Scandic journal of Advanced Research and Reviews

Access Control for Cyber-Physical Systems

Shahzad Ahmed [1]and Muhammad Waqar Naeem[2]

1, PhD scholar, Department of Management sciences, Islamabad, Pakistan.

2, MS Scholar, Department of Law and Economics, Islamia University of Bahawalpur, Punjab, Pakistan.

Email: waqarnaeem845@gmail.com

Introduction to Cyber Physical System:

The cyber physical system is defined as a mechanical mechanism which is organized by computational units that work in collaborative manner, specifically, actuators and sensors which capture data from a specific process and control its parameters following the set of defined guidelines, hence accomplishing an interaction between the computational and physical apparatuses (Misra *et al.*, 2013). These mechanisms have been integrated deeply in critical infrastructures such as transport, energy and commonly in all industrialized control systems for many decades. The primary objective of achieving resilient, self-adaptable, and intelligent machines in this framework has been relieved in recent centuries by the increasing reasonability of sensors and the swift development of innovative communication protocols and networks. It has resulted in the constant generation of higher data volumes and integrated with information technology (Chen *et al.*, 2012).

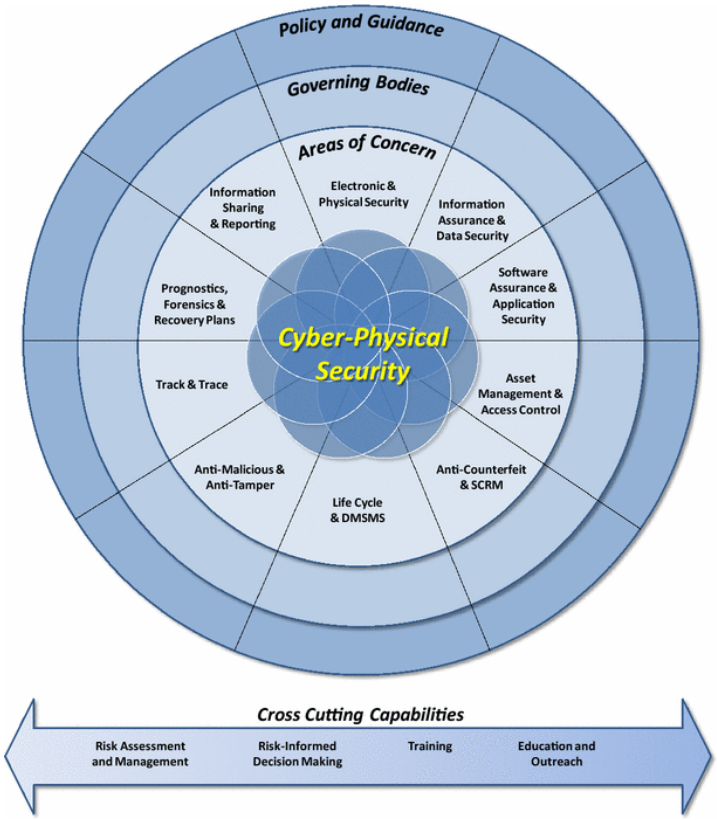

Figure 1. Cross Setting Capabilities of Cyber Physical Security (Yuan, Sun and Liu, 2016)

The equivalent of the industrial technology modernization that is referred as "operational technologies" and the interrelationship of cyber physical systems with external networks such as internet bring out the advent of new cyber-security threat and risks. Few of these are inherited from the data retrieval paradigm and others come from the developing integration between information and operational technology assets (Yuan, Sun and Liu, 2016). Consequently, there has been an upsurge of vulnerabilities in the developed sector in last few years, as few reports exhibited. Multiple studies discussed the attack paths for example presence of malware, social and phishing engineering, denial of service and vulnerabilities exploitation in communication protocols to interrupt traffics (Fawzi, Tabuada and Diggavi, 2014). With respect to access and authorization control, which are the major concentration of this sector, large number of misuses implied by resources and the misappropriation of the node identities which can even effect the complete systematic working behavior (Mahmoud, Hamdan and Baroudi, 2019).

As stated by the reports, the worldwide market of cyber-physical system is expected to see a CAGR of 8.7 percent during the age of 2018 and 2028. In 2017, the market was worth US$ 55,075.3 Million and is probable to reach an estimation of US$ 137,566.0 Million by the end of

2028. Australia's growing cyber security industry has an exceptional opportunity to bring solutions and services as a source of economic development itself, in a worldwide-competitive, export-fronting industry (Ding *et al.*, 2018).

