nigeria computer society
www.ncs.org.ng
Digital Inclusion:
Opportunities, Challenges and Strategies

Full Paper

# THEORETICAL FOUNDATION OF CYBER PHYSICAL SYSTEMS AND INTERNET OF THINGS

**S.O. Maitanmi**
Computer Science Department,
Babcock University,
Ilisan Remo, Ogun State, Nigeria
maitanmi@yahoo.com

**S.A. Idowu**
Department of Computer Science,
Computer Science Department,
Babcock University,
Ilisan Remo, Ogun State, Nigeria
saidowu07@gmail.com

**V.E. Kulugh**
Department of Computer Science
Nasarawa University,
Keffi. Nigeria
vkulugh30@gmail.com

**ABSTRACT**

The study is aimed at presenting basic inventory of Cyber Physical Systems (CPS) vis-à-vis Internet of Things (IoTs) and also present current research issues and challenges in this aspect of computing and development. Despite the non clear cut difference between IoTs and CPS especially with regards to Health Systems, CPS connects the physical processes with embedded systems without necessarily making use of the internet as a medium of connection. Therefore, there is no CPS without IoT, and the implementation of IoT in a physical system will lead to a CPS. The study further justified the differences in terms of its Architecture/correlation, application areas and future benefits.

**Keywords:**
Actuators. Cyber Physical Systems, Embedded systems, Internet of Things, Sensor

## 1. INTRODUCTION

The definition of Cyber Physical System (CPS) varies from one author to another depending on the understanding. The term CPS is sometimes mistaken for 'cybersecuirty' which concerns the confidentiality, integrity and entire security of the cyber space which has no connection with physical process (Lee, 2015). Research shows that CPS may certainly involve many challenges such as security and privacy concerns, which are never the only concerns. According to the research carried out by Lee, (2015) who convincingly defined CPS as an orchestration of computers and physical systems, usually with feedback loops where the physical processes have the tendency of affecting computations and vice versa. CPS is about the intersection, not the union of the physical and the cyber as displayed in figure 1.

The physical systems include automotive systems, manufacturing, medical devices, military systems, assisted living, traffic control and safety, process control, energy conservation, power generation and distribution, HVAC (heating, ventilation and air conditioning), aircraft, instrumentation, water management systems, trains, physical security (access control and monitoring), asset management and distributed robotics (telepresence, telemedicine). CPS may not necessarily need Internet to function but would effectively carry out its operations with the aid of sensors, actuators and other embedded technologies like Bluetooth, printers, ATMs, thermostats, calculators, cell phones, video game consoles among others. The term CPS was coined in 2006 by Helen Gill at the National Science Foundation in the United States (Naoufel, 2015).

While the Internet of Things (IoT) refers to a world-wide network of interconnected heterogeneous objects (objects and machines) that are uniquely addressable and are based on standard communication protocols (Naoufel, 2015). These include sensors, actuators, smart devices, Radio Frequency Identification (RFID) tags, embedded computers, mobile devices, among others. An author also defined IoTs as a technology which involved the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure (Kumar, 2009).

IoTs is the technology enabling the inter-connection of all types of devices through the Internet to exchange data, optimize processes, monitor devices in order to generate benefits for the industry, the economy, and the end user. It is composed of network of sensors, actuators, and devices, forming new systems and services (Kumar, 2019). IoTs is intrinsically an essential part and aspect of CPS and an enabling technology that helps build the synergy between physical systems and the computation and communications worlds (domain). There is no CPS without IoTs, and the implementation of IoTs in a physical system will lead to a CPS.

