# Advanced Communication in Cyber Physical System Infrastructure, Protocols, and Challenges

**[1]Anandakumar Haldorai, [2]Ravishankar.C. V, [3]Qaysar S. Mahdi, [4]G. Jawaharlal Nehru**

[1]Sri Eshwar College of Engineering, Coimbatore, India.
[2]Sambhram Institute of Technology, Bangalore, Karnataka, India.
[3]Faculty of Engineering, Tishk International University-Erbil, Kurdistan Region, Iraq.
[4]ST. Martins Engineering College, Secunderabad, Telangana, India
*[1]anandakumar.psgtech@gmail.com, [2]cvravishankar@yahoo.com, [3]qaysar.mahdy@tiu.edu.iq, [4]gjnehruceg33@gmail.com*

2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT) | 978-1-6654-9360-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICECCT56650.2023.10179710

**Abstract – In contemporary developments like Cyber Physical System (CPS) and the Internet of Things (IoT), computerized integrated connection is seen as a trend. Some of the unique research issues in CPS include security, confidentiality, business intelligence, participatory monitoring, and smart decision making. A secure infrastructure, reliable protocols, and high-quality solutions are just a few of the other Wireless Sensor Networks (WSN) obstacles that must be overcome. This paper provides a critical survey of advanced communications and sensing in CPS infrastructures, protocols as well as challenges. A CPS framework, including its protocols and implementations, are described in this work. Mobile Sensor Information Agent (MSIA) signifies a software-centric mobile sensor system. It operates as a plug-in with the CPS framework and scalability mobile apps. With the MSIA, data from numerous external sensors may be collected and sent to the cloud as needed. Integration with the real environment is essential to CPS's stability and security as well as its dependability and resilience. Emerging Software-Defined Networking (SDN) technologies may be coupled with CPS architecture as a communications network to build this system. Thereby, it is feasible to enhance the performance of the system utilizing an SDN-based CPS architecture**

**Keywords – Cyber Physical System (CPS), Software-Defined Networking (SDN), Mobile Sensor Information Agent (MSIA), Internet of Things (IoT)**

## I. INTRODUCTION

A Cyber-Physical System (CPS) [1] is one in which devices and communications networks (such as utility networks, automobiles, and factories, for example) are linked to the physical environment created by humans. Sensors and actuators link the actual world to the virtual one. The basic role of CPS sensors is to measure and convert physical quantities into electrical impulses. A cyber system is used to sample and quantize this electrical signal before it can be used in the computer. Actuators in the physical environment are controlled by the cyber system, which utilizes these quantities to compute and deliver control orders. As a means to solve environmental, economic, and social concerns, CPS is currently the subject of research in both the private and public sectors.

As in the real world, CPS provides assistance to those in need. With its ability to analyze mission essential data in real time, the Internet of Battlefield Things is presently becoming a vital CPS application. In terms of research and execution, CPS presents several challenges. Various branches of study have come together to study it. Just a few of the current challenges that need to be solved include communications networks, environmental conservation, surveillance systems, and power transmission systems. In order to increase service quality, we must also develop user-friendly hardware and software interfaces.

These smart sensors have been used in a range of IoT applications recently. Commercial products and technology are used in a variety of ways across time. Wireless, affordable, and simple to use are just a few of the advantages of the CPS sensor ecosystem, which includes tablet computers. Sensors like GPS, accelerometer, accelerometer, recorder, magneto, and motion detector are being incorporated to new gadgets. The goal of CPS [2] is to make things easier and link anybody, anywhere, at any time. Because of this, we need a scalable and interoperable shared platform. Data analytics, participative sensing, privacy, and visualization are all part of the CPS problem, as are architecture, protocols, security, and service quality. However, the vast majority of cloud-based CPS systems are built using this technology. The two fundamental roles of CPS as it moves into the digital age are as follows: improved communication amongst real-time data from multiple sources and input from the cyberspace Analytics and computing of intelligence data.

As a new paradigm for network management and reconfiguration, Software-Defined Networking (SDN) [3] is gaining momentum. Computing infrastructure and forwarding may now be separated, allowing programs and network services to use the underlying technology without having to learn about it. SDN's key advantages include improved security and the ability to virtualize whole networks. The SDN controller ensures that all CPS endpoints and linkages are secured by disseminating consistent privacy and policy information. Furthermore, by making it simpler to gather data on network utilization, SDN may assist CPS in detecting unusual behavior.

To transmit real-time data produced by detectors in the physical infrastructures, such as switching devices, gateways, WiFi and ZigBee are employed [4]. Control instructions are sent to physical devices over the same communications networks utilized by the cyber systems. A high-performance communications system is essential to CPS's ability to respond quickly and effectively.

Communication infrastructures like this may be created using SDN and CPS. As a consequence, we created an SDN-based CPS architecture. Network activities may be managed and verified on the fly. The global view and automation properties of the SDN controller enable more efficient control, setup, monitoring and fault diagnosis and repair in SDN-based CPS.

The rest of the paper is organized as follows: Section II provides a definition of the relevant terms used in this paper. Section III reviews the relevant literatures used in this research. Section IV proposes the architecture for CPS. Section V analyses the mobile sensing platforms in IoT prototypes; which Section VI focusses on the machine-to-machine communications protocols. Section VII reviews the CPS challenges and recommends a framework for performance enhances. Lastly, Section VIII draws conclusions to the whole research.

## II. DEFINITION OF TERMS

### *A. Cyber-Physical System (CPS)*

A computer model where devices are supervised or managed by computer-centric methods is known as a Cyber-Physical System (CPS) or an autonomous system [5]. To understand cyber-physical systems, it is important to understand how the physical and software elements interact with one another, how they work at various geographical and temporal scales, and how they interact in ways that alter depending on the environment. Cybernetics, mechatronics and process science (CPS) are all intertwined in CPS, as is the theory of cybernetics. Embedded systems are often used to describe process control. While a strong connection between the physical and computational parts is important in many systems, embedded systems place a greater focus on the computational aspects. However, unlike the Internet of Things (IoT), CPS has a greater level of coordination and integration between physical and intellectual parts, making it more comparable to CPS. Automated avionics are an example of a CPS system. The smart grid is another example. For example, cyber-physical systems may be found in aircraft, automotive, biochemical mechanisms, civil and energy infrastructures as well as in healthcare and industry.

The word "cybersecurity," which deals with the CIA (Confidentiality, Integrity and Availability) of data [6] but has not inherent relations to the physical processes, is sometimes used interchangeably with "CPS," according to some sources. As a result, the word "cybersecurity" only has a tenuous connection to the field of cybernetics. While security and privacy are obviously major considerations when it comes to CPS, they are far from the only ones. As IoT (Internet of Things), fog computing, TSensors (Trillion Sensors), M2M (Machine to Machine), and Industry 4.0 become more prevalent, CPS become significantly relevant (like the cloud, though nearer to the ground). All of these signify a perspective of a system, which connect out digital and physical worlds together in a vibrant way.

