International Journal of Basic and Applied Sciences, 14 (2) (2025) 119-124

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/s5wzx363
Research paper

Toward Pervasive Intelligence Systems: Looking Ahead in Cyber-physical World in Pervasive Computing

S. V. Manikanthan [1] *, Dr. L. R. Aravind Babu [2], Dr. Anu Priya George [3], Dr. P. S. G. Aruna Sri [4], M. Venkatesan [5]

[1] Melange Academic Research Associates, Puducherry, India
[2] Department of Computer Science and Information Science, Annamalai University, Annamalai Nagar, Tamil Nadu, India.
[3] Associate Faculty, Demont Institute of Management and Technology, Dubai, UAE
[4] Professor, Department of Internet of Things, Koneru Lakshmaiah Education Foundation, Vaddeswaram
[5] Assistant Professor, Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai
**Corresponding author E-mail: prof.manikanthan@gmail.com*

Received: May 6, 2025, Accepted: May 18, 2025, Published: June 10, 2025

Abstract

The physical world is becoming filled with communication and computing units that communicate with one another and users; almost everything will be able to gather data and react to relevant stimuli. Through sensing, computing, and transmission components, real-world elements interact with cyberspace in this technologically advanced situation, leading to the so-called convergence of the Cyber-Physical World (CPW). However, the ubiquitous computing environment and IoT devices are susceptible to various threats due to their dynamic operation and the requirement to manage private and sensitive data. A high degree of safety guarantee is necessary for smart environments, such as trusted context producers and consumers, which should shield private data from exposure or surveillance. A unique, lightweight security architecture that authenticates and preserves the context of providers and receivers is proposed in the research, along with a discussion of the primary cyber threats in smart environments. Several recent research studies have proposed a definition of CPS that encompasses all the characteristics mentioned in the various domains. We contrast those several CPS plans, talk about some related concepts and technology, and wrap up by outlining the primary research issues in the field.

Keywords: *Cyber-Physical World (CPW); Cyber Threats; Communication; Pervasive Computing; Bid Data.*

1. Introduction

As Mark Weiser first predicted almost 20 years ago, ubiquitous services and gadgets are everywhere, infiltrating and integrating into our everyday lives [1]. Our ecosystems are already changing because of the interconnection of the digital and physical worlds provided by GPS-enabled devices, e-readers, mobile recording devices, portable computers, and other devices. Using these gadgets and other technologies, data about the physical world—such as that gathered by nodes of sensors—is smoothly converted into the virtual realm, where it is designed to modify online apps and services about the real environment. This may even alter or change the outside world by using motors, as shown in Figure 1.1. This makes room for the development of novel services that enhance comprehension and engagement with the physical environment and social activities within it, as well as more broadly, to foster the potential related to "supplemented perceiving and interaction" in both the social and physical realms.

A typical perception of a pervasive computing system is the idea of an online environment superimposed on the real earth to keep an eye on it constantly and possibly make wise decisions to modify the virtual environment (computers and software) to human requirements. Nonetheless, academics studying pervasive computing are finding new avenues for investigation due to the convergence of the Cyber-Physical World (CPW). It is true that in a world that has convergent information, actions generated in the physical environment have the power to influence and change social and personal contexts, which in turn may have an impact on how data and services are managed online. This last element is becoming a very difficult research topic that requires more thorough studies.