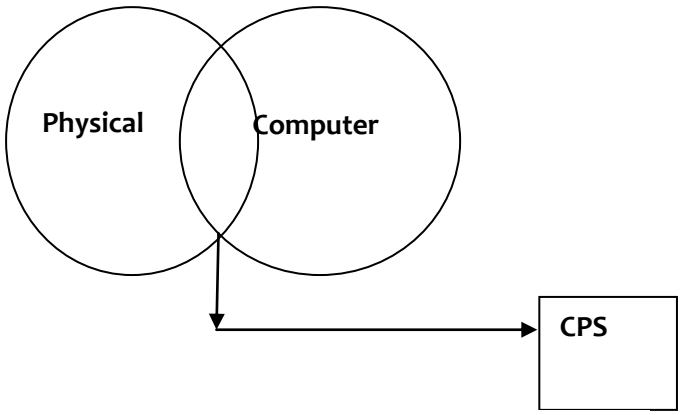


**Figure 1:** Diagram showing the definition of CPS

IoTs are divided into two categories; the wearable ones and Microcontroller/ Microprocessor driven embedded IoTs devices. Some of the embedded devices like Alduino Lillypad are minisque which are used for wearable materials. Other IoTs devices are graphically shown in figure 2.

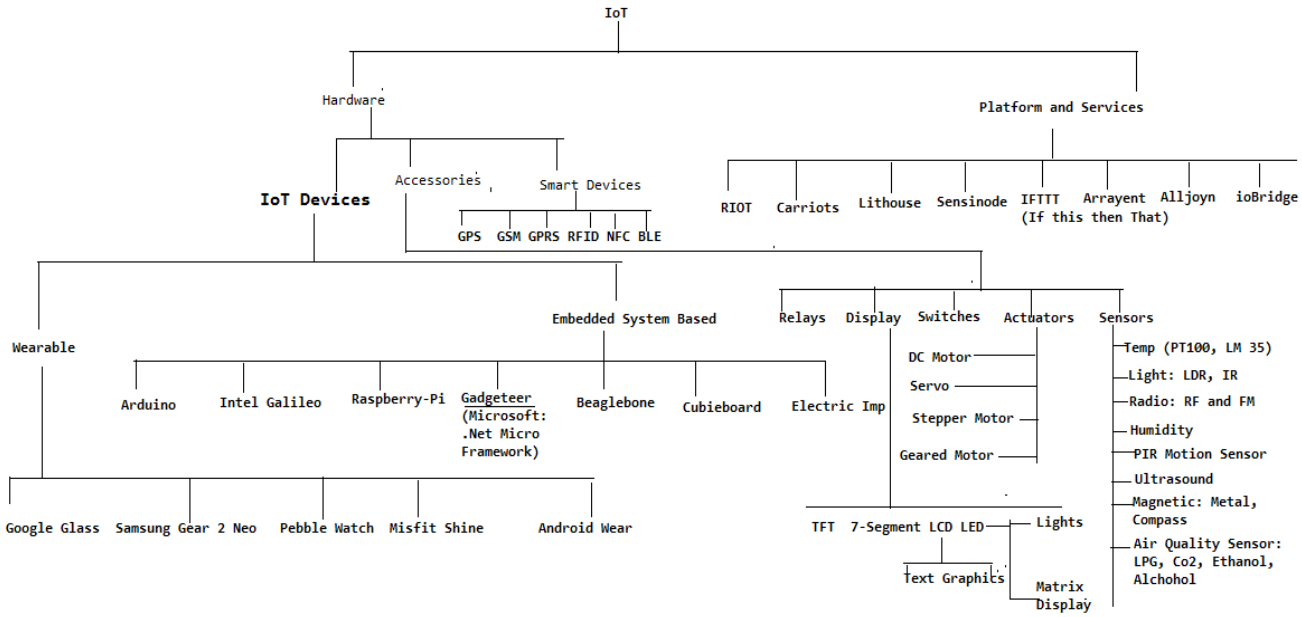


**Figure 2:** IoTs Architecture. Source: (Koubaa & Anderson, 2010

The large-scale nature of IoT-enabled CPS raises a number of specific challenges ranging from system-level management and control to data analytics (Koubaa & Anderson, 2010). System-level challenges include novel scalable methods for global system control, effective development of large-scale management platforms, well-defined control interfaces for IoT technologies and various IoT standards. Data related challenges include effective data collection, cleaning and storage, data latency and real-time analytics. IoT and mobility are driving more data into enterprises and Big Data Analytics has become an essential component for extracting value from data.