### *B. Software-Defined Networking (SDN)*

In order to increase network performance and surveillance, software-defined networking (SDN) technologies allow for dynamic, programmatic effective system design. SDN is just like cloud computing in contrast to network management. The static design of conventional networks is addressed by SDN. Through the separation of the packet forwarding (data plane) from the packet routing (control plane), SDN aims to consolidate network intelligence into a single component (control plane). As an SDN network grows, so does the control plane, which is made up of one or more regulator devices that are regarded to be its brain. Centralization, on the other hand, has drawbacks in terms of security, scalability, and elasticity, and this is the primary issue with SDN. For a long time after its inception in 2011, the OpenFlow procedure (for communicating remotely with network plane components in order to determine the path taken by data packet across network switches) has been associated with SDN. Since 2012, however, proprietary systems have also made use of the phrase. Open Network Environment (ONE) and Nicira's virtualized network platform are two examples of these technologies.

### *C. Mobile Sensor Information Agent (MSIA)*

This can be solved by using mobile agents to address the difficulties highlighted above. Like conventional programs, mobile agents may roam across the internet and carry both their own state as well as the code they are responsible for. It's fairly uncommon for these agents to migrate and conduct application-specific functions such as reading devices and collaborating with other agents. In [7] demonstrates how a fluid program may be designed that can adjust to WSNs' complexity, for example. Using mobile agents, WSNs may be dynamically reprogrammed, allowing for the introduction of new agents and the deactivation of existing ones. It is also possible to run numerous programs simultaneously on the same node. Section III below provides a literature analysis related to the research.

## III. LITERATURE REVIEW

The architecture of an autonomous system was proposed by [8]. To monitor machinery, this design is most commonly used. To keep records of the results of the computation, local storage is employed. It is necessary to record all of the signals coming from a production system. Besides signal processing, decision-making also incorporates character extraction. The author argued that architecture should be more flexible and available. To create a working prototype, CPS must be put to the test. Using a smart grid 8C architecture, a smart factory can be built, according to [9]. Extraction and storage of data for traceability are the primary goals of this architecture.

Physical procedures are networked with machines, and techniques coordinate and manage the physical phenomena via a network in the CPS, the newer iteration of digital systems Most full-blown CPSs are based on systems of interconnected physical components. There has recently been a lot of interest from universities and businesses in this new approach because it offers a wide range of advantages such as autonomous function and security. Using CPS and the Internet of Things (IoT), a powerful tool for simplifying industrial processes is created. There have been many large corporations that have adopted CPSs as a result. Due to years of preferred maintenance and weak connections, stiff, overburdened infrastructures leave behind a bad Quality of Service (QoS) [10] that reduces the feasibility of new service integration and raises the threat of attack.

Consequently, the CPS is confronted with several dangers and issues associated with Industry 4.0, such as a shortage of managerial focus on data security and protection. Having a resilient network is important to a network provider because it prevents assaults and ensures elevated amounts of robustness. Wide-ranging dangers, like the RTT latency varying from millisecond to millisecond with increasing data capacity, may be mitigated by more robust networks. This is the most prevalent stumbling hurdle for time-sensitive e-health applications. An important problem has recently been solved with SDN. It is referred to as "separating control and data planes" in network architecture when the two are separated. If the situation calls for it, this can be a social networking site or a business application. The Control position is called the network's "brain" because a logically centralized controller is in control of routing decisions. The Data plane contains components that are both digital and physical. Southbound APIs (generally OpenFlow) are used by the network interface and other cyber-physical framework components, while northbound APIs are used by the applications layer.

When it comes to Software-Defined Networking (SDN), a global view of the entire network reduces logistics while allowing for flexibility and orchestration. Because of its consistent network administration, network management may be combined with more complex techniques, like the cyber-physical system. The visibility, effective utilization of network devices, and convergence of service offerings provided by software-defined networking may assist increase the resiliency of a network. Building more robust computer networks with the help of machine intelligence may be an option. Machine learning methods may be employed in cyber-physical systems as software-defined networking includes a logically centralized controller. In light of the network data at hand, the network operator is in a better position to make more robust traffic forwarding decisions and routing rules.

Now, smart IoT technologies are playing a major role in the medical sector. Such a system relies on outdated networks that can't endure a natural catastrophe. E-health networks are seeing an upsurge in traffic as more confirmed corona cases are reported in the current epidemic. As a result of the increased volume, e-health networks are becoming overburdened and even experiencing outages. The e-health networking must be bolstered in order to fight this problem. It is explained in detail in [11] how to establish safe and trustworthy e-health networks. Block chain may be used to protect e-health networks against counterfeit pharmaceuticals. Transfer learning is used by [12] to identify and categorize cervical cells. In [13] demonstrate merging cloud computing and computing capabilities with SDN for high-end functionality and QoS guarantee.

A virtualized flow management system with SDN assistance and a safe Lattice-based cryptosystem are all included in this composite architecture. According to [14], an SDN-based edge computing platform for healthcare is presented. Because of the improved resource usage and edge cooperation, the suggested framework has a lower ligancy and a greater throughput. The [15] offer a multi-tier computing and networking structure based on SDN technology. Depending on the kind of healthcare and the level of demand, the duties are performed externally on behalf of the end points. SDN-based security enforcement architecture for healthcare data sharing systems is presented by [16]. It is the goal of the Service Release Model (SRM) to allow service providers to control data services depending on user authorization. There is also a retreat available in contrast to the model of information flow that they supply.

ISA-95 The 0th level of the hierarchy is occupied by physical process production. The manipulation and sensing processes are quite similar to those seen in Level 1. In Level 2 manufacturing process inspection, monitoring, and control. Level 3 focuses on the activities and results of workflows. In addition, it contributes to manufacturing and production, as well as to warehouse and computer systems. Managing customer relationships and the supply chain are all part of Level 4's focus. Network and system behavior can be monitored and understood using a real-time monitoring tool. Effortless monitoring must be made available to the general public so that researchers can focus on integrating architecture, monitoring, and security. Several researchers e.g., [17] have proposed a CPS framework to help CPS become more flexible and scalable while also increasing its security, availability, and responsiveness to changing business needs. However, only a small percentage of people pay attention to the actual hardware, communications, and other components. Section IV provides a proposal of a CPS architecture.

