DOI: https://doi.org/10.52131/pjhss.2023.1102.0454

Pakistan Journal of Humanities and Social Sciences

Volume 11, Number 02, 2023, Pages 1475–1484
Journal Homepage:
https://journals.internationalrasd.org/index.php/pjhss

PAKISTAN JOURNAL OF HUMANITIES AND SOCIAL SCIENCES (PJHSS)
INTERNATIONAL RESEARCH ASSOCIATION FOR SUSTAINABLE DEVELOPMENT

# Cyber-physical Systems and Artificial Intelligence: The Role of Cyber Security, Machine Learning, Threats and benefits to Modern Economies and Industries

Syed Gulfraz Naqvi[1], Sheriyar Sheraz[2], Ikhlas Mehmood[3], Muzzamil Yasin[4]

[1] School of Commerce and Accountancy, University Management Technology Lahore, Pakistan.
Email: gulfraz.naqvi@umt.edu.pk
[2] School of Commerce and Accountancy, University Management Technology Lahore, Pakistan.
[3] School of Commerce and Accountancy, University Management Technology Lahore, Pakistan.
[4] School of Commerce and Accountancy, University Management Technology Lahore, Pakistan.

## ARTICLE INFO

***Article History:***

| | |
|---|---|
| Received: | May 06, 2023 |
| Revised: | June 17, 2023 |
| Accepted: | June 18, 2023 |
| Available Online: | June 19, 2023 |

***Keywords:***
Artificial Intelligence
Robotic Automation
Machine Learning

***Funding:***
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## ABSTRACT

We have seen several applications based on embedded system principles evolve during the last 20 years. However, embedded systems are only useful for standalone, modest-sized applications. The use of artificial intelligence (AI) in cyber-physical systems is now and, in the future, faced with several difficulties. It also looks at how machine learning, the contemporary economy, and business interact with cybersecurity and artificial intelligence. The emphasis of the literature study is on developing a conceptual framework that will enable automation at both the technological and human levels, hence enhancing AI's resilience. Paradigm changes are a reality in contemporary culture. New technologies that provide high-performance computing capabilities that allow the development of intricate artificial intelligence systems are a contributing factor in these shifts. These advancements have made it possible for brand-new cybernetic systems to emerge, in which artificial intelligence models are employed to carry out specific jobs inside the system using continually produced data. On the one hand, cyber systems are being used more and more often in isolated applications. On the other hand, there is still discussion around the simultaneous integration of cyber systems with other cyber systems, the creation of straightforward cognitive structures, and the profound autonomy of interaction with physical systems. Widely open issue that has only been addressed philosophically in select texts.

Corresponding Author's Email: gulfraz.naqvi@umt.edu.pk

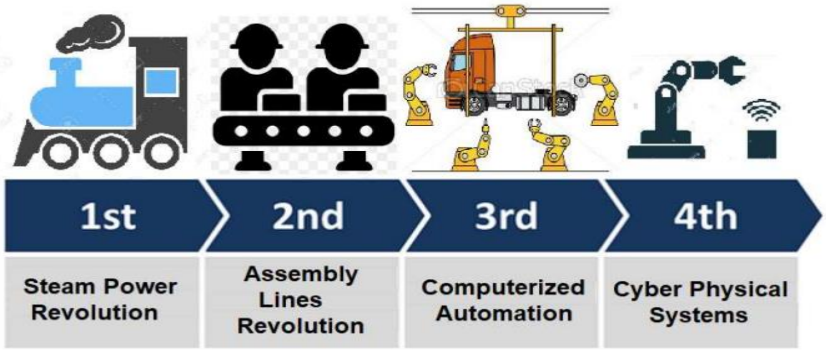
## 1. Introduction

Our economies and society are already being transformed by artificial intelligence (AI), and the emergence of AI decision-making has spurred a discussion about the possible risks and the need for more transparency in AI decision-making (from Fine Licht et al., 2020, forthcoming). Self-built technologies are still conceivable given our present technical advancements(Kammerer, 2020) upcoming. It is also feasible to create cognitive architectures that mimic the behavior of really intelligent people, including "motivation, emotion, personality, and other relevant aspects" (Sun, 2020). These results give rise to worries about the development of "Borg-eye and We-I" collective subjects, which result from the fusion of many subjects' wishes into one collective (for instance, through networked wearable gadgets; (Liberati, 2020). This clarifies research queries concerning how our economy and society are changing as a result of the emergence of AI decision-making and how we may increase the transparency of AI decision-making. Given that invasive self-construction procedures resembling really intelligent human manifestations set off the collective creation based on the desires of many individuals, these questions contribute to a deeper understanding of the topic at hand. The Industrial Internet of Things (IoT) is one example of this intrusive technology. Internet of Things (IoT) technologies have received a lot of interest recently from the government, business, and academic communities.

