Cyber-Physical Systems

Husnara Khan Daljeet Kaur

Department of Computer Science Department of Computer Science

Gyan Ganga College of technology Gyan Ganga College of technology

Jabalpur M.P India-482002 Jabalpur M.P India-482002

Email:husnarakhn@gmail.com Email:daljeetkaurkalsi83@gmail.com

**ABSTRACT**

Systems that combine computation with physical operations are known as cyber-physical systems (CPS). Physical processes are monitored and controlled by embedded computers and networks, typically through feedback loops where computations are affected by physical processes and vice versa. Such systems have far greater economic and societal potential than has been recognized, and significant investments are being made globally to advance the technology. The physical components of such systems introduce safety and reliability requirements that are qualitatively different from those in general-purpose computing, which poses significant challenges. Additionally, physical and object-oriented software components differ qualitatively from one another. Traditional abstractions based on method calls and threads are ineffective. In particular, the paper raises the question of whether the current state of networking and computing technology is sufficient to serve as a foundation for CPS in order to examine the difficulties in designing such systems. It comes to the conclusion that improving design processes, increasing abstraction levels, or formally or informally verifying designs built on current abstractions will not be sufficient. We will need to rebuild computing and networking abstractions in order to fully utilize CPS. These abstractions must jointly incorporate computation and physical dynamics.

Cyber-physical system development presented new difficulties for people. One of the trickiest issues with a variety of cyber-attack defenses is ensuring the information security of cyber-physical systems. This paper's goal is to analyze and categorize previously published research papers on the safety of cyber-physical systems. Cyber-physical system philosophical issues are brought up. Investigated is their impact on various facets of peoples' lives. The basic operating principle of a cyber-physical system is described. The primary challenges and solutions in attack modeling and detection, security architecture development, and consequences of cyberattack estimation are noted. Analyzed are the primary forms of threats and attacks against cyber-physical systems. On cyber-physical systems, a proposed attack tree is presented.

**Key word -:** Cyber-Physical System, Security, actuation

**I .INTRODUTION**

A cyber-physical system (CPS) integrates computational and physical components to continuously monitor and control physical processes.Simply put, a cyber-physical system is a network of computing devices that interact with one another and the physical world through sensors and actuators in a feedback loop. These systems combine sensing, actuation, computation, and communication capabilities and make use of them to raise the overall performance, security, and dependability of physical systems.

The goal of a cyber-physical system is to track how physical processes behave and take appropriate action to alter that behavior in order to improve and optimize the performance of the physical environment. A cyber physical system (CPS) typically consists of two main parts: a cyber system and a physical process. The cyber system, which is a networked system of numerous tiny devices with sensitive computing and communication capabilities, is typically used to monitor or control the physical process. The physical process in question can be the outcome of a natural occurrence, a human-made system (like an operating room), or something completely else. However, as the contact between the physical and cyber systems increases, the physical systems are more susceptible to the cyber system's security weaknesses. To further comprehend what is meant by the term "cyber-physical systems," picture billions of various technical gadgets, the majority of which are connected to the internet and/or have digital technology installed on them, interacting with one another within a complex ecosystem .In other words, CPS refers to a collection of physical items (referred to as "hardware") that are controlled by computer algorithms that are primarily software-based. Personal computers fall under the definition of CPS devices. Technically, a physical device that is controlled by algorithms could be regarded as a computer. In this case, CPS would represent every digital computer in the world, not just "standard" PCs but also any other electronic device that uses digital algorithms or may be a development of such a device. Cyber-Physical Systems have intricate relationships between physical (or "hardware") and software components that allow them to operate in a number of spatial and temporal modes. They are capable of acting in many ways and changing their behavior in reaction to the circumstances, giving the simulation a "lifelike" aspect. It is critical to understand that CPS covers a wide range of technology. essentially any mechanical item that can be programmed.