## IV. PROPOSED ARCHITECTURE FOR CPS

The entire CPS architecture presented in this research is shown in **Fig. 1**. There are several CPS implementations, and we look for the commonalities among them. Each of CPS's divisions may be summed up as follows: There are four levels in the operating system of a device.

### *A. Application Layer:*

There are a variety of applications that may be supported by an application layer, including those in the smart home and the city, as well as those in the automotive industry. It gives an end-to-end CPS outcome from a telecommunications standpoint. Manufacturers, on the other hand, have their own CPS applications.

### *B. Service Layer*

The CPS platform is at the heart of the CPS architecture. For CPS applications, it performs operational functions like as protocol conversions, terminal management, and route forwarding. This layer also includes a name and address system as well as mobility sensing and a device search function.

### *C. Transport Layer*

As a bridge between data communications and bridge sensing networks, it plays an important role in many applications. Standardized format acts as a conduit for translation and acquisition of events. Private or public networks are used for all data transmissions inside the CPS network.

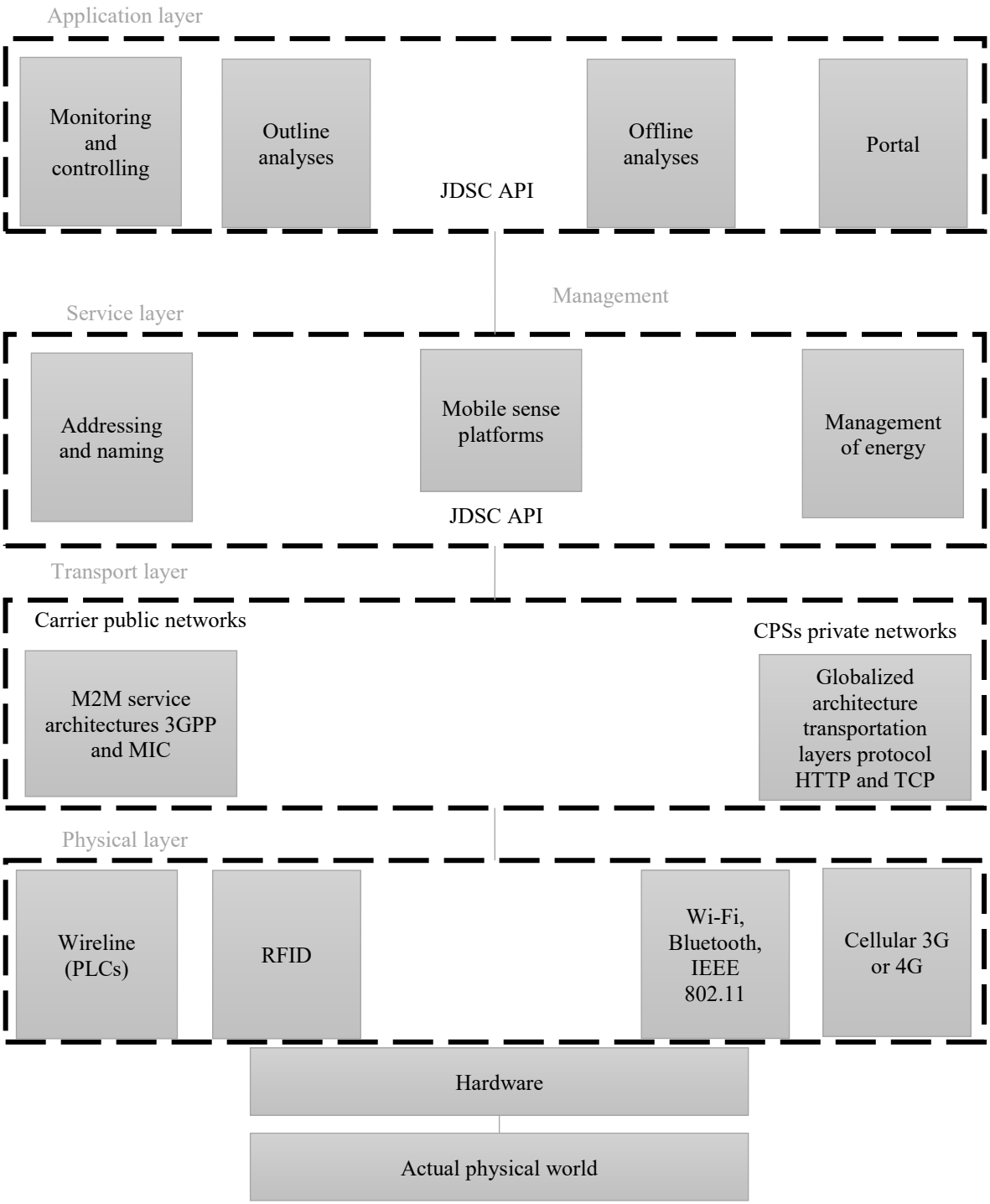


**Fig. 1:** Enhanced CPS architecture

### *D. Physical Layer*

The physical layer is the most basic in CPS design. Actuators and sensors are used in this layer of CPS. It may be corded or wirelessly linked. Zigbee, Bluetooth, RFID tags, and Wi-Fi for example, are widespread protocols for wireless communication systems.

## V. MOBILE SENSING PLATFORMS IN IOT PROTOTYPE

Sensor services are an integral part of the CPS paradigm. There has been a rise in the usage of tablets and smartphones in combination with mobile sensing equipment. For mobile sensing, we've come up with the Mobile Sensor Information Agent (MSIA). With the CPS framework and extensible mobile applications, it's like plugging into something already existing. An intermediary device, the MSIA collects and uploads data from a number of external sensors as required. A variety of scenarios, both cooperative and

solitary, were used to test MSIA [18]. This initiative aims to answer a variety of questions. Energy-efficient and efficient information analysis, network connectivity, cost-effective infrastructural foundation for CPS application, and significance of linking sensor networks are our primary goals for this paper. Addressing these issues requires an understanding of and action on the subsequent research challenges: (i) Data is processed locally before being sent to the cloud utilizing a variety of devices with varied computational resources and tags, (ii) and by offering efficient and simple methods to link detectors to low-level computing equipment.

Numerous methods have been proposed in attempt to address some of the issues described above. However, there are a number of downsides to these solutions. In this quick study, we can highlight the flaws and design constraints of a CPS element, which should be applied on resource-restricted devices. In spite of the fact that a number of hardware elements are open source, it is challenging to expand and integrate with software systems. They also have their own hardware components that fulfill similar purposes as MSIA's. However, these items are custom-made. We feel that since most individuals are already acquainted with cellular telephones and how to use them, it will be simpler for people to embrace. It is also a big problem when gadgets do not operate with solutions from different vendors. For instance, a sensor created for a single solution cannot be interlinked to a software program for a different solution. As a consequence, we recommend middleware that is independent of any one provider.