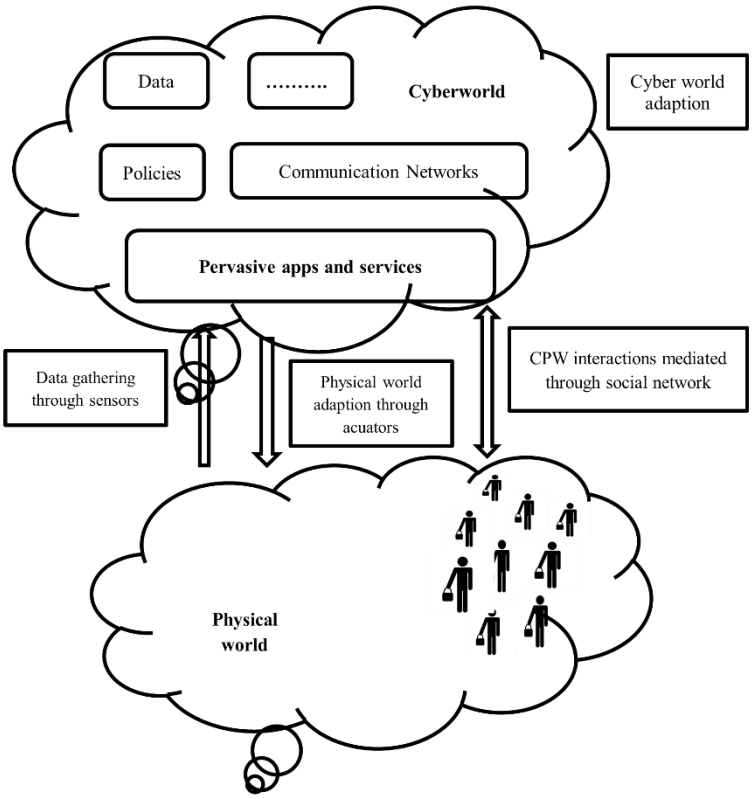

Fig. 1.1: Relationships in the Real and Virtual Worlds.

Human social structures can be crucial in regulating the dissemination of information online and, consequently, the development and coordination of ubiquitous applications and services. The social links that allow people to efficiently manage and disseminate enormous volumes of data are embedded in electronic gadgets by converting interpersonal communication into the online realm, as illustrated in Figure 1.2. The electronic social network is the name given to the resulting network. Human social networks have exceptional structural characteristics and dynamism that can have a big impact on the standard of the information (such as relevancy, dependability, trust reputation, etc.) and how it spreads both offline and online.

In this work, we try to examine the new research problems, difficulties, and prospects in the domain of smartphones and ubiquitous computing that result from the close connections between the real and virtual worlds.

A variety of intelligent devices, such as RFID tags, controls and sensors, sensor-rich cell phones, and closeness sensing technologies, are enabling the convergent CPW to develop an integrated and incredibly dense facility to track the physical environment and, as a result, collecting data on customer habits, needs, and dynamics.

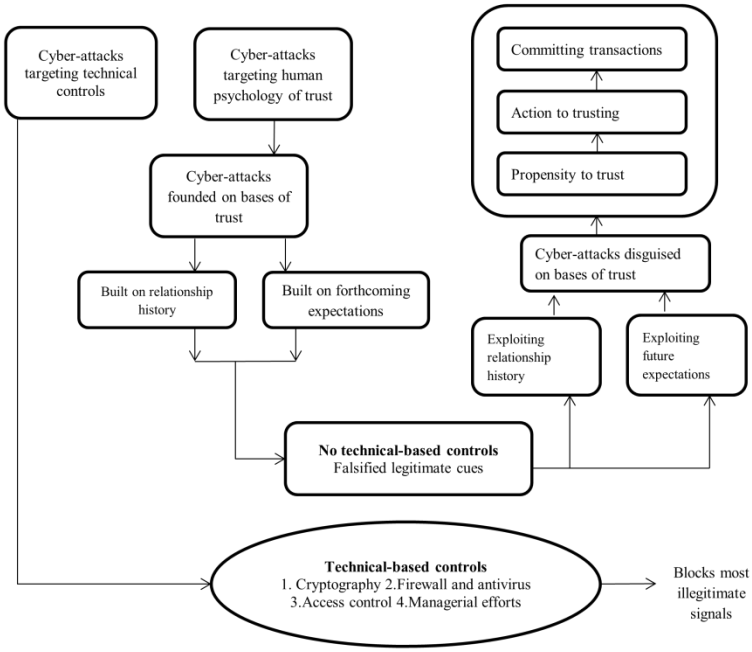

Fig. 1.2: Social Links between People and Electronics.

