT | Information and Communications Technology, |
| IT | Information Technology |
| MSI | Microsatellite instability |
| MMR | Mismatch repair |
| SMD | Surface-mount technology |
| ICS | Industrial control systems |
| PLC | Programmable Logic Controller |
| PCA | Principal component analysis |
| IDS | Intrusion detection system |
| IPS | Intrusion prevention system |
| VPN | Virtual private network |
| CIA | Confidentiality, Integrity, Availability |
| IoT | Intent of Things |
| AMI | Advanced Metering Infrastructure |
| DoS | Denial of Service |
| FDI | False Data Injection |
| CAN | Campus Area Network |
| IMD | Implantable Medical Devices |
| V2V | Vehicle to Vehicle |
| V2I | Vehicle to Infrastructure |
| MAP | Mean Arterial Pressure |
| NIST | National Institute of Standards and Technology |
| MDCF | Medical Device Coordination Framework |

b) Smart Grid Systems: Although power grid is being used for decades, smart grid is the next generation grid for generating electricity with advanced functionalities. At local level, it is economically and environmentally feasible by allowing the consumer to have better control over their usage of energy. While at the national level, it enhances the control over emission, global load balancing and saves the energy.
c) Medical Devices: Cyber and physical capabilities have been incorporated to improvise medical devices with an aim to deliver better health care services. These medical devices are designed to serve the patients by being implanted inside the patient's body (IMD's [7,8,10]) or worn by them in the form of wearable devices. Such devices are smart and they have wireless capabilities to communicate with other devices. This communication is being provided by programmer, require for updating and reconfiguring the devices. Wearable device is more helpful in tracking minor activities of patients.
d) Smart Vehicles: Smart Vehicles are vehicles that are more environmentally friendly, more fuel-efficient, safer, and have improved usability and convenience. Through depending on a number of 50–70 networked computers, called Electronic Control Units (ECUs), these developments were made possible. ECUs [11] are responsible for monitoring and regulating different functions such as engine emission control, brake control, entertainment (radio and multimedia players) and comfort features (cruise control and opening and closing of windows). Such innovations are most needed technology in current era scenario (i.e., to reduce traffic congestion, accidents, etc., over the road/region).

### 2.2. *Trends in medical cyber physical system (MCPS)*

As we have discussed about wearable devices, and IMDs, now we discuss importance of CPSs in medical applications, i.e., medical devices that are software-intensive, such as infusion pumps, ventilators and patient monitoring. These medical devices are attracting many people to make their life convenient and easier to life (via identifying causes of diseases or curing diseases). However, having a major transformation to these devices creates new challenges in the respective application (also providing/opening new opportunities for the research community). The main trends in medical devices can be summarized as follows:

a) New software-enabled functionality: Via software-based design (of medical device systems), for example, robotic surgery, proton therapy treatment, new technology is introduced in medical devices using embedded system principles. This (robotic surgery) requires high-resolution images and haptic feedback to be processed in real time. Whereas, it is one of the most technology-intensive treatments (proton therapy treatment) and involves one of the largest networks of medical devices. This delivers specific doses of radiation to patients with cancer, providing precise instructions from a cyclotron for patients for the treatment of the proton beam. The bigger problem is that the same beam is distributed to different patient locations and has to be moved from location to location, opening up the possibility of interference with beam scheduling and beaming. Several researchers have been studying the security of proton therapy machines in the previous decade, but mostly their research focuses only on one device, i.e., faces emergency shutdown. Proper analysis and evaluation of such large and complex structures is therefore one of the major challenges facing manufacturers/industry of medical devices.
b) Increased connectivity of medical devices: Medical devices are increasingly relying on software in the current era, i.e., they are equipped with network interfaces. Such integrated medical devices allow a decentralized network of medical devices that must be properly designed and tested in order to perform some function or look like patients (cure diseases). These medical devices are used for patient tracking and for integration with Electronic Health Records (EHR) to store patient data through local connection of individual devices to integrated patient monitoring or remote monitoring in a tele-ICU setting [12]. Capabilities of such medical devices in the current scenario are limited in scope and regulation by device manufacturers or healthcare practitioners, resulting in increased patient safety and new treatment procedures. Medical Device Plug-and-Play (MD PnP) Interoperability initiative [13] is an initiative that offers an open standard system for safe and scalable medical device interconnectivity, as well as enhancing patient safety and efficiency in health care.
c) Physiologically closed-loop systems: In general, many clinics have a caregiver to monitor the system (or more than one). An anaesthesiologist, for example, controls a patient's sedation during a procedure and determines when to take action to change the sedative stream. Yet, in the medical community, there is a concern that such dependence on "person in the loop" could compromise patient safety. A vital warning sign may be ignored by caregivers who are often overworked and function under extreme time pressure. Nurses may not be in a position to handle multiple patients at a time, but they can handle a machine that will be a great relief for the caregiver and can improve patient care and health. Although a computer (machine) can never completely replace the caregiver (in feeling/emotions), it can minimize the workload substantially, calling attention to the caregiver only when something out of the ordinary happens. Scenarios based on closed-loop physiological regulation have been used for some time in the medical device industry. Patient-Controlled Analgesia (PCA) [14] is a clinical-based condition benefiting from the approach of the closed loop. PCA infusion pumps are commonly used to supply opioids, i.e., after surgery, for pain management. PCA pumps give a button to the patient to ask for a dose when they decide they want it instead of using a schedule provided by a caregiver.

A properly configured PCA device should not allow overdose as it is designed with limits on how many doses it will produce, regardless of how often the button is pressed. This safety mechanism, however, is not enough to cover all patients' requirements. Many patients may experience overdoses if the pump is mis-programmed, if the pump developer overestimates a patient's maximum dose, if the incorrect amount of the drug is loaded into the device, or if someone other than the patient is pressing the button (PCA-by proxy), among other reasons. PCA infusion pumps are currently involved in a wide range of adverse events, and proven protections such as drug libraries and programmable thresholds are not sufficient to resolve all the clinical practice scenarios [15]. Therefore, in order to solve such cases, we needed efficient medical devices to look at patients in the near future (also devices needed to calculate the level of the drug in the body of the patient).

d) Continuous Monitoring and Care: Due to the high cost of in-hospital care, there has been a growing interest in exploring alternatives such as home care, assisted living, telemedicine, and supervision of sports activities. Mobile tracking and home monitoring of vital signs and physical activity make it possible to assess safety at all times remotely.

