CYBER-PHYSICAL SYSTEMS

Abstract

Systems that Integrate Computation Are those that perform physical operations. Physical activities are observed and managed by embedded networks and computers typically use feedback loops where computations have an impact on physical processes and vice versa. Significant investments are being made globally to advance the technology because such systems have much greater economic and societal potential than has been realized. These systems have safety and reliability requirements that are qualitatively different from those in general-purpose computing due to their physical components., which poses significant challenges. Additionally, physical and object-oriented software components differ qualitatively from one another. Traditional methods-based and thread-based abstractions 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.

The development of cyber-physical systems presented new challenges for people. Assuring the information security of cyber-physical systems is one of the trickiest problems with a variety of cyber-attack defenses. The purpose of this paper is to review, evaluate, and classify previously published research papers on the

Authors

Husnara Khan
Department of Computer Science
Gyan Ganga College of technology
Jabalpur M.P India-482002
Email:husnarakhn@gmail.com

Daljeet Kaur
Department of Computer Science
Gyan Ganga College of technology
Jabalpur M.P India-482002
Email:daljeetkaurkalsi83@gmail.com

security of cyber-physical systems. Philosophical issues regarding cyber-physical systems are raised. Their effect on various facets of people's lives is being looked into. A cyber-physical system's fundamental operating principle is described. The main issues with and remedies for 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

To continuously monitor and manage physical processes, a cyber-physical system (CPS) combines computational and physical components.A network of computing devices that communicate with one another and the physical world through sensors and actuators in a feedback loop is known as a cyber-physical system. In order to improve the overall performance, security, and dependability of physical systems, these systems combine sensing, actuation, computation, and communication capabilities.

A cyber-physical system's objective is to monitor how physical processes behave and take the necessary steps to change that behaviour in order to enhance and optimise the physical environment's performance. A cyber system and a physical process make up the two fundamental components of a cyber physical system (CPS). In most cases, the physical process is monitored or controlled by the cyber system, which is a networked system of multiple tiny devices with sensitive computing and communication capabilities. The physical process at play could be a result of a natural phenomenon, a system made by humans (like a operating room), or something else entirely. The physical systems, however, become more vulnerable to the security flaws in the cyber system as the interaction between the physical and cyber systems grows. Imagine billions of different technological devices, most of which are connected to the internet and/or have digital technology installed on them, interacting with one another within a complex ecosystem to get a better understanding of what is meant by the term "cyber-physical systems."In other words, CPS refers to a group of real-world objects (referred to as "hardware") that are managed by mostly software-based computer algorithms. According to that definition, personal computers are CPS devices, and technically, a physical object that is subject to algorithmic control could be considered to be a computer. In this scenario, CPS would stand in for all digital computers worldwide, not just "standard" PCs but also anything else equipped with an electronic system that employs digital algorithms -or could be a development of these systems.Physical (or "hardware") and software components are intricately entwined in Cyber-Physical Systems, enabling them to function in a variety of spatial and temporal modes. They can act in a variety of ways and alter their behavior in response to the situation. resulting in a "lifelike" feeling. It is crucial to realize that CPS encompasses a huge variety of gadgets. pretty much any engineered device that can be programmed in some way.