### 1.1 Problem Statement

Internet of things (IoTs) and Cyber physical systems (CPS) are coming in a rapid level into the information technology world and developed countries are ready to invest money into these research areas. However, some researchers argue vehemently that this is going to be another old wine in a new bottle. How logical is this assumption? How is CPS or IoTs different from the existing technologies of robotic, embedded systems, co-operative agent based systems, WSN, autonomous, telemedicine among others. Therefore this research is aimed at giving clear and

Architectural views to both terms with respect to their Architectural/Correlation differences, application areas and future benefits.

### 1.2 Objectives of the Study

The main aim of this article is to present a critical study of the existence of the theoretical foundation that supports Cyber Physical Systems and Internet of Things while the specific objectives are to;

i. Present an overview of distinguishing characteristics of CPS and IoTs with respect to architectural correlation or variation.
ii. Present issues and challenges in CPS and IOTs research.

## 2. ARCHITECTURAL CORRELATIONS OR VARIATIONS/EMBEDDED SYSTEMS

The Correlation and Variation in the Architecture of both would easily be detected if the two terms are explained with respect to embedded systems.

### 2.1 Embedded System

Embedded System is a special purpose computer designed to perform one or more functions (Park, 2006). To be specific, embedded system means a system with memories, processor and input/output integrated with software to control hardware in order to perform distinctive assignments. It also consists of microprocessor and ROM containing software and running the application software to perform specific objective as seen in figure 3.

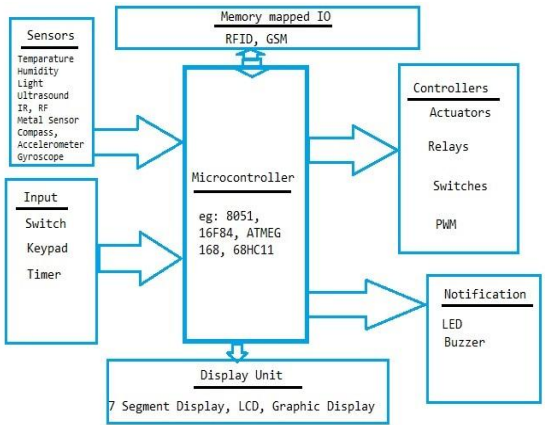


**Figure 3:** Embedded System: Source (Park, 2006)

From figure 3, the heart of the embedded system is a reduce instruction set computing (RISC) family microcontroller like PIC 16F84/Atmel 8051/ Motorola 68HC11 and so on. Most important thing that differentiates these microcontrollers with microprocessors like 8085 is their internal read/writable memory erasable programmable read only memory (EPROM). So you can develop your light weight program and burn the program into the hardware. These programs keep on running in a loop (as part of the benefits of CPS).

Interestingly in most embedded system, a single program is burn with several subroutines. So unlike the personal computer (PC), microcontroller device is an embedded system running a single program infinitely. This would connect several input and output devices with these microcontrollers which are either memory mapped or I/O mapped. This simple hardware includes LCD display, buzzers, keypad (numpad) or even a printer. It connects several sensors through A/D interface. The devices can control Higher Power/Voltage/Current rating devices like fans, motors, bulbs using drives devices like relay-optocoupler and others.

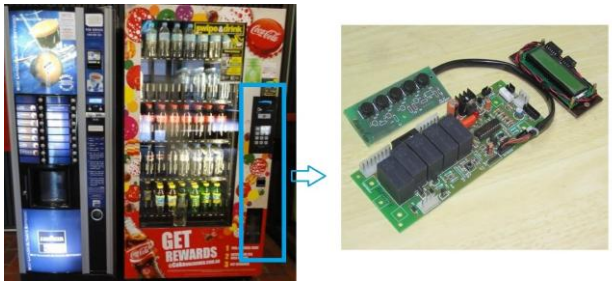


**Figure 4:** Beverage Vending Machine and its Embedded System. Source: (**Park, 2006**)

From figure 4, the display and switches are shown on the right hand side. This shows the function of the embedded system working in drinks dispenser. The resources are linked with the dispenser which would not be released without the acknowledgment of the equivalent money.