Also, several medical devices are in tend to measure heart rate, breathing rate, blood-sugar level, stress level, and skin temperature (of a patient/person). Nonetheless, with no real-time diagnostic capabilities, these tools' function/operate in store-and-forward mode. Closed-loop technology in physiology will allow real-time clinical assessment of vital signs and will require constant care.

### 2.3. Cyber security vs network security vs information security

Cyber-security is a part of information security, which is a bigger part. Cyber security is used to protect an organization's networks, computers, and data from unauthorised digital access, attack, or damage by using a wide range of processes, technologies, and practises. InfoSec makes sure that both physical and digital information is safe from being accessed, used, disclosed, disturbed, altered, reviewed, recorded, or destroyed. The goal of InfoSec is to keep data safe in any form, while cyber-security only protects digital data. As a result, network security's job is to protect the IT infrastructure of the company from all kinds of cyber threats like viruses, worms, and Trojan horses as well as hacker attacks, denial of service attacks, spyware, and a lot of other attacks. A network security framework has many parts that work together to make us more secure. Most networks have firewalls, anti-virus software, intrusion detection and prevention systems (IDS/IPS), and Virtual Private Networks (VPN) to keep things safe.

This section talks about work done on cyber physical systems, such as trends and work done in the last decade (to make CPS or MCPS more secure) in great detail. Also, this section talks about the differences between cyber, information, and network security in a clear way. Now, in the next section, we'll talk about the security needed in CPSs, as well as the difference between CPS security and other systems' security, like in a company.

## 3. Security in Cyber Physical Systems (CPSs)

In this paragraph, we give several examples of how important safety is in CPS. Security control usually refers to things like cryptography, access control, detection of intrusion, and a lot of other things (used in IT systems). They are very important when it comes to protecting the infrastructure of an ICT. Cyber physical systems that aren't going to make mistakes in the near future are going to be needed a lot. This is because there are going to be a lot of attacks like this in the future. These are some of the security requirements for different uses of CPSs:

- Based on the case, not having or not having enough protection in the CPS could be very bad. For example, if the safety of CPS used in a nuclear plant has been harmed, the result could be a threat to the whole world. There was an attack on Iran's nuclear power plants called Stuxnet in 2010. There are also a lot of old systems in big industrial control systems. This is also true. Many people have been working on things like "lightweight cryptographic mechanisms" (to keep data safe, accessible, and secure) over the last decade. But there is still a lot of work to be done in all of them. Keep in mind that having some level of security is better than having no security at all. Security

is an important part of an ICS, and it needs a lot of help from the research community.

- Consumers could lose service and the utility company could lose money if smart grid security is breached, which could happen. Smart grids can also be attacked from afar, which could cause a lot of people to lose power. There could be health and safety consequences if there are power or energy outages, such as malfunctions of medical machines, data loss at data centres, and even an increase in crime rates [16]. So, security is an important part of Smart Grid CPSs (also to protect user information in systems).
- Patients' safety could be at risk if wearable devices and IMDs that are targeted by hackers are not properly protected. Goals for safety and privacy (CIA: Confidentiality, Integrity, and Availability): licenced agencies should be able to access and use accurate data; they should also be able to recognise and customise devices, upgrade code, and make sure that devices are available. So, security in a medical app is very important to protect the user's or patient's personal information.
- Manufacturers of cars are trying to come up with new technologies that will make their cars more useable and comfortable for their customers. Vehicles are usually built to be safe, but this may not be the most important thing to think about when researchers designing them. Security protects the ability of the car to run in non-violent accidents. Safety, on the other hand, was not part of the design, but an extra feature. The new features of the car need to communicate wirelessly and physically affect parts. Such two technologies are used in smart cars to deal with most security flaws or attacks. We need safe and effective ways to fight back against these attacks.

For critical control systems or CPSs to be properly protected, the technology that underlies them must meet certain performance standards. This way, well-tested safety mechanisms and standards can be used.

### 3.1. Security parameters

There are a lot of factors that are used when it comes to CPSs in order to make sure that the systems they protect are safe enough (real world applications). Our security rule must keep CPSs safe from any kind of threat or attack.

It has become more and more clear in recent years that the safety of control systems has become a very important part. The most common difference between control systems and IT protection is that control systems don't need to be patched or updated. For example, it may take months to figure out how to take a computer offline for an upgrade. It's not worth it to stop an industrial computer to install new security patches all the time. During a software update on March 7, 2008, a device used to keep track of chemical and diagnostic information from the plant's business network started up again. This caused a nuclear power plant to be shut down by accident. There was no data to show that there was a drop in water reservoirs, which meant that there was not enough water to keep nuclear fuel rods cool. The computer restarted, which caused this mistake. It is important for control systems to make decisions on their own, but they also need to make them in real time (another control system property). As a security issue, availability has been looked at a lot. In real time, though, it has a stricter operating environment than most other IT systems.

This section talks about a number of security parameters and requirements for security in CPSs, so this is the last part (i.e., in smart grid, smart control systems, etc.). Now, in the next section, we'll talk about a few different types of security threats in Cyber Physical systems (i.e., in smart grid, smart medical devices, smart control systems, etc.).

## 4. Security threats in cyber-physical systems

In the previous section, we talked about the security requirements for four different applications of CPSs. Now, we need to talk about some possible threats in each of these applications. It talks about five types of threats (criminal, financial, political, privacy, and physical) and how they affect five things, like the source, target, motive, vector, and outcome [17] (refer Table 2, in appendix A). Now, some other cyber physical attacks are being talked about in this part.

### 4.1. Real-world cyber physical attacks

This discusses about Cyber (C), Cyber-Physical (CP), and Physical (P) attacks on a number of CPS applications that harm CPS systems, and how to avoid them. Publicly known attacks are very rare, and it's very hard to get back or figure out what happened right away. Attacks are grouped in this chapter based on where the injuries are. Cyber-attacks that don't hit sensors or actuators are called “cyber.” Physical attacks that target physical parts are called “physical.” Cyber-physical attacks, on the other hand, are attacks that affect physical components by way of cyber components. However, this isn't new when it comes to extortion control systems. A lot of countries now have terror and physical attacks are used to try to get money from people. Cyber-attacks [32–36] are a natural next step in the evolution of physical attacks because they are faster, cheaper for the target, don't have to be limited by distance, and are easier to make and manage. It is now possible to list some cyber and physical attacks on CPS as:

**A. Cyber attacks on cyber physical systems**

a) Industrial Control System Attacks: In 2010, an attack called “Stuxnet” caused damage to several nuclear plants in Iran. Recently, hackers from the United States have carried out a number of cyber-attacks on Iran. Thus, two types of attacks have been found on ICS.