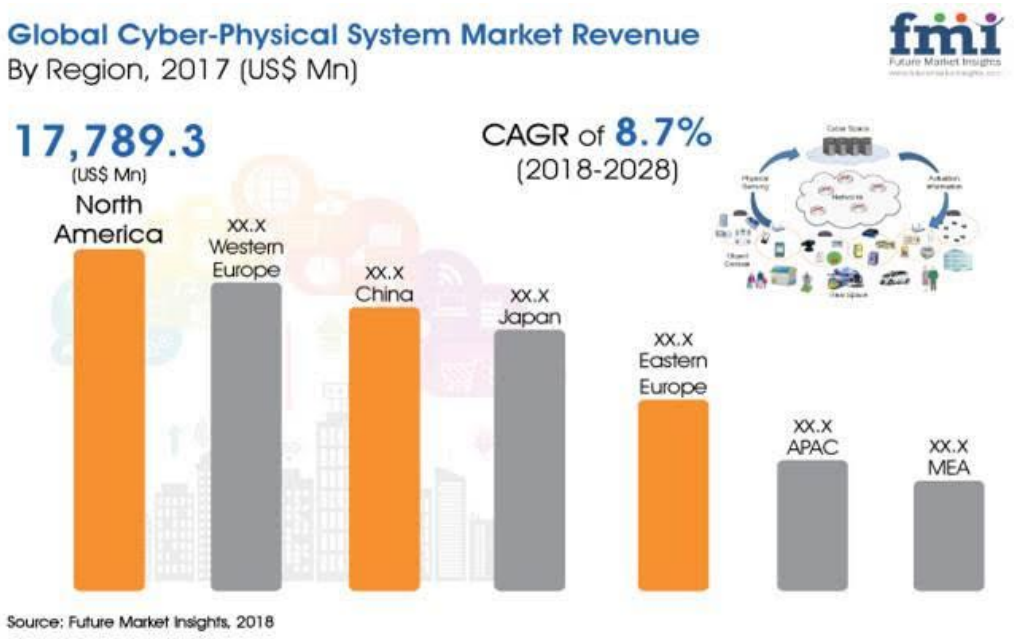

Figure 2. Global Market Statistics of Cyber Physical Security (source FMI)

Overall, these matters make security the foremost concern for the adoptions of such innovative technologies in different critical setups (Monostori *et al.*, 2016). In this complicated situation, when any factor could interact potentially and collaborate with any other factor, access control is crucial to control the permissions of users, programs and peripheral devices when they appeal to use definite resources within the infrastructures (Jazdi, 2014). The information technology integration and particularly the cloud computing applications of conservative access manage models in developed systems, for more than a few reasons. These can be precised in the distribution of information among diverse bodies with different extents of performance, regulations, and sensitivity (Wang *et al.*, 2016).

So, it becomes obligatory to analyze the complete requirement ranges which access control offers in the future scenario, with the intention of accurately adapt the existing models and suggest new strategies which meet such situations. Above all, it is beneficial to consider how new security

approaches can affect the physical domain by presenting an extra direction in the monitoring and control processes (Monostori *et al.*, 2016).

Requirements of Access control

In order to recognize the access control system requirements in the cyber physical system infrastructures, it is compulsory to review firstly how industrialized networks are affected by the information technology integration. A conventional control network follows the described architecture in the ISA-95 standards (Shafi, 2012). In this manner, the productive procedure constitutes itself of the pyramid base (level 0), while devices which cooperate with it (namely, RTUs, PLCs,) are remained in level 1. In the level 2, the devices included which control the production procedure (namely, HMIs, SCADAs systems), and those which control the workflows (namely, MES) are placed in level 3 (Ashibani and Mahmoud, 2017). To end, the uppermost level comprises the infrastructures of inventory, logistics, planning and enterprise resource planning. The implementations of cyber-physical systems within this framework mean to introduce advanced computational capabilities and connectivity technologies to certify a real-time data acquirement from the physical domain and intellectual data managements (Ding *et al.*, 2018).

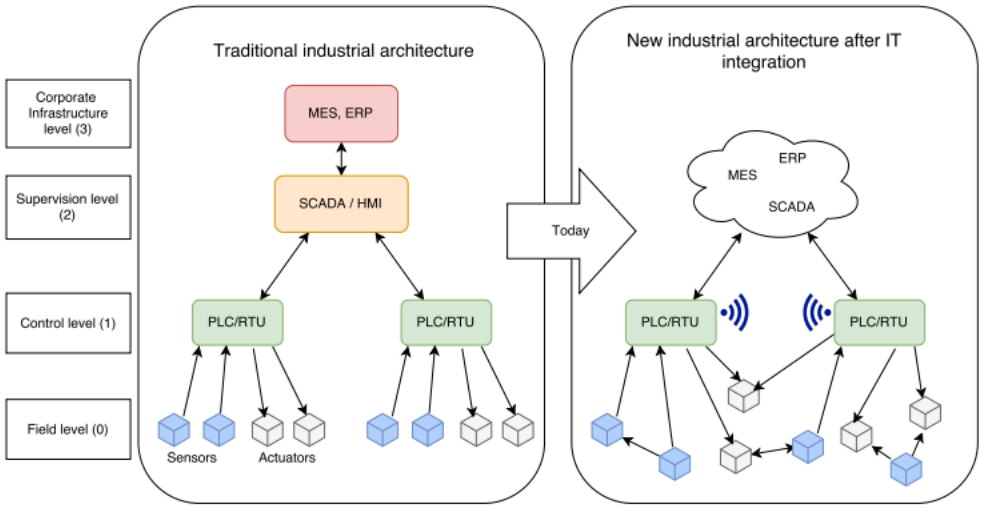

Figure 3. Cyber Physical Security Architecture (Ding *et al.*, 2018)

