Cyber Physical Systems: The Role of Machine Learning and Cyber Security in Present and Future

Sravanthi. K, Shamila. M, Amit Kumar Tyagi [0000-0003-2657-8700]

Department of Computer Science & Engineering, Malla Reddy Engineering College, Hyderabad, India

School of Computing Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India.

sravanthireddy.k8@gmail.com, shamila.m@gmail.com, amitkrtyagi025@gmail.com

Abstract

Today's technology is changing very rapidly and making an important place in the heart of humans. For example, when internet connected things after connect with other devices, they make a big system which solve complex problems and make people life easier and longer to live. One of biggest/ popular revolution of technology is "Cyber Physical System". Cyber Physical systems (CPSs) are the systems/ mechanism which are controlled and monitored remotely. CPSs system work with connecting other systems through Internet and its users (by computer-based algorithms). In near future in Industry 4.0 revolution, the uses of cyber physical systems will be on top position. Using such systems give invitation to attackers for performing attacks. But an attacker can harm a physical and cyber space easily, i.e., affecting physical processes will affect computations (also efficiency of CPS systems). For example, nuclear facilities were affected in 2010 (in Iran) by poplar attack "Stuxnet". Also, an attacker can control a medical device remotely which will be affected the condition of patients (also will leak private information of patient/ hospital employee). Such serious concerns are being highlighted in this article using machine learning and cyber security frequently (time to time) or an alternative schedule. Maintaining such system is really a difficult task, so if do we can save a lot of energies and unwanted attacks, etc., in overall. Hence, this article is being written with considering future serious concerns and challenges with CPSs, and listing out of such critical issues one by one (in detail).

Keywords: Internet of Things, Cyber Physical System, Machine Learning, Cyber Security, Malware.

1. Introduction

Machine learning convert the data into decisions and actions faster and precisely. Machine learning technique use the data for descriptive purpose (to analyse what happened), diagnostic purpose (to study why did it happen), prediction (describing about what will happen in future) and also for prescriptive purpose (which include decision support and decision automation). Machine learning is a subset of artificial intelligent which enable thesystem to learn with the help of training data set rather than being explicitly programmed. Machine learning helpsto make predictions (which can change) when it is exposed to new data. The new advancement in technology causes production of huge amount of data. Which is called as big data. We need to utilise this data to create an intelligent system with the support of machine learning. So, we can consider big data and machine learning are compliment to each other. With the invention of Internet of Things (IoT)technology, the rate of growth of data being generated is exponential. We need to make use of this data in an efficient manner. Machine learning can use to predict the future. Different techniques or application used to implement machine learning techniques are:

(i) Supervised learning: Decisions are made with the help of labelled data. Ensemble learning is an extension of supervised learning where different simple models are combined to solve the task.
(ii) Unsupervised learning: It is used in the absence of labelled data. Decisions are made with the help of properties of data.
(iii) Semi supervised learning: It is used when combination of labelled and unlabelled data is present. It is utilize the advantage of supervised and unsupervised methods.

(iv) Reinforcement learning: It is an environmental driven approach which mainly uses trial and error method for learning. Active learning is a subclass of this type where user is active participant in the learning process.The main goal is to optimize the model quality by acquiring knowledge from users.

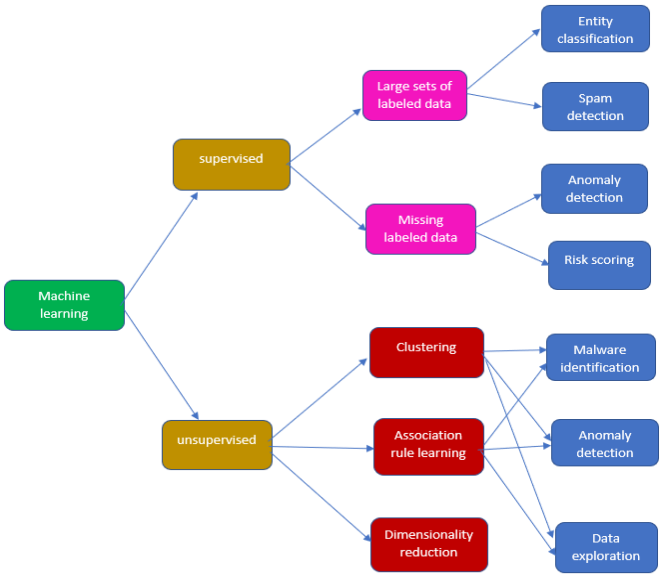

Figure 1: Types of Machine Learning Techniques [1]