- Communication protocols: There were a lot of attacks that took advantage of flaws in communication protocols. For example, a SCADA device showed how to fool the address resolution protocol.
- Espionage: DuQu and Flame are two examples of hacking ICS attacks that can be used to spy on people. Flame, for example, targeted and found many ICS networks in the Middle East in 2012. The main goal of this malware was to get private information from companies, like their addresses and the keys they typed.

Many countries are being attacked by hackers or people who aren't supposed to be there every day. Now, countries are using these attacks as a weapon to cause as much damage as possible to the other country (the enemy).

b) Smart Grid CPS Attack: This is the most common example of a smart grid attack. Blackout is the most common. Attackers can do cyber-attacks on Smart grids [23], which could cause a blackout (i.e., no lights at all) in a country. When it happened in Europe and the United States a few times in the last decade, it was very important.

c) Medical CPS attack: A distributed system is vulnerable to cyber-spies, insider attacks, and other types of attacks. This is one of the main threats. An insider can damage or tamper with any medical devices and make machines do what he wants. An intruder could also harm people by jamming the wireless signals that medical devices use to keep people healthy. This would make the device unusable and not be able to deliver the therapies needed.

d) Smart Vehicles Attacks: Controlling a vehicle or car from afar or through an outside attack is a big problem. Any vehicle could be hijacked by an attacker, which could cause a big accident on the road.

**B. Physical attacks on cyber physical systems**

Several physical threats/attacks have been listed in various applications of CPS in Table 2 (refer appendix A). some of the popular physical attacks in previous decades are: i) in 2006, A computer at a water filtering plant in Pennsylvania (USA) was hacked by an attacker and used as its own spam and pirated software distribution system [19]. ii) At the Davis-Besse power plant in Oak Harbor, Ohio, machines infected with the

Slammer worm shut down security monitor systems in January 2003. iii) In 2000, the assault on the sewage control system of the Maroochy Shire Council in Queensland, Australia (which was carried out by the disgruntled ex-employee of the contractor firm that had built the respective control system). Now, this section discusses a threat model in CPS with an example.

### *4.2. An adversary model in cyber physical system*

A thorough look at the security of any system is needed to figure out what risks are likely to happen in the near future. Creating an adversary model is a way to figure out how wide the problem is and how risky it is. As far back as the last decade or so, cybercriminals have been hacking computers wherever they can find them (even in control systems). Such attacks may not be targeted (i.e., they are not meant to harm control systems), but they may have negative side effects: control systems that have been infected with malware may not work the way they should. These attacks are important from a security point of view because they are caused by insiders, people who have access to the computers and networks used by control systems. Even if control networks were completely isolated from public networks and the Internet, attacks by insiders could still happen. Employees who don't like their jobs are the main source of targeted computer attacks at the moment. Most of the time, these workers do not work in groups. Their actions may not be as harmful as those of larger, more organised groups. This is a big problem in CPS that needs to be solved, and it needs practical and realistic solutions.

This could be because terrorist groups and criminal gangs could try to get into security structures. There is no proof that terrorists or activists have used computer attacks to get into control systems. There is, however, some evidence that criminal groups may be involved. These days aren't new, but CPS programmes are getting a lot of attention for their money-making purposes. It is used to coerce and intimidate, like Iran and Iraq have had physical attacks for a few years now. In the near future, most military powers are looking at new threats, such as cyberattacks on other countries' physical infrastructure.

- Attacks: Attackers can do things like resonance attacks on control systems to get into them (i.e. attacks that are not feasible in conventional IT systems). There were some sensors or controllers that were hacked by someone else, making the physical system go back and forth at its resonant frequency.
- Consequences of an Attack: To our knowledge, no one has looked at the possible effects of attacks on important infrastructures. SCADA security reports may sound like they're overreacting, but it's important to remember that a user can get access to a control system that doesn't belong to them. Most control systems have safety measures in place to avoid major disasters.

Thus, this section talks about a lot of different threats to many CPSs, such as financial, political, and privacy threats. Now, in the next section, we'll go over some of the problems that many CPSs have.

## 5. Security challenges in cyber physical systems

The words challenge, threats, and vulnerabilities are used together in this work (paper). Challenges are questions that haven't been answered yet, and we want to encourage people to do research to find out how to solve them. Vulnerabilities are internal (security) flaws in a system that can be exploited by outsiders. Threats are things that could be bad for a system.

### A. General CPS security challenges

a) Security by Design: Most CPS are not designed with security in mind because they are not connected to other networks, like the internet. This means that security isn't taken into account in the design of most CPS, because they are not connected to other networks. Physical security, then, was almost the most important way to keep people safe.
b) Cyber Physical Security: Physical security, then, was almost the most important way to keep people safe. CPS designers need to change how they think about security so that both the cyber and physical aspects are taken into account. This could help us better predict and stop future cyber-attacks that have physical consequences. We need to build structures for both parts of the solution (cyber-physical solution) that have been overlooked before.
c) Real-Timeliness Nature: The requirement in real time is a requirement that affects the state of defence if it isn't met. Networks that are under attack need to make quick decisions in CPS to stay alive. That way, a CPS security design that takes into account the interactions between physical and cyber aspects shows the whole world. This allows for better risk assessment and threat detection as well as more resilient solutions [20]. There must be lightweight and hardware-based mechanisms built on top of cryptographic mechanisms to improve real-time interaction and deadlines, so this is what needs to happen.
d) Uncoordinated Change: There are a lot of people who work with the CPS. It includes people who make, use, own, and run things, as well as people who work for them. It's important that they are properly managed, even though their roles and rights are different. A lot of people, as well as the different parts of the CPS, need to be taken care of during the transition (a problem that we should not ignore). It's important for stakeholders in a community of CPS parts to work together at some point. Some ways to make things better, like upgrading hardware, updating or changing applications, and adding new features [21]. Keep in mind that any unplanned changes to CPS security (i.e., new vulnerabilities) could make the system less secure and could be a big problem for a country to deal with.