Other simple embedded systems are washing machine, ovens, AC controller, Cars, Hand held ticket printers, Hotel Mini Bill printers among others.

### 2.2 Benefits of Embedded Systems

**Autonomous:** This involved building a specific system to a particular application. For example, some standard peripherals and a specialized program can turn a microcontroller unit into washing machine controller or an oven controller. Also embedded systems can be built specifically to fulfill a particular requirement. Unlike a PC which you cannot work with without a monitor, an embedded system may not mandatorily need a display unit.

**Low Cost**: The cost of the microcontroller unit is insignificant compared to the cost of a complete system.

**Low Space:** Figure 4 shows that the space occupied by an embedded device is quite smaller than the space where a laptop will occupy.

**Low power:** Most of the commonly used microcontrollers operate at 5v with 5v regulated power which can be provided through a simple 9v standard battery with voltage regulator or directly from the main source by using a voltage rectifier with filter circuit.

**I/O Speed:** The input and output speed of an embedded device is usually faster than a complete system.

### 2.3 Architectural Correlation

The IoTs architecture is entirely based on the existing Internet infrastructure – meaning IoTs can run on the OSI models without significant modifications, the CPS on the other hand needs a modified form of the OSI Model for it to function (Graham, Baliga & Kumar, 2009).

**Table 1:** Mapping from OSI model to an architectural network control. Source: (Graham, Baliga & Kumar, 2009)

| **OSI Model Architecture for network controlled** | | |
|---|---|---|
| **3. APPLICATION LAYER** | | **5. CONTROL SOFTWARE** |
| **6. PRESENTATION LAYER** | | **8. VIRTUAL COLLOCATION** |
| **10. SESSION LAYER** | | **9. (MIDDLEWARE)** |
| **11. TRANSPORTATION LAYER** | | **13. TCP, UDP** |
| **14. NETWORK LAYER** | | **16. IP** |
| **17. DATALINK LAYER** | | **19. NETWORK INFRASTRUCTURE** |
| **20. PHYSICAL LAYER** | | |

The IoTs enjoys this leverage largely due to the already existing standardization of the Internet, which historically existed in the past as independents networks. The Cyber Physical Systems on the other hand lack this standardization and hence are scattered and operate as private networks with each performing a specific task related to the environment where it operates; their integration into a single interoperable network will give rise to the Cyber Physical Internet (CPI) (Koubaa & Anderson, 2010). This means that as security is been perfected, the CPI will eventually integrate with the IoTs for enhanced information interchange.

## 3. CHALLENGES OF CPS VS IOTS

Advances in many technology areas such as significant drop in the cost, size and energy efficiency of sensors, actuators and processors, micro-scale and nano-scale fabrication technologies, system software, high performance computing systems to real time embedded systems alongside economic and social gains driven by societal and industrial demands in areas like air and ground traffic management, energy grids, population and environmental issues have fuelled tremendous growth in CPS and IoTs technologies in recent years (American Internet Group, (2014): Oks, Fritzsche & Möslein, 2017). However, these have thrown up new challenges that have the potentials to undermine the economic and social benefits of these technologies. The major point is that of ensuring that they are protected from being compromised by threats which seeks to exploit their vulnerabilities. This is largely occasioned by the emerging nature of both technologies as their threats landscape is yet to be fully understood, (Graham, Baliga & Kumar, 2009). The IoTs are however more exposed to compromises because their architecture which is built and driven by the existing Internet infrastructure when considered against the inherent risk in any system that is connected to the Internet. For instance, the research carried out by American Internet Group, (2014) further argued that in an IoTs enabled environment with widespread mobile technology, privacy of individuals will be largely compromised via device-to-device data exchanges, also