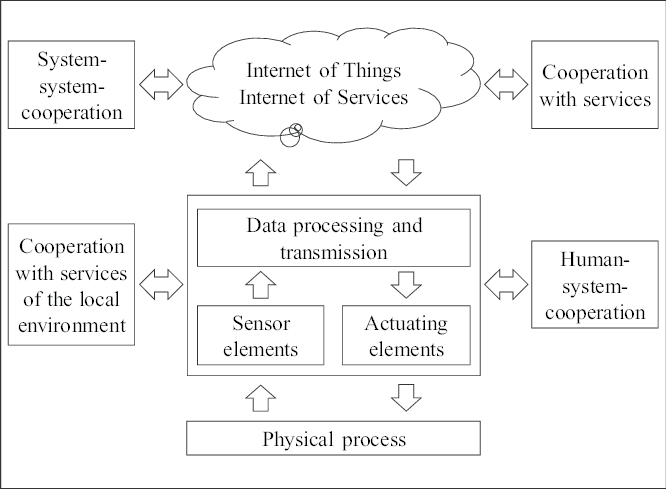


FIGURE. 1

**II. EASE OF USE**

By employing existing sensor, computing, and network technologies, a system known as a cyber-physical system (CPS) can successfully integrate cyber and physical components. Physical-cyber-social computing is a novel computer paradigm that was made possible by cyber-physical-social (CPS) and cyber-social systems (CSS). Extensions of physical systems that also include social space and telltale signals of human activity are known as cyber-physical-social systems (CPSSs). Some of the key technology trends that support CPS are Internet of Things (IoT), Big Data, smart technologies, cloud computing, etc. CPSs serve as the foundation for the growth of smart manufacturing, smart healthcare, smart infrastructure, smart cities, smart vehicles, wearable technology, mobile systems, defense technology, meteorology, etc. The number of CPS applications is growing significantly, which raises a lot of security and confidentiality concerns.Information security is the maintenance of information's availability, confidentiality, and integrity.

**Confidentiality-** is the quality of not making information available or disclosing it to unapproved people, groups, or processes.

**Integrity-** is the quality of being accurate and thorough.

**Availability-** is the quality of being reachable and usable at the request of a legitimate entity.

Additional attributes that could be important are authenticity, accountability, non-repudiation, and reliability. Due to the extensive usage of wireless technologies for data collection, transmission, and control commands, when a wireless sensor network (WSN) is employed, information security systems are becoming more and more important in the business. CPS devices are more vulnerable to intrusions and attacks because of their autonomy and distant location. When using several devices at once, some of them may get compromised. There are several brand-new challenges . This paper's goal is to assess and classify previous work on CPS security in order to better understand how such systems are genuinely secured. The purpose of this study is to provide an overview of the current state of CPS security, assisting researchers and practitioners in identifying limitations and gaps in current research on CPS architecture and intrusion detection, as well as their potential in the future and their practical applicability in the context of actual projects.

**CPS philosophical issues**

Modern people's world and identity are both undergoing rapid change. Things start to become more "virtual" and lose their "materiality." The economy is also becoming more and more virtual as online banking and crediting develop and more people shop online where they can only see a picture or an image of the item they will ultimately receive.

**Operation of CPS in general**

The cyber layer and the physical layer are typically the two main layers of the CPS architecture. Variables that represent sensor data and control variables that represent control signals are both present in the CPS's current state. A set point is the value that a particular process parameter should be at all times. The controllers in CPS determine the separation between the values of the process variables and the corresponding control points. Once this offset has been determined.

**Architecture of a CPS**

A CPS may include a number of integrated static/mobile sensor and actuator networks that are governed by intelligent decision-making. Cross-domain sensor cooperation, heterogeneous information flow, and intelligent decision-making are characteristics of CPSs. Effective connectivity is the foundation for the integration of various CPS component types. The CPS depends on the applications of key functions in various combinations. CPS takes into account computational elements that make use of information and common knowledge.

**CPS security threats**

Cyber threats have an impact on:

A) The confidentiality required to maintain the security of user personal data in the CPS and prevent an attacker from trying to change the state of the physical system by "eavesdropping" on communication channels between the actuator and the controller and the sensors;

B) Integrity, when information or resources can be altered without consent;

C) The availability of management in the event of computer technology failures

**Attacks on CPSs in a tree**

The dangers could be intentional, unintentional, or environmental. The following are some examples of typical threats: physical harm, natural disasters, loss of vital services, radiation malfunctions, compromise of information (such as eavesdropping, software tampering, etc.), technical difficulties, unauthorized actions (such as data corruption), and compromise of functions (such as forging and rights abuse).

**open problems**

CPSs impose high demands on quality, safety, security, and privacy but also have a high potential for developing new markets and addressing social risks. To successfully combat both internal and external changes, fundamental scientific research is required to reach a predictable level of verification and measurement quality.

The following tasks are included in the future research directions based on the analysis of the most recent CPS security studies that was done above:

There are some features of the cyber-physical system that are restricted.