IoT may be defined as the use of IoT technologies to enhance manufacturing and industrial operations. IoT and Industry 4.0 (I4.0) are closely related terms that refer to a paradigm shift in industrial production, a collection of strategic initiatives to support national industry, emerging business assets, processes, and services, as well as a brand that denotes a particular historical and social era. A study of the considerable academic, governmental, and industrial literature is conducted once the research gaps have been discovered. Specific research questions are then produced from these research gaps. Current study on how the fusion of the intricate and linked Internet of Things (IoT) with Cybernetic Physical Systems (CPS) initiates the inevitable and self-sufficient development of artificial cognition is seriously lacking. In the topic of how technological advancements cause the inevitable and autonomous development of artificial cognition in complex, linked, and interconnected socio-technical systems, the significance of these research gaps is considered via a survey of the literature and a taxonomic analysis. The Tesla automobile is an illustration of how artificial intelligence (AI) is used in combination with Internet of Things (IoT) gadgets. The automobile employs artificial intelligence (AI) to assess the state of the road, the best speed, the state of the weather, and forecast the movements of other vehicles and pedestrians. In the framework of COVID-19, using smart buildings is another example. The Internet of Things (IoT) and artificial intelligence (AI) can be used as sensors to unlock doors and switch on lights, but they can also be used to forecast when it is most efficient to heat or cool a building. Future Cyber-Physical Systems (CPS) will perform a variety of tasks, including biological and health monitoring, robotic systems, intelligent edge devices, and many more. They will also be utilized to remedy natural catastrophes, human mistakes, and hostile activities.

These systems, which have become intriguing application domains for artificial intelligence, include the Internet of Things, IoT, and "smart systems" settings. Considering the increased CPS standards, there are various difficulties that AI techniques, models, and tools must overcome. For instance, non-functional needs such limited resources (memory, CPU), power consumption, device and user safety, delay-tolerant connectivity, and decision-making autonomy must get consideration from designers. Figure 1 illustrates how CPS has been referred to by many academics as the fourth industrial revolution.

**Figure 1: The Timeline of Industrial Revolutions**

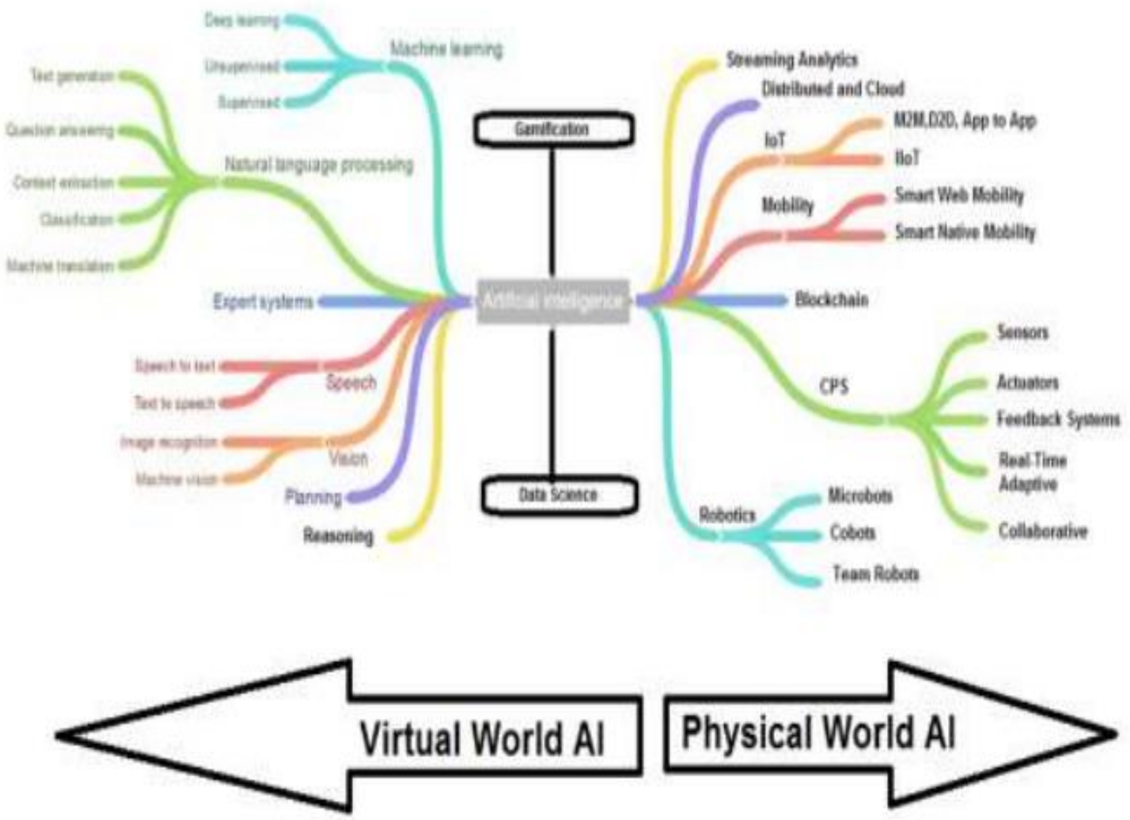


Cyber-physical systems are constructed from and depend on the seamless fusion of physical elements like robots and other equipment with computer algorithms. Such systems often include numerous (multi-agent) decision-making entities. CPS is regarded as a smart factory in the industrial industry (Fiaidhi, 2018). With the aid of AI, manufacturing companies are able to automate more of their operations than ever before. Deep learning may be used in factories for a variety of tasks, such as planning, scheduling, and preventive maintenance (Edwards, 2021). The use of AI has the potential to significantly increase the efficacy and efficiency of decision-making in settings with a great deal of complicated data, while also allowing these intelligent systems to incorporate a larger quantity of information. A new branch of AI with an emphasis on SCP is shown in Figure 2 (Fiaidhi, Mohammed, & Mohammed, 2018).