However, we may alter their makeup and structure by expanding human connections with cyber-world communities, which could have an impact on how people exchange information in the real world. In addition, human social networks are crucial for accessing and shar-

ing the vast amounts of data available in the online realm because they create overlapping connections among users, their devices, and their surroundings, that is, elements of the material world, since users are increasingly creating and/or accessing data on their gadgets.
The close cooperation and integration of cyber and physical assets, which results in previously unheard-of abilities, is a key differentiator of CPS [2]. With CPS, we must now examine what is changing or shifting in the real world, whereas earlier cyber systems were typically thought of as the passive, dumb component of the physical world. The usage of relationships, which introduces complexity and possible instability along with configurability and scalability, is a key distinction between CPS and an embedded system or standard control system. Additionally, CPS has far tougher performance limits and sensors and actuators with much higher intelligence. Examples of early CPS are now appearing in a variety of industries, including robotic vacuum devices for homes, Automotive gadgets such as autonomous driving and anti-theft devices, mobile phone location services, power grid field devices, human cardiac pacemakers, flight management, and electrochromic cabin windows, gaming, recreation, and sensing systems. However, many of the technologies that are in use now are either much more able to perform richer cyber-physical connections or do not concentrate on them.
By closely integrating the resources and dynamics of the tangible and engineering, Future CPS is expected to enhance cyber-physical relations by integrating cyber systems' processing and connectivity at large dimensions and depths, ranging from nano-systems to globally distributed systems-of-systems [3]. Every physical process and component (such as car engines and brakes) has cyber capabilities built-in; socializing is used at many and extreme scales; there are several time and space scales of complexity; there are movements of system reconfiguring and organization; there are high degrees of control and automated loops that close at all performed scales; System lifespans range from years to many years; and extreme heterogeneity is observed across devices and protocols.
The paper is organized as follows from this point on: An instance of the key elements of cybersecurity in the manufacturing sector is given in Section 2. Subsequently, Section 3 introduces the predictive manufacturing systems paradigm and provides recommendations for creating a cyber-physical system design structure, detailing various important model elements. Lastly, a sudden overview of the necessary research and a future prognosis for manufacturing cyber-physical systems are provided.

2. Related works

We can now more easily link between the online and physical worlds because of the widespread use of smart devices with different MEMS sensors, such as smartphones and smartwatches [4]. For instance, the inertial sensors that are included in smartphones, including gyroscopes and accelerometers, allow us to continuously monitor human movements while taking pictures. We may decrease the needless energy usage for phone-based photography in this way by efficiently identifying the user's actions during the shooting process. Furthermore, the emergence of small, inexpensive, and clever chips like RFID opens new possibilities for battery-free sensing.
An enormous amount of data is produced in an infrastructure that is dominated by CPS. The corporate systems are not currently built for such operations, and it may not be the best idea to transmit the data that is required to get the gist to a central location. Therefore, depending on their features and abilities [5], business processes that need data to reside on a CPS could outsource that portion of their capability to execute directly on the CPS or a collocated system. Distributing business intelligence is a major motivator in addition to the load distribution across firms and the real-world infrastructure. Nowadays, the majority of CPS rely on running independently or supplying data to independent services. However, as CPS networks and communication grow, they will be able to collaborate, exchange information, participate in ecosystems, and overall be active components of a more sophisticated system.
Products based on ubiquitous computing can be made to be worn, embedded, lightweight, interconnected, and even implanted [6]. The wireless information gadgets in use today can ad hoc connect to both local Internet networks and mobile phone networks. They view the characteristics of pervasive computing as follows: Mobile computing has a high LoM and low LoE, typical corporate computing has a low LoE and low LoM, omnipresent computing has a high LoE and high LoM, and low LoM and high LoE. In our daily routines, computer technology has been able to go from leading edge to the backdrop thanks to its independence from location and access paradigms.
People, Integrated technology as well as reality all coexist in hybrid systems like CPS and the closely related IoT. They therefore present unique design problems for human–technology interaction because of their hybrid character [7]. However, CPS According to CPS, human-technology interaction must be addressed in terms of transactions between embodied individuals who are integrated into a milieu and engage in organic interactions with a technical setting. Because there are so many embedded computers, this environment has improved properties. As a result, individuals in these intelligent environments are subject to both mental and physical pressures. To put it another way, CPS calls for treating the behavioral aspects of the body in tandem with the mental aspects highlights a particular STS difficulty rather than just being an instance of STS.
The area of co-designing, planning, and oversight has been extensively researched in the field of embedded and real-time systems. However, co-design difficulties have been reexamined in several ways since the introduction of CPS. For instance, because CPS are usually networked control systems, current research has examined how network latency affects system stability regarding the compromise between immediate scheduling and reliability [8]. The study's output is a non-periodic controller strategy that can ensure system stability overall while consuming the fewest possible computational resources. Programming abstractions should be used to compile physical attributes such the rules between the two sciences, safety, power and real-time limitations, resources, robustness, and security features.