**Reactive Systems**: Reactive systems, on the other hand, constantly exchange inputs and outputs with their surroundings. Take a look at a cruise control program in a car as a traditional example of reactive computation.

**Network Connectivity**: In order to communicate between the cyber and physical worlds, CPS systems must rely on network connectivity.

**Robustness & Reliability**: CPS must have effective reliability in order to guarantee safe and efficient operation in dynamic environments.

**Concurrency**: In cyber-physical systems, refers to the coordinated simultaneous execution of a number of tasks or processes.

**Real-Time Computation**: CPS systems have the ability to perform real-time computation, enabling them to make dynamic decisions based on physical, real-world data.

**Applications that are safety-critical**: In CPS applications, where system safety takes precedence over system performance and development.

**Characteristics**

• It combines cyber components that are networked and connected with physics.

• CPS systems must seamlessly monitor and manage physical processes.

• In CPS systems, the feedback loop is made up of sensors and actuators.

• Devices in CPS systems are made to interact with and control physical processes.

• When compared to IoT devices, CPS systems are more complicated.

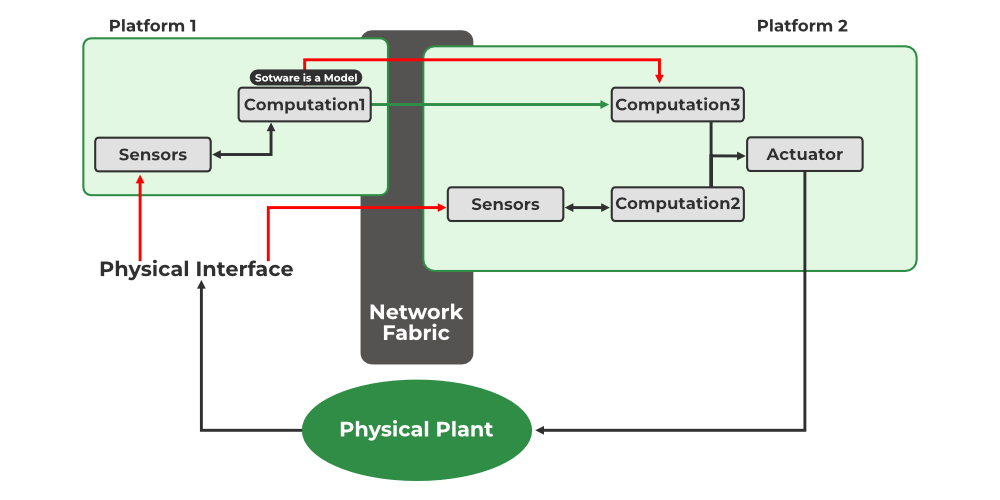


FIGURE.2

# III. Aims and scope

**A. Networks and networked systems**, where intelligent agents exchange data to enhance overall performance for both cyber and physical components. Sensor, vehicle, robot, camera, aerial, social smartphone networks, wireless networking technologies, and autonomous ad hoc networks are some of his specific research interests.

• network-enabled infrastructure management with applications like smart power grids and transportation systems • internet of things and machine-to-machine communications • network-enabled computation, coordination, and actuation • scalability of complex networks

**B. Modelling and Control**, which develops and applies mathematical and computational methods to enable creative design, in-depth analysis, and fresh understandings of the underlying principles.

Particular interest areas include:

• control theory that clearly reflects a cyber-physical perspective, such as networked control, distributed optimization, and distributed learning

• modeling of tightly integrated physical processes, software, computation platforms, and networks; applications in mobile sensor networks, internet-connected cars, etc.

**C. Data management**, which involves the creation of novel techniques for accurately collecting, storing, transferring, and analyzing massive amounts of data and dataflow.

Data processing and management (such as big data and cloud computing) and location-based services are some of the specific areas of interest.

• web of things; smart cameras; context management based on computer vision.

**D. Hardware and Software**, where innovative test-bed designs and software implementations will greatly increase the quickness, effectiveness, and dependability of next-generation CPS. Following are some specific areas of interest: • Embedded systems applications (pervasive computing, real-time control technologies);

Low power, energizing, and device miniaturization systems; resource-constrained systems; standards and middleware.

**E. Additional Emerging Areas that are forming new problems**, fresh concepts, and fresh rules. For instance, smart living technologies like smart cities, smart homes and offices, wearable devices, learning devices, etc., as well as incentive, security, trust, and privacy issues in CPS.

