International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A STUDY OF CYBER PHYSICAL SYSTEM DEVICES IN CLIENT-SERVER

MATTIGUNTA CHIRANJEEVEI, DR. RAJEEV YADAV

DESIGNATION- RESEARCH SCHOLAR MONAD UNIVERSITY HAPUR U.P
DESIGNATION- (PROFESSOR) MONAD UNIVERSITY HAPUR U.P

ABSTRACT

The term "cyber physical systems" (CPS) refers to the increasingly common practice of embedding internet connectivity and sensing/transmitting capabilities into everyday things. Think about a smart home app that uses CPS gadgets. Due to its many benefits, such as saving time and money and improving human comfort and energy efficiency, the IoT has been increasingly popular in recent years. In a cyber-physical system, the low-capacity sensor node is crucial. These diverse devices communicate with one another across a wireless network to function as either clients or hosts on the internet. Due to resource limits including little storage capacity, restricted computing power, and limited energy backup, the well-known security methods employed in desktop computers cannot run on these systems. Secure AuthKey is an easy-to-use authentication and key agreement system. The suggested technique is meant to solve the security and privacy problems that plague modern constraint-based CPS programs. A lightweight approach for authenticating cyber-physical objects is one of the expected outcomes.

KEYWORDS: Cyber Physical System, Client-Server, human comfort and energy efficiency, computing power, CPS programs

INTRODUCTION

A wide variety of objects, from simple tools to advanced robotic systems, have resulted from automation. Work-saving equipment has been changing from mechanically controlled to computer systems since the 1940s, when computers became commonplace and the field of cybernetics was established. In military settings, cybernetics aimed to automate tasks like sensing and controlling that were previously performed by people. Robotics (devices able to perform semi-autonomous physical manipulation) is a direct outgrowth of this study. The Internet was envisaged in the 1960s, ushering in novel means through which humans might communicate across geographic and linguistic boundaries using computer networks. The

convergence of mechanical labor, data processing, and communications technology may have been inevitable, but its future directions and effects remain unclear.

The current automation movement is often referred to by phrases like "Internet of Things," "Cyber Physical System," "Ubiquitous Computing," and "Pervasive Computing." All of these expressions are shorthand for various forms of technology that contributed to the design and implementation of the automated system. The automation process is shifting toward cyber physical systems.

An active system, CPS employs hardware and software to convert a non-digital system into an electronic one, complete with its own set of rules for operation. With CPS, even the simplest machine may perform like a high-tech gadget. These gadgets often have modest computing power, consume little energy, and have a limited capacity for storage. In the electronic world, a new generation of systems is being developed. It's the use of computation to achieve integration of physical systems. Computational algorithms are programs that can be run on computers to accomplish a wide variety of tasks. Computers connected to a network keep tabs on and control all the machinery's myriad mechanical operations. As a result, it paves the way for automated technologies that require fewer operators. As a result, mishaps in the system as a result of user error are reduced. Examples include "smart" electronics and "smart" buildings and vehicles. As far as CPS is concerned, the Internet of Things is the engine that drives the global economy. It's being put to use in the construction of high-tech dwellings and urban areas.

COMPONENTS OF CYBER PHYSICAL SYSTEM

Figure 1 shows the various parts of the CPS. The CPS implementation was specified by these parts in various contexts.

There are three main components that make up the CPS layout:

1. Things or Objects
2. Infrastructure and processing
3. Analytics and software applications.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