The objective is to collect data from each linked machine and run particular analysis to extract further insights, delivering feedbacks from cyber fields back to the physical fields. In fact, this development is bring up by the implementations of various communication protocols because of the hardware and software standardization (Humayed *et al.*, 2017): within the range of field bus

protocols (specifically, wireless IO-Link, HART, ether-CAP) to working protocols with TCP/IP and Ethernet, for example HART/IP, IP/Ethernet, CAN-open, PROFINET, Ethernet POWERLINK, and TCP/Modbus (Giraldo *et al.*, 2017). The instance of standards developed for the interoperable managing of all kinds of industrial tools, such as CIP, MT and OPC-UA Connect are particularly fascinating. In general, this developed the evolution of the old-fashioned architecture in the direction of a decentralized and distributed model (Johansson *et al.*, 2014).

As stated by the new architecture models, devices found in the low architecture levels interoperate with each other to communicate all the constituents of the infrastructures, within the range of machines and operators or the products themselves, so as to collect data. In contrast, the cloud computing is supportive to deliver supervision as a facility and communicate easily with diverse substations. In this manner, a collaborative setting can be formed by different companies, whose constraints and applications may vary, making it challenging to reach a worldwide settlement or the adoption of any mutual agreement (Zhang, Qing and Bin, 2013).

In such complicated state, access control systems installed either in the field devices, cloud resources and PLCs with the objective to control what every entity should be capable to access and the networks which can be accepted, have the capability to deal with a variety of tools. Real solutions are still in their beginning, because of the necessity for the fine-grained and dynamic mechanisms which deals with numerous users and controlled resources. Thus, it is easy to define the following collection of particular requirements, on the basis of an extensive evaluation of the literatures in order to study the features of models essential for such a specific context:

Scalability

Access control should take into consideration the definition of novel users and composite strategies, while not presenting operational expenses. It must be extensible in terms of the amount of resources and users controlled, together with the adaptation to innovative technologies such as operating systems, communication protocols, over well-defined interfaces. It is significant that the access control system contains a situational cognizance of all involved elements at all times in the authorization judgments. It encompasses parameters for example the sum of total connected devices along with accessible resources (Monostori, 2014).

Dynamicity

In modern cyber physical system, the services are remotely accessed by a large number of protocols and technologies that are also removed or added on demands. Owing to modern information technology, various applications might be integrated in the life cycles of products, within the range of monitoring processes (such as real-time performances and inventory) to dynamic processes of manufacturing that may possibly change dynamically their certain parameters. Virtualization components of modern computing also offer scalability with respect to resource allocations that in returns introduces a challenge for access control systems with the mechanism of multiple accounts of users (Liu *et al.*, 2017).

Flexibility

Proposed devices should also offer an informal administration to describe which attributes must be used for credentials, which authorizations could be shifted or with the description of trust relations between different bodies such as server users. The access control system can be updated permanently with facts about the multiple workflows inside the organizations, by making use of specifications language which supportive to complicated logic rules (Bonci, Pirani and Longhi, 2018).