• social M2M networks, the effects of CPS on society, and creative elements.

**Some Things to Think About CPS**

**As a Social and Cultural System, the CPS**

The word "Cyber" comes from the Greek prefix "-" or "kubernetes," which in classical literature denotes "guide," "governor," and "steerman" or "pilot." The phrase was not initially connected to technology or computers. It was first proposed by mathematician Norbert Wiener. Cyberspace is therefore more of a type of controlled technology and government where scientists can interact with the outside world. This is related to the well-known "reign of the machines" idea that was made popular by a number of science fiction films. This concept is strongly tied to the concept of androids. For instance, terminology like cyber-space, cyber culture, cyber money, cyber war, and cyber fighters can be used to describe the social and cultural depiction of cyber-physical systems.

A writer like Philip K. Dick, for instance, does a great job of illustrating the dangers and challenges of such systems, which can occasionally "mimic" life itself, such as humans or animals, in his books about the Cyber-Culture and its implications for daily life. In nations like the USA or Japan, where "traditional" society has largely disappeared and where CPS plays a significant and expanding role, there is a clear and dominant cyberculture. This gives rise to ideas in popular culture like the "CyberPunk" and "CypherPunks" movements, in which hackers contend with a oppressive Cyber-Physical System (CPS) that is either autonomous (as in the movie "Matrix") or ruled by a ruling elite.

**B. The Discipline of CPS**

CPS can be thought of as a discipline that focuses on technology and calls for mathematical models. CPS combine centuries-old abstract mathematical modeling with more recent developments in computer science, which only last a few dozens of years. Following the Turing-Church model, CPS combines abstraction of dynamical systems, linear algorithms, differential equations, etc., with computer-based data processing. CPS is a hybrid discipline that combines computer science, engineering, and math.

**Cognition-based CPS and smart devices**

Here are some scenarios that could involve cognitive CPS, such as those that frequently involve "Smart-something":

• An audio player that automatically adjusts the volume in response to various environmental factors (a "smart-audio player").

• A "Smart car," which adjusts its speed based on traffic conditions

• Homes with automatic temperature control and energy-saving features (so-called "smart houses" or "domotics")

Be aware that the idea of a self-regulating system is not new. Thermostats are just one example of a non-CPS device that can achieve self-regulation without the use of a digital processor or digital sensors.

However, these scenarios might eventually result in circumstances where computers "decide" on behalf of users what is good or bad for them. These scenarios, which could be amusing, scary, or even good, have been extensively and copiously described in "Sci-Fi" literature.

**D. IoT and CPS**

IoT, or the "internet of things," is unquestionably connected to CPS, and the two ideas are linked. IoT, on the other hand, is significantly more constrained than CPS in that it "only" concerns about network connections, but CPS operates more like a vast ecosystem where greater interactions between the devices exist rather than "just" network connections. There are very notable similarities between the Internet of Things (IoT) and CPS. The Internet of Things (IoT) is a speculative future in which billions of (smart) gadgets connected to the internet gather data, assign tasks, and receive feedback.

There are numerous challenges shared by CPS and IoT. However, there are some significant differences between the two because CPS engineering is based on the extensive relationship between computers and computation in general (the "software" part) and the rest of the world, such as the "hardware," whereas IoT is based only on internet-connected embedded systems acting as "smart" devices. This makes CPS a generalized and all-encompassing software/hardware conception of the world.

**E. Non-digital/Digital Interaction or CPS and Modems**

Modems and UARTs, which convert digital signals into analog ones and vice versa, are essential for communicating with the "outside" physical world. They are essential to the existence of CPS.

**IV. LITERATURE SURVEY**

System Cyber-Physical

The field of information and communication technology (ICT) has experienced significant success and advancement in recent decades, and is anticipated to grow significantly more in the near future and draw a lot of attention. ICT is one of the many applications in the field of information technology. Embedded components in various devices have emerged as a crucial element that affects many facets of our lives. Computer systems that are embedded as a part of a complete system and are created to carry out specific tasks, typically in real-time, are known as embedded systems. Mobile devices like MP3 players and smart phones are examples of embedded systems, as are large systems like plant control systems. The relationship between the physical and digital worlds today has set CPS apart from older embedded systems. The integration of computational and physical processes is a key feature of CPS. In these systems, various computationally based devices collaborate in a network to monitor, sense, and act upon the elements of the physical world.