### B. Industrial control system challenges

a) Change Management: In an ICS environment, many Internets of Things (IoT) devices must be replaced, changed, or deleted. These devices build different systems that must be replaced, changed, or deleted (at one place). A system update in ICS, for example, needs to be planned carefully to avoid problems. Also, many investors can change the security posture of the ICS system without their knowledge, so we need to coordinate change management to avoid and track security-related changes in the ICS system [22].
b) Malicious Insider: A malicious insider is very hard to find or stop because the attack is taking place inside of a company, either intentionally or unintentionally. For example, an insider might use her or his trust and inside information to launch an attack like the attack on Maroochy water and sewage system (through remote attackers), or the spread of Stuxnet. This is just one example (through a USB stick). In this case, insiders could accidently use a virus-infected laptop or USB stick that could give an ICS access point to outsiders. So, figuring out who is an insider attacker is the biggest problem that many research groups don't think about or don't pay attention to.
c) Secure Integration: The integration of new components into older systems must be done in a safe way in order to avoid new security flaws. Notice that ICS relies a lot on old systems that could be vulnerable to flaws. Because there are so many old parts in ICS, it is not possible to replace them all with new, safer ones. So, short-term solutions need to be found to keep ICS from having any problems.

### C. Smart grids challenges

a) Change Management: It's not easier to deal with changes in smart grids than it is with ICS, but it isn't easier. Even though smart grids are more complicated and have more people involved, they can't handle changes very well. It makes change management a must-have for healthy smart grids.

b) Two-Way Communication: A smart grid has two-way communication because of the Advanced Metering Infrastructure (AMI). Unlike the power grid, AMI allows smart metres to communicate with utility companies that are close to customers' homes, which makes them easier for physical attackers to get to. It has become more difficult to keep these devices safe in smart grids, where there are more devices than before.
c) Access Control Mechanisms: Smart Grids have a wide reach and a lot of investors, so they need to have good access control mechanisms. It is important to keep an eye on and control all possible access to the network, data, or devices of smart grids. For emergency situations, it is always best to give the people or groups who are supposed to help enough power.
d) Privacy Concerns: People are worried about how their data will be used. As smart grids become more common, this has become a big problem for people. Not only should the data of customers be encrypted, but it is also important to suggest anonymization techniques to keep attackers from deducing patterns or encrypted data to reveal private information. This is called “anonymization.” Thus, we need to make sure that the mechanisms we build can encrypt and aggregate data both safely [24].
e) Explicit Trust: In this case, there should be no clear trust given to sensed data and commands that have been sent. Alternatively, new ways must be found to identify false data and commands that are not authorised [25]. FDI attacks can be hard to detect because of the large size of smart grids, which make it hard to use certain algorithms that only look for problems [26].
f) Comprehensive Security: It's good to have high-level security in smart grids. It's bad at lower levels (due to the limited capabilities in the devices on low-level). As a result, the level of security that must be put in place at each level may not be the same. Many research groups need to come up with lightweight solutions in order to do this. At all levels of the smart grid, encryption is also important to keep information private and secure. This is to avoid any security breach.

### D. Medical devices challenges

a) Security Versus Usability: This can also happen if a device has too much security. For example, not being able to change the unit when the patient is in a critical condition. So, a person with IMD might be in a situation where another health care provider or doctor needs help right away. The provider doesn't have cryptographic keys or access rights that allow him or her to change the IMD, so not having the IMD could be very dangerous.
b) Add-On Security Versus More Code: Security is important, but the cost of putting it in should not be too high. Making IMDs more secure could make the code bigger, which could make medical devices more likely to be taken back. So, cryptographic operations that also affect how medical devices work and how much they cost (be available to patients) need to be made as light as possible.
c) Limited Resources: Cryptographic mechanisms use a lot of power (a limited resource) and must keep that power up for a long time (long time). Devices that need surgery to be put into a patient's body, for example, need to work for a decade or two at the most (at least). Another thing to note is that many attacks may try to drain a battery to make a device not work, which is called a Denial of Service (DoS) attack [27]. Keep in mind that the device gets signals from people who don't want them and processes them. This can be a problem and drain the battery. So, new control mechanisms need to be made so that medical devices don't respond to any kind of malicious interactions, which is why they need to be made.

### E. Smart Vehicles challenges

a) When manufacturers put COTS and third-party modules into smart cars, there are conflicting security assumptions at the edges of integrations. Manufacturers of cars need to make sure that COTS integration is stable and that other parts work well. It should make sure that the manufacturer of a car doesn't make any concessions in terms of security.
b) If the gateway Electronic Control Units (ECU) can be bypassed, then many different types of attacks can be used against it (such as bypassing it and getting into restricted bandwidths) [28]. Separating critical and non-critical ECUs, using Ethernet/IP communications, and replacing gateway ECUs with Master-ECUs are all effective ways to make our cars work better.
c) Parts and components of vehicles are made or bought (imported) by other partners in the vehicle industry. To make sure there aren't any security holes or patches, both the seller and the buyer should pay more attention to the needs for security, assessment, and testing. From the start of the design process, manufacturers must think about safety.
d) Because of the assumption that the CAN network is isolated, it is vulnerable. New protocols that assume that there could be malicious attackers are needed.
e) V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communications are going to have a lot of new security problems in the next few years. These threats are needed to stop efficient solutions and let them work.

Hence, this section discusses various identified critical challenges (in the past decade) in smart Vehicles, smart medical devices, industrial control systems, etc. Now, next section will discuss more challenges (especially) in medical cyber physical systems.