3. Methods and materials

3.1. Autonomic behavior of the cyber world infrastructure

The CPW converging situation is distinguished by an important amount of portable electronics that people bring with them or that are scattered throughout the surroundings [9, 10]. The parts of the cyber architecture should be able to connect and interact with one another dynamically and opportunistically, as well as adapt to the continuously changing physical/social reality [11].
Enforcing autonomic, self-managing, and adaptable behavior at the infrastructure and device levels is a well-known research topic to guarantee that these devices collaborate and can adjust to changing situations at the service levels. The CPW converge scenario involves decentralization, distributed devices, and the ability for users and developers to add new services at any moment. This can prevent programmers and system managers from remaining in the command loop and directly intervening in the system for settings and upkeep tasks.
Recent efforts at network and service levels aim to encourage autonomous and responsive behavior in pervasive systems for computing. However, we believe most existing proposals have drawbacks when considering future circumstances.

3.2. Limitations of current approaches to autonomic adaptation

Several models of autonomous computing include incorporating "add-ons" into existing frameworks, including "à la IBM," which advises attaching complex control circuits to current systems to facilitate self-management. Current frameworks are typically too complex for CPW infrastructures, which need to be lightweight due to the restricted capabilities of ubiquitous and portable gadgets and the dispersion of the scenarios.

Numerous alternative theories suggest relying on methods that are completely decentralized and lightweight, frequently influenced by phenomena of nature like self-adaptation and self-organization. Despite the potential and guarantees of nature-inspired methods, most current proposals do not fully address the problem of nervous self-adaptation; instead, they use natural guidance only to implement algorithmic solutions or to realize shared services at the framework or user level.

Recent research on pervasive computing has concentrated on social features and novel social services, but fails to recognize the level of society as a distinct aspect of the more widespread computer fabric. Users, not just customers or service providers, play an integral role in the broader infrastructure through human sensing, actuation, and processing skills. Autonomic adaptation methodologies cannot be used just for emerging CPW situations or the confluence of them.

3.3. Emerging challenges

Considering the aforementioned factors, we think that the modeling and architecture of upcoming widespread and Portable Computing widespread computing systems need to be thoroughly rethought rather than searching for one-off fixes to adaptation issues from, constrained perspectives. Even if this can be difficult, it is important to consider a fundamental and comprehensive approach to address the intricate requirements of adaptation and self-governing conduct that accompany such systems. The ultimate objective should be to make these systems inherently able to manage themselves, collective adaptation, and autonomy, with the separation between the social, infrastructure, and service levels becoming hazy or nonexistent.

The achievement of this overarching objective raises the following global research questions and difficulties.

- Comprehensive situation-awareness:

Over the years, pervasive computing has acknowledged the necessity for context-awareness. However, the difficulties related to context awareness have changed significantly in recent years. On the one hand, it is no longer difficult to obtain the information required to provide context-awareness. More thorough Levels of consciousness that are higher than are typically required while using models of contextual computing will be necessary for autonomous adaptation actions in future scenarios. Most current context-awareness approaches leave it. [12] It is the responsibility of every system component to retrieve and analyze the data required to make judgments about adaptation. However, this work might become too difficult to manage if awareness is required to encompass both occurrences happening at the various levels of the structure and the strict localization of components. Creating new tools to give components of the extensive computer network expressive and condensed representations of complex multidimensional situations is a significant research challenge to properly regulate each operation of each element in a collectively structured manner.

- Top-down vs. Bottom-up:

Understanding the concept of "power of the masses" becomes crucial when discussing the participatory ubiquitous computing processes of communal adaptations, as pervasive systems for computing are growing into extremely large sources of enormous amounts of data, including many users. Nowadays, small-scale systems are usually used to study most of the self-adaptation and autonomy phenomena and mechanisms. There will be millions of customers, gadgets, and information items in future CPW convergence situations. Understanding how and to what extent these phenomena are significantly more effective than those currently achieved with more traditional types of distributed computation and artificial intelligence techniques, they will be required to display kinds of adaptability and situation-awareness (or visible "intelligence") at such huge scales.