CPS has a wide variety of uses and applications. Large-scale systems like those in the healthcare, automation, transportation, and smart grid are among them. Additionally, a novel idea for mobile cyber-physical applications using multiple sensor-equipped smart phones and mobile Internet devices is emerging. Understanding and resolving the complex interaction between physical and computational elements is the most crucial issue in all varieties of CPS. The cyber section of these systems consists of a set of actuator units and control logic. The physical section consists of a set of sensor units. The term "Cyber-Physical Systems," which refers to the combination of computations, communications, and control, has become a significant and crucial research topic.Due to the term's broad scope, it is challenging to give a single definition, but it can be described as a physical engineering system whose operation is managed, monitored, and integrated by a computational core. Understanding physical and computational processes separately is not sufficient or sufficient in the context of CPS. Understanding how the physical and computational components interact is crucial because CPS is about the intersection.

By illustrating the key steps in the CPS workflow, the following steps have been defined:

**Monitoring**: This fundamental task involves keeping an eye on the processes taking place in the physical world. By using this feature, CPS can send feedback on previous actions and guarantee that future operations are carried out correctly.

Data collected from sensors is aggregated by the networking function. In the CPS, numerous networked sensors are producing data in real-time. While this is happening, various services must interact and talk to the network.

**Computing**: The third step, or computing step, should involve analyzing the data that was tracked in steps one and two and aggregated in steps three. This function is in charge of determining whether the analysis's result satisfies the criteria that were previously defined. If not, corrective measures are carried out by the computing section. A data-center CPS, as an illustration, can be used to find the temperature increase.

**Actuation**: Actuators send and carry out the results produced by computing elements. Actuators are capable of performing a variety of tasks, including altering physical processes and correcting cyber behavior. For instance, turning off a system in advance of an explosion that is likely.

CPS have a lot more features, options, and services than could be offered by embedded systems. Users are unable to affect embedded systems. Embedded systems typically are not visible to the user and can only assist with automated tasks. In embedded systems, the user has full control over every action that could possibly be taken. In contrast to embedded systems, CPS collaborates with services, local systems, the Internet of Services (IoS), and the Internet of Things to act based on data gathered from the physical world in real-time and react to this data through predefined orders. (IoT) . CPS outperforms embedded systems in various ways. CPS are more dependable, secure, productive, robust, and flexible . As an illustration, the damages caused by an explosion in a gas station or in a car accident can be reduced with the aid of a quick response recorded from the sensors. Additionally, these systems can aid in more precise robotic surgeries that cause less discomfort, blood loss, etc. As a result, research on CPS is expanding more quickly and is now very important. Given its endless potential, CPS has the potential to improve people's quality of life.

**characteristics of CPS**

The following list of CPS's essential attributes can be summed up:

**A. System of systems**: Unlike embedded systems, CPS is a complex system made up of numerous subsystems that interact with one another and are also capable of functioning independently. As a result, the CPS complexity exceeds that of a typical standalone embedded system.

**B. Control, communication, and computation interactions**: CPS should be automated, and human factors should never be included in the control loop. Therefore, while designing the system, the elements of control, communication, and computing should be taken into account simultaneously.

**C. Tightly coupled cyber and physical worlds**: In CPS, the physical and digital worlds must coexist harmoniously. Large-scale wireless and wired networks consequently assume a crucial role.

**CPS submissions**

CPS are currently used in a number of industries, such as robotics, manufacturing, assisted living, traffic control, energy conservation, advanced automotive systems, and critical infrastructure (like power and water). The applications of CPS in three different fields—healthcare and medicine, aerospace, the electric power grid, and automotive systems—are discussed in this section.

**A. Medicine and health care**

Home care, operating rooms, robotic surgery, national health data, electronic patient records, etc. are all included in the health care domain. These systems, which are primarily computer-controlled and some of which operate in real-time, demand an excessive amount of timing accuracy and safety. The medical CPS (MCPS) or health care domain in CPS makes it simpler for patients and doctors to communicate with one another online so they can get better care. Doctors can now monitor patients remotely rather than locally using stand-alone systems with the aid of MCPS. Current complicated massive connections between systems using wires in healthcare environments frequently result in a crisscross of cables known as "malignant spaghetti," which is a serious vulnerability that endangers the lives of patients. Wireless technology significantly improves system safety. In MCPS, system reliability is crucial, and one of the researchers' top priorities is to raise overall reliability by implementing novel theories and technologies.