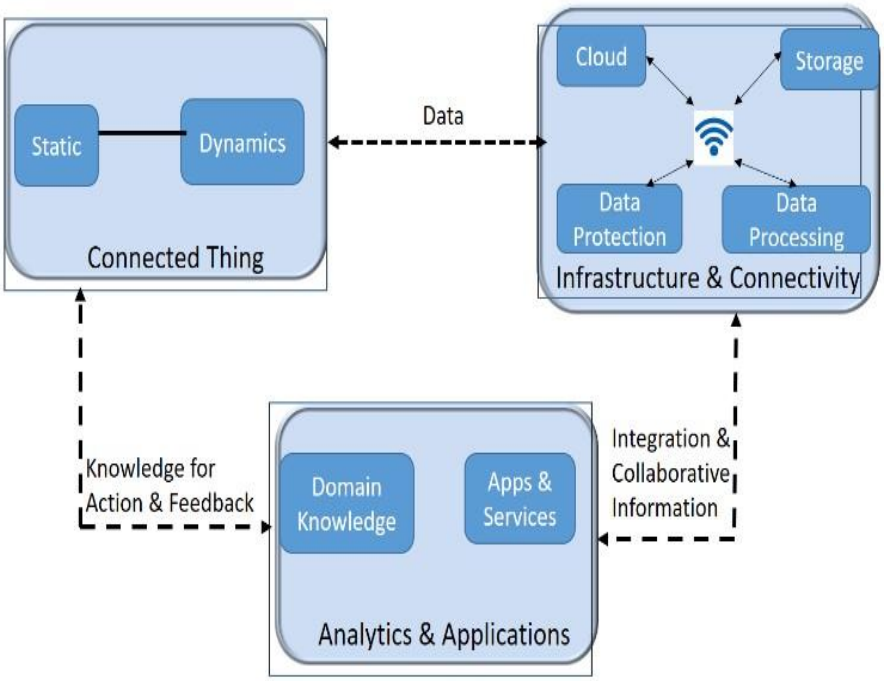

Figure 1: Components of Cyber Physical System

Artifacts, or connected things, can observe their environment and report back on it. Things can be put in either dynamic or static settings, depending on their characteristics. Unlike living things, inanimate objects don't adapt to their environments. They are always obedient to the settings in the program's configuration file. Things that are dynamic are designed to adapt to their environment and act accordingly. Things need at least two capabilities to be useful: data collection and data transmission to CPS applications. Storage and processing power are provided by this part of CPS, and the system can also make use of numerous intelligent processing technologies, such as cloud computing, databases, and others. Many Internet of Things databases are now hosted in the cloud and deployed in a variety of settings. Information is stored on a decentralized system and accessed as needed. Information is protected from many threats. Analytics and software apps employ CPS data to give users new features or functionalities and help them make informed choices. Data is gathered from a particular field and then transferred to the cloud using programs, where it may be accessed and used over the internet. Agricultural data from the Current Population Survey (CPS) is a good example. Sensors and CPS-based devices are used to gather agricultural data on individual plots of land, including crop information. This information is sent to the cloud via a mobile app developed for the agriculture industry. Information gathered online is analyzed and processed to produce useful recommendations for farmers and landowners. The tips offered will aid the farmer in his efforts to increase crop yields.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

CONCEPTION IN CYBER PHYSICAL SYSTEM

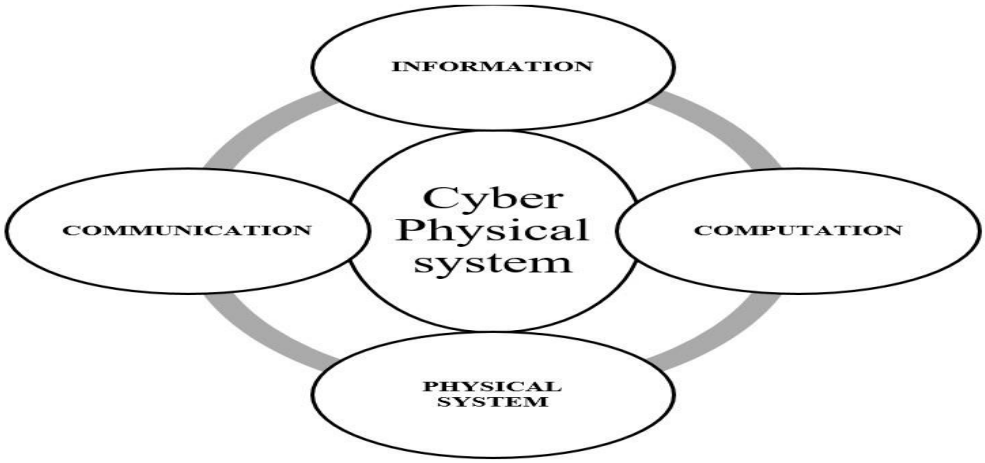

Figure 2: Conceptions in Cyber Physical System

Cyber Physical System has four conceptions shown in figure 2.