## 6. Challenges in medical cyber physical system

As discussed above, some challenges exist in medical devices and this section discusses some other challenges prevalent in Medical Cyber-Physical System (MCPS) which are needed to be solved in the near future by researchers/scientists. Note that some useful points or details like uses, open issues, challenges of (in) MCPS can be found in Ref. [33]. Hence, some other critical challenges in MCPS listed here as:

a) High Assurance Software: Medical devices use technology to automate some features, like hardware (like security locks) and other things. But it is well known that software development is too important to keep MCPS safe.
b) Interoperability: It is important to make sure that the medical devices that work together are safe, accurate, efficient, and secure and that they have been certified.
c) 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.
d) Autonomy: The analytical knowledge that MCPS 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.
e) Security and Privacy: security and privacy of MCPSs is very important, because MCPSs collect medical data and also manage the data they collect. Because of this, it's important to keep them safe from anyone getting their hands on or changing any of their information. Such an act can cause the patient to lose their privacy, be discriminated against, be abused, or even be hurt by someone else.
f) Certifiability: MCPS needs a cost-effective way to show that medical device software is reliable and safe, like by getting medical device certification.
g) Executable clinical workflows: Today, more and more medical devices connect with each other and work together so that they can build and deploy MCPS quickly to provide efficient clinical

services to a (given) patient. Patients' safety is the biggest problem with putting MCPS 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.

h) 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 MCPS 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.

i) 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.

j) 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 PCA situations. We need more simple methods to help us solve the problem of designing and analysing things. These methods could make some comprehensive models less complicated.

k) 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 (having similar medical conditions). Patients may have a very different reaction to treatment, which could cause a lot of confusion and waste time in MCPS. 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. This is how it works: (EHR). In that case, we need to make algorithms that can be changed to fit a patient's specific needs. Our plan is to look at the patient's exercise history in the EHR and change the thresholds for the alarms, so that there are less false alarms, as well. In the near future, we will be able to use "smart alarm services" in medical devices to cut down on false alarms.

l) User Centred 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.

m) Infrastructure for Medical-Device Integration and Interoperability: At the moment, only one company is developing distributed MCPS that use a proprietary communication protocol (making regulatory approval simpler, but reducing the benefits of inter-device communication). There are many open standards (interconnectivity) that are the norm when it comes to MCPS (including basis for interoperability of medical devices). 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.

n) Compositionality: Techniques like temporal induction can help keep MCPS 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. Treatments can interfere with each other by changing how the body responds to them. "Mixed criticality" is an example of this. Mean Arterial Pressure (MAP) measurement is based on where the patient and the sensor are in relation to each other. Because the bed of the patient, which is a medical device of Class I, which is the least important in the FDA classification, is raised, the reading of the MAP changes. If the MAP sensor is part of a system that keeps an eye on things like a patient's vital signs, the sudden change could cause false alarms or other bad behaviour. This problem was used to give the monitoring system more information about the environment. Trying to figure out how to make these devices while taking these things into account is hard.

o) 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 MCPS network (by re-programming devices). 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 MCPS). We need to come up with some effective ways to deal with problems in electronic health records.

p) 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.

Hence, this section discusses various identified critical challenges (in the past decade) in medical cyber physical systems. Now, next section will suggest some countermeasures or solutions for such critical (identified) problems/challenges (identified in Section 5 and 6).

## 7. Some counter measures/solutions

Most of the efforts to protect control systems (especially SCADA) have so far been based on reliability (protecting the system from random errors). Hence, an essential issue is protecting control systems against several malicious cyber-attacks.

- **Prevention:** Preventing attacks on medical devices is a better way to deal with them than waiting for them to happen. Many companies are working on ways to keep their chemical, oil, and gas, and water facilities safe, like by making sure they have safety plans in place. NIST has also released a Guide to Industrial Control System (ICS) Security [29,30] to talk about how to keep control systems safe, as well. Sensor networks are also used in process control systems like SCADA [31]. There are two groups working on standardising the communication between them. Safety of these wireless communication devices/ideas can be made more secure by setting up confidentiality and integrity mechanisms that work both hop-by-hop and end-to-end (with providing necessary protocols for access control and key management).

- **Detection and Recovery:** When an attack is successful, there is no way to stop it. Security engineers have come to realise that detection and response are important. Control systems are used to look at network or computer system traces for signs of intrusion. Attacks that aren't visible from the IT side can be found by looking at the physical system for signs of trouble. However, algorithms haven't been used to look for deception attacks on estimation and control algorithms. Further, no one has come up with a way to tell if controllers or sensors have been hacked, but if the people who run the systems are told, we can detect many attacks. However, research on human-computer interaction is important and difficult, because not only do we need recovery with a person in the loop, but we also need to be able to recover without a person in the loop. As a result, new problems can be seen when people look at and design a safe system after using autonomous real-time decision-making algorithms that control the real world. So, a control theory that changes how fault detection and isolation works is needed to come up with autonomous and real-time detection and response algorithms for safety-critical apps.
- **Resilience:** Today, there are many ways to make control systems that can withstand even the most serious attacks. Redundancy, for example, is a way to make sure there isn't just one place where things could go wrong. Diversity is a way to keep all copies (the extra redundancy) from being corrupted by a single attack method. So, we need to come up with a new, more robust control and estimation algorithm that looks at real-world models of attack (from a security point of view). So, making access control policies (closed-loop dynamics of controlled systems) isn't enough without taking into account the results of "what if" type questions. The way closed-loop dynamics work when network parts are attacked must be based on this kind of analysis.
- **Deterrence:** People who commit crimes outside our borders are more likely to be deterred if we have good laws, good police, and good international partnerships.

Hence, this section provides several countermeasures/solutions to identified challenges or problem in various cyber physical systems. Now, next section will list some open issues or key finding in CPS for researchers (as future work). In continuation to this, several open issues will be discussed in Medical cyber physical system (with noticing importance of such system in future).

## 8. Open issues/key finding in cyber physical system

When it comes to engineering, today's Cyber Physical System is at a high point, which makes it a very complex, multi-scale system that can change. These systems are being used in a wide range of applications in some of the most important sectors, and they have also sparked a desire for researchers to look into other solutions. Those are the main findings of our research work.