- Decentralized control:

Accordingly, models and methods must be used in conjunction with the existence and utilization of collective adaptation phenomena. This allows for the "by design" management of the general conduct of the pervasive networks and their component pieces. It goes without saying that since the systems are inherently decentralized, these control tools ought to be as well. This will lead to the difficult problem of establishing the framework and identifying the instruments for the decentralized management of intricate CPW situations. Additionally, to determine whether this regulation is effective, appropriate "measures" to describe the actions of the mechanisms under control must be found. Since the target scenarios are large and will exist to meet the various needs of numerous actors rather than the challenge of creating effective measurements for possible CPW scenarios can be a challenging study topic in and of itself, with a single, well-defined (and hence easily measurable) goal.

- Diversity and resolvability:

Most of the research on collective adaptation to date has concentrated on systems with a finite number of constituent classes. This does not, however, even come close to capturing the growing variety of elements (devices and services) of upcoming and developing CPW convergence scenarios, nor their ongoing development. To support a continual process of value collaboration in the overall ubiquitous infrastructures, it is imperative to provide diversity and resolvability for feedback from users and personalization. However, variety and adaptability are also acknowledged to be important factors in cooperative adaptation and cognition within complicated ecosystems and organisms, respectively, in addition to being possible sources of complexity.

- Mechanism designs:

To maximize the benefits of future CPW scenarios, given the availability of autonomic and advantageous networking and computing technology, it is necessary to make sure that every component that is available—devices, services, and human actors—is probably going to use their capacities to communicate with one another in a way that is both opportunistic and efficient. For the numerous and varied components of the CPW system to interact adaptively, it is necessary to discover and create new interaction mechanisms. Numerous strategies, usually according to auction procedures, have previously been put up to encourage helpful and/or advantageous exchanging of perceptions equipment [13]. However, it is anticipated that CPW's converging possibilities in future decades will necessitate the development of new pricing and incentive structures.

To sum up, a lot of significant research difficulties arise from the necessity of establishing fresh groundwork for the design and architecture of autonomous and self-adaptive CPW environments and systems. By no means is the above short list all-inclusive. The list specifically ignores the numerous interdisciplinary problems that come with comprehending large-scale socio-technical organisms and their combined adaptive behaviors, thereby utilizing the most recent insights from applied psychological sociology, culture in the fields of anthropology, macroeconomics, biological systems the environment, and complexity science.

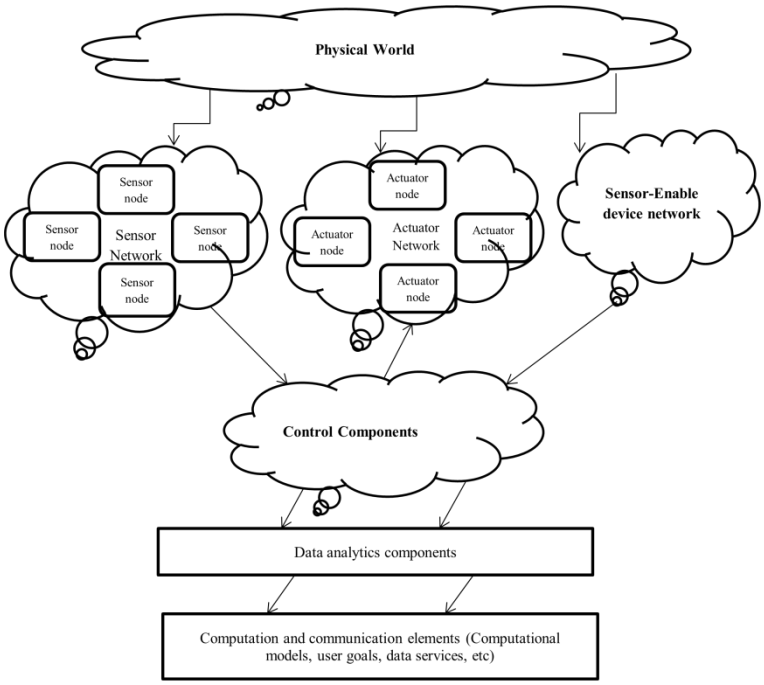

Fig. 3.1: A Comprehensive Perspective on CPS.

A general holistic perspective of CPS that considers all of the earlier elements is depicted in Figure 3.1. As we can see, depending on the technological domain under consideration, simpler perspectives are conceivable.