Robotic automation is already beginning to heavily rely on artificial intelligence. For instance, John Deere currently manufactures autonomous, highly autonomous, driverless agricultural tractors. Robotic automation applications that use machine learning and cloud services provide manufacturers new chances to boost productivity and dependability. Beyond the limitations of plants, artificial intelligence has taken us to a new plane. Although they have long dominated manufacturing floors, modern robots no longer conduct repetitive mechanical work.

They operate as intelligent bridge builders between the real-world smart manufacturing and the power of virtual reality.

**Figure 2: AI Role in Bridging the Virtual and Physical Words**

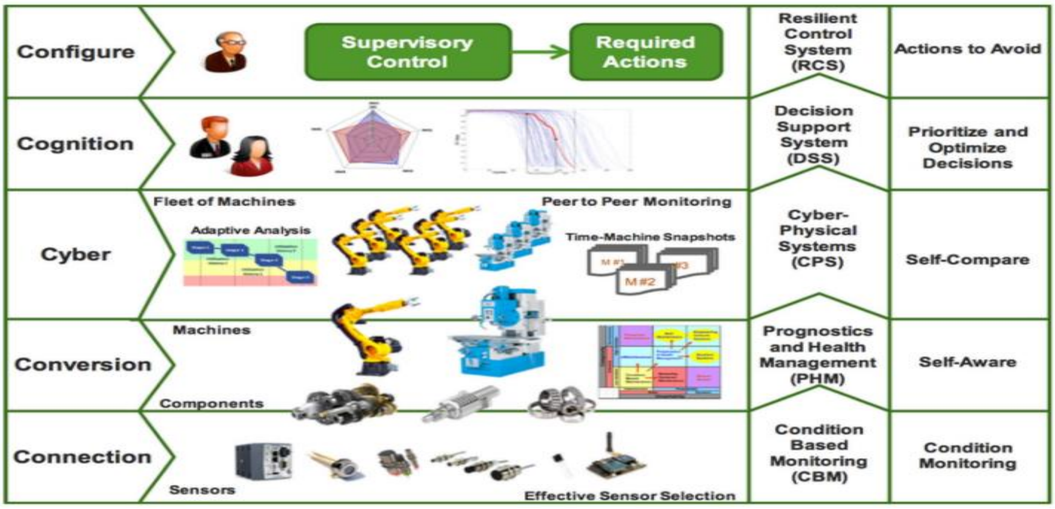


Data are converted into choices and actions more quickly and correctly thanks to machine learning. Machine learning approaches employ data for normative reasons (including decision assistance and decision automation), predictive purposes (predicting what will happen in the future), diagnostic purposes (studying why it occurred), and descriptive purposes (analysing what happened). A subset of artificial intelligence called "machine learning" enables computers to learn without explicit programming by using training data sets. When exposed to fresh data, machine learning assists in making predictions (which may alter). Massive volumes of data have been produced because of recent technological advancements. What big data is. Using machine learning, we must utilize this data to build an intelligent system. As a result, we may say that big data and machine learning are complementary. The volume of data created has increased tremendously with the development of Internet of Things (IoT) technologies. Effective utilization of this data is required. Future predictions may be made using machine learning.

## 2. Literature Review

The goal of the literature study is to highlight the key ideas in the more than 90 academic, governmental, and business studies, white papers, and other materials that were mostly released between 2010 and 2020. We mostly utilize Google Scholar and the Web of Science Core Collection to find data records. We discovered that Google Scholar was more adaptable for curating academic material by include additional search phrases. Use the Boolean value: and the search results are restricted, as an example, when adding several keywords to the Web of Science Core Collection. We are searching for papers on the following topics: artificial intelligence, industrial internet of things, internet of things, cybernetic physical systems, and industry 4.0. Only 25 data entries were found in this Web of Science Core Collection search. The data records increase from one Boolean AND to one Boolean OR, but they become less relevant to related subjects and concentrate on the one topic that the Boolean: OR was used to look for. We conducted the same Google Scholar search again for all the following topics: artificial intelligence, industrial internet of things, internet of things, cyber-physical systems, and industry 4.0. The identical Google Scholar search turned around 20,700 items of data. We thus employed both the Web of Science Core Collection and Google Scholar for our chosen data records to guarantee the relevancy of all the subjects we investigated, but as Google Scholar has a significantly bigger number of articles, we mostly used Google Scholar. scholarly search engine that examines the greatest database of documents. We see this as a strong justification for choosing the most relevant data records since both databases include articles from the same journals and Google Scholar is more effective at employing Boolean values for searches over a wide range of themes. Grounded theory was used to categorize the ideas that were thought to be the most important (Glaser & Strauss, 2017). The Methods chapter has a comprehensive description of this process. The developing idea categories fundamentally follow the "all you see is data" method (Glaser & Strauss, 2017) to categorize the most important concepts found in more than 90 distinct sources. There are several investigations. The words "economic potential," "cognitive design," "risk engineering," "correlation effects," "cognitive feedback," and "unrecognized and obsolete data" may all be found throughout the text. These six words are only a few of the many others that have developed from our analysis of the literature about the architecture of cybernetic physical systems. We group these ideas into categories and rebuild the 5C, or five-level cyber-physical system architecture, that is already in use (Figure 3).