cybersecurity events will rise astronomically with tens of thousands of billions of nodes connected on the IoTs ecosystem bearing in mind the fact that each device on the network is a gateway for compromise by threat actors as the attack surface is expanded by the minute as new nodes join the network; for example, a whole city's electrical grid can be brought down by a single hacker. Similarly, as proven by the research of World Economic Forum, (2015) which was a survey on the risk associated with the Internet of Things found out that an overwhelming majority of the respondents were concerned about the security implications in terms of cybersecurity, privacy compromises and potential disruption to existing business models with attendant budgetary consequences. Again, there are issues of privacy, security and trust that needs attention; there are a number of privacy implications arising from the ubiquity and pervasiveness of IoTs devices such as inferring locations from things associated with people and other informed individuals who may want to keep private; large-scale applications and services based on the IoTs are increasingly vulnerable to disruption from attack (DoS/DDoS) or information theft. Issues of trust will certainly arise, frameworks have to be in place to assure users that the information and services been exchanged on the IoTs platforms can be relied upon (Vermesan & Friess, 2013).

Though, the architecture of CPS is not based on the Internet necessarily, thus it has less exposure to threats than the IoTs as most CPS operate in an enclosed ecosystem with less contact with public connectivity, this however does not preclude them from attacks as no system is breach-proof. According to Chen, (2010), the stuxnet worm was designed specifically to attack CPS as it was speculated that it was used to compromise Bushehr nuclear plant in Iran alongside other similar systems in Iran, India, Idonesia and Pakistan. Chen, (2010) further argued that its initial infection vector is a USB stick instead of the Internet; this suggests that the attackers were very familiar with the primary target and knew it was not reachable by the Internet. Certain attacks on CPS are not directed at the CPS but affects them as a cascading effects of attacks directed at other IT based infrastructure. For example, in 2006, an attacker compromised a computer at a water filtering plant in Pennsylvania and used it as its own distribution system for spam and pirated software (Esposito, 2006). Another famous example of these types of attacks occurred in January 2003, when computers infected with the Slammer worm shut down safety display systems at the Davis-Besse power plant in Oak Harbor, Ohio. The Slammer worm was not designed to attack control systems, but the use of commodity information technology (IT) software by control systems allowed this general purpose worm to infect computers used in safety critical systems (Alvaro etal, 2010). It must be noted that most CPS (such as ground/air transportation systems, power grid systems, medical and health care systems, disaster monitoring, dam control and warning systems) are safety critical systems and must be secured from attacks as well as design with resilience in mind (Kim & Kumar, 2011),

Another critical issue associated with CPS and IoTs is energy. As an illustration, one of the essential challenges is connecting physical things and computers in an interoperable way while taking into account the energy constraints bearing in mind the fact that communication is the most energy consuming task for devices. For this purpose, a number of low energy consuming standards have been proposed namely; IEEE 802.15.4, Bluetooth Low Energy (Bluetooth LE), Ultra-Wide Bandwidth (UWB) Technology and RFID/NFC standards (Vermesan & Friess, 2013).

## 4. APPLICATION DOMAINS

It is impossible to envisage all potential CPS and IoTs applications bearing in mind the fact that they are still emerging technologies and the diverse needs of potential users, (Kim & Kumar, 2011). IoTs will find applications in the following areas of

human endeavor: Machine-to-machine communication, Telehealth: remote or real-time pervasive monitoring of patients, diagnosis and drug delivery, Continuous monitoring of, and firmware upgrades for, vehicles, Asset tracking of goods on the move, Automatic traffic management, Remote security and control, Environmental monitoring and control, home and industrial building automation, Smart applications, including cities, water, agriculture, buildings, grid, meters, broadband, cars, appliances, tags, animal farming and the environment (FreeScale, 2014). According to Kim & Kumar (2011), the application domains of CPS will cover transportation, energy, medical and defense; they further suggested that it is expected that CPS can potentially revolutionize how we interact, operate, and construct many engineered systems which our modern society critically depends on, such as automobiles, aircraft, power grid, manufacturing plants, medical systems, and buildings. It must be noted from the foregoing that there is a significant overlap in the application domains of the two technologies. This paper discussed in greater details the applications associated with "smart things" with respect to IoTs and Smart factory, industrial smart data, industrial smart services in CPS respectively in the following section.