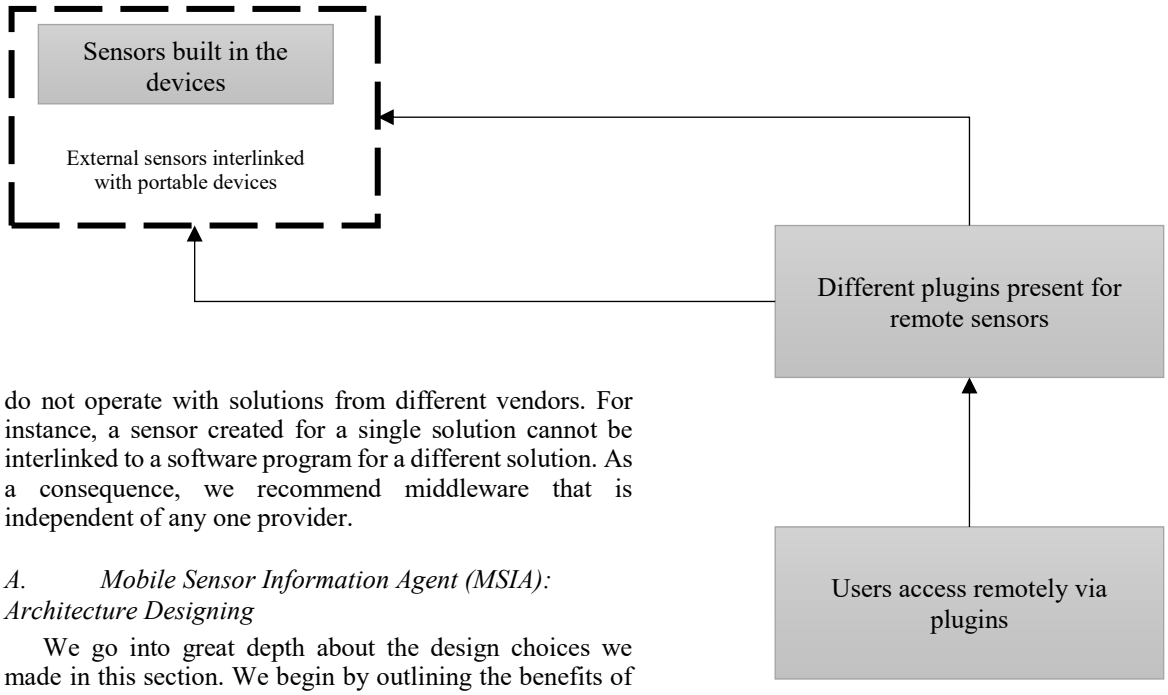


**Fig. 2:** Plugins installations and distribution

### *A. Mobile Sensor Information Agent (MSIA): Architecture Designing*

We go into great depth about the design choices we made in this section. We begin by outlining the benefits of a plug-in architecture. As a follow-up, we go through the MSIA architecture as a whole in more detail. Third, describe the interactions between MSIA instances and other GSN cloud-centric cases. Lastly, we determine succinctly that information could be MSIA applications and distributed programs as

### *B. Architecture for Plug-ins*

MSIA implemented plugin architectures to meet the three aforementioned requirements: ease of use, scalability, and a sense of shared ownership. A plug-in is a standalone software element that adds a particular functionality to a traditional software program. To potentially adjust communication between particular sensors and MSIA, every plug-in in MSIA will transform general communication signals into sensor-specific instructions. It is possible to customize a program if it supports plug-ins. This plug-in may be installed and configured on the fly, as well.

a) Scalability: A plug-in technique allows MSIA to work with sensors from all around the globe. A goal is to create plugins for MSIA that enable it to interface with sensors given. The plug-in also takes up very little storage capacity (e.g., 24KB). Because of this, even on a device with low resources, many plugins may be stored. In addition, when memory is running low, MSIA automatically eliminates unnecessary plugins. The MSIA program may be reduced in size by separating plugins from the primary application. Thousands of plugins are accessible on application stores, however in practice only a limited number of plugins have been integrated to effectively support connections. Moreover, the plug infrastructure permits us to develop MSIA in the future generation, most in the context of automated sensor installation and detection of the plug-in based on contextual data.

b) Community-centric Developments: Infrastructures that permit humans to communicate with the developers' groups, and possibly support multiple sensors via community-centric developments. Future versions of our software are projected to be open sourced and free. It is possible to start designing plug-ins for different sensors by using the standard interface that we offer with the MSIA program. Our sample plug-in source code just requires developers to add their own code in accordance with the

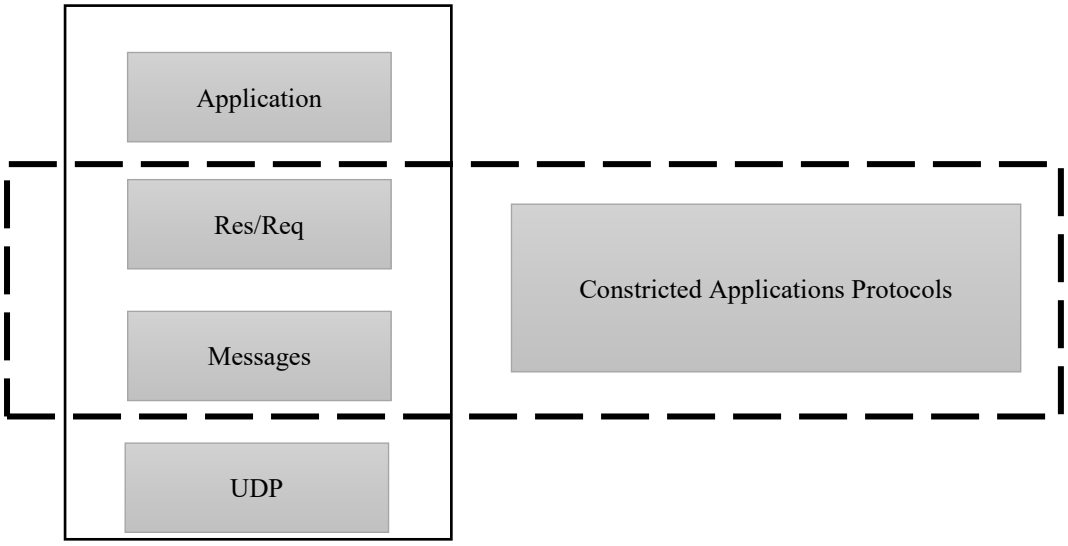


**Fig. 3:** CoAP stacking

specified instructions. The number of detectors enabled by MSIA is expanding as plug-in models become more widely available.

c) Serviceability: Data from sensors can be collected more easily using MSIA since it does not need any scripting. Only the proper matching plug-in may be downloaded from an application platform by users. MSIA understands how to interface with every plug-in program because of a highly standardized plug-in structure (see **Fig. 2**)

MACHINE-TO-MACHINE COMMUNICATION PROTOCOLS

Communication between machines is the most critical enabler of CPS. Results relating to IPv6 integration with wireless technology and CPS technologies are of particular interest here. There are two kinds of CPS performance now Doi: non-IP based and IP-based. Popular non-IP options include ZigBee and INSTEON as well as WAVE2M and Z-Wave. Due to the variable system communications, these techniques are incompatible with CPS development. TCP/IP, on the other hand, is the internet's standard traditional communications protocol. So, the future of CPS networks is IP-based outcomes.