**Figure 3: The 5 Levels Cyber Physical System Architecture—Commonly Referred to as 5C Architecture**



Machine learning methods provide tremendous potential to help cybersecurity, as we covered in the introductory section. Different computer security issues have been successfully solved using a variety of machine learning techniques. The detection and classification of brute force assaults may be done using machine learning tasks. Account masking may be found via anomaly detection. Cluster analysis may be used to enhance fraud investigations. Below, a few other uses are briefly covered.

Phishing detection (Abu-Nimeh, Nappa, Wang, & Nair, 2007): Phishing is a sort of cybercrime in which the victim contacts the target by phone or mail to gain passwords, bank account information, and personally identifying information. The use of this information to access significant accounts may result in identity theft and financial loss. Different machine learning methods, including logistic regression (LR), classification and regression trees (CART), Bayesian additive regression trees (BART), support vector machines (SVM), random forests (RF), and neural networks (NNets), were evaluated by researchers. Additionally, research has shown that when compared to other classifiers, LR has the best accuracy and a reasonably high recall. In order to identify phishing, Zhuang, Ye, Chen, and Li (2012) employed clustering techniques such hierarchical clustering and k-medoids and reached 85% performance. Identifying malicious network activity that compromises the confidentiality, integrity, or availability of systems on the network is the main objective of a network intrusion detection (NID) system. In order to defend against distributed denial-of-service (DDoS) assaults,Subbulakshmi, Mercy Shalinie, Suneel Reddy, and Ramamoorthi (2010) built an alert categorization system with the use of neural networks (NN) and support vector machines (SVM). In contrast to the support vector machine, which had a classification accuracy of 99 percent, the researchers reported that the neural network had an average classification accuracy of 83 percent. A hybrid method is put out by Shamila, Vinuthna, and Tyagi (2019) to identify intrusions in wireless sensor networks (WSNs).

Utilize clustering strategies to streamline the processing of information, using support vector machines (SVM) and misuse detection strategies to identify network abnormalities.

## 3. Modern Economics: c=Cyber-physical Systems and Artificial Intelligence

The advantages of merging operational technology with the Internet are all connected to greater productivity via simpler access to operational or production data, whether essential infrastructure or cyber-physical systems are being considered inside a factory. On the one hand, business owners may obtain operational technology data, highly aggregated and processed data that offers insights into operational and production processes and enables them to improve and adjust to changes in these processes. On the other hand, it is simpler and quicker to install software upgrades for OT systems (Almada-Lobo, 2015; Jeschke, Brecher, Meisen, Özdemir, & Eschert, 2017). Consider the dangers to vital infrastructure and industrial facilities, mostly caused by cyberterrorism and cyberwarfare. We must take into account the harm that the comparable assaults may do as well as how simple they are to execute. Power, water, and transportation networks (air, road, and river) comprise critical infrastructure. After World War II, it became obvious that a strike on such infrastructure might have a significant negative impact on a nation's economy and welfare. The 1984 Bhopal tragedy in India is a second illustration of the damage brought on by an industrial mishap (Yang, Khan, & Amyotte, 2015). Thousands of people died in an accident brought on by a poor or non-existent safety mechanism. Is it possible that a cyber assault on the Internet may be to blame for such an accident? This question's response is dependent on two elements. First, it would be helpful if we could locate instances of computer worms or viruses that are advanced enough to alter the settings of cyber-physical systems. Second, are current IT security solutions sufficiently protected from these kinds of attacks? The Stuxnet worm is the clearest illustration of a very sophisticated attack software in this context. The worm searches the computer it has penetrated for a certain programmable logic controller (PLC).

The worm won't start doing anything detrimental until these PLCs are found and the operating system and other system settings exhibit the desired values. Change a regulated industrial system's operational settings such that the action kills the system without sounding an alert. The possibility of targeted assaults on certain cyber-physical systems is well shown by this example. The Stuxnet virus still upgrades software on infected USB drives to further its objectives. These systems may now be accessed directly over the Internet. OT systems are often more secure than pure IT systems, for instance by using a so-called double-firewall demilitarized zone. Additionally, evaluations of the security features of such systems have been done for (Lu, Zhao, Zhao, Li, & Zhang, 2015; Pretorius, 2016). The overall security of OT and IT systems, however, continues to be unconvincing. The one-man Institute, a centre for data protection and cutting-edge technology, has published a study titled "2017 Cost of Data Breach Study." This study is a computer security research report that covers 419 firms in 13 countries and is sponsored by the US computer giant IBM. The US, UK, Germany, Australia, France, Brazil, Japan, Italy, India, Canada, and South Africa are among the nations covered. The Middle East and the ASEAN (Association of Southeast Asian Nations) region are the areas covered. Figure 22 on page 27 of this study shows that it takes an average of 214 days to discover a data breach brought on by a hostile or criminal assault, and an average of 77 days to keep the data leakage going after it has been discovered. This gives a smart computer virus or worm enough time to examine the system and launch the proper assault.