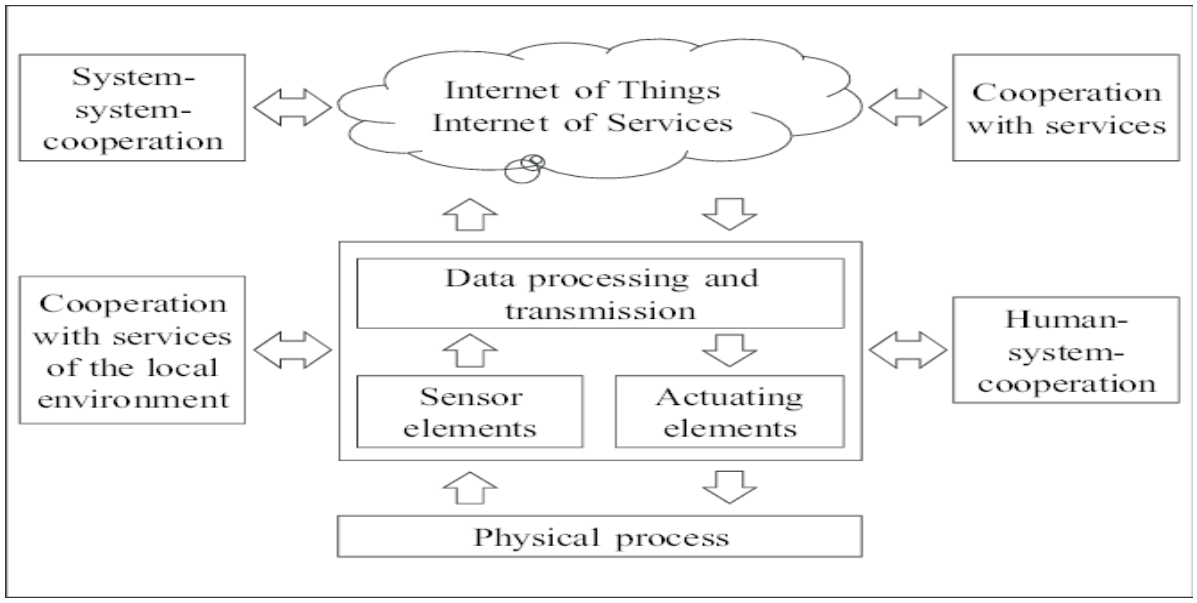

Figure: 1

II. EASE OF USE

A system known as a cyber-physical system (CPS) can successfully combine cyber and physical components by utilizing modern computing, sensor, and network technologies. Cyber-physical-social (CPS) and cyber-social system (CSS) have given rise to a new computing paradigm known as physical-cyber-social computing. Cyber-physical-social systems (CPSSs) are extensions of physical systems that also incorporate social space and telltale signs of human interaction. Some of the key technological trends that support CPS include Internet of Things (IoT), Big Data, smart technologies, cloud computing, etc. the advancement of wearable technology, mobile systems, defense technology, meteorology, smart manufacturing, smart healthcare, smart infrastructure, smart cities, and smart vehicles, etc. is based on CPSs. Applications for CPS are expanding quickly, which causes a number of security and confidentiality issues.

Information security is the maintenance of information's availability, confidentiality, and integrity.

- **Confidentiality-** is the trait of not revealing information to or making it available to unapproved individuals, groups, or processes.

- **Integrity-** consists of being precise and thorough.

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

Additional properties that might be important include authenticity, accountability, non-repudiation, and reliability. Due to the industry's extensive use of wireless technologies for data collection, transmission, and control commands, where a wireless sensor network (WSN) is used, information security systems are becoming more and more necessary is used.

The autonomy and remote location of CPS devices increase the risk of intrusions and attacks. Working with numerous devices at once can compromise some of them. The CPS security presents a number of new difficulties. IoT device proliferation increases systems' susceptibility to cyber attacks. Security threats modeling; creation of a formal method for CPS vulnerabilities assessment; creating dependable and fault-tolerant architectures to handle the processing of physical and cyber threats that are rapidly evolving. To meet CPS requirements for security, dependability, and confidentiality of personal data, new methodologies and technologies (such as people-centric sensing, wireless and quantum sensors, wearable biosensors, 2D/3D multi-sensor systems, etc.) need to be developed. In order to better understand how such systems are actually secured, the purpose of this paper is to analyze and categorize existing studies in CPS security. The purpose of this study is to provide an overview of the current state of CPS security while assisting researchers and practitioners in identifying limitations and gaps in current research on CPS architecture, intrusion detection, and their potential in the future as well as their practical applicability in the context of actual projects.

1. 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.

2. Operation of CPS in general

The two primary layers of the CPS architecture are typically the cyber layer and the physical layer. The current state of the CPS includes variables that reflect sensor data as well as control variables that represent control signals. A set point is the constant value that a certain process parameter should have. The distance between the values of the process variables and the relevant control points is decided by the controllers in CPS. Once this offset is established.

3. Architecture of a CPS

Multiple integrated static/mobile sensor and actuator networks that are controlled by intelligent decision-making may be found in a CPS. CPSs are characterized by cross-domain sensor cooperation, heterogeneous information flow, and intelligent decision-making. 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.

4. CPS security threats

Cyber threats have an impact on:

a. The secrecy necessary to preserve the security of user personal data in the CPS and stop an attacker from attempting to change the state of the physical system by "eavesdropping" on communication channels between the actuator, controller, and sensors;

b. Integrity, where data or resources can be changed without permission;
c. Management's accessibility in the event of computer technology failures.

5. Attacks on CPSs in a tree

There may be environmental, intentional, or accidental risks. Physical harm, natural disasters, the loss of essential services, radiation malfunctions, information compromise (such as eavesdropping, software tampering, etc.), technical challenges, unauthorized actions (such as data corruption), and compromised functions (such as forging and rights abuse) are a few examples of typical threats.

6. 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.