As shown in figure 1 machine learning methods have been used in many areas of science because of special characteristics like adaptability and scalability. Some of the application of machine learning include weather forecasting, image processing (like face recognition, fingerprint identification, moving object recognition etc.),e-health care, cyber security etc. The importance of cyber security is increasing dramatically because of the remarkable usage of online applications, social network, IoT based systems, cloud and web technologies. Cyber security is body of technologies which protect the inter-connected systems over the internet from cyber-attacks (unauthorized person used to access data form online data centres). Cyber security is used to prevent damage and attack on Cyberspace (virtual computer world which is made up of many network devices connected over the internet to perform data exchange activities). The key characteristic of cyberspace an interactive and virtual environment for a wide spectrum of participants. The future of Cyber security is not about human or machine-it is about human intelligence and machine.

The objective of cyber security (strategy) is not to avoid 100% the attacks, which is not possible; but to minimize the "attack". The number of attack perpetrators will be always bigger than the number of people trying to protect against attacks. Cyber machine learning solutions must be capable of addressing well scoped problems. It should integrate with existing tools and architecture. The system should allow frictionless performance evaluation. Machine learning is becoming more remarkable in the field of cyber security. The machine learning task like regression can be applied in cyber security for fraud detection, classification technique can be applied to spam filters, clustering can be applied for forensic analysis, Dimensionality reduction can be used for face recognition etc.

Generally, Cyber Physical System (CPS) was introduced in 2006. Cyber physical systems are feedback systems which are intelligent, real time, adaptive or predictive in nature and can be networked or distributed. CPS requires improved design tools that enable design methodology. These methodologies must support scalability, complexity management and also verification and validation. CPS has applications in different fields like healthcare, robotics, manufacturing, transportation etc. Figure 2 represents different components of CPS. The main characteristics [2, 3, 4 and 5] of CPS are as follows:

- Integrated: CPS is integration of both physical and cyber design.
- Resource constrained: The software is embedded in all physical components and the resources like bandwidth, computation speed is limited.

- Feedback controlled: This system supports high level of automation and person-device interaction.
- Networked and distributed CPS include network of wired or wireless network, Bluetooth, GSM etc.
- Complex: CPS is strictly constrained by granularity of time and spatiality.
- Dynamic reconfiguration: CPS system is adaptable in nature.
- Reliable: Since CPS is large complicated system, reliability and security is very much required.

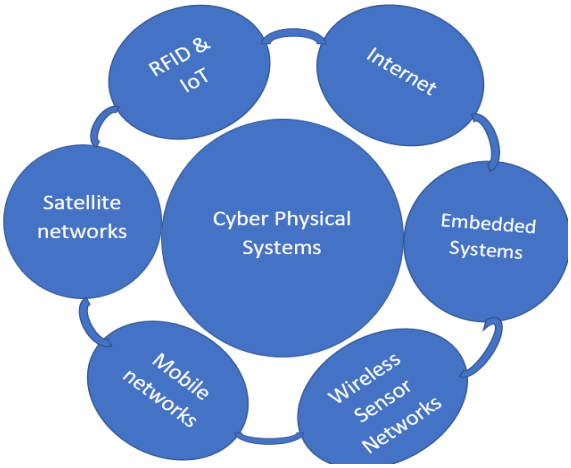

Figure 2: Components of Cyber Physical System [6]

Hence, in this section we discussed the different machine learning technique and how they can be utilised in cyber security. The remaining portion of this paper is organised as: the coming section discusses about the existing work done in this field. Section 3 discusses motivation behind writing this work (article). In section 4, we discussthe importance of machine learning and cyber security towards CPS in current and future. Section 5 discusses several useful scenarios for future with extended technology (using cyber security, and artificial intelligence). Later, we explained the different challenges and issues in cyber physical system in section 6. In the similar section 6, we also discuss the opportunities in this field. In the last in section 7, we explored some future enhancement, which can be done in this particular area.