- Cyber-physical systems have become a lot more common, but there are still some parts of the field that aren't well-defined or that are still being studied. It takes a lot of work to make CPSs work in the real world. This includes a lot of cross-disciplinary knowledge, tight integration of the enabling technologies, and careful attention to the human and environmental aspects.
- It is very important for a system to have a common vocabulary, comprehensive concepts, abstract models, system frameworks, and standards that work together. Conceptualization, development, implementation, and testing of CPSs all need a strong theory and method for abstracting to work well (also conceptual and computational abstractions, i.e., which is useful for both human and computational agents).
- Abstractions should be used in formal models to make it easier to write down, build, and connect CPSs. mathematical logic and numerical calculations must be used to make continuous control models (of physical systems) and to make discrete digital models (of physical systems) (with higher level of integration). Many concepts, such as synergy, compositionality, time-correct control and operation, goal-oriented learning, and so on, also need to be looked at by the research community.
- Advances in software, information, communication, and control technologies made it even easier for electromechanical and computer technologies to get smaller and smaller.
- It is very easy to identify, profile, and assess CPSs because they all have a lot of different things that make them unique. There are a lot of big differences between CPSs in terms of how they work, how they look, and how they can be used, but also in terms of their intelligence, adaptability, and self-management.
- Many scientific, technological, and application problems arise because of their inherent characteristics, such as symbiosis, complexity, heterogeneity, uncertainty, adaptability, scalability, robustness, safety, security, and so on. These characteristics get extra attention from the research community.
- Everybody can use CPSs, and they can be used for anything at any time. CPSs are built on the idea that they can be used anywhere, from home and work to hospitals and entertainment. They can also be used for other things at any time. In addition to having 100% connectivity and reliability, they also need to be able to provide instant and context-appropriate response, inform themselves and store the information they get or make, make reliable decisions either alone or together, and be self-aware, self-sustaining, self-adapting, and self-repairing.
- CPSs need to be able to learn at the first, second, and third levels. Sensors and miners are used to get information about the system. Miners then use the information to think about how to make the system run better in predefined task windows. Using second-level learning, CPSs can learn about the environment in which they work, and they can adapt to changing situations (to keep a static norm state) by changing their functions. Third-level learning lets them change their structure and function based on the mix of synchronous and asynchronous events that come in.

Since many unrelated ideas and technologies will not lead to the next generation of CPSs, this means they won't come together to form them. Systems (holistic) interconnections, model-driven specification and real time computation will lead to it being built. Platforms and components will be used to build it. It will be built with minimal intrusion.

### 8.1. Open issues in medical cyber physical system (MCPS)

During our research, we have found a few things that need to be done in the field of Medical Cyber Physical System (MCPS). These issues can be called:

#### 8.1.1. Security and privacy

Security and privacy issues are being talked about in MCPS, which is when medical devices can talk to each other. An attacker who wants to get into an MCPS network can also harm or kill patients by reprogramming tools, as we talked about above. With closed-loop monitoring, automated therapy delivery, and warnings, the greater flexibility of MCPS could make the problem worse. There are four groups of people who can be targeted by an MCPS, and they can choose from any of them.

- **Patient:** An attacker tries to hurt the patient's health right in front of them. Targeting the MCPS parts of sensing, processing, communicating, and giving treatment is usually the best way to do this for example, someone could hack into an infusion pump and make it give out more medicine than it needs to.
- **Data:** An attacker gets into MCPS health data from individual patients in an unapproved way. Patients may not be able to keep their identities private, which could lead to discrimination and misdeeds.

- **Device:** People try to do denial of service (DoS) attacks on the MCPS in a number of ways, which means that it can't do its job properly, resulting in privacy loss or the failure of CPS systems.
- **Institutions:** The goal is to break up or get a lot of access to patient data or organisational network information from the inside of the institutions.

There are medical devices that are made to be able to send data in the future, like sensor readings or event logs, but they can't be used to do anything. In this way, we will be able to get over security and privacy concerns in medical devices. Also, device manufacturers should come up with some effective ways to keep their products safe, such as relying on security through obscurity. To keep medical devices and the Medical Device Coordination Framework (MDCF) from being hacked, we could start encrypted communications and save information in a block using Blockchain connects. As a first step, we could build trust in the devices and the clinical workflow.

*8.1.2. Continuous monitoring and care*

Today's patients need to be looked after all the time, so we need to come up with medical devices that can help (i.e., monitoring, decision support, and delivery of therapy). These devices may come up with new ways to get health care, like home-based or ambulatory care, which could help cut down on the overall cost of health care. They also send notifications in case of emergencies, so the person who comes first can get the most up-to-date information about the patient's health. These systems are made to track a wide range of conditions, like cardiovascular and neurological problems, as well as meta-physiological state information (sleep, wakefulness, fatigue), activity monitoring, and a lot of intense environmental medical monitoring (e.g., space).

There are always problems with patient modelling and simulation, user-centred design, the design of medical devices, and the continuous monitoring and care of patients in MCPS. These are the main issues. MCPS has four issues that need to be looked at by computer and other research communities. These are:

- Reduce the amount of time it takes to set up and use security solutions.
- Dealing with the different types of MCPS that don't work with system-wide solutions.
- Making security solutions easier to use (including transparency)
- Taking into account the security implications of security solutions and decisions.

Hence, this section discusses several essential issues in Cyber Physical Systems (including medical devices, smart grids, etc.). Now, next section will discuss several important opportunities in Cyber Physical Systems for future (in detail).

## 9. Opportunities for cyber-physical systems

They are very good at stopping the damage that disasters do to society and the economy. Cyber Physical System technologies can help. There are a lot of technologies for rapid evacuation management systems that can track environmental and geographical problems that are spread out across a large area, figure out how damage spreads, and figure out how to control traffic. These technologies can be used to stop the bad effects of disasters. There are a lot of ways that CPS research can help close the gap between the amount of food or other things people want and the number of things they have. Precision farming, smart water management, and efficient food distribution are all examples of technology that can help solve this problem. This means that more food can be consumed and more food can be made. Because of this, some of the opportunities for cyber physical systems:

- There were almost no car accidents, very few injuries, and a lot less traffic congestion and delays.
- Buildings and cities that use less electricity.
- Medical and healthcare systems that are smart, reliable, and flexible.
- Generation and distribution of electricity that doesn't go down
- Farming with a lot of fruit
- Faster and more safe evacuation in the event of any disaster.
- Assists for busy, old or disabled people all their lives.
- Users can get high-quality medicine at anytime, anywhere.
- It takes less time and money to test complex CPS systems (like avionics) that use only a few magnitude orders.
- Building and cities that are aware of energy
- Physical critical infrastructure that needs to be checked before it breaks down.
- One off system is used in high-tech CPS buildings to avoid fatal injuries.

The Cyber Physical System (CPS) systems also made mobile healthcare more popular, because they made it easier for patients to get efficient solutions or services. This is why it became more popular. So, this section talks about how cyber physical systems can help future researchers, scientists, and governments. In the next section, we'll sum up this work in a very short way, and then we'll talk about some future improvements and work.