### *C. Protocols Stack WSN*

The WSN, IPv6 and IP have been established for more constrained networking frameworks.

a) Constrained Application Protocol (CoAP): A resource-constrained network and node are the focus of this protocol. CoAP is a REST-based protocol. POST, GET, DELETE, and PUT are all stateless actions that correspond to Universal Resource Identifiers (URIs). In contrast to HTTP, the CoAP protocol is not based on it. CoAP is a datagram-oriented protocol that acts like UDP and functions as a subset of the HTTP protocol. The CoAP stack's layer structure is seen in **Fig. 3**. Four kinds of CoAP messages are available for transmitting information [19]: i) Confirmable (CON), acknowledgement is vital. ii) Non-Confirmable (NON), acknowledgement is not vital. iii) Acknowledgement (ACK), conformation messages are to be obtained and vital. iv) Reset (RST), representations of confirmable messages acknowledged but could never be processed.

b) RPL: Routing in low-power and lossy systems is defined here. Four standardizations are required for routing: Home Automation (RFC5826), Industry Control, Building Automation, and Urban Environment (RFC5548) are all subcategories of the RFCs (RFC5673)

c) 6LoWPAN: Using IPV6 is the best way to communicate wirelessly (see **Fig. 4**). Flexibility, generality, and durability are the hallmarks of IPV6.

## VI. CPS CHALLENGES AND PERFORMANCE ENHANCEMENT

Cyber Physical System is the most sophisticated level of traditional information systems. Networks, modules, actuators, as well as sensors comprise the CPS architecture. As the flexibility of CPS rises, so does the need for adequate design, architecture, and enforcement of CPS in important social applications. It's also necessary to maintain and operate the sophisticated CPS system. In addition, there are system-related technical concerns, such as validation of the system, accuracy, and timing behavior. Integrating an IT system into an operating system is the most significant obstacle. To make a process more efficient, organizations are turning to CPS.

### *A. Challenges*

#### *1) CPS Complexity*

**Fig. 5** depicts our entire approach to CPS intricacy. Human programmers interacting with CAE technologies and the appropriate data and knowledge are in charge of developing and executing CPS via Collaboration Information Processing Systems (CIPS).

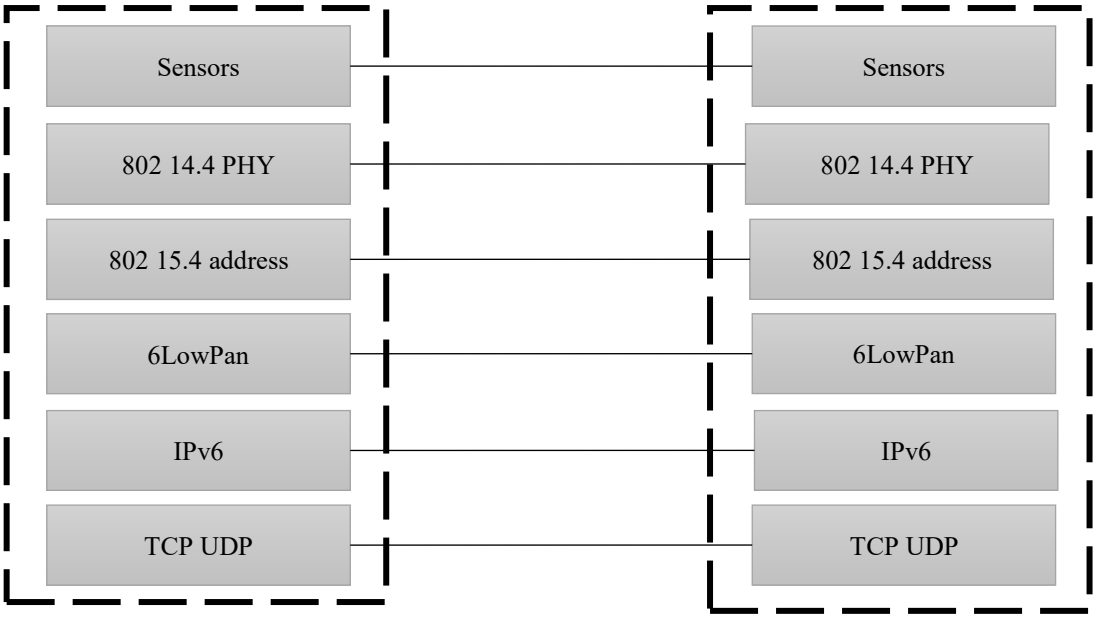


**Fig. 4:** Locality of 6LowPan within IPv6 stack

This means that CPS might be operating in a setting that includes people and other kinds of systems (such as natural or social systems, as explained in [20]. Secondly, in our view, complexity is related with systems. The system depicted in **Fig. 5** contains both CPSs and CIPSes.

In terms of dealing with the CPS's complexity, there are consequences for human and project capacity; that is to say, the facets will be closely linked to the CIPS's limits. As a result, it is necessary to devise strategies to bridge the gap between the CPS's complexity and the constraints of CIPS. Its first contribution is to bring together all of the present viewpoints into a unified framework. I analyze the interconnections between the various CPS components, and (ii) how these systems differ from one another in order to better understand some of the factors that contribute to complexity in CPSs.

"Subjective complexity" relates to how individuals perceive systems, whereas "objective sophistication" alludes to the technical or functional aspects of a technology. An example of the former are metrics relating to CPS optimization's intrinsic issue size and algorithmic complexity. One example of this is the impression that one cannot understand the behaviors of a CPS. Though complexity is always growing, In [21] claims that as new devices are acknowledged and better understood, it actually decreases in terms of subjective complexity. We think this is an option because the CIPS would have to cope with the CPS. If even a medium amount of CPS is too much for humans to handle, it's understandable. Complexity increases the difficulty of predicting system behavior and understanding its ramifications. Trade-offs become more challenging and subjective as a result.