### 3.1. Cyber-Physical Business Systems based on Artificial Intelligence

The CPS security dangers at various levels are briefly summarized by CPBS-AI, together with the scientific obstacles standing in the way of the development of security solutions. The methodological limits of static capacity detection and monitoring systems are thoroughly examined by CPBS-AI. It is investigated why IPSS is inefficient in spotting, averting, and neutralizing low-level threats. In tracking applications, NN can predict assaults and eliminate threat concerns using a VSC-based nonlinear monitoring system. The special complexity and challenges of these networked systems make it more difficult to secure CPS networks. One example is the constrained computational power of CPS devices. Security systems must function successfully and within tight parameters without using up all the resources. Therefore, it is crucial to thoroughly investigate the CPS architecture, the application, and the related security concerns while creating a unique security solution. The source of security risk for CPS is physical domain behaviour rather than legacy technology, necessitating physical security and stability for a variety of applications. To implement effective preventative actions, security threats must be classified.

A cyber-physical system is a bigger distributed system made up of networked actuators, detectors, control processing components, and communication devices. This is shown in the image below.

**Figure 4: CPBS-AI Framework Process**

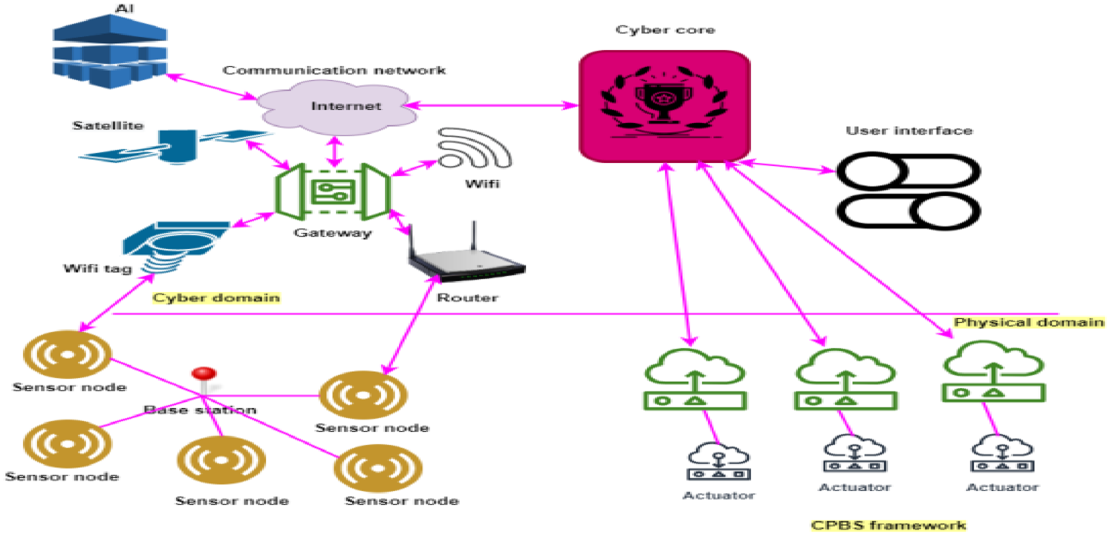


Figure 4 depicts the distinctive organizational structure of CPS. Typically, Wi-Fi tags, satellites, Wi-Fi devices, and routers interact with gateways and management systems in the CPS to form a network configuration that links these parts together. The Internet's communication network is maintained by various sensor nodes. A gateway and Wi-Fi are used to send data from satellites to the user interface. To each sensor node, a router sends data. The physical domain and the user interface exchange information. Both cable and wireless communication are used to transmit sensor data to the network domain for synchronization and activation. The Internet backbone network's system transformation and self-organization may be successfully facilitated by delivering the network core's computational output to the physical domain. CPS is renowned for its predictable behaviour and real-time management skills in AI systems due to its capacity to function in real time. The capacity of CPS to link systems that would otherwise be separated from the network core explains why it has becoming more widely used in the sector. The prevalence of CPS highlights the need of effective security measures. Rapidly identifying high-priority CPS security vulnerabilities in base stations necessitates a quantitative model, which is needed for vulnerability scanning as part of reconnaissance requirements. CPS safety. The privacy issue in CPS is depicted in this model as a vulnerability dependency graph with a directed graph topology. The sites of CPS that are most susceptible to an attack are determined using the graph used to evaluate system risk. Acyclic graphs have the drawback of becoming so large that they are impracticable, when possible, dangers to the system are found. Larger industrial designs cannot utilize this model because of this restriction.