## 10. Conclusion

Because of new technology, there have been a lot of new ideas (like fog computing, edge computing, compressed sending, and so on) in the last decade. Cyber physical systems are being used in a lot of important applications to do a lot of complicated things quickly (efficiently). Many problems, important issues, and research gaps have been identified and included in this article. Possible solutions are also discussed (as a suggestion) for a wide range of applications, such as medical care, industrial control, smart transportation, and more. In this article, we have talked about the current state of the field of secure control (in CPS). We still don't know how to solve most of our research problems, but we agree that future research in specific applications can add an extra layer of security (protection) to CPS/control systems. So, this paper looked at a lot of important issues that need to be worked on in computing, communication, and control technology (for the cyber-physical systems of the future). In addition, we've talked about some other research issues, like how to keep things stable, how to make things work better, and how to model, design, and build things. We looked at some recent research articles in these areas. Researchers who work with Cyber Physical Systems, especially to improve the security of CPSs, should do their best to fix or list issues, research gaps, challenges, or any other open problem. This work can be expanded to encourage research into how to combine CPS with IoT and different cloud computing technologies, such as Google Cloud Platform (GCP). It can also be used for research on how to use resources more efficiently by integrating CPS with transportation and energy systems, how to make medical devices work better together, and so on.

## Competing interests

We, the authors declare that we have no competing interests regarding publication of this work.

## Authors' contributions

Both Amit Kumar Tyagi and N Sreenath have contributed equally. N Sreenath has analysed, and approved the final manuscript for publication.

## Appendix A

**Table 2**
Threats on Several Applications of Cyber Physical Systems

| | Industrial Control System (ICS) | Smart Grids | Medical Devices | Smart Vehicles |
|---|---|---|---|---|
| ***Criminal Threats*** | It's possible for an intruder who knows a lot about an ICS application to use wireless capabilities (vector) to get into and mess with the system (source). | A smart metre and the utility company communicate with each other so that thieves who want to rob a house can figure out private information about the home's occupants, like whether or not they're home (consequence). | Hackers can use wireless tools to harm patients and change their health conditions by injecting or retransmitting legitimate commands (vector). This can change the device's state and expected operations, which can lead to an unwelcome health condition (consequence). | It's possible for someone to hack into a car's ECUs and cause it to crash or lose control by exploiting a weakness in the wireless interfaces (source) (consequence). |
| ***Financial Threats*** | By tampering with physical equipment or injecting false data (vector), a customer (source) can cause a financial loss to the utility (target). The customer is trying to lower a utility bill. | A customer (source) might try to change a company's billing system (target) so that he or she can lower the electricity bill (consequence). Utility companies (source) may also be interested in getting private information from their customers (target) by looking at how much electricity they use and how often they use different types of appliances in their homes (vector) to give this information to advertisers, which is a violation of their privacy (consequence). Another way for someone to cause a blackout is to take a lot of smart metres (target). | | |
| ***Political Threats*** | By spreading malware or accessing field devices (vector), a hostile nation can start a cyber-war against another country. This can happen by shutting down a plant, sabotaging components, or polluting the environment (consequence). Intelligence agencies (source) can spread malware (vector) on other countries' CIs (targets), which could lead to serious attacks that could break the confidentiality of important data (consequence). | A hostile country can start a cyber-war against another country's national power system (source) by getting remote access to the smart grids' infrastructure (vector). This can lead to large-scale blackouts, disturbances, or financial losses (consequence). | Cyberwar has another way for a country that is threatening to attack political figures (source). They could attack their medical devices by exploiting the devices wireless communications (vector), which could cause a critical health issue or even death (consequence). | A cyber-war can be started by a country that isn't friendly (source) against national transportation roads and their commuters (target) by hacking into smart cars that can be fully controlled from afar (vector). This can cause large-scale collisions and critical injuries (consequence). |
| ***Privacy Threats*** | | | This is what happened: A hacker (source) used wireless hacking tools (vector) to get information about a patient's medical device, a disease, or any other private information (target). This violated the patient's privacy and confidentiality (consequence). At different places, the medical devices that are used to communicate with other people, such as hospitals, store a lot of private information. An attacker (source) with spying motives (motive) wants to get unauthorised access to such data (target) by getting into the networks that connect the legitimate parties involved (vector). This results in a breach of privacy (consequence). | A hacker (source) can listen in on private conversations in a Vehicle (target) by exploiting flaws in the TCU (vector). This results in a breach of privacy (consequence). When a hacker (source) exploits the GPS navigation system (vector), for example, he or she can track a Vehicle (target). This can lead to privacy violations (consequence). Some driving habits and traffic violations can also be exploited by vehicle manufacturers without the driver's help. This is because they can get Vehicles' logs stored in ECUs (source). It's possible that manufacturers will also sell this information to insurance companies. |
| ***Physical Threats*** | Putting heat or cold on a sensor that measures the temperature of a specific environment (target) can make it send false readings to the control centre, which makes them look bad (consequence). | An attacker (source) could vandalise (vector) parts of smart grids (target) that aren't covered by the power grid, which could cause problems with administration and even power outages (consequence). | In order to stop the medical service or even change the configurations of a medical device (target), an attacker (source) can physically tamper with it. The user won't be able to get the medical service they want, which could lead to bad health conditions (consequence). | An attacker (source) can easily get into a car and attack a malicious device or mess with the car's outside parts (vector), which can cause accidents (consequence). |

## References


[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),", 2016.

[2] L. Vegh, Cyber-physical systems security through multi-factor authentication and data analytics, in: 2018 IEEE International Conference on Industrial Technology (ICIT), 2018, https://doi.org/10.1109/icit.2018.8352379.

[3] A. Cardenas, S. Amin, S. Sastry, Secure control: towards survivable cyber-physical systems, in: 2008 the 28th International Conference on Distributed Computing Systems Workshops, 2008, https://doi.org/10.1109/icdcs.workshops.2008.40.

[4] J. Wan, M. Chen, F. Xia, et al., From machine-to-machine communications towards cyber-physical systems, ComSIS 10 (3) (June 2013).

[5] mit Kumar Tyagi, S.U. Aswathy, G. Aghila, N. Sreenath, AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology, IJIN 2 (2021October) 175–183.