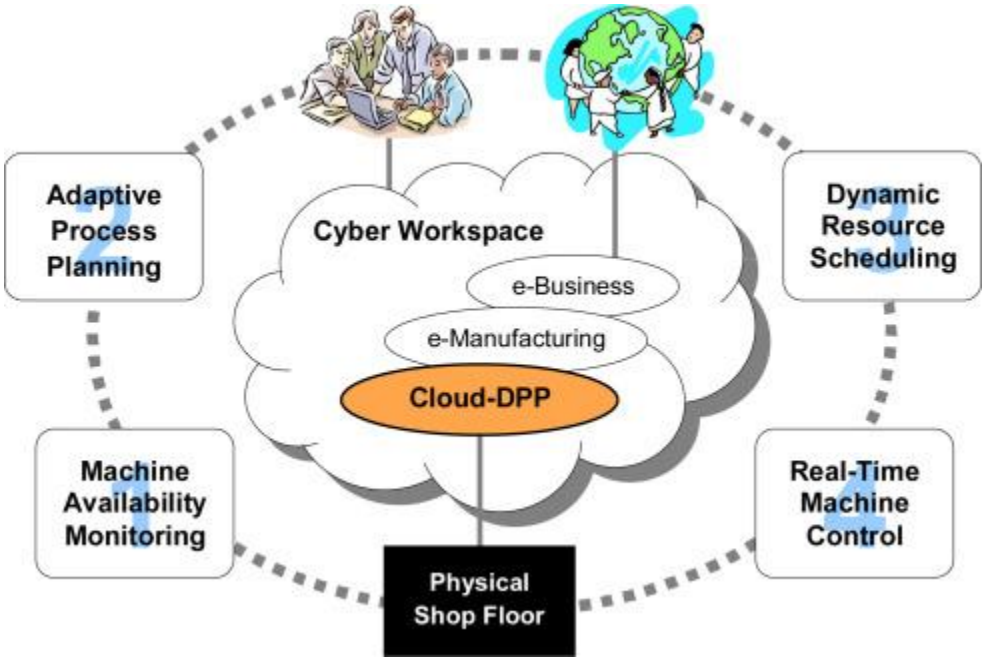

Figure 5. Cyber Workplace (Jazdi, 2014)

Services Quality

Disquiets the computational complication of access control processes, that may enhance the response time for authorization resolutions, particularly in resource controlled strategies (specifically, both for autonomy and computation) (Bordel *et al.*, 2017). In this regard, wireless communication systems must be taken into consideration, since they can bounds bandwidth and cause delays in transmissions. Thus, the access control service should control the connection requirements between networks with diverse demands of service excellence, by trying if there are inexpensive resources to accept such networks. Consequently, that admittance control makes balance within the entire system load. However, it might be hard to achieve in reality, as it is time to deal with a decentralized architectures (Alguliyev, Imamverdiyev and Sukhostat, 2018).

Access Control to Cyber-Physical Systems and Security Incident Handling

As the whole, the security in access control service is categorized into two parts: control security and information (data) security. Information security includes make safe information in the course of data processing, aggregation, and wide-scale distribution in the network environments, particularly open loosely joined networks (Lu *et al.*, 2015). Control security includes solving any control concerns in the network environments and securing the control system from any attack on control algorithms and system estimations. Information security concentrates on data protections, such as by using encryptions, while control security concentrates on caring the control systems dynamics against cyber-attacks (Chen and Chang, 2012).

Unique Features

In information technology systems, access restrictions and controls can be implemented without distressing the system facilities. In contrast, any information technology protection methods applied for cyber physical systems could delay or affect the real-time responses of the physical zones that generally demand real-time responds. Such as, the major risk factors for information security are expanded connectivity, unified protocols, consolidated technologies, and public information accesses, which typically cause insecure networks (Lopez and Rubio, 2018). Therefore, applying these strategies for may affect unfortunately real-time responds and offer potential challengers with several new prospects to disturb the services. However, because of the

exceptional characteristics, traditional approaches and strategies of security are not adequate to address security challenges because of the dissimilarities in connectivity and specifications from cyber physical systems (Misra *et al.*, 2013).

Along with the security objects of traditional cyber systems, legitimacy is found to be the foremost security aim. Legitimacy points out that all communications and transactions must be certain that are between authentic parties in all associated procedures for example sensing, actuation, or communication, hereafter confirming that the source of all actions which impacts highly upon the system was issued and originated from a trusted side. In other forms, cyber systems authenticity seeks to authorize both authenticate and communicated parties and confirm any connected development. The confidentiality is graded the first security motif for cyber systems after availability, authenticity, integrity, and confidentiality (Buini, Peter and Givargis, 2017).

Secured access to devices

It has become a great challenge to access the devices securely. If verification is not or is supported poorly, illegal matters will gain access and cause system manipulation, therefore, neither implementations at the application layers, nor trusting any causal binary codes will be guaranteed (Saleem, Tan and Buchanan, 2017).