**B. Aerospace**

In order to significantly increase aviation safety, CPS research has a significant impact on both aircraft design and air traffic control. The following are some important research questions in aerospace CPS:

In addition to tradeoffs between their potentially incompatible goals, new functionalities include

(i) increased capacity, improved safety, and increased efficiency; (ii) integrated flight deck systems that progress from current displays and concepts for pilots to future autonomous systems; (iii) vehicle health monitoring and management; and (iv) safety research pertaining to aircraft control systems.

Design verification and validation of extremely complex flight systems is one of the major challenges. The price of verification and validation also rises as a result of the constant growth in the complexity of flight systems. Methodologies for thorough and methodical high-level validation of various system safety properties and requirements are part of the research on the verification and validation of aviation flight-critical systems. This is assessed at every stage, from initial design to implementation, maintenance, and modification; understanding tradeoffs is also crucial.

**C. Grid of power**

a grid of power Power electronics, the power grid, and embedded control software make up the CPS. High levels of security, fault tolerance, and decentralized control are necessary when designing this kind of CPS. Research on a smart power grid has recently attracted a lot of attention. The public has shown a great deal of interest in the development of smart power grids, which makes it a top priority for decision-makers. Protecting the energy infrastructure from failure and outside assaults is of the utmost importance. For instance, in certain unanticipated circumstances, a failure in one area of the electrical power grid can spread throughout the grid, causing numerous failures and blackouts. The main goal is to create a reliable power grid network by integrating real-time control into the composition of the grid's cyber and physical components. Security policy, intrusion detection, and mitigation in particular, must address potential external attacks and should be carefully considered.

**D. Systems Automotive**

Vehicle systems today are far more sophisticated than purely mechanical ones. Everywhere, automotive systems are in use. Each car has between 30 and 90 embedded and networked processors in various systems like the airbag system, engine control, brake system, and door locks. Additionally, cars can connect to one another and communicate through cellular networks, Internet, and vehicle-to-vehicle networks. System safety and security are now of the utmost importance in this circumstance. These systems ought to ensure dependability for sophisticated networked software.

A small accident can cause significant damage and claim many lives, making automotive CPS one of the most vital systems that must be carefully secured. Nearly 42,000 fatal accidents occur in the US each year, a number that could be significantly decreased by using more intelligent systems to assist the drivers. Current technologies for preventing collisions are passive and rely heavily on the driver's input. Therefore, there is a lot of interest in collision avoidance automation. It is anticipated that near-zero automotive traffic fatalities and significantly less traffic congestion will be possible thanks to cutting-edge technologies for onboard sensing and in-vehicle computation, as well as with GPS and inter-vehicle information exchange. Unmanned vehicles may benefit from some new solutions as CPS continues to develop. Unmanned vehicle and intelligent road integration as a CPS is the focus of research.

**structure topology**

For CPS, there are three primary topologies:

**A central topology** Data is gathered from distributed sensors in this topology, and a single middleware is used to monitor all sensors and actuators. This topology offers a more secure environment and makes managing and controlling CPS easier. However, using this tightly coupled centralized topology would be problematic because more devices are being added every day, which increases the complexity of every system.

**B. Distributed topology**: Each physical device in this topology has a very small "middleware" program installed on it. Controlling the physical component and establishing connections with other peer-to-peer sections are the responsibilities of this middleware. For instance, agents and actors could be part of a middleware. While moving across networked sensors, these entities offer adaptive load balancing and monitoring. Because it is possible to add as many physical devices and computing elements as are required without interfering with other elements, this topology, as its name implies, offers scalable systems. On the one hand, because there is no bottleneck point in this topology, it can reduce network congestion. On the other hand, because physical devices have constrained resources and are more difficult to manage, complex computations cannot be carried out.

**C. Nested topology**: This topology is created by combining the two preceding topologies. This topology allows the local CPS networks, which can be either centralized or distributed, to make up more than one cyber-physical system.