There are many different interpretations of the term "emergence" when used in relation to complexity theory. What it takes to figure out a system's properties based on the qualities of its sections and their interactions is not a trivial matter. "It's not a trivial issue". Due to the incapability to truly understand the interactions between various components, occurrence can have either beneficial or unfavorable consequences. Studying the complexities of a project is a worthwhile endeavor. A wide range of complexity-related variables can be linked to project cost overruns, delays in schedule, and poor system performance (or metrics). 39 variables were measured in 75 development projects by senior software engineers and project managers. We found that having a steady set of stakeholder relationships and a high level of cognitive fog 3 were both associated with more problematic outcomes (cost, schedule, and performance). Problematic outcomes were found to be associated with all three of these factors of com- plexity (cost, schedule, and performance).

*2) Context Discovery, Storage, and Processing*

It was considered that semantically annotated data relating to sensors had already been collected and was ready to be used. Each internet-enabled object, however, needs to collect context information. In addition, while obtaining these context datasets are challenging, some like battery life, can be access from the item directly. The sources of data provided by the item producer or technical documentations could be necessary to obtain context data such as item's expected lifetime. Fusion (such as pattern recognition) data collection over a particular set of time is fundamental to generate more contextual data, e.g., reliability and accuracy. In addition, each sensor must have its context information separately maintained. In order to collect and model context information, an API that supports this has not yet been developed. We used semantic modeling techniques to model context information in this paper. TDB and SDB are the data storages that are being used.. NOSQL data store is a state-of-the-art storage technology that should be considered and evaluated. Adding to this, MapReduce can be used to improve the speed of querying.

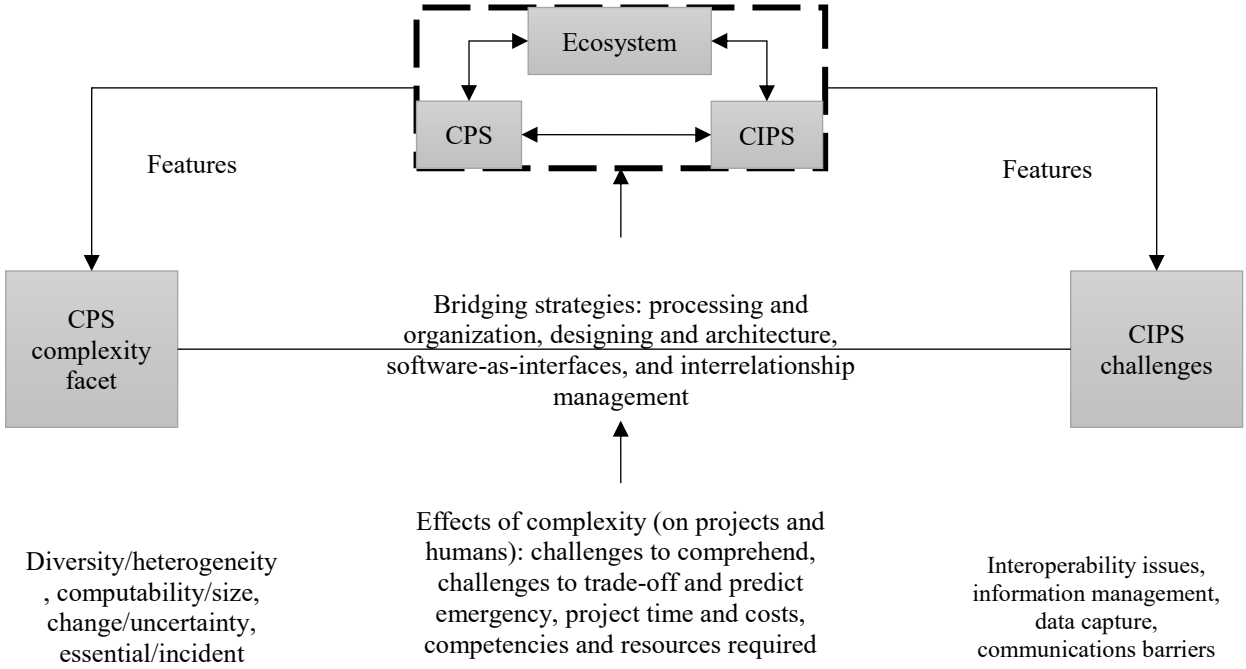


**Fig. 5:** An overview of complexities in CPS

*3) Automated Smart Device Configuration*

Smart devices are assumed to have been configured and linked to the cloud in this paper. It's a difficult task to identify, locate, and configure smart things. As a result of the dynamic nature of smart gadgets, this is a particularly difficult problem to solve. Even when a device is not in the specified location, it is critical to keep track of its context information. An individual smart device's MAC address might be utilized to potentially identify it. The location of the smart devices, on the other hand, may drastically alter some of the perspective information. Pressure sensors can be used to enhance the performance of smart objects in a shopping mall. Natural conditions such as temperature, breezes, floods, and other weather conditions can significantly alter accuracy if we use the same object beyond of the mall. As a result, it becomes more difficult to maintain proles that are aware of their location. Along with geographic location, time of day, and calendar day, seasonal variations could have a vital effect on contextual data like reliability. Consider the above-mentioned factors when deciding on a model for context information.

*B. Performance Enhancement*

*1) Proposed SDN-based CPS Framework*

Cyber-Physical Systems (CPSs) are the focus of recently developed words such as Industrial 4.0, the Fourth Industry Revolution, or the Industrial Internet; that is, sophisticated systems where physical elements or activities are controlled remotely by cyber components. Communication and data-processing operations are handled by these parts. This diagram illustrates the connection between the physical and cyber domains, where the management plane should provide sufficient performance in satisfying various criteria associated with system manageability, security, dependability, and so on. Numerous CPS-related applications, such as transportation and industrial automation, as well as electrical power grids, have garnered significant attention in recent decades.

These new CPSs are built on top of classic Industrial Control Systems (ANSI/ISA-95 model), which use a hierarchical structure for the data collection and processing aspects of a Networked Management System (NCS). Isolation models have traditionally been used in the construction of industrial automation networks, in which the control of OT is independent from the IT viewpoint. A CPS, however, is often structured as a network that connects all of the physical and computational pieces in a production infrastructure, rather than a hierarchical structure. CPSs are so important since they allow for complete integration of manufacturing processes and communications. For the first time, a complete examination of the needs of rising CPS is presented in this research. When designing communication systems for dynamic performance, it is essential that the network configuration responds to any changes in the physical device settings. Network protocols and sophisticated control systems working together to create a new environment for CPS applications is an exciting prospect for the future. With this, SDN may play a key role in the construction of CPSs.