1. Physical system

A prototype is a part of a physical system that has not yet been created. It's less exciting and exciting and more static. It has to be manually operated. Most notably, the management of the system requires the involvement of a human who performs a work from a physical device. Time is needed to finish a job while using this method. Because of its environment, the equipment frequently malfunctions.

2. **Computation**

Modifying a physical object with a computer program to add intelligence. These instructions will require either supplementary hardware or a modification to the existing hardware architecture of the machine. A smart device is one that can be programmed with commands and instructions, which the system will then follow and execute. Computation allows for more capable and autonomous devices. Computing gives previously passive items new levels of functionality. Computation helps to transform a simple physical device into an intelligent one by keeping tabs on and regulating the device's fundamental duty or physical process.

3. Communication

When utilizing a plethora of tools, it is crucial that they are able to communicate with one another. Even if two devices are to perform a series of actions, they must communicate with one another. The Cyber Physical System is able to communicate via both wired and wireless means. Home automation, healthcare equipment, low-powered radio equipment, and so on all make use of communication protocols like Bluetooth (Connectivity Standards Alliance, n.d.), a wireless ad-hoc network that connects diverse physical equipment.

4. Information

Devices are the executors of computation, while communication facilitates interaction between devices. The data the device collects is put to use in analyses and for dissemination to other devices. The more data it has, the better decisions it can make, so it can be considered more intelligent. The device will analyze data to determine the best course of action in an emergency.

CHARACTERISTICS OF CYBER PHYSICAL SYSTEM

Both the benefits and cons of a Cyber Physical system are outlined.

As technology develops, smaller and more affordable devices with appropriate processing power, battery life, and storage space become available. This shift in thinking makes it possible to incorporate low-scale physical devices, which in turn paves the way for numerous new uses and possibilities. The four elements listed below make up the CPS framework:

1. form of AI is the use of computational technology based on neural networks to analyze CPS data and make more informed decisions.

2. Intelligent computer technology: Numerous cutting-edge computational methods, like as cloud computing, will be useful in organizing CPS data and creating new uses for it.

3. dependable communication: depending on the IoT network's stability, data about the objects or things that are used in the network will always be accessible via wired and wireless networks.

4. a heightened awareness of the physical world allows for a broader range of Internet of Things applications to be implemented. The CPS-based network sensors' information collection and network communication capabilities are seamlessly built in.

ADVANTAGES OF CYBER PHYSICAL SYSTEM

The following are a few of the many benefits of a CPS:

1. information is continually monitored and recorded; things are always watching and taking notes. The collected information is shared with an outside party for analysis or to aid in decision making.

2. gather as much data as you can from many sources quickly so you can make a well-informed choice. Things allow for data to be accessed from anywhere and at any time.

3. CPS allows you to manage and keep an eye on your gadgets regardless of where you happen to be. A smart home's electronics can be monitored, for instance, from afar.

4. the artifacts or sensors utilized in CPS architecture are cheaper when compared to the total cost saved by CPS applications. This means the CPS app has several potential uses.

DISADVANTAGES OF CYBER PHYSICAL SYSTEM

The following are some of the disadvantages of the CPS:

1. there is the problem of incompatibility: many different manufacturers supply the items and objects that might be used in different CPS applications. However, they are unable to ensure compatibility and interconnection due to the lack of international standards.

2. there is a deficiency in CPS standards and designs.