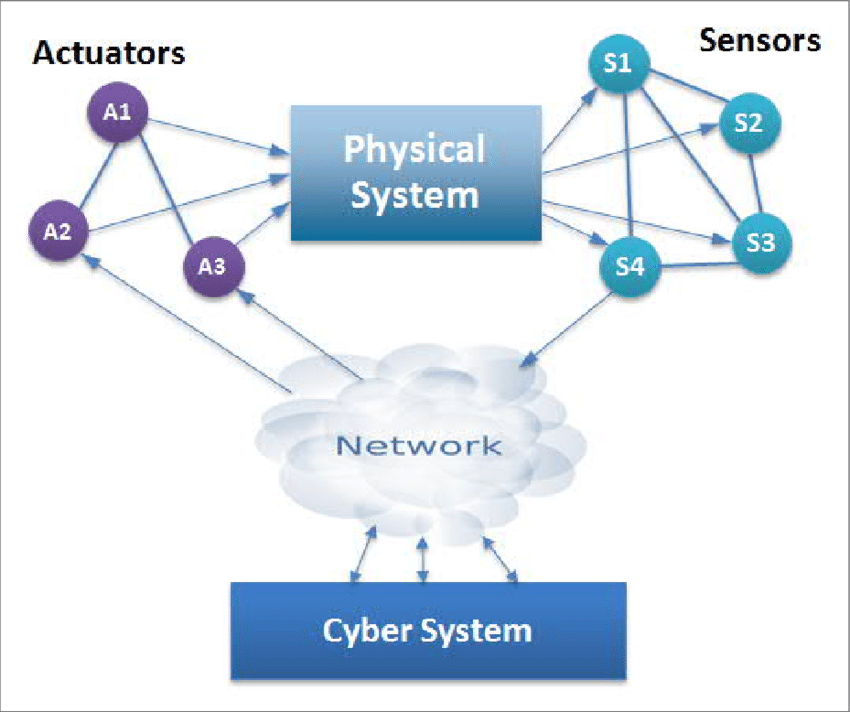


FIGURE.3

**Three-tier CPS structure**

The components of a three-tier CPS architecture are as follows:

• Service Tiers: The service tier creates a computing environment and makes use of various services, including CC (Cloud Computing).

• Environmental Tiers: Comprises tangible objects and comes into contact with users in the intended setting.

• Control Tiers: Based on the monitored data that has been collected from sensors, these tiers of control make controlling decisions. With the help of a service tier consultant, this tier identifies the appropriate services and offers the ones that physical devices have requested.

**Challenges in CPS**

CPS is a very active and important area of research today, and researchers are challenged to address a wide range of issues, including the integration of the physical and virtual worlds, architecture layers, and system desig

The following six issues are covered in CPS:

• Hybrid and control systems. To integrate time-based and event-based systems for feedback control, a new mathematical theory is necessary. The theory ought to work for hybrid systems with various geographic and temporal scopes.

• Mobile and sensor networks. One of the crucial steps in CPS is the gathering and aggregation of information from a vast amount of unprocessed data. Therefore, for CPS, a mobile network that can self-organize and reorganize itself is needed.

• Abductions. For real-time embedded systems and computational abstractions, a new resource allocation scheme is necessary to ensure that the system can achieve scalability, fault tolerance, optimization, etc. Therefore, new distributed real-time computing and communication techniques are needed to accommodate the emergence of new technologies and needs.

• Development based on models. Although there are numerous model-based development techniques currently in use, they fall far short of CPS requirements. For computing, communications, and physical dynamics at various scales, locations, and time scales, abstraction and modeling are required.

Validation, certification, and verification. Different formal methods ought to be able to communicate with one another without danger. The system should undergo testing and compositional verification.

• Sturdiness, dependability, security, and safety. The security and safety of CPS are the most important issues. System security, safety, robustness, and reliability should be ensured in uncertain environments, as well as against security threats and errors caused by the physical world and physical devices. To be able to resolve and mitigate problems, CPS's mechanisms should be time-based, location-based, and tag-based security problems

There are three main categories for CPS security:

There are three types of security: perception security, transport security, and processing center security. Perception security ensures the security and accuracy of data collected from physical environments, while transport security prevents data from being lost during transmission processes. Processing center security includes physical security and safety procedures in servers or workstations.