The control and data planes of software-defined networks are separated. It is possible for external organizations to obtain a worldwide view of the network using standard protocols such as OpenFlow, ForCES, or the combination of PCEP and BGP Link State Dissemination (BGP-LS, RFC 7752) techniques. Because of the programmability they enable, software-defined networks (SDNs) are becoming more popular in industrial settings as well as data centers. Existing SDN architectures may be enhanced in this fashion to provide CPS domains with industrial-grade QoS capabilities. The purpose of this study is to examine important material on the incorporation of

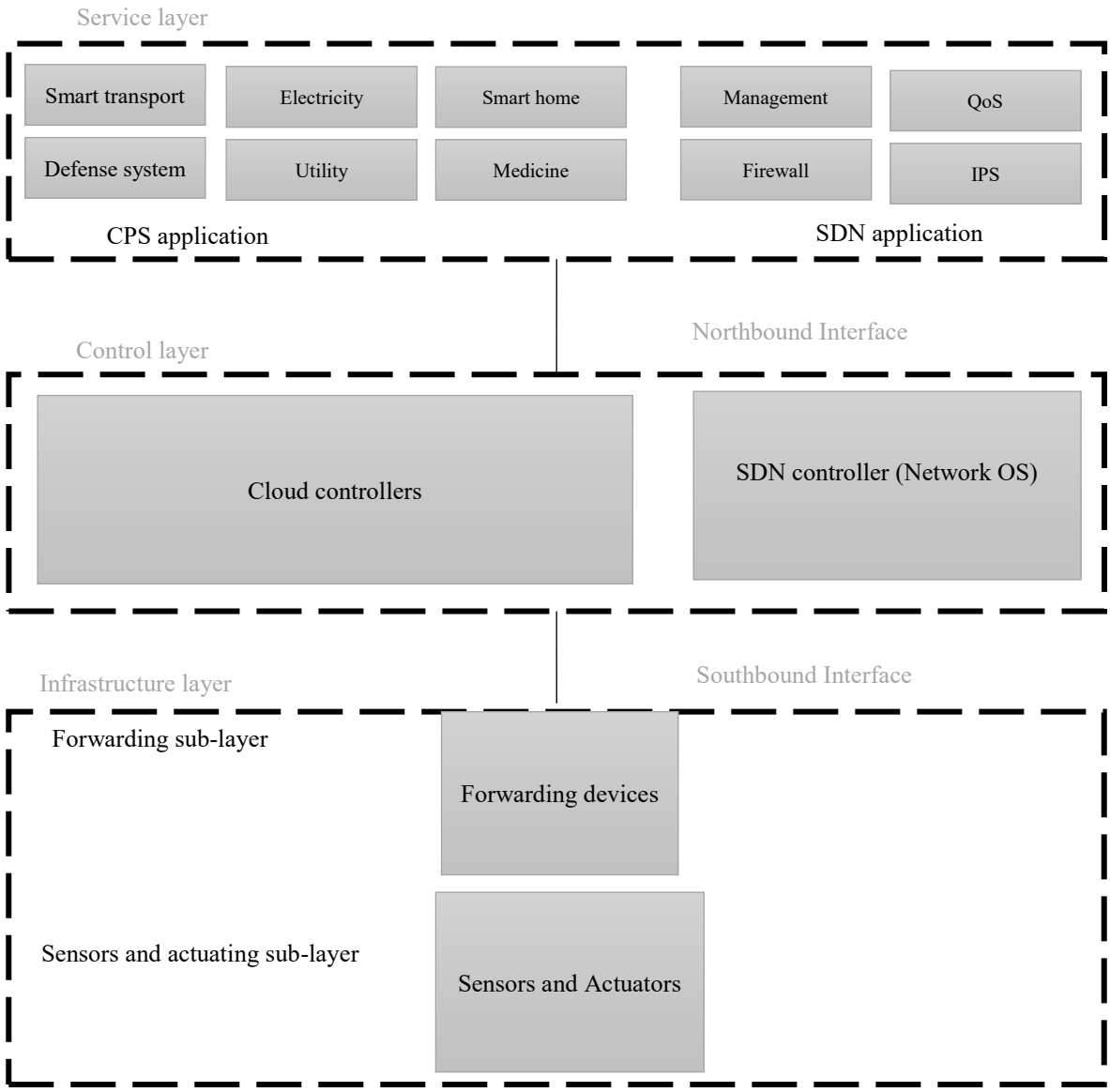


**Fig. 6:** Proposed CPS model (SDN-based)

SDN in crucial CPS communications in order to contribute to the future development of software-defined cyber-physical systems.

An SDN-based architecture for cyberphysical systems (CPS) that may be configured, managed, and controlled via the control layer is shown here (see **Fig. 6**). Layers one through three make up the planned architecture. Sensory and actuator sublayer and processing sublayer make up the infrastructure layer, which is further subdivided into two parts: Sublayers of sensors and actuators are located in this layer. Data from physical systems may be gathered by these sensors and sent to a cloud supervisor through forwarding mechanisms for additional processing. When the control plane (SDN manager or cloud manager) sends a command to the actuators, they carry it out. Openflow (OF) circuits and gateways are used in the forwarding sublayer to send control and data/information sessions to the SDN

supervisors and internet controllers. There are two types of controllers at the control layer: one for SDN and the other for cloud. Mainly, the SDN controller handles and monitors communication devices. To ensure that devices can communicate securely and reliably, it also runs a number of programs (such as routing, QoS, and IDS). When it comes to CPS, the cloud controller manages a group of servers. CPS services (e.g., smart home, national grid, etc.) are provided by the service layer utilizing the cloud controller. SDN-based CPS delivers additional networking services, such as routing, QoS, and security.

Using a central SDN controller to manage and regulate the network, the suggested SDN-based CPS architecture may offer protection against different kinds of assaults by providing continuous access control, implementing effective and efficient security rules, and so on. In spite of this, centralized SDN controllers have a number of concerns with dependability and security. SDN controllers, on the other hand, may fail owing to hardware or software malfunctions.

SDN controllers may be infected with malware by an attacker. Open-Flow protocol issues or connection failures may cause the control layer and data plane to become separated. Network functionality and, as a result, communications between devices, might be jeopardized if an application software has defects. As a result, we're working to create an SDN-based CPS architecture that's both safe and robust, in the hopes of reducing future physical and cyber risks.