2. Related Work

As we discussed in the introduction section machine learning techniques have a vast opportunity to support cyber security. Various machine learning methods have been successfully implemented to address different computer security problems. Machine learning task can used to detect and classify brute force attack. Anomaly detection can be applied to identify account masquerading. We can make use of cluster analysis to enrich fraud investigation. Some of the other applications are briefly discussed below.

a) Phishing detection [7]: Phishing is a cybercrime, where target contact the individual via mail or phone calls and trap personally identifiable information, banking and credit card data, and passwords.The information is then used to access important accounts and can result in identity theft and financial loss.Researchers compared different machine learning techniques like Logistic Regression (LR), Classification and Regression Trees (CART), Bayesian Additive Regression Trees (BART), Support Vector Machines (SVM), Random Forests (RF), and Neural Networks (NNets)". And the studies show that LR has the highest precision and relatively high recall in comparison with other classifiers. Zhuang et al. [8] used clustering solution like hierarchical clustering and k-medoids for phishing detection and obtained 85%performance.

b) Network intrusion detection: The main aim of Network Intrusion Detection (NID) systems is to identify malicious network activity, which causes confidentiality, integrity, or availability violation of the systems in a network. Subbulakshmi et al. [9] constructed Alert Classification System with the help of Neural Networks (NNs) and Support Vector Machines (SVM) against Distributed Denial of Service (DDoS) attacks.The researchers claimed that average accuracy of neural network alert classification is 83% whereas for support vector machines, it is 99%.Sedjelmaci and Feham [10] propose a hybrid solution for detecting intrusions in

a Wireless Sensor Network (WSN). A clustering technique is implemented for reducing the amount of information to process andSupport Vector Machines (SVMs) with misuse detection techniques are employed for detecting network anomalies.

c) Key stroke dynamics authentication: Key stroke dynamics help to identify the timing information regarding when the key is pressed and released while a person is using the keyboard. Revett et al. [11] proposed applying a Probabilistic Neural Network (PNN) for keystroke dynamics. Also, PNN was compared to a multi-layer perceptron neural network (MLPNN) with back-propagation and observed that training time of PNN is 4 times less than MLPNN.

d) Breaking human interaction proofs (CAPTHAs): Chellapilla and Simard [12] propose how the Human Interaction Proofs (or CAPTCHAs) can be broken by utilizing machine learning. The researchers studied with seven various HIPs and observed the common strengths and weaknesses. The proposed approach is aimed at locating the characters (segmentation step) and employing neural network [13] for character recognition. The experiments are conducted with yahoo mail blocks, register, Ticketmaster, and Google HIPs.It was reported that the segmentation stage is relatively difficult due to computational expense.

e) Cryptography: Yu and Cao [14] implemented a fast and efficient cryptographic system based on delayed chaotic Hopfield neural networks. The researchers claim that the proposed system is secured due to "the difficult synchronization of chaotic neural networks with time varying delay".Kinzel and Kanter [15] explained how two synchronized neural networks can be used for a secret key exchange over a public channel.The researchers have claimed that it is computationally infeasible to perform some attacks.

f) Social network spam detection: Fake accounts, bulk messaging, spreading malicious links are key to social spamming.K. Lee et al. [16] observed that spammers exploit social systems for employing phishing attacks, disseminating malware, and promoting affiliate websites. For protecting social systems against those attacks, a social honeypot was developed for detecting spammers in social networks like Twitter and Facebook. The proposed solution is based on Support Vector Machine (SVM) and has a high precision and lowfalse positive rate.

Currently some techniques are available to handle the complexity of CPS. They are mentioned briefly.

- Process based approaches.
- Model based approaches.
- Architecture based techniques.
- Organisational approaches.

Even though these methods work well for current systems, it cannot withstand the next generation CPS. Hence, this Section 2 discusses work related to cyber physical system (including application and existing methods) in detail. Now, next section will discuss about motivation behind this work.