### 3.2. The Role of Intelligent Robots?

As they work alongside people in production, robots are emerging as a new form of worker. Industrial robots are typically articulated arms with six axes of motion (or six degrees of freedom) that are used in production. The classic layout offers the most flexibility. Cartesian, SCARA, cylindrical, triangular, polar, and vertical joints are the six primary categories of industrial robots. There are, however, a few other robot setup variants. These categories each provide various collaborative arrangements. Axes are the name given to the arm's joints. Industrial robots are often used for intense, quick, and precise tasks including welding, painting, assembling, PCB pick and place, packing and labelling, palletizing, product inspection, and testing. Robotics in manufacturing increased at an average annual rate of 12% between 2011 and 2016, mostly in the automotive and electronics/electrical manufacturing sectors. By 2020, more than 3 million industrial robots will be in use in industries throughout the globe, predicts the International Federation of Robotics (IFR, 2018). In 2017, the number of industrial robots sold worldwide reached a new high of 387,000 units. This was a 31% rise over the previous year (2016: 294,300 units). China saw the largest growth in industrial robot demand, up 58%. Sales increased 6 percent in the United States and 8 percent in Germany over the prior year. These are early results from Steven Crowe's 2018 World Robotics Report. Low-volume, high-mix manufacturing is expanding, nevertheless, because of consumer demand for a wider range of goods. Industrial robots may be configured to operate in a variety of settings, but they cannot swiftly adapt to and reuse your manufacturing facilities at the appropriate pace. The need for smart factories with digitally linked machinery is rising because of the new CPS revolution idea (Fiaidhi, 2018).

A smart factory's supply chain results in faster reuse, shorter product development cycles, fewer product flaws, and reduced downtime for equipment. The term "smart factory ecosystem" refers to the seamless interaction between highly automated systems at all levels and systems that are completely interconnected and adaptable to learn from and respond to changing conditions. The idea of a "smart manufacturing unit (SMU)" is a key component of such an ecosystem since it suggests the possibility to increase value both within the factory's walls and across the supply network. Each SMU is a flexible system that conducts the full production process independently, automatically optimizes performance throughout the larger network, and adapts to and learns from new situations in real-time or almost real-time. SMUs are capable of functioning within the confines of a plant, but they may also be linked to a worldwide network of comparable production systems or perhaps a larger digital supply network. When, when, and how it is required, SMU makes all manufacturing process information accessible to small, medium, and big businesses as well as to the manufacturing supply chain, spanning the product life cycle and numerous industries. To facilitate SMU integration and flexibility, recent developments in assistive technology, such cobots and exoskeletons, broaden the spectrum of jobs that robots can carry out.

Industrial robot technology is still in its infancy and is pricey. They often take the role of people in risky and monotonous work using massive caged machines. These robots have a variety of issues, including as vision issues (since they lack the capacity to detect and navigate things, including humans), and dexterity issues (due of their still-limited mechanical, moving, and gripping skills). As a result of advancements in digital technology and the creation of self-driving vehicles, the price of off-the-shelf hardware is falling, resulting in the appearance of smaller, more manoeuvrable robots on the factory floor. In response to several global efforts, such as the Kickstarter campaign (www.kickstarter.com), which supports low-cost entry-level industrial arms like Fablabs for non-traditional markets, low-cost robot ideas are flooding in from all over the globe. These more affordable, lighter robots may be fitted with sensors that enable them to collaborate with people in industrial environments, resulting in "cobots" or "FabLab robots" that can carry out activities like gripping tiny things, watching, and even learning Robots handle "edge cases". An example of a Kickstarter project is Niryo One (https://niryo.com/), which is a 6-axis robotic arm designed for manufacturers, educational institutions, and small companies. It is a low-cost industrial robot. The robot is 3D printed and runs Robot OS, Arduino, and Raspberry Pi.

### 3.3. Necessity of Machine Learning and Cyber Security

To more effectively identify risks, we may employ security analytics. Alarms and signals may also be prioritized using it. This aids in speeding up the process of issue solving. Machine learning methods may be used to strengthen cybersecurity. The examples that follow are only a few.

- Cybersecurity companies analyse and analyze huge data volumes, some of which may be historical or threat intelligence data spanning many years, using data science techniques.
- Using machine learning methods, F-Secure has been able to handle classification, clustering, dimensionality reduction, and regression issues.
- Implementing authentication systems, assessing protocol implementations, assessing security for testing human-computer interactions, analyzing data from smart meters, and other tasks may all be accomplished with the help of machine learning.

A significant use of machine learning methods is in cybersecurity. Mathematical models cannot be used to handle all cybersecurity concerns, including virus detection, intrusion detection, and data breaches. system (Shamila et al., 2019), the software should be put on the broadest network of healthcare organizations. According to ABI Research (Mackenzie Gavel) by 2021, machine learning in cybersecurity will drive spending on big data, intelligence, and analytics to $96 billion." Because the employer accesses the data at this endpoint, these systems are referred to as endpoints. We must implement machine learning models in our customers' healthcare industry networks and provide them access to real-time network activity analysis to identify cybersecurity risks. To estimate the likelihood of suspicious behaviour, machine learning builds an understanding of typical network activity and utilizes it as a reference. A user's conduct is marked as fraudulent if it seems to drastically stray from system standards. One vendor of anomaly detection machine learning for a healthcare organization is Darktrace. Cybersecurity systems may quickly identify trends and gather knowledge to identify defences against related assaults by using machine learning. In plain English, we may explain that machine learning enables cybersecurity teams to successfully thwart assaults and quickly address ongoing attacks. For machine learning to be successful in cybersecurity, data is essential. The core of machine learning is creating new patterns and utilizing various algorithms to analyse them. To do this, we want a large dataset that represents a wide range of probable outcomes from various situations. Be aware that data quality is just as important in this situation as data quantity. Data must be accurate and timely. IoT networks and other applications increasingly create enormous volumes of data every day. These types of huge data cannot be managed by traditional data management systems, but they can be effectively handled by big data frameworks. As a result, we can draw the conclusion that machine learning techniques are necessary for the implementation of an effective cybersecurity system and that complete/relevant data is essential for successful machine learning approaches. As a result, we mention or discuss the significance of machine learning approaches in cybersecurity in this section. We also discuss how data are used to create machine learning algorithms. To imagine the future of cybernetic physical systems, we mix several existent technologies in the following section.