7. 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.

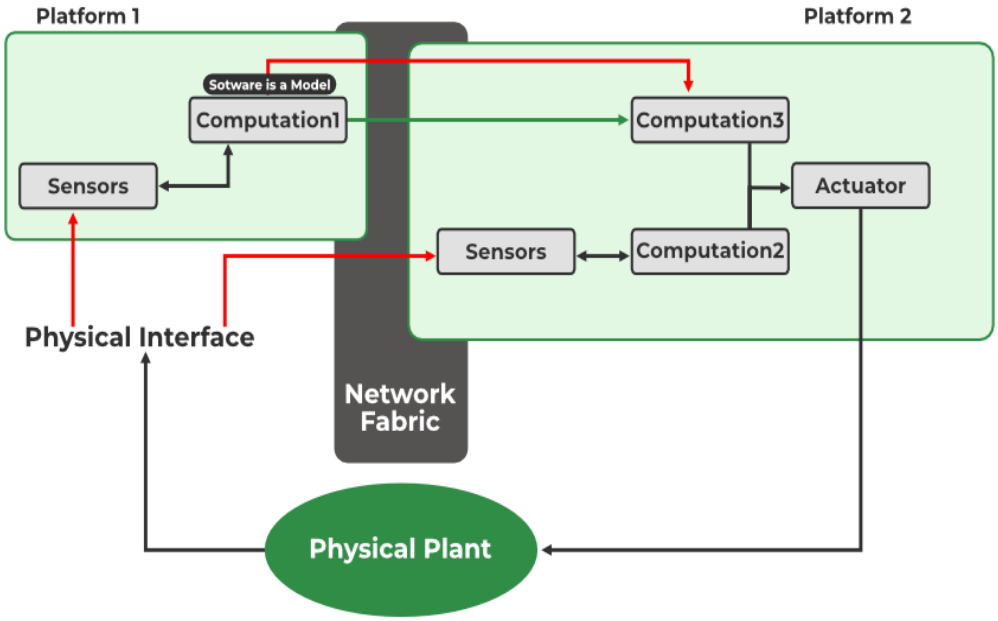

Figure: 2

III. Aims and scope

A. Intelligent agents exchange, data over networks and networked systems to improve system performance for both cyber and physical components. His particular research interests include sensor, vehicle, robot, camera, aerial, social smartphone networks, wireless networking technologies, and autonomous ad hoc networks.

- Internet of Things and machine-to-machine communications
- Network-enabled computation, coordination, and actuation
- Scalability of complex networks
- Network-enabled infrastructure management with applications like smart power grids and transportation systems

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, incentive, security, trust, and privacy issues in CPS; smart living technologies such as smart cities, smart homes and offices, wearable devices, learning devices, etc. social M2M networks, the effects of CPS on society, and creative elements.

8. Some Things to Think About CPS

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

The term "Cyber" is derived from the Greek prefix "-" or "kubernetes," which means "guide," "governor," and "steerman" or "pilot" in ancient texts. The term was not originally associated with computers or electronics. Norbert Wiener, a mathematician, introduced it. Therefore, cyber is more of a form of directed technology and governance where science can communicate with the real world. This connects to the well-known "reign of the machines" paradigm popularized by several movies in science fiction literature. The idea of androids is closely related to this concept. The social and cultural representation of cyber-physical systems, for example, can be found in terms like cyber-space, cyber culture, cyber money, cyber war, and cyber fighters.

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.

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

The concept of IoT, or the "internet of things," is undoubtedly related to that of CPS, and the two concepts are intertwined. However, IoT is much more limited than CPS in that it "only" cares about connections between devices, whereas CPS functions more like a vast ecosystem where greater interactions between the devices exist rather than "just" network connections. The Internet of Things (IoT) and CPS do in fact have a lot of significant overlaps. The Internet of Things (IoT) is a hypothetical future in which information is gathered, tasks are distributed, and feedback is received by billions of (smart) devices connected via the internet.

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

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 way the physical and digital worlds interact today distinguishes CPS from earlier embedded systems. A crucial component of CPS is the integration of computational and physical processes. In these systems, a network of various computing-based devices works together to monitor, sense, and respond to the components 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. The most important problem in all types of CPS is comprehending and resolving the complex interaction between physical and computational elements. These systems' cyber component is made up of a number of actuator units and control logic. There are several sensor units in the physical section. 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, However, it can be categorized as a physical engineering system, with a computational core in charge of managing, supervising, and integrating its operation. In the context of CPS, knowing physical and computational processes separately is neither necessary nor sufficient. 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

- Increased capacity, improved safety, and increased efficiency;
- Integrated flight deck systems that advance from present displays and concepts for pilots to future autonomous systems;
- Monitoring and managing the health of vehicles; and
- 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 The research on the verification and validation of aviation flight-critical systems includes high-level validation of various system safety properties and requirements. Understanding tradeoffs is also essential. This is assessed at every stage, from initial design to implementation, maintenance, and modification.