3. Motivation

Cyber physical systems are necessity and mostly used infrastructure (by governments/ industries) to solve many challenging problem ofcurrent day today life. As we know that Rapid and correct decision-making in a big data environment (also a critical/ large environment) is a big task. The integration of Internet of Things (IoTs) which is called Cyber-Physical Systems (CPS), is used to transform the industry or manufacturing or other applications into the next level.But, irrespective of benefits (and improvement) of CPS,many issues and problems we face in our life like lack of smart analytical tools,which affect industries, i.e., not to handle large amount of data/ big data (which is generated by Internet ConnectedDevices). Also, skilled people are not enough to handle or tracking or analysis these devices or infrastructure. Also, popular vulnerabilities may occur on these IoTs/ internetconnected things. Hence, the integration of cyber security and machine learning in cyber physical systems is necessary requirement. Using machinelearning techniques, skilled people can tract or hunt threats on web (also on CPS) in minimum time. We start writing article related to this topic because this technology or CPS in near future can be very useful in generating efficient, and robust solution via optimal decision making. This work will focus on existing trends, issues challenges in the development of industrial big data analytics and CPS using machine learning and cyber security in the respective area. Hence, this section discusses our main

motivation behind writing this paperon “Cyber Physical System”. Further, next section will discuss about the need (or necessity) of machine learning in cyber security.

4. Necessity of Machine Learning and Cyber Security

We can use Security analytics todetect threats better. It is also useful to prioritize the alerts and signals. Which help to find the solution of the problem in less time. We can utilise machine learning technique to make the cyber security more powerful. Some of the examples are mentioned below.

- Cyber security companies are making use of data science methods to process and analyse large set of data which can be either historic or threat intelligence data for many years.
- F-Secure have been using machine learning algorithms to solve problems such as classification, clustering, dimensionality reduction, and regression.
- Machine learning can also be used for successful implementation of authentication systems, evaluating the protocol implementation, assessing the security of human interaction proofs, smart meter data profiling, etc.

Cybersecurity is a significant area for the usage of machine learning techniques. Modern Cybersecurity threats like malware detection, intrusion detection and data leakage can’t be solved by using mathematical models alone. ABI Research [17] forecasts that "machine learning in cyber security will boost big data, intelligence, and analytics spending to $96 billion by 2021." In healthcare, to secure all systems through which a hacker could access sensitive information [18], the software would need to be installed in the larger network of the healthcare company. These systems are called endpoints because the employers access the data at this end. For detecting cybersecurity threats, we need to install machine learning model within the client healthcare company network and permitted to analyse activities of network in real time. Machine learning develops awareness of what normal network activity looks like and use this as reference to determine the probability of suspicious activity. If user activity looks like deviates far from system norm, then it flags as fraud activity. Darktrace is an example of machine learning vendor for anomaly detection in healthcare companies.

By using machine learning, the cyber security systems can easily analyse the pattern and can attain knowledge to find counter measures to avoid the similar attacks. In simple terms we can tell that machine learning helps cybersecurity groups to prevent threats effectively and also to respond active attacks in real time. The role of data is critical for the success of machine learning in cyber security. Machine learning is all about developing new pattern and analysing it using different algorithms. In order to achieve this, we require wide set of data which represent many potential outcomes from different scenarios. Note that here not only the quantity, the quality of data also matters. The data must be complete and relevant. Now a day’s huge amount of data is produced by the network of IoT and other applications. Traditional data management system failed to manage this different variety huge sized data but big data frame work can handle this data effectively. So, we can conclude that, to deploy effective cyber security system, machine learning methods is required and we need complete /relevant data to attain efficient machine learning techniques. So, in this section, we included/ mentioned the importance of machine learning technique in cyber security. We also described the role of data in implementing machine learning algorithms. In the next section, we will see the future of cyber physical system in combination with different existing techniques.