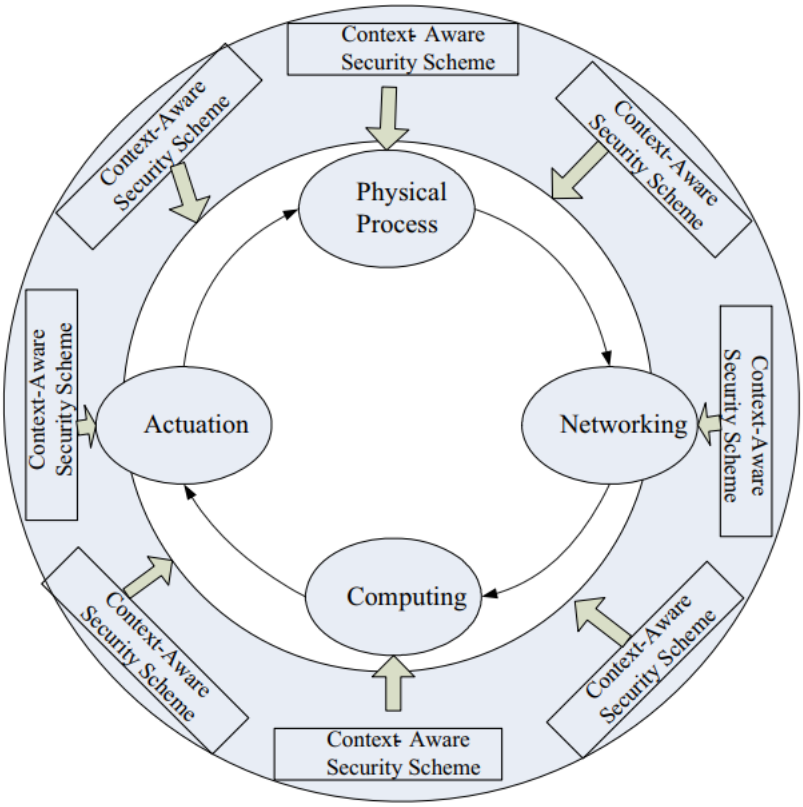

Figure 6. Cyber Security and its different constraints (Giraldo *et al.*, 2017)

Securing data transmissions

The security of data transmission is compulsory so as to detect malicious and impostor activities in cyber physical system communication networks and block unofficial accesses. As an instance, attackers attempt to interrupt the physical features of system timing behaviors and power consumptions for data analysis being send and receive. Few attackers aim to disturb networks by launching Denial-of-Service attacks or disturbing the topology of different routes. Few terminal devices that are not comprehensive computer systems do not have higher data processing and communication aptitudes, or sufficient storage capabilities. It makes the devices more susceptible to penetrate (Korukonda *et al.*, 2017).

In contrast, inside the terminals of industrial control systems, the connectivity that depends upon the standards of open networking supports to improve system performances and decreases operational expenses. Though such terminals directs to more effective and efficient operations, they expose the systems to complex possibilities of malicious and intrusion attacks, for example

distributed service denial, malicious code (malware), unauthorized access, and eavesdropping (He *et al.*, 2018). Another element that leads directly to vulnerability is the designing procedure which always reserved in processing speed, time, power consumptions and hardware resources. Furthermore, embedded systems are manufactured by experts with limited experience of security concerns, and concentrate more on functionality, performance and error corrections as compared to security. It, in turn, leads to system vulnerabilities and may leak protected data to undesired or unauthorized users (Lopez and Rubio, 2018).

Securing applications

The purpose of application layer is to combine different security challenges and applications. The matters of privacy protection of users can be analyzed by hackers which lead to leakage of private data along with privacy loss. Since this data may comprise present and past locations which are visited by the users, few techniques of data protection at this layer contain anonymous space, location camouflage, or space encryptions. As well, several applications in this layer implement to users' personal life, and so need to be secure (Horváth and Erdős, 2017).

Data storage Security

Protection of secret stored data in cyber physical system devices is really a significant matter. Most of the cyber physical devices, for example sensors are little, connected via wireless and resource-controlled nodes. Though many software based solutions apply cryptographic methods for data encryption in these devices, they are not enough because of weak processing abilities and the memory constraints of such tools. Consequently, lightweight mechanisms of security are most appropriate (Yoon *et al.*, 2017).

Securing Actuation

Actuation security is defined as any actuation actions should be issued from authorized bodies. It ensures that the control commands and delivered feedback are protected and correct against attackers. Internet security issues also tangled on account of using it as a transmission layer in cyber physical system connections. On the whole, security must be applied for the whole system as one end-to-end security structure instead of for only the security operating machinery at every

layer. Furthermore, hardwearing computations and larger memory necessities are the primary requirement at present of any anticipated security package (Alcaraz and Lopez, 2020).