4. Implementation and experimental results

When installed correctly and with the necessary redundancy, the layer of cyber-physical devices can use sensors to give authority over position and actuators to modify any stage of the manufacturing process. For instance, [14], Figure 4.1 shows how the manufacturing process conditions for an engine component change when a complex event occurs, such as the engine component deforming as a result of the forces exerted by the clamping and cutting devices during the production procedure. Due to the results of the performance control procedure, the FEA process is typically carried out offline. A manufacturing system with a lot of sensors, however, might be capable of recognizing the complex event and indicating the possible issue in the online environment. In this instance, the FEA would be carried out in the cyberspace realm and would accurately depict the happening of the complex incident described here.

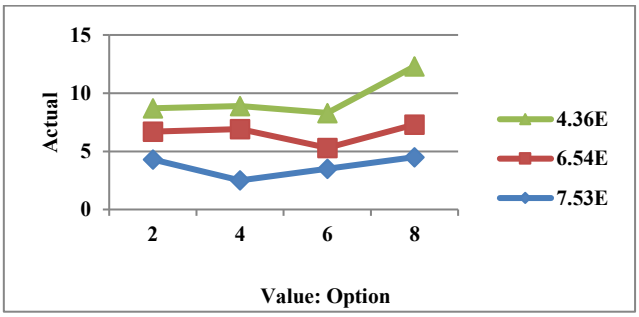

Fig. 4.1: Managing Manufacturing Processes and the Occurrence of Complex Events: Finite Element Analysis.

The offline modeling for the engine element and cutting tool profiles during rotational movement during manufacture is shown in Figure 4.2. The online emulation would be made possible by the M-CPS cyber world, allowing for the real-time transmission of the necessary adjustment decisions to the actuators situated in the physical world. Each of the data interchange functions of the suggested M-CPS model is scaled to a specific degree of cloud mode settings, which include public, community [15], and private clouds. This scaled architecture improves the security and transparency of the shared data while allowing only authorized resource access.

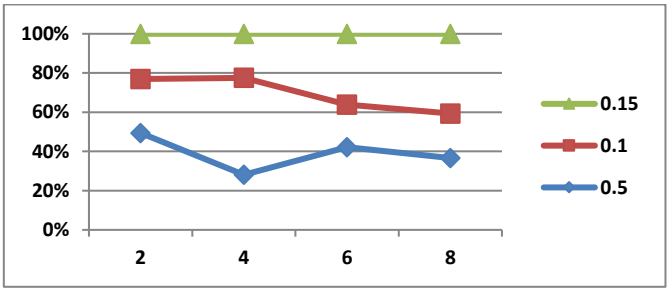

Fig. 4.2: Simulated Component and Tool Blade Path Profiles for Monitoring Manufacturing Processes and Complicated Event Occurrences.

It's unclear if improved usability is possible in the last scenario; a single person has a network made up of several wireless devices at their house or place of business. The concerned user must integrate a new gadget into the current secure wifi setting. Once more, this "enrollment" procedure needs to be secure and compatible with a wide range of devices without being onerous. The fact that not all of the existing devices may be "awake" or physically present when the new device is being enrolled complicates the issue. Additionally, since a single person controls the entire network, it seems sensible to presume that there is some kind of "master device" that is owned and run by that user.

5. Conclusions

We have examined new research issues that arise from the confluence of the physical and digital realms in this work. Large volumes of data will be moving from the real world to the virtual one (and vice versa) because of this convergence, providing researchers studying pervasive and mobile computing with a wealth of new research opportunities. Data gathered by sensors dispersed throughout the physical world is a vital resource for comprehending human behavior and the socio-physical environment in which people live. This data can be utilized to modify the virtual environment to suit human requirements and potentially influence the real world via actuators. The foundation for the creation of novel computing and communication paradigms (such as opportunistic computation and networking) based on (cellular) social networks is an understanding of human behavior and social connections. Since the data will be a crucial component of the CPW convergence, suitable methods are required to assess the data's quality, choose reliable sources, evaluate them, and store the data for convenient access and retrieval.

The creation of self-organizing strategies is necessary to adapt the vast number of devices in the cyber world to the quickly evolving physical and social world due to the complexity of the cyber world and the necessity to modify their behavior to the human/social context. Furthermore, a variety of security and privacy issues are raised by the widespread use of tiny, ever-increasingly affordable computing devices in everyday life.