## VII. CONCLUSION

In the real and virtual worlds, the development of a Cyber-Physical System (CPS) has emerged as a viable avenue for improving communication between humans, objects, and other things in both. CPS has led to a fast expansion in the number and kinds of smart devices linked to the Internet, bringing with it the present concerns of flexibility, availability, efficiency, and scalability, security of the Internet-of-Things (IoT) system. Physical and computational processes are combined in CPS. The suggested CPS architecture is flexible and enables commercial applications. A real-time broadcasting and communications system may be integrated with the CPS standards and protocols that have been developed. For an SDN-based CPS which enhances data security, connectivity, and quality of service, we provided a framework. A safe and robust SDN-based CPS architecture will be designed and developed in the future to eliminate both physical and cyber risks.

## VIII. REFERENCES


[1]. S. Yadav, "A resilient hierarchical distributed model of a cyber physical system", Cyber-Physical Systems, pp. 1-24, 2021. Doi: 10.1080/23335777.2021.1964101.

[2]. J. Park, S. Lee and T. Yoon, "Designing Goal Model for Autonomic Control Point of Cyber-Physical Systems (CPS)", Indian Journal of Science and Technology, vol. 8, no. 19, 2015. Doi: 10.17485/ijst/2015/v8i19/76692.

[3]. K. Benzekki, A. El Fergougui and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): a survey", Security and Communication Networks, vol. 9, no. 18, pp. 5803-5833, 2016. Doi: 10.1002/sec.1737.

[4]. Andrea Vilan and Pamela Walker, “A Review of CPS Design and Vulnerability Analysis", vol.2, no.3, pp. 110-119, July 2022. doi: 10.53759/181X/JCNS202202014.

[5]. G. Chen, Z. Sabato and Z. Kong, "Formal interpretation of cyber-physical system performance with temporal logic", Cyber-Physical Systems, vol. 4, no. 3, pp. 175-203, 2018. Doi: 10.1080/23335777.2018.1510857.

[6]. Sidny Chalhoub, “A Critical Review of the Applications and AI Techniques for Anomaly Detection", vol.2, no.3, pp. 098-109, July 2022. doi: 10.53759/181X/JCNS202202013.

[7]. H. Hu and Z. Yang, "Mobile-Agent-Based Adaptive Data Fusion Routing Algorithm in Wireless Sensor Networks", Journal of Electronics & Information Technology, vol. 30, no. 9, pp. 2254-2258, 2011. Doi: 10.3724/sp.j.1146.2007.00296.

[8]. Z. Kitowski, "System Architecture of Mission Planning and Autonomous Surface Vessel Control", Solid State Phenomena, vol. 210, pp. 252-257, 2013. Doi: 10.4028/www.scientific.net/ssp.210.252.

[9]. A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid", IEEE Transactions on Smart Grid, vol. 4, no. 2, pp. 847-855, 2013. Doi: 10.1109/tsg.2012.2226919.

[10]. W. Urban, "Perceived quality versus quality of processes: a meta concept of service quality measurement", The Service Industries Journal, vol. 33, no. 2, pp. 200-217, 2013. Doi: 10.1080/02642069.2011.614337.

[11]. Anandakumar Haldorai, Shrinand Anandakumar, “An Design of Software Defined Networks and Possibilities of Network Attacks", vol.2, no.3, pp. 088-097, July 2022. doi: 10.53759/181X/JCNS202202012.

[12]. D. Peters, J. Harting, E. Klijn and K. Stronks, "Conditions for policy innovation in policy networks to establish integrated public health policy", European Journal of Public Health, vol. 24, no. 2, 2014. Doi: 10.1093/eurpub/cku166.134.

[13]. S. Minoofam, A. Bastanfard and M. Keyvanpour, "TRCLA: A Transfer Learning Approach to Reduce Negative Transfer for Cellular Learning Automata", IEEE Transactions on Neural Networks and Learning Systems, pp. 1-10, 2021. Doi: 10.1109/tnnls.2021.3106705.

[14]. J. Son and R. Buyya, "A Taxonomy of Software-Defined Networking (SDN)-Enabled Cloud Computing", ACM Computing Surveys, vol. 51, no. 3, pp. 1-36, 2019. Doi: 10.1145/3190617.

[15]. C. Li, L. Zhu, W. Li and Y. Luo, "Joint edge caching and dynamic service migration in SDN based mobile edge computing", Journal of Network and Computer Applications, vol. 177, p. 102966, 2021. Doi: 10.1016/j.jnca.2020.102966.

[16]. W. Ao and K. Psounis, "Approximation Algorithms for Online User Association in Multi-Tier Multi-Cell Mobile Networks", IEEE/ACM Transactions on Networking, vol. 25, no. 4, pp. 2361-2374, 2017. Doi: 10.1109/tnet.2017.2686839.

[17]. Y. Meng, Z. Huang, G. Shen and C. Ke, "SDN-Based Security Enforcement Framework for Data Sharing Systems of Smart Healthcare", IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 308-318, 2020. Doi: 10.1109/tnsm.2019.2941214.

[18]. A. Faro, D. Giordano and C. Spampinato, "Integrating location tracking, traffic monitoring and semantics in a layered ITS architecture", IET Intelligent Transport Systems, vol. 5, no. 3, p. 197, 2011. Doi: 10.1049/iet-its.2010.0141.

[19]. X. - and J. -, "The Mechanism of Wireless Sensor Network Data Collection Based on Mobile Agent", International Journal On Advances in Information Sciences and Service Sciences, vol. 4, no. 12, pp. 266-274, 2012. Doi: 10.4156/aiss.vol4.issue12.31.

[20]. Aisling Yue Irwing and Alen Macline, “Strategic Analysis of the Advanced Computing Infrastructure and Future Directions”, Journal of Computing and Natural Science, vol.1, no.3, pp. 077-084, July 2021. doi: 10.53759/181X/JCNS202101012.

[21]. E. Ko, "An Error Synchronization running on Gateway Software Stack based on CoAP", The Journal of Korea Institute of Information, Electronics, and Communication Technology, vol. 9, no. 1, pp. 114-119, 2016. Doi: 10.17661/jkiiect.2016.9.1.114.

[22]. D. Sonnenwald, "Contested collaboration: A descriptive model of intergroup communication in information system design", Information Processing & Management, vol. 31, no. 6, pp. 859-877, 1995. Doi: 10.1016/0306-4573(95)00002-x.

[23]. S. Borzillo and R. Kaminska-Labbé, "Unravelling the dynamics of knowledge creation in communities of practice though complexity theory lenses", Knowledge Management Research & Practice, vol. 9, no. 4, pp. 353-366, 2011. Doi: 10.1057/kmrp.2011.13.

[24]. H. Anandakumar and K. Umamaheswari, “An Efficient Optimized Handover in Cognitive Radio Networks using Cooperative Spectrum Sensing,” Intelligent Automation & Soft Computing, pp. 1–8, Sep. 2017. doi:10.1080/10798587.2017.1364931