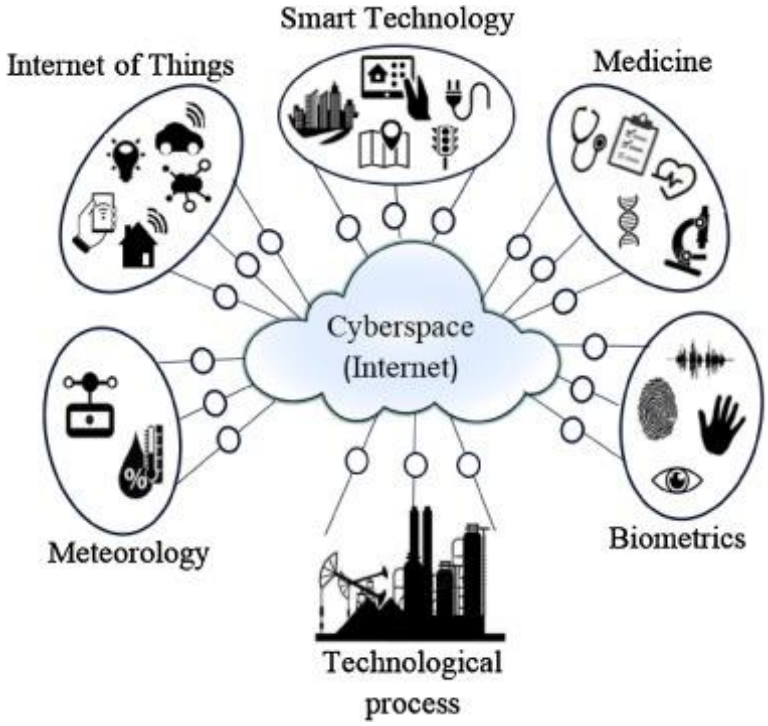

Figure 7. Cyber Security Access Control Sectors (He *et al.*, 2018)

Access Control to Cyber-Physical Systems and Hardware Vulnerabilities

Architecture and Abstraction

It is well recognized that well-manufactured architectures and abstractions are critical for the technology success. Representative instances that have developed the information technology revolution of the 20th century are the Von Neumann Architecture, a fundamental design model for stored digital program computers, and the Open Systems Interconnection (OSI) Model, communication architecture design which has built in the Internet success of nowadays (Saleem, Tan and Buchanan, 2017). In the same way, finding the accurate architectures and abstractions for cyber physical system which can be appropriate to diverse application domains can be critical for an effective cyber physical system revolution in the current period (Yoon *et al.*, 2017).

Networking and Computing Foundations

The central attributes of physical systems are concurrency and time. But, neither of both is appropriately modeled and controlled in today's networking and computing schemes. No extensively used programming languages have chronological stuffs in these semantics. The thread that is a programming abstract for synchronized implementation is called very problematic to use and challenging because of its counter-intuitive abstractions. Networking tools which are extensively used today present considerable unpredictability and delays. Computing software and hardware systems are intended and built for improved throughput at the expenditure of probability. Therefore, additional research on networking and computing systems that can integrate naturally temporal features of physical systems is a significant research zone (Akhuseyinoglu and Joshi, 2017).

Hybrid Systems and Control

One stimulating attribute of cyber physical system is that there are constricted connections between the discrete and continuous dynamics of physical systems. For a long phase, mathematical formula on the basis of differential equations has been used effectively by scientists and engineers to analyze and model dynamics of physical systems. In contrast, the theoretical basis for cyber systems has been founded on discrete mathematics for example graphs theory, automata theory, etc (Sciancalepore *et al.*, 2018).

The advent of cyber physical system has stimulated efforts at developing a new hybrid system, theoretical foundation which can capture both discrete and continuous dynamics all at once, for system analysis and design. There has been momentous progress over the past 20 years on hybrid systems study. But, there still remain several open difficulties for example hybrid system reachability with continuous nontrivial dynamics, automatic control algorithms synthesis for wide range hybrid systems, discrete abstraction approaches for decidable hybrid model systems generation, etc. (Bello *et al.*, 2017).