[6] E. Bartocci, M. Cherry, J. Glimm, R. Grosu, s.A. Smolka, F.H. Fenton, Toward real-time simulation of cardiac dynamics, in: Proceedings of the 9th International

Conference on Computational Methods in Systems Biology - CMSB 11, 2011, https://doi.org/10.1145/2037509.2037525.
[7] Ellen Nakashima, Greg Miller and Julie Tate, https://cyber-peace.org/wp-content/uploads/2013/06/.
[8] I. Tibrewal, M. Srivastava, A.K. Tyagi, Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks, in: A.K. Tyagi, I. Abraham, A. Kaklauskas (Eds.), Intelligent Interactive Multimedia Systems for e-Healthcare Applications., Springer, Singapore, 2022. https://doi.org/10.1007/978-981-16-6542-4_1.
[9] M. Thomas, P. Kumar, v.k Chandna, Design, development, and commissioning of a supervisory control and data acquisition (SCADA) laboratory for research and training, IEEE Trans. Power Syst. 19 (3) (2004) 1582–1588, https://doi.org/10.1109/tpwrs.2004.826770.
[10] F. Xu, Z. Qin, C. Tan, B. Wang, et al., IMDGuard: securing implantable medical devices with the external wearable guardian, in: 2011 Proceedings, IEEE INFOCOM, 2011, https://doi.org/10.1109/infcom.2011.5934987.
[11] G. Bird, M. Christensen, D. Lutz, P. Scandura, Use of integrated vehicle health management in the field of commercial aviation, in: Proc. of NASA ISHEM, 2005.
[12] C.M. Lilly, E.J. Thomas, tele-ICU: experience to date, J. Intensive Care Med. 25 (1) (2009) 16–22, https://doi.org/10.1177/0885066609349216.
[13] Tao Li, Feng Tan, Qixin Wang, Lei Bu, Jian-Nong Cao, &Xue Liu, from offline toward real time: a hybrid systems model checking and CPS codesign approach for medical device plug-and-play collaborations, IEEE Trans. Parallel Distr. Syst. 25 (3) (2014) 642–652, https://doi.org/10.1109/tpds.2013.50.
[14] J.A. Grass, Patient-controlled Analgesia, Anesth. Analg. 101 (Supplement) (2005) S44–S61, https://doi.org/10.1213/01.ane.0000177102.11682.20.
[15] I. Lee, O. Sokolsky, Medical cyber physical systems, in: Proceedings of the 47th Design Automation Conference on - DAC '10, 2010, https://doi.org/10.1145/1837274.1837463.
[16] Powering Business Worldwide Eaton, Power Outage Annual Report: Blackout Tracker, 2014 [Online]. Available: http://www.eaton.com/%20blackouttracker.
[17] A. Humayed, J. Lin, F. Li, B. Luo, Cyber-physical systems security—a survey, IEEE Internet Things J. 4 (6) (2017) 1802–1831, https://doi.org/10.1109/jiot.2017.2703172.
[18] E. Chien, L. OMurchu, N. Falliere, W32.duqu: the precursor to the next Stuxnet, in: Presented at the 5th USENIX Workshop Large Scale Exploits Emergent Threats, Berkeley, CA, USA, 2012, p. 5.
[19] M. Conway, L. Jarvis, O. Lehane, Cybercrime-Funded Terrorism and the Threats Posed by Future Technologies, Appealing Economics and Targets", 2017.
[20] A.A. Cárdenas, et al., Attacks against process control systems: risk assessment, detection, and response, in: In Proc. 6th ACM Symp. Inf. Comput. Commun. Security, Hong Kong, 2011, pp. 355–366.
[21] M.E. Luallen, Critical control system vulnerabilities demonstrated— and what to do about them, in: A SANS Whitepaper, Nov. 2011.
[22] K.A. Stouffer, J.A. Falco, K.A. Scarfone, Guide to industrial control systems (ICS) security: Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC), in: NIST, Tech. Rep. Sp, Gaithersburg, MD, USA, 2011, 800-82.
[23] F. Li, B. Luo, P. Liu, Secure information aggregation for smart grids using homomorphic encryption, in: In Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Gaithersburg, MD, USA, 2010, pp. 327–332.
[24] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, D. Irwin, Private memoirs of a smart meter, in: Proc. 2nd ACM Workshop Embedded Sens. Syst, Energy-Efficiency Build., Zürich, Switzerland, 2010, pp. 61–66.
[25] S.K. Das, K. Kant, N. Zhang, Handbook on Securing CyberPhysical Critical Infrastructure, Elsevier, Waltham, MA, USA, 2012.
[26] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur. 14 (1) (2011). Art. no. 13.
[27] M. Rushanan, A.D. Rubin, D.F. Kune, C.M. Swanson, Sok: security and privacy in implantable medical devices and body area networks, in: Proc. IEEE Symp. Security Privacy (SP), Berkeley, CA, USA, 2014, pp. 524–539.
[28] K. Koscher, et al., Experimental security analysis of a modern automobile, in: Proc. IEEE Symp. Security Privacy (SP), Oakland, CA, USA, May 2010, pp. 447–462.
[29] D. Kleidermacher, M. Kleidermacher, Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development, Elsevier, San Diego, CA, USA, 2012.
[30] Guidelines for smart grid cyber security, NIST Nistir, Gaithersburg, MD, USA, Tech. Rep. 7628 (2010).
[31] D. Choi, H. Kim, D. Won, S. Kim, Advanced key-management architecture for secure SCADA communications, IEEE Trans. Power Deliv. 24 (3) (Jul. 2009) 1154–1163.
[32] Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal, Medical cyber physical systems and its issues, Procedia Comput. Sci. 165 (2019) 647–655, https://doi.org/10.1016/j.procs.2020.01.059. ISSN 1877-0509.
[33] Amit Kumar Tyagi, G. Aghila, A wide scale survey on botnet", Int. J. Comput. Appl 34 (9) (November 2011) 9–22 (ISSN: 0975-8887).
[34] Amit Kumar Tyagi, Article: cyber physical systems (CPSs) – opportunities and challenges for improving cyber security, Int. J. Comput. Appl. 137 (14) (March 2016) 19–27. Published by Foundation of Computer Science (FCS), NY, USA.
[35] G. Rekha, S. Malik, A.K. Tyagi, M.M. Nair, Intrusion detection in cyber security: role of machine learning and data mining in cyber security, Adv. Sci. Technol. Eng. Syst. J. 5 (3) (2020) 72–81.
[36] S. Mishra, A.K. Tyagi, Intrusion detection in internet of things (IoTs) based applications using Blockchain technolgy, in: 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 123–128, https://doi.org/10.1109/I-SMAC47947.2019.9032557.