5. Future with Extended Technology

Cyber Physical System (CPS) are increasingly adopted (implemented) in many automobile companies and deployed with new domains. This intimates that future CPS is to face an increase in functional and extra-functional requirements. Functional requirements include predictive maintenance and increasing automation levels of CPS. Extra-functional requirements include safety, cyber-security, and environmental sustainability. Many new CPS applications are cross-domain (ability to access automatically or send information to other security domains) in nature. For example, automated cars implementing robotics technologies and usage of

telecom networks for smart machines, both pose a great opportunities and challenges. Advances in technology allow completely new types of integration and communication in CPS across:

- Technological fields such as physical, embedded, networked and information systems. For example, cloud and edge computing.
- Standalone systems, for example intelligent transport systems (integration of vehicles and infrastructure).
- Stages of the life cycle, in general making data available throughout the life cycle and enabling upgrades to software. These are concepts in DevOps (Development-Operations integration) associated with continuous software development, integration and deployment with feedback from operational systems.

There is a rapid growth in CPS by increasing levels of automation and intelligence including data analytics. These characteristicsdepend on the artificial intelligence techniques, it includes machine learning.AI and data analytics opportunities are seen as game-changers, stated by a report by the National Science and Technology Council in US [19]. Context awareness is important for new types of AI-based CPS, including the ability to understand that entities are currently part of the near-environment and to conclude what their objectives are. The growth and development of AI technologies in a number of application domains is likely to drive increasing levels of automation. Future CPS will also be charged with increasingly difficult tasks in open environments due to their ability to solve societal challenges and generate revenue. To oppose traditional manufacturing applications, highly advanced technologies are deployed and spread throughout society. For example, automated driving cars without human intervention on public roads and robot-human collaboration systems.

Smart CPS is responsible for dynamic changes in environment. (For example, highly variable traffic environments that changes rapidly with changing human behaviours and CPS infrastructures).It generally means that not all operating conditions are known a priori (at the time of system development) see example [20]. The wider implications indicate that open CPS faces a number of existing and new forms of uncertainties from partially unknown environments, vulnerabilities in safety and attacks (predict attack by proving “attacker models”) and modifying CPS itself (due to partial failures).Uncertainty can apply to aspects for parts of a CPS and all life cycle stages. By taking various sources of uncertainty into account, it is important to plan a systematic treatment [21].

It is clear that the possible characteristics of future CPS would require new ways of reasoning regarding system level properties and composability. In the following we expand multidimensional CPS composability topic and describe what we see as specific composability challenges like human-CPS, CPS integrating AI, trustworthiness, and CPSoS.

- **Human-CPS Integration:**

  Regardless of the system type and automation level, humans are showing more interest to interact with CPS as developers, operators, users and maintainers. Major number of challenges for human-machine interaction caused by increasing levels of automation. For example, in some cases humans may need to act in emergency situations (pilots in aircraft). We are currently moving to higher levels and more intelligent systems, and the lessons learned in automation history remain extremely important in improving support for human interaction with highly capable CPS [22].A fundamental idea for the human CPS is to consider, i.e., what determines an agent's action or inaction. Deviations in the normal behaviour of human agents need to be identified, in particular behaviour leads to decision/actions for CPS functioning [23].

- **AI with CPS:** New types of applications are enabled by AI and Machine learning technologies. While using machine learning in terms of neural networks raises doubt about how to deal with robustness, transparency, predictability and how to verify effectively-cost, validate and assure such systems [24,25].

- **Trustworthiness:**To current CPS, security risks already exist and will increase as, CPS is increasingly adopted, connectedand used by open source software.Absolute security and safety are not possible so online actions

are necessary to deal with security breaches and safety-related anomalies.In addition, the increasing use of CPS makes their available increasingly important, which means that traditional unsafe solutions aren't an option. Future systems must implement fault tolerant systemswhile balancing the rise for complexity due to redundancy, adaptability and fall-backmeasures. Finally, essential issues related to ethics, liability and assurance are recognised. Who will take responsibility if CPS fails, what are the decisions made by highly automated systems and what is required for future CPS for assurance case [23].

- **Cyber-Physical Systems of Systems (CPSoS):** Future CPS could be part of CPSoS.Such systems can also be in relation to multiple domains due to their novelty and scale and greater number of stakeholder's jurisdictions, regulations and standards to be taken into consideration [26].

Hence in this section we briefly described the future scope of cyber physical system in the current era. Now in the next section we will discuss some of the challenges and issues related to cyber security and also the opportunities in detail.

6. Issues, Challenges and Opportunities in Cyber Physical Systems

There are many issues and challenges (also various opportunities) for bright future of Cyber Physical Systems (CPS) in our environment, few of them will be discussed below.