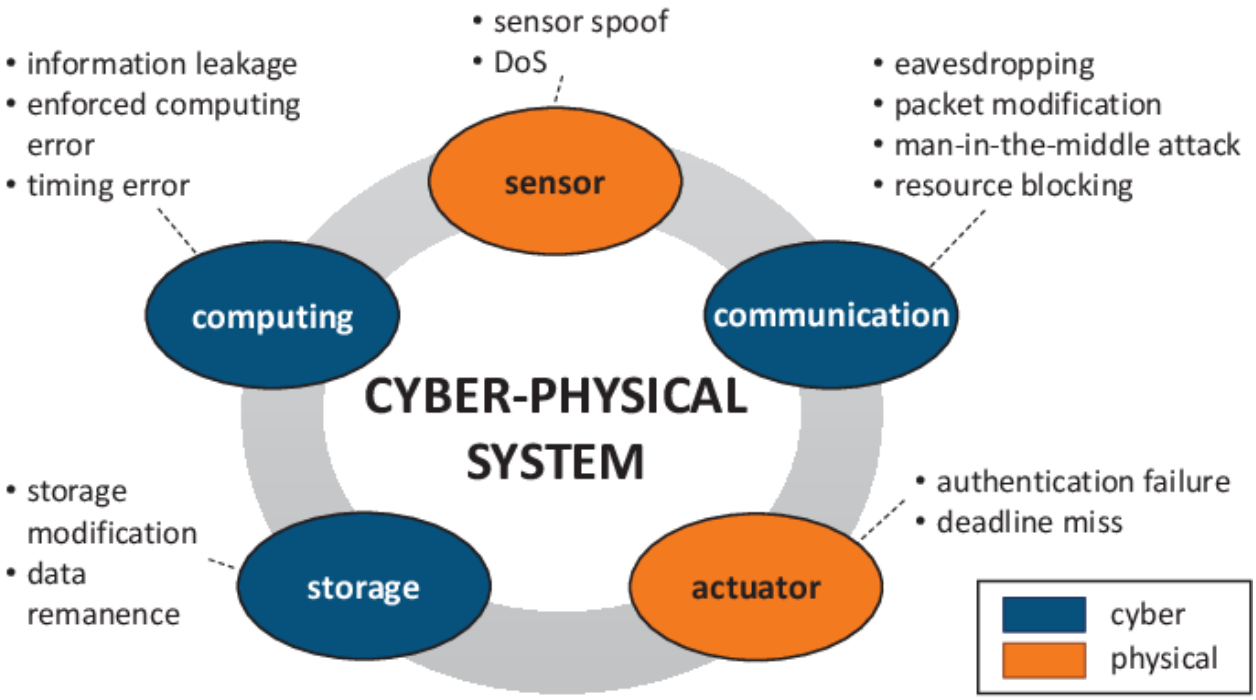

Figure 8. Cyber Physical Security System Parameters (Saleem, Tan and Buchanan, 2017)

Validation, Certification, and Verification

In the course of manufacturing and development of an innovative engineered system, validation and certification is one of the most labor and time consuming as well as cost demanding progressions overall. It is predominantly true for systems which require high reliability, for example airplanes, medical devices, automobiles, etc (Humayed *et al.*, 2017). As an instance, certification spends in excess of 50 percent of the resources capitalized in developing novel safety-perilous systems in the aviation commerce. The situation is alike in the automotive, medical, energy, and other safety-precarious engineering. In addition, as the complexity of cyber physical system is increasing significantly, validation and certification process is becoming even more costly and challenging (Fawzi, Tabuada and Diggavi, 2014).

To address such a tough matter, there have been many research efforts on cyber physical system conducted in the past decade. Model-based development, design, and verifications are predictable to play a significant role in the drive headed for cost-effective and competent evidence-based certifications (Ding *et al.*, 2018). Though, to understand the idea of this approach in reality, there are still various technical trials that prerequisite to overcome, for example new compositional system-wide models for verification, more developments on formal verification algorithms to

control nontrivial (industrialized) cyber physical system models, driven model design and development devices which can allow integrated validation and verification of general cyber physical system at the designing stage (Monostori *et al.*, 2016).

Conclusion

As discussed before, several cyber physical system applications are protection critical systems, such as, air and ground transportation systems, healthcare and medical systems, power grid systems, disaster warning monitoring systems, etc. Therefore, it is vital to ensure inclusive constancy of physical systems to circumvent catastrophic circumstances. However, as there are several sources in the sensing, physical, networking, actuation and computational domains which can build systems to behave anomalously, it is very stimulating to accomplish this objective in cyber physical system. Quite a lot of uncertainties are existent in physical systems along with surrounding surroundings. Many kinds of failures can arise at any place and on any time in cyber and physical systems. There can also be security attacks from challengers. Therefore, accomplishing system-wide safety, robustness, and security is a main research challenge in future.

References:

Akhuseyinoglu, N. B. and Joshi, J. (2017) ‘A risk-aware access control framework for cyber-physical systems’, in *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*. IEEE, pp. 349–358.

Alcaraz, C. and Lopez, J. (2020) ‘Secure interoperability in cyber-physical systems’, in *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*. IGI Global, pp. 521–542.

Alguliyev, R., Imamverdiyev, Y. and Sukhostat, L. (2018) ‘Cyber-physical systems and their security issues’, *Computers in Industry*. Elsevier, 100, pp. 212–223.

Ashibani, Y. and Mahmoud, Q. H. (2017) ‘Cyber physical systems security: Analysis, challenges and solutions’, *Computers & Security*. Elsevier, 68, pp. 81–97.

Bello, L. Lo *et al.* (2017) ‘Guest editorial special section on new perspectives on wireless communications in automation: From industrial monitoring and control to cyber-physical systems’, *IEEE Transactions on Industrial Informatics*. IEEE, 13(3), pp. 1393–1397.

Bonci, A., Pirani, M. and Longhi, S. (2018) ‘A database-centric framework for the modeling, simulation, and control of cyber-physical systems in the factory of the future’, *Journal of Intelligent Systems*. De Gruyter, 27(4), pp. 659–679.

Bordel, B. *et al.* (2017) ‘Cyber–physical systems: Extending pervasive sensing from control theory to the Internet of Things’, *Pervasive and mobile computing*. Elsevier, 40, pp. 156–184.

Buini, H. M., Peter, S. and Givargis, T. (2017) ‘Adaptive embedded control of cyber-physical systems using reinforcement learning’, *IET Cyber-Physical Systems: Theory & Applications*. IET, 2(3), pp. 127–135.

