IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 2, Issue 5, January 2022

An Overview on Cyber Physical System

Prof. Nitu Sahu and Vishal Yadav
Asst. Professor and Research Scholar
St. Rock's College of Commerce and Science, Borivali (W), Mumbai, India

Abstract: *A cyber-physical system (CPS) is made up of various independently interacting parts, such as control, communication, and computational systems. Cyber-physical systems largely change how humans interact with the physical world, and depending on how sensitive the control system is and what information it contains, each system has a different level of security requirement. Given the impressive advancements made in CPS technologies in recent years, security and trust mechanisms must be improved to prevent security breaches and data leakage from integration elements. This essay focuses on many levels of security and privacy issues. Applications of CPS institute at different levels of integration, ranging from nation-wide power grids, to medium scale, such as the smart home, and small scale, e.g. ubiquitous health care systems including implantable medical devices.*

Keywords: Cyber, Physical, System, Cloud, Computing, IOT

I. INTRODUCTION

Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other. NSF is a leader in supporting advances in the fundamental knowledge and tools to make cyber-physical systems a reality. Cyber-Physical System (CPS) is a system that can effectively integrate cyber and physical components using the modern sensor, computing and network technologies. A new computing paradigm, known as cyber-physical-social or physical-cyber-social computing has originated from CPS and cyber-social system (CSS). Cyber-physical-social systems (CPSSs) expand CPSs and include social space and signs of people's participation and interaction. The widespread adoption of CPS is connected with the concept "Industry 4.0", which forms the process of combining technologies and knowledge, providing autonomy, reliability, systematicity, and control without human participation. Key technological trends underlying CPS include Internet of Things (IoT), Big Data, smart technologies, cloud computing, etc.

CPSs are the basis for the development of the following areas: smart manufacturing, smart medicine, smart buildings and infrastructures, smart city, smart vehicles, wearable devices, mobile systems, defense systems, meteorology, etc. The rapid growth of CPS applications leads to a number of problems with security and confidentiality. According to ISO/IEC 27001:2013, information security is the preservation of confidentiality, integrity, and availability of information. Confidentiality – property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Integrity is the property of accuracy and completeness. Availability – property of being accessible and usable upon demand by an authorized entity. Other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. Due to the widespread use of wireless technologies for data collection and transmission and control commands, where a wireless sensor network (WSN) is used, there is a growing need to develop information security systems in the industry.

The remote location of CPS devices and their autonomy lead to the risk of intrusions and attacks. A mechanism is controlled or observed by computer-based algorithms in a cyber-physical system (CPS), also known as an intelligent system. Physical and software components are intricately entwined in cyber-physical systems, able to function at various spatial and temporal scales, display a variety of distinct behavioral modalities, and interact with one another in context-dependent ways. CPS integrates theories from multiple disciplines, including design, process science, mechatronics, and cybernetics. Embedded systems are a common term used to describe process control. The emphasis in embedded systems is typically more on the computational components and less on a close relationship between the computational and physical components. Having a similar fundamental architecture, CPS and the Internet of Things

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 2, Issue 5, January 2022

(IoT) are also comparable; however, CPS presents a higher combination and coordination between physical and computational elements.

II. INFORMATION TECHNOLOGY

Information technology (IT) is the process of using computers to generate, process, store, retrieve, and share various types of data and information. Information and communications technology includes IT (ICT). An information technology system (IT system) is typically an information system, a communications system, or, more specifically, a computer system, complete with all peripheral devices, software, and hardware, that is used by a small number of IT users.

The term "information technology" in its modern sense first appeared in a 1958 article published in the Harvard Business Review; authors Harold J. Leavitt and Thomas L. Whisler noted that although humans have been storing, retrieving, manipulating, and communicating information since the development of the earliest writing system "The name of the new technology has not yet been given. It will be referred to as information technology (IT)." Three areas make up their definition: processing procedures, the use of statistical and mathematical methods in decision-making, and the computer modeling of higher-order thinking. Information technology is also a branch of computer science which can be defined as the overall study of procedure, structure, and the processing of various types of data.

III. CLOUD COMPUTING

The on-demand availability of computer system resources, in particular data storage (cloud storage) and processing power, without direct active supervision by the user, is known as cloud computing. Functions in large clouds are frequently dispersed over several sites, each of which is a data center. Cloud computing often uses a "pay as you go" model, which can help reduce capital expenses but may also result in unanticipated running expenses for users. Cloud computing depends on resource sharing to accomplish coherence.

The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs and helps the users focus on their core business instead of being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization .Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. Infrastructure as a service" (IaaS) refers to online services that provide high-level API s used to abstract various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup, etc. A hypervisor runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.

IV. INTERNET OF THINGS

The Internet of things (IoT) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network and be individually addressable.

There are a number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of privacy and security, and consequently, industry and governmental moves to address these concerns have begun, including the development of international and local standards, guidelines, and regulatory frameworks. The IoT can connect various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. In addition to general manufacturing, IoT is also used for Processes in the industrialization of construction. The term IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.

SMART GRID

A smart grid is an electrical grid which includes a variety of operation and energy measures including:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 2, Issue 5, January 2022

Advanced metering infrastructure (of which smart meters are a generic name for any utility side device even if it is more capable e.g. a fiber optic router)

Smart distribution and circuit breakers integrated with home control and demand response (behind the meter from a utility perspective)

Loan control switches and smart appliances, often financed by efficiency gains on municipal programs

Energy efficient resources: Renewable energy resources, including the capacity to charge parked (electric vehicle) batteries or larger arrays of batteries recycled from these or other energy storage.

V. CONCLUSION

Everywhere there is a presence of the Cyber Physical systems. It uses sensors to gather data, computes, and sends alarms to the systems. It is urgently necessary to view the machines in cyber systems as a system of systems rather than as a single thing or machine.. When they are categorized into different subsystems then CPS will also be able to work like the human systems where the subsystems work together.

The human body possesses a completely integrated, secure private network that can only be breached in order to collect the body's important messages. It never permits outside interference because outside influence hurts the internal system and degrades it. A completely integrated and connected private network that only remotely communicates with other untrusted systems when necessary is required for CPS. Intelligence must be built on smart data that can be gleaned through analysis of the massive data gathered from networked sensors. For statistics to aid in making wise decisions, experience must be translated. To ensure smooth operation, the entire process of calculation, control, and communication must be integrated, just like in a human system Fear and pain are two crucial ideas that keep the human system functioning properly and are absent from the CPS.

There have been several examples of how the human system functions when it is integrated. The areas of interest as well as potential application domains have also been emphasized. For the cyber physical system to be more sociable and practical, the social component must be integrated. The idea of "people in the loop" also applies to CPS employees. However, the presence of people as an outside force will prevent systemic communication. Humans are a part of the social CPS as a means of incorporating their perspectives. In order to effortlessly deliver solutions for the CPs various subsystems, including the cyber, social and physical systems.

REFERENCES

[1]. US National Science Foundation, Cyber Physical System(CPS)"

[2]. Daintith, John, ed. (2009), "IT", A Dictionary of Physics , Oxford University Press