i. **Smart Cities**

A smart city ensures a networked urban society shares in the benefits of intelligent traffic management, smart energy grids and security. GSM Association, (2014) proposed that smart city technology takes the critical elements that makes up the city and ensures an online real time interconnection using the IoTs, the critical elements considered by many cities or nations investing in this technology are: energy (smart grid), traffic management and security. It is therefore safe to say that the smart grid like traffic and security is a subset of the smart city. American Internet Group, (2014) expanded the elements of the smart city in this manner; smart cities are not just a network of municipal services, such as electricity and water, truly smart cities combine elements from all urban stake-holders, including citizens, government and business. And, once again, a broad spectrum of implementation models is emerging in different parts of the world.

The smart cities will be driven largely by expansion of the current cities, projected to have the potentials of collapsing or blurring the existing boundaries thus forming mega cities, it is estimated that by 2025, over 60% of the world population will live in cities, this will account for the creation of mega cities which over 55% are estimated to come out of the developing countries of China, Russia and Latin America (Frost & Sullivan, undated).

Vermessan & Fries, (2013) considered eight elements of the smart city to include: "Smart Economy, Smart Buildings, Smart Mobility, Smart Energy, Smart Information Communication and Technology, Smart Planning, Smart Citizen and Smart Governance." This suggests that deployment of IoTs to smarten the cities will require a multi-disciplinary approach; the technology team will work extensively with a gamut of stake holders to understand requirements that will be translated into sensing and actuation. In all these, security must be thought through from ground zero. However, it is worthy of note that this technology is currently been deployed and test run in cities across the world.

ii. **Smart grid**

The smart grid essentially suggests smart energy deployment systems that see beyond fossil and nuclear energy sources, the future points to renewable energy platforms that calls for greater efficiency on the management of energy supply chain so that wastages are effectively trapped and blocked on the grid, guarantying only energy needed is supplied and consumed, there is potential mutual benefit for both consumer and the energy companies.

Based on the foregoing, the smart grid promises a routing of energy the same way packets are routed on today's Internet Vermessan & Fries, (2013) sees it this way, the Smart Grid is expected to be the implementation of a kind of "Internet" in which the energy packet is managed similarly to the data packet—across routers and gateways which autonomously can decide the best pathway for the packet to reach its destination with the best integrity levels. This has given rise to a new concept and technology referred to as the Internet of Energy (IoE) and consequently the Energy of Things (EoTs), this will allow for transparent power distribution, energy storage, grid monitoring and communication, thus units of energy will be transferred where and when needed. This in turn will give way for effective power consumption monitoring from local individual devices and appliances to national and international levels (Vermessan et al, 2011).

iii. **Smart Factory**

There is a great variety of application fields for CPS in the smart factory; Oks, Fritzsche & Möslein, (2017) suggest as follows: primary among them is the production itself, the production process in a CPS platform will synchronize the technical, mechanical and digital processes with minimal tolerance for process time. To reach the requirements of a forward-looking and competitive production planning and control, these systems should be self reconfiguring, self-optimizing, adaptive, context-aware, and real-time capable. A CPS installed on the production line will provide capabilities for: machine-to-machine communication, plug-and-produce machinery interconnections and automated guided vehicles as well as supervisory control and data acquisition and system reconfiguration mechanisms with an integration of human-machine interaction. To ensure a seamless production process, the **e-procurement application module** has to be integrated into the smart factory; this will enable optimum order quantity and reorder levels to be automatically computed with real time data from production, warehousing and incoming orders. Chen, Mirowski, Ho & Yu, (2014) suggests the Integration of the smart factory with the smart grid as another application domain of CPS in the production process; this will utilized the smart grid's features of the Energy of Things (EoTs) also referred to as intelligent grid to ensure optimal utilization of electricity.

iv. **Industrial Smart Data**

The previous section reviewed a number of application fields in the smart factory which have the common thread of generating high volume of data. This high volume of data captured through sensors need to be stored, processed and aggregated to produce contextualized information. This when done properly will provide a platform for understanding trends that will enable informed forecasting, which in turn will provide valuable resources for industrial smart services (Oks, Fritzsche & Möslein, 2017).