Chen, D. *et al.* (2012) ‘Modeling access control for cyber-physical systems using reputation’, *Computers & Electrical Engineering*. Elsevier, 38(5), pp. 1088–1101.

Chen, D. and Chang, G. (2012) ‘A Survey on Security Issues of M2M Communications in Cyber-Physical Systems.’, *TIIS*, 6(1), pp. 24–45.

Ding, D. *et al.* (2018) ‘A survey on security control and attack detection for industrial cyber-physical systems’, *Neurocomputing*. Elsevier, 275, pp. 1674–1683.

Fawzi, H., Tabuada, P. and Diggavi, S. (2014) ‘Secure estimation and control for cyber-physical systems under adversarial attacks’, *IEEE Transactions on Automatic control*. IEEE, 59(6), pp. 1454–1467.

Giraldo, J. *et al.* (2017) ‘Security and privacy in cyber-physical systems: A survey of surveys’, *IEEE Design & Test*. IEEE, 34(4), pp. 7–17.

He, Q. *et al.* (2018) ‘Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems’, *Computer Networks*. Elsevier, 140, pp. 163–173.

Horváth, G. and Erdős, G. (2017) ‘Gesture control of cyber physical systems’, *Procedia Cirp*. Elsevier, 63, pp. 184–188.

Humayed, A. *et al.* (2017) ‘Cyber-physical systems security—A survey’, *IEEE Internet of Things Journal*. IEEE, 4(6), pp. 1802–1831.

Jazdi, N. (2014) ‘Cyber physical systems in the context of Industry 4.0’, in *2014 IEEE international conference on automation, quality and testing, robotics*. IEEE, pp. 1–4.

Johansson, K. H. *et al.* (2014) ‘Guest editorial special issue on control of cyber-physical systems’, *IEEE Transactions on Automatic Control*. IEEE, 59(12), pp. 3120–3121.

Korukonda, M. P. *et al.* (2017) ‘Handling multi-parametric variations in distributed control of cyber-physical energy systems through optimal communication design’, *IET Cyber-Physical Systems: Theory & Applications*. IET, 2(2), pp. 90–100.

Liu, Y. *et al.* (2017) ‘Review on cyber-physical systems’, *IEEE/CAA Journal of Automatica Sinica*. IEEE, 4(1), pp. 27–40.

Lopez, J. and Rubio, J. E. (2018) ‘Access control for cyber-physical systems interconnected to the cloud’, *Computer Networks*. Elsevier, 134, pp. 46–54.

Lu, C. *et al.* (2015) ‘Real-time wireless sensor-actuator networks for industrial cyber-physical systems’, *Proceedings of the IEEE*. IEEE, 104(5), pp. 1013–1024.

Mahmoud, M. S., Hamdan, M. M. and Baroudi, U. A. (2019) ‘Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges’, *Neurocomputing*. Elsevier, 338, pp. 101–115.

Misra, S. *et al.* (2013) ‘Efficient medium access control for cyber–physical systems with heterogeneous networks’, *IEEE systems journal*. IEEE, 9(1), pp. 22–30.

Monostori, L. (2014) ‘Cyber-physical production systems: Roots, expectations and R&D challenges’, *Procedia Cirp*. Elsevier, 17, pp. 9–13.

Monostori, L. *et al.* (2016) ‘Cyber-physical systems in manufacturing’, *Cirp Annals*. Elsevier, 65(2), pp. 621–641.

Saleem, K., Tan, Z. and Buchanan, W. (2017) ‘Security for cyber-physical systems in healthcare’, in *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*. Springer, pp. 233–251.

Sciancalepore, S. *et al.* (2018) ‘On the design of a decentralized and multiauthority access control scheme in federated and cloud-assisted cyber-physical systems’, *IEEE Internet of Things Journal*.

IEEE, 5(6), pp. 5190–5204.

Shafi, Q. (2012) ‘Cyber physical systems security: A brief survey’, in *2012 12th International Conference on Computational Science and Its Applications*. IEEE, pp. 146–150.

Wang, D. *et al.* (2016) ‘Recent advances on filtering and control for cyber-physical systems under security and resource constraints’, *Journal of the Franklin Institute*. Elsevier, 353(11), pp. 2451–2466.

Yoon, S. *et al.* (2017) ‘Fast controller switching for fault-tolerant cyber-physical systems on software-defined networks’, in *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, pp. 211–212.

Yuan, Y., Sun, F. and Liu, H. (2016) ‘Resilient control of cyber-physical systems against intelligent attacker: a hierarchal stackelberg game approach’, *International Journal of Systems Science*. Taylor & Francis, 47(9), pp. 2067–2077.

Zhang, L., Qing, W. and Bin, T. (2013) ‘Security threats and measures for the cyber-physical systems’, *The Journal of China Universities of Posts and Telecommunications*. Elsevier, 20, pp. 25–29.