Future research on the suggested predictive M-CPS will concentrate on creating simulation models that function in the cyber world and creating Big Data algorithms suitable for industrial processes. The issue of scheduling a group of tasks across a number of computers, as in HDFS distributed file systems, must be considered by computer processing on Big Data platforms. Computer performance at extremely high loads must be examined.

References

[1] Conti, M., Das, S. K., Bisdikian, C., Kumar, M., Ni, L. M., Passarella, A., ... & Zambonelli, F. (2012). Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence. Pervasive and mobile computing, 8(1), 2-21. https://doi.org/10.1016/j.pmcj.2011.10.001.

[2] Ahmed, S. H., Kim, G., & Kim, D. (2013). Cyber Physical System: Architecture, applications and research challenges. 2013 IFIP Wireless Days (WD), 1-5. https://doi.org/10.1109/WD.2013.6686528.

[3] Ma, M., Lin, W., Pan, D., Lin, Y., Wang, P., Zhou, Y., & Liang, X. (2018). Data and decision intelligence for human-in-the-loop cyber-physical systems: reference model, recent progresses and challenges. Journal of Signal Processing Systems, 90, 1167-1178. https://doi.org/10.1007/s11265-017-1304-0.

[4] Ning, H., Liu, H., Ma, J., Yang, L. T., & Huang, R. (2016). Cybermatics: Cyber–physical–social–thinking hyperspace based science and technology. Future generation computer systems, 56, 504-522. https://doi.org/10.1016/j.future.2015.07.012.

[5] Karnouskos, S. (2011, July). Cyber-physical systems in the smartgrid. In 2011 9th IEEE international conference on industrial informatics (pp. 20-23). IEEE. https://doi.org/10.1109/INDIN.2011.6034829.

[6] Horváth, I., & Vroom, R. W. (2015). Ubiquitous computer aided design: A broken promise or a Sleeping Beauty?. Computer-Aided Design, 59, 161-175. https://doi.org/10.1016/j.cad.2014.10.006.

[7] Noor, A. K. (2011). Intelligent adaptive cyber-physical ecosystem for aerospace engineering education, training, and accelerated workforce development. Journal of Aerospace Engineering, 24(4), 403-408. https://doi.org/10.1061/(ASCE)AS.1943-5525.0000128.

[8] Kant, V. (2016). Cyber-physical systems as sociotechnical systems: a view towards human–technology interaction. Cyber-Physical Systems, 2(1-4), 75-109. https://doi.org/10.1080/23335777.2017.1289983.

[9] Babiceanu, R. F., & Seker, R. (2016). Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Computers in industry, 81, 128-137. https://doi.org/10.1016/j.compind.2016.02.004.

[10] Cook, D. J., & Das, S. K. (2012). Pervasive computing at scale: Transforming the state of the art. Pervasive and Mobile Computing, 8(1), 22-35. https://doi.org/10.1016/j.pmcj.2011.10.004.

[11] Vuong, T. P., Loukas, G., & Gan, D. (2015, October). Performance evaluation of cyber-physical intrusion detection on a robotic vehicle. In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (pp. 2106-2113). IEEE. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.313.

[12] Moldovan, D., Copil, G., & Dustdar, S. (2018). Elastic systems: Towards cyber-physical ecosystems of people, processes, and things. Computer Standards & Interfaces, 57, 76-82. https://doi.org/10.1016/j.csi.2017.04.002.

[13] Cheng, Y., Zhang, Y., Ji, P., Xu, W., Zhou, Z., & Tao, F. (2018). Cyber-physical integration for moving digital factories forward towards smart manufacturing: a survey. The International Journal of Advanced Manufacturing Technology, 97, 1209-1221. https://doi.org/10.1007/s00170-018-2001-2.

[14] Parnianifard, A., Jearavongtakul, S., Sasithong, P., Sinpan, N., Poomrittigul, S., Bajpai, A., ... & Wuttisittikulkij, L. (2022). Digital-twins towards cyber-physical systems: a brief survey. Engineering Journal, 26(9), 47-61. https://doi.org/10.4186/ej.2022.26.9.47.

[15] Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 8(4), 3559-3591. https://doi.org/10.1007/s40747-022-00667-z.