### 3.4. Cyber-Physical Systems Enabled by Artificial Intelligence

The purpose of this study is to illustrate and analyse how artificial intelligence may be used in higher-level cyber-physical systems to enable system cognition. AI may play a significant role in control systems for lower-level systems, such as those that do fault detection or real-time behaviour prediction (Nogueira et al., 2018). Predictive models for process optimization have been used in architecture and by (Subraveti, Li, Prasad, & Rajendran, 2019; Ye et al., 2019); both in 2019. This issue has been studied in the literature, as was already indicated. System complexity, however, rises as they develop. Automated systems of today often consist of several parts that must cooperate and sync. To enable CPS at scale, the operational management and decision-making level tools must be upgraded. Therefore, a critical technology for achieving large-scale CPS, bridging CPS, and offering in-the-moment autonomous guiding is artificial intelligence. Cognition, which can describe, represent, and learn complicated behaviour and interactions between system components and system data, is a key skill that AI can provide systems. This may be done by training AI models in supervised or unsupervised fashion to carry out these tasks. The AI model may also continually learn from the system, giving the CPS versatility. As a result, there is an increasing need for research on the creation and incorporation of massive AI networks. It's critical to remember that these remarks discuss the use of AI at a higher level of CPS to carry out human duties. A chemical unit may therefore develop the capacity to vertically integrate its own management at all levels, interact with the CPS structure, and carry out management activities independently via the use of artificial intelligence.

As stated in (Gamer, Hoernicke, Kloepper, Bauer, & Isaksson, 2019), recent advancements have made the concept of systems that can run independently with less human intervention more and more appealing. Emerging car industry with autonomous transportation systems. The concept's prerequisites include modularity, discretion, functional equality, data sharing, situational awareness, and self-management. It is built on high autonomous controllability and autonomy-friendliness. This concept hasn't been completely explored in the literature or by subsequent writers after (Koshijima, Niida, & Umeda, 1996) have been making references to it ever since, most likely owing to a lack of technology. A positive step towards implementing large-scale, AI-driven CPS principles is the Internet of Things (IoT). Industrial IoT networks now provide a vast network of linked computers where data is continuously shared and made accessible in real time. IoT can thus offer the essential social context for AI models to interact with one another, share knowledge, and coordinate the management of systems. An extensive assessment of the use of artificial intelligence in cyber-physical systems was carried out by Radanliev et al. in 2020. Additionally, the identification of dynamical systems by artificial intelligence is still an unresolved issue. One of the most significant ways to depict dynamic chemical engineering systems, which are often extremely nonlinear, have lengthy stabilizing periods, and need regular interventions considering their future states, is dynamic artificial intelligence (AI). A recurrent neural network (RNN) is the approach that is best appropriate in this scenario. Deep neural network (DNN) technology stands out among RNN approaches for its effective use in resolving issues in a variety of fields. To take use of the potential of DNNs to solve a variety of issues in the industry, however, there is a dearth of recent research around process engineering (Oliveira et al., 2020). Chemical engineering procedures have not seen a lot of deep learning applications. The capacity of AI/Deep Neural Networks (DNN) to address issues pertaining to system dynamics is still being developed, even though the area is currently developing (Oliveira et al., 2020). The self-management, teamwork, and virtualization capacities necessary for the large-scale development of cognitive CPS are also made possible by distributed artificial intelligence technologies.

## 4. Conclusion

There is an issue with the integration of physical space with Industry 4.0 enabling technology in the fast-evolving paradigm of modern industry. Humanity's demand for sophisticated CPS with cognitive capabilities, which provide these systems autonomy without human intervention, is growing because of the dynamics of contemporary society. The goal of combining operational technology (OT) with information technology (IT) in industrial and infrastructural systems is undoubtedly to boost productivity and efficiency by facilitating simpler data interchange between OT and IT systems. This facilitates highly automated processes in international supply and value chains, which is related to smart factories. The motivation behind autonomous and semi-autonomous drones is to enable tasks like remote inspections and surveys and rescue missions in dangerous places. Humans could not previously enter these marketplaces without being severely exposed to these risks. We need sophisticated maintenance solutions for production and many control applications due to our quick growth. As noted, AI may assist in reducing the human effort required to identify risks or vulnerabilities in cyber/cyber-physical systems. Due to the prevalence of cybercrime today, cybersecurity is essential for all organizations, particularly those that link to or operate online. The smart industry of the future must optimize not just its own production process but also the usage, upkeep, and recycling of created goods and resources. On the other hand, for two real-world industrial situations that may encompass many phases of a product life cycle, such as the manufacturing phase, usage phase, and maintenance, the integration of Cyber-Physical Systems (CPS) and Intelligent Products (IP) is crucial.

## References

Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). *A comparison of machine learning techniques for phishing detection.* Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit.