3. there is the issue of security, as CPS devices have less storage space and computing capacity than other devices. Traditional security algorithms will not work to keep them safe. Many CPS applications transport data between CPS objects or things and gateways in plain text, making the data vulnerable to interception. This was reported by a group of researchers

CONCLUSION

The constraints of processing power, memory size, and backup power are the primary targets of cyber physical system security mechanisms. Many prior studies have relied on preexisting, resource-intensive algorithms or security frameworks. Researchers highlight the many problems with and solutions to CPS system security. Currently available security algorithms run nicely on CPS systems thanks to the improved hardware support. However, a lightweight security mechanism that supports and functions with minimal hardware capabilities is necessary for constraint-based applications. This study's primary focus is on recommending a security mechanism compatible with the pre-existing constraint-based CPS software.

REFERENCES

Ahmad, I. *et al.* (2018) 'Security Aspects of Cyber Physical Systems', *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–6.

Alotaibi, B. and Alotaibi, M. (2020) 'A Stacked Deep Learning Approach for IoT Cyberattack Detection', *Journal of Sensors*, 2020. doi: 10.1155/2020/8828591.

Ashibani, Y. and Mahmoud, Qusay H (2017) 'Cyber physical systems security : Analysis , challenges and solutions', *Computers & Security*, 68, pp. 81–97. doi: 10.1016/j.cose.2017.04.005.

Ashibani, Y. and Mahmoud, Qusay H. (2017) 'Cyber physical systems security: Analysis, challenges and solutions', *Computers and Security*, 68, pp. 81–97. doi: 10.1016/j.cose.2017.04.005.

Bernardi, S. *et al.* (2021) 'Security modelling and formal verification of survivability properties: Application to cyber–physical systems', *Journal of Systems and Software*, 171(xxxx), p. 110746. doi: 10.1016/j.jss.2020.110746.

Brachmann, M. *et al.* (2012) 'End-to-end transport security in the IP-based internet of things', *2012 21st International Conference on Computer Communications and Networks, ICCCN 2012 - Proceedings*. doi: 10.1109/ICCCN.2012.6289292.

Capossele, A. *et al.* (2015) 'Security as a CoAP resource: An optimized DTLS implementation for the IoT', *IEEE International Conference on Communications*, 2015-Septe, pp. 549–554. doi: 10.1109/ICC.2015.7248379.

Capra, M. *et al.* (2019) 'Edge computing: A survey on the hardware requirements in the Internet of Things world', *Future Internet*, 11(4), pp. 1–25. doi: 10.3390/fi11040100.

Chen, Y., Kar, S. and Moura, J. M. F. (2015) 'Cyber-physical systems: Dynamic sensor attacks and strong observability', *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2015-Augus(1), pp. 1752–1756. doi: 10.1109/ICASSP.2015.7178271.

Chen, Y., Kar, S. and Moura, J. M. F. (2017) 'Dynamic Attack Detection in Cyber-Physical Systems with Side Initial State Information', *IEEE Transactions on Automatic Control*, 62(9), pp. 4618–4624. doi: 10.1109/TAC.2016.2626267.

Chen, C.-M., Hsiao, H.-W., Yang, P.-Y. and Ou, Y.-H. (2013). Defending malicious attacks in Cyber Physical Systems. [online] IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/6614240/.

D'Amico, A. *et al.* (2011) 'Integrating physical and cyber security resources to detect wireless threats to critical infrastructure', *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, pp. 494–500. doi: 10.1109/THS.2011.6107918.

Dai, B. *et al.* (2019) 'Enhancing Physical Layer Security in Internet of Things via Feedback : A General Framework', *IEEE Internet of Things Journal*, PP(c), p. 1. doi: 10.1109/JIOT.2019.2945503.

Dhanjani, N. (2010) 'Abusing the Internet of Things', *Malaysian Journal of Microbiology*, p. 312.

Esterle, L. and Grosu, R. (2016) 'Cyber-physical systems : challenge of the 21st century', *Elektrotech. Inftech.*, (November), pp. 299–303. doi: 10.1007/s00502-016-0426-6.