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.

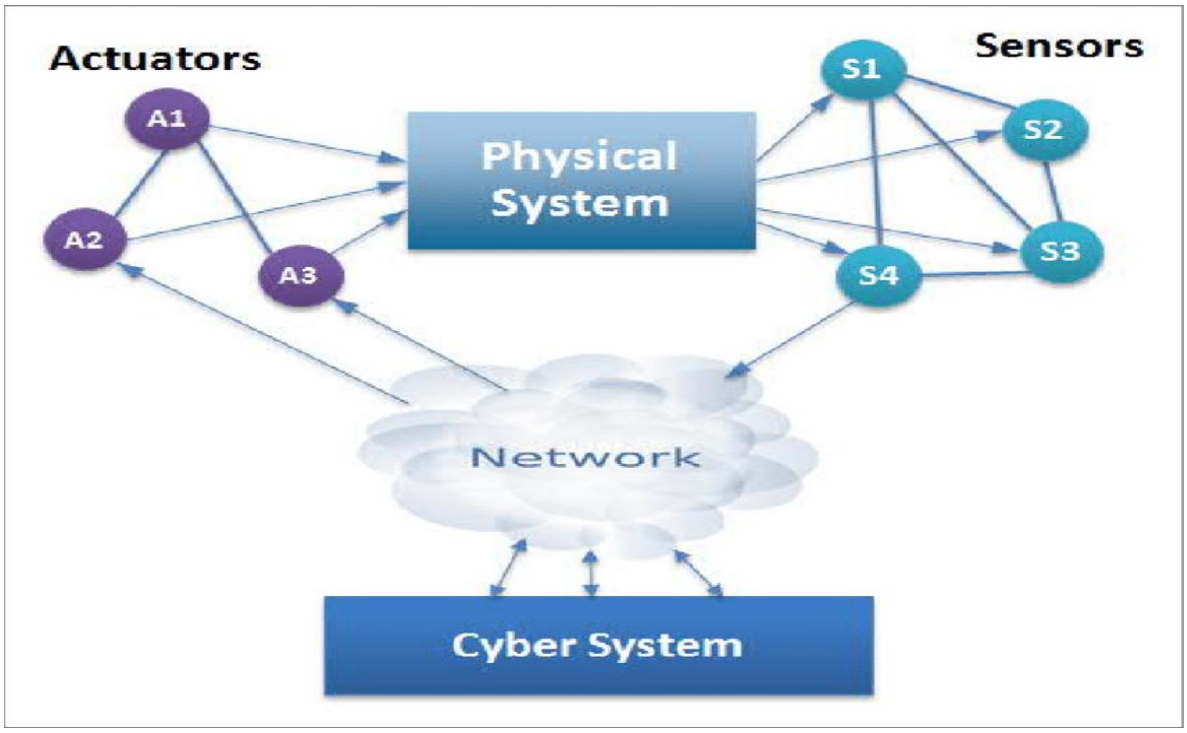

Figure: 3

Three-tier CPS structure

The components of 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. A new resource allocation strategy is required for real-time embedded systems and computational abstractions in order to guarantee 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 While transport security prevents data loss during transmission processes, security ensures the security and accuracy of data collected from physical environments. Physical security and safety protocols in servers or workstations are both included in processing center security.

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 discuss a variety of challenges and future research needs as well as a new security framework that we propose for CPS. Opportunity

The following developments are having an impact on the creation of cyber-physical systems:

- Increasing use of machine learning (ML) and artificial intelligence (AI): These technologies are beginning to be incorporated to enable more complex data analysis and decision-making. The Internet of Things (IoT), which uses sensors and other devices to connect physical objects to the internet, is becoming increasingly integrated with this technology.

.

VI. CONCLUSIONS

In this paper, we examine the security issues and problems pertaining to cyber-physical systems and propose a security framework for CPS. We hope that these challenges and issues will serve as sufficient fodder for discussions to come 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. The advancement of CPS and was noted. Automation, healthcare, infrastructure development, and many other industries can all benefit from the functionality of CPS systems. Cyber-Physical Systems (CPS) are complex systems that combine computational and physical elements in real time to achieve predetermined goals.

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] 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*.