## 5. The Future of IOTs and CPS

Much as the two technologies differ in architecture as it relates to the Internet, they both share the same architectural foundation of embedded systems; challenges in terms security though at varying degrees; they also have overlapping applicability in many considerations especially on the basis of "smartness", it therefore points to the fact that in the near future, the two technologies will have significant convergence. For instance Oks, Fritzsche & Möslein, (2017) suggested a model where the smart factory's strategic suppliers, subcontractors and other strategic partners are integrated into the strategic production network forming a kind of extranet; the model also suggest the integration of the intelligent energy grid to ensure that energy is supplied on demand. Smart products, smart product related data are all pointers to the fact of this convergence since the product which have left the factory already, still

have potentials to continually interact with the smart factory.

**5.1 A quick glance into the web.**

i. CPS emphasizes hybrids systems and formal verification of dynamical systems while IoTs has roots in communication networks and wireless communication. This tends to influence the focus of research in conferences that highlight the particular topic.

ii. Cyber-physical systems create synergy among the entities of the physical and cyber space, by integrating analogue and computational hardware, middleware, and cyberware, while IoTs emphasizes communication protocols. Both also consider issues of privacy and security, among many others.

iii. IoTs devices are Cyber-Physical Systems, but CPSs are not necessarily connected to the Internet and thus, not necessarily IoTs devices.

iv. IoTs is of an infrastructure nature that maintains a hierarchy of communication networks that collects information by sensing, exploring, processing and aggregating, and distributes it in a demand-driven and controlled way.

v. IoTs aims at functional connectivity and relationships in the physical space (among analogue and digital entities),

vi. The operation control of IoTs is typically rooted in the purpose and implementation of the system(s). The highest level operation control of CPS is supposed to come from real life processes that they implement or support (e.g. in the case of a CP greenhouse, it is concurrently derived from the plants and the surrounding environment). In addition to being resilient and adaptive, which are also characteristics of IoT, CPS as a whole or constituents of it may be autonomously evolving and self-replicating.

vii. The current view from US National Science Foundation (NSF) is that Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components.

viii. Internet of Things is an architecture that comprises specialized hardware boards, Software systems, web application interface protocols (APIs), which together creates a seamless environment which allows smart embedded devices to be connected to the Internet such that sensory data can be accessed while control system can be triggered over Internet.

## 6. CONCLUSION

CPS as discussed can occur without the Internet connection but through embedded systems such as the Bluetooth, printers, washing machines, vehicles and other sensor activated devices while IoTs cannot function without the Internet. However, IoTs is CPS but CPS is not IoTs. Supports was further given in areas of architectural correlation, application areas, challenges on both sides and future challenges which all pointed to the fact that CPS is quite different from IoTs even though they have a number of similarities.

## 7. REFERENCES

Alvaro et al, 2010. Challenges for Securing Cyber Physical Systems [Accessed from] https://pdfs.semanticscholar.org/939e/684cf1b5f98188c1ae4867829003b7e35844.pdf on 08/01/2018]

American International Group- AIG, 2014. Internet of Things: Evolution or Revolution? http://www.gather.com/it/page:jsp?id=1466

313

Berry, G, 2015. The Constructive Semantics of Pure Esterel-Draft Version . Available online: online: http://www-sop.inria.fr/meije/esterel/doc/main-papers.html

Benveniste, A. Berry, G, 1991. The Synchronous Approach to Reactive and Real-Time Systems. IEEE Proc. 1991, 79, 1270–1282.