**Intrusion detection with CPS**

The three most crucial CPS issues are security, availability, and reliability. The first two are susceptible to security problems. The biggest problem facing critical infrastructures like CPS, which are deeply ingrained in the modern world, is security. Securing CPS becomes increasingly crucial as this integration grows. A compromised sensor, node, or subsystem can prevent the CPS from functioning properly. Therefore, it is crucial to strengthen CPS's security and lessen the likelihood of assaults and intrusions. These days, IDS is used in the design of the best security solutions. One of the top priorities for security research in various companies around the world is the CPS intrusion detection system. In order to increase CPS security against cyberattacks, this thesis aims to conduct a survey on the difficulties with CPS intrusion detection, compare the existing techniques, and enhance one of the popular intrusion detection techniques used in CPS. A thorough analysis of the current CPS intrusion detection methods is given in the following chapter. In order to organize the current CPS intrusion detection schemes, a classification tree is also introduced.

**V. FUTURE ENHANCEMENT**

Future technological advancements will be significantly facilitated by our increased ability to communicate, control, and interact with the physical world. Last but not least, we suggest a new security framework for CPS and talk about a number of difficulties and research issues that need to be solved in the future. Opportunity

The following trends are influencing the development of cyber-physical systems:

• Growing integration with the Internet of Things (IoT): The Internet of Things (IoT), which uses sensors and other devices to connect physical objects to the internet, is becoming more and more integrated with this technology. ...

• Greater use of machine learning (ML) and artificial intelligence (AI): These technologies are starting to be incorporated to allow for more sophisticated data analysis and decision-making. ..

.

**VI. CONCLUSIONS**

We examine the security concerns and issues relating to cyber-physical systems in this paper and suggest a security framework for CPS. We hope that these difficulties and problems will provide enough inspiration for upcoming discussions and an interest in the research being done on security issues for CPS. The system becomes dysfunctional as a result of the attacks on CPS. This causes a variety of serious financial losses as well as a chain reaction of issues for both people and organizations. It is anticipated that CPSs will have a significant influence on the real world and are a promising paradigm for the development of present and future engineering systems. Instead of focusing on the cyber or physical system separately, the CPS concept emphasizes the design of complex systems. This essay defines CPS and provides background information. The technical foundation and distinguishing characteristics of CPS, the operating principle of CPS, and philosophical issues were all thoroughly discussed. As a result, we have provided a brief introduction to cyber-physical systems in the preceding section. It was noted that the development of CPS and. The functionality of CPS systems can be used to advance a variety of industries, including automation, healthcare, infrastructure development, and many more. Cyber-Physical Systems (CPS) are intricate systems made up of both physical and computational components that work together in real-time to accomplish specific objectives.

**REFERENCES:**

[1] Kaiyu Wan,K.L. Man,D. Hughes, Specification,Analyzing for Cyber-PhysicalSystems(CPS),Engineering Letters,2010.

[2] Elinor Mills, Hackers broke into FAAWallStreet2009.

[3] Leavitt, Neal, Researchers Fight to Keep Implanted Medical DevicesSafe from Hackers,August 2010.

[4] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, 2014, pp. 4242-4268.

[5] C. Sonntag, "Towards Enhanced EU‐US ICT Pre‐competitive Collaboration-Opportunity Report of the EU Project PICASSO.[Hrsg.] C. Sonntag und S. Engell. Revised version V1. 0.1 (March 19, 2017). 2017," ed.

[6] K. Ashton, "That „internet of things‟ thing," RFID journal, vol. 22, 2009, pp. 97-114.

[7] I. Stojmenovic, and F. Zhang, “Inaugural issue of „cyber-physical systems‟,” Cyber-Physical Systems, 1(1), 2015, pp.1-4.

[8] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," Sensors, vol. 15, 2015, pp. 4837-4869.

[9] S. Sierla, B. M. O‟Halloran, T. Karhela, N. Papakonstantinou, and I. Y. Tumer, "Common cause failure analysis of cyber–physical systems situated in constructed environments," Research in Engineering Design, vol. 24, 2013, pp. 375-394.

[10] T. Sanislav, G. Mois, S. Folea, L. Miclea, G. Gambardella, and P. Prinetto, "A cloud-based Cyber-Physical System for environmental monitoring," in 2014 3rd Mediterranean Conference on Embedded Computing (MECO), 2014, pp. 6-9.

[11] Y. Zhou, Q. Xiao, Z. Mo, S. Chen and Y. Yin, “Privacy-preserving point-to-point transportation traffic measurement through bit array masking in intelligent cyber-physical road systems,” in 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, pp. 826-833.

[12] E. A. Lee, "Cyber physical systems: Design challenges", Proc. 11th IEEE Int. Symp. Object Compon.-Oriented Real-Time Distrib. Comput. (ISORC)*, pp. 363-369, May 2008.*