Almada-Lobo, F. (2015). The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES). *Journal of innovation management, 3*(4), 16-21. doi:https://doi.org/10.24840/2183-0606_003.004_0003

Edwards, J. (2021). Building a Smart Factory with AI and Robotics: Whitepaper. *Robotic Bussiness Review.–2021*.

Fiaidhi, J. (2018). Extreme automation: a new game-changing technology. *IT Professional, 20*(2), 88-90.

Fiaidhi, J., Mohammed, S., & Mohammed, S. (2018). The robotization of extreme automation: The balance between fear and courage. *IT Professional, 20*(6), 87-93.

Gamer, T., Hoernicke, M., Kloepper, B., Bauer, R., & Isaksson, A. J. (2019). The autonomous industrial plant-future of process engineering, operations and maintenance. *IFAC-PapersOnLine, 52*(1), 454-460. doi:https://doi.org/10.1016/j.ifacol.2019.06.104

Glaser, B. G., & Strauss, A. L. (2017). *Discovery of grounded theory: Strategies for qualitative research*: Routledge.

IFR. (2018). *IFR 2018 Positioning Paper, Robots and the Workplace of the Future, International Federation of Robotics*. Retrieved from https://ifr.org/downloads/papers/IFR_Robots_and_the_Workplace_of_the_Future_Positioning_Paper.pdf

Jeschke, S., Brecher, C., Meisen, T., Özdemir, D., & Eschert, T. (2017). *Industrial internet of things and cyber manufacturing systems*: Springer.

Kammerer, F. (2020). Self-building technologies. *AI & SOCIETY, 35*(4), 901-915. doi:https://doi.org/10.1007/s00146-020-00962-8

Koshijima, I., Niida, K., & Umeda, T. (1996). A micro module approach to the design and control of autonomous decentralized chemical plant. *Journal of Process Control, 6*(2-3), 169-176. doi:https://doi.org/10.1016/0959-1524(95)00047-X

Liberati, N. (2020). The Borg–eye and the We–I. The production of a collective living body through wearable computers. *AI & SOCIETY, 35*, 39-49. doi:https://doi.org/10.1007/s00146-018-0840-x

Lu, T., Zhao, J., Zhao, L., Li, Y., & Zhang, X. (2015). Towards a framework for assuring cyber physical system security. *International Journal of Security and Its Applications, 9*(3), 25-40.

Mackenzie Gavel, M. *ABI research blog*. Retrieved from https://www.prnewswire.com/

Nogueira, I. B., Ribeiro, A. M., Requião, R., Pontes, K. V., Koivisto, H., Rodrigues, A. E., & Loureiro, J. M. (2018). A quasi-virtual online analyser based on an artificial neural networks and offline measurements to predict purities of raffinate/extract in simulated moving bed processes. *Applied Soft Computing, 67*, 29-47. doi:https://doi.org/10.1016/j.asoc.2018.03.001

Oliveira, L. M. C., Koivisto, H., Iwakiri, I. G., Loureiro, J. M., Ribeiro, A. M., & Nogueira, I. B. (2020). Modelling of a pressure swing adsorption unit by deep learning and artificial Intelligence tools. *Chemical Engineering Science, 224*, 115801. doi:https://doi.org/10.1016/j.ces.2020.115801

Pretorius, B. H. (2016). *Cyber-security and governance for industrial control systems (ICS) in South Africa.* Retrieved from http://hdl.handle.net/10413/15261

Shamila, M., Vinuthna, K., & Tyagi, A. K. (2019). *A review on several critical issues and challenges in IoT based e-healthcare system.* Paper presented at the 2019 International Conference on Intelligent Computing and Control Systems (ICCS).

Subbulakshmi, T., Mercy Shalinie, S., Suneel Reddy, C., & Ramamoorthi, A. (2010). *Detection and classification of DDoS attacks using fuzzy inference system.* Paper presented at the Recent Trends in Network Security and Applications: Third International Conference, CNSA 2010, Chennai, India, July 23-25, 2010. Proceedings 3.

Subraveti, S. G., Li, Z., Prasad, V., & Rajendran, A. (2019). Machine learning-based multiobjective optimization of pressure swing adsorption. *Industrial & Engineering Chemistry Research, 58*(44), 20412-20422. doi:https://doi.org/10.1021/acs.iecr.9b04173

Sun, R. (2020). Potential of full human–machine symbiosis through truly intelligent cognitive systems. *AI & SOCIETY, 35*, 17-28. doi:https://doi.org/10.1007/s00146-017-0775-7

Yang, M., Khan, F., & Amyotte, P. (2015). Operational risk assessment: A case of the Bhopal disaster. *Process Safety and Environmental Protection, 97*, 70-79. doi:https://doi.org/10.1016/j.psep.2015.06.001

Ye, F., Ma, S., Tong, L., Xiao, J., Bénard, P., & Chahine, R. (2019). Artificial neural network based optimization for hydrogen purification performance of pressure swing adsorption. *International Journal of Hydrogen Energy, 44*(11), 5334-5344. doi:https://doi.org/10.1016/j.ijhydene.2018.08.104

Zhuang, W., Ye, Y., Chen, Y., & Li, T. (2012). Ensemble clustering for internet security applications. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42*(6), 1784-1796.