Clarke, E.M.; Grumberg, O.; Peled, D. 1999. *Model Checking*; MIT Press: Cambridge, MA, USA.

Chen, S. Mirowski, P. Ho, T.K. and Yu, C. 2014. Demand forecasting in smart grid, [Accessed from]https://www.researchgate.net/publication/263128858_Demand_Forecasting_in_Smart_Grids [on 02/01/2018]

Chen, T. M. 2010. Stuxnet, the Real Start of Cyber Warfare?, *IEEE Network*, the Magazine of Global internet Networking [Accessed from] https://www.researchgate.net/publication/224194430_Stuxnet_the_Real_Start_of_Cyber_Warfare [on 20/11/2017]

Esposito, R. 2006. Hackers penetrate water system Computers [Accessed from] http://blogs.abcnews.com/theblotter/2006/10 / hackers penetra.html [on 26/12/2017]

Freescale, 2014. What the Internet of Things (IoT) Need to Become a Reality, www.freescale.com/IoT

Frost and Sullivan (undated) "Mega Trends: Smart is the New Green" [Accessed from] http://www.frost.com/prod/servlet/our-services-page.pag?mode=open&sid=230169625 (On 20/10/2017)

GMS Association, 2014. Understanding the Internet of Things (IoT) [Accessed from] https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf [on 20/11/2016]

Kim, K and Kumar, P. R, 2011. An Overview and Some Challenges in Cyber-Physical Systems [Accessed from] http://cesg.tamu.edu/wp-content/uploads/2014/09/An-Overview-and-Some-Challenges-in-Cyber-Physical-Systems.pdf [on 10/01/2018]

Koubaa, A. and Anderson, Bjorn, 2010. A Vision of Cyber-Physical Internet [Accessed from] https://www.researchgate.net/publication/228955564_A_Vision_of_Cyber_Physical_Internet [on 12/01/2018]

Lee, E.A. 2014. Constructive Models of Discrete and Continuous Physical Phenomena. *IEEE Accessed 2014, 2, 1–25.*

Lee, E.A, Sangiovanni-V. 1998. A Framework for Comparing Models of Computation. *IEEE Trans. Comput. Aided Des. Circuits Syst.* 17, 1217–1229.

Oks, S.J, Fritzsche, A and Möslein, K.M. 2017. An Application Map for Industrial Cyber-Physical Systems, *Springer International Publishing Switzerland*

Graham, S. Baliga, G. and Kumar, P. 2009. Abstractions, Architecture, Mechanisms, and a Middleware for Networked Control," *IEEE Transactions on Automatic Control*, vol. 54, no. 7, pp. 1490–1503

Golomb, S.W. 2014. Mathematical models—Uses and limitations. *IEEE Trans*. Reliab. 1968. R–20, 130–131.

Park C.S. and Chou P. H. 2006. Eco: ltra-wearable and expandable wireless sensor platform, *Proceedings of the International workshop on Wearable and Implantable Body Sensor Network*, pp.158-162

Vermesan, O. et al, 2011. Internet of Energy—Connecting Energy Anywhere Anytime In Advanced Microsystems for Automotive Applications: Smart Systems for Electric, Safe and Networked Mobility, *Springer*, Berlin.

Naoufel B. 2015. Cyber-Physical Systems: Structure, Communication and Behavior. The European High Impact Initiative for Cyber Physical Systems. Munich Germany.

Vermesan, O and Friess, P., 2013. *Internet of Things – Converging Technologies for Smart Environment and Integrated Ecosystem*, Rivers Publishers, Aalborg, Denmark

World Economic Forum, 2015. Partnering for Cyber Resilience: Towards the Quantification of Cyber Risk, at http://weforum.org (accessed on 08/01/2017)

Wiener, N., 1948. *Cybernetics: Or Control and Communication in the Animal and the Machine;* MIT Press: Cambridge, MA, USA, 1948.