- **Security**

Security is a major challenge in Cyber Physical Systems for present generation and future. All features of CPS are connected through internet and this is the actual reason for security threats, i.e., everything is globally connected. So, there is possible for affecting everything in a malicious attack. There is no perfect solution for security attacks until we stay globally connected. If we want to prevent attacks, don't store information in databases which are globally connected, which is not possible in reality. So, as long as we stay connected globally, we have to invest into security improving solutions. Few examples to demonstrate the importance of caring about security:

- Stuxnet cyber-attack [27] found world-wide attention.
- Cyber terrorism is a real threat to our organizations.

- **Safety**

CPS (Cyber Physical Systems) are also a potential threat because they are integrated tightly into the physical environment. Errors can extend into the physical parts of the information processing part of the system and can pose a risk to humans, animals and our environment. For example, jet planes, self-driving cars and devices in health sector. There may be different safety threats: they may result from design errors, improper specifications, failure of hardware devices. To achieve safety, there should be some formal verification techniques or use of special languages for programming like synchronous languages [28].

- **Reliability**

Reliability implies the probability that the expected service will be provided on time. Reliability criteria for tolerated failure levels can take the form of ceilings. Main aim of dependable systems is to avoid service failures such as hardware errors, environmental conditions specified out of the range to achieve reliability.

- **Energy efficiency**

Major CPS (Cyber Physical Systems) is mobiles or the systems which are having limited energy. As a result, such type of systems either have energy harvesting or they have to use batteries. In both cases, utilization of energy should be done more carefully.

- **Heterogeneity**

CPS connects many devices and different types of components. Such as analog components, digital components. Components are designed for different purpose by different companies. Achieving interoperability between componentsi.e., heterogeneity is a challenge in CPS.

- **Timing predictability**

One of the most important physical quantity is time. In addition, the timing behaviour of information processing becomes very critical by linking information processing to physical systems. In fact, most CPS devices are in real time systems. Within, a time interval defined by the environment it is appropriate to respond to such systems. The importance of this requirement is often underestimated. Most of the systems are designed to provide quick response time in many cases, but may fail due to some others. To avoid such cases for CPS, hardware-software stacks are changed, entire design may change.

- **Dynamism**

Desktop systems are fixed at particular locations. Changing of their network interface happen in rare cases. For CPS, the network connection is kept on changing every time. Wireless LAN, Bluetooth, mobiles can be used by different networks. Each will vary in its speed and cost. The quality of connection varies every time. Network delays may be different. Because of this, network connection has to provide a high level of fault tolerance. The availability of energy and external devices and computational load also change time to time. By the above issues operating conditions may be highly dynamic.

- **Multidisciplinary Nature**

Designing of CPS requires varies domain knowledge, it includes physics and computer science. For most of the applications knowledge is required from disciplines like medicine, mechanical engineering, biology, chemistry. Due to tight academics for student it is not possible to incorporate all into one. Hence, it is very important to adopt CPS concepts in educational programs such that all core knowledge is gained.

The different types of cyber physical systems and the attacks to which it is susceptible is briefly described in table 1.

The fusion of computing and the physical environment provides many opportunities in cyber physical systems. In the following, by listing few of the popular areas, we would like to show the large set of opportunities.

- **Smart Home**

With respect to various metrics, there are many opportunities for enlightening life at home. For example, safety levels, energy efficiency and comfort can be improved better and we can assist elderly people. Target of smart home is ambient assisted living. We can improve safety and energy efficiency by connecting various devices in a home. One of the special cases is zero-energy building. Main aim of such buildings is to produce as much energy as it consumes, on average at least. By using smart ventilation, solar cells, control of blinds, energy-efficient heating and lighting we can turn this vision into reality. For actual use of features, consumption of energy is adjusted. For example, AC (Air Conditioner) temperature should be less in empty rooms.

- **Transportation and logistics**

Transportation is the most popular application of cyber-physical systems. The known fact that in automobile industries no car is sold out unless it has more features than the previous models, features are provided by

the Information and Computation Technologies (ICT) components. It includes engine control, safety features like electronic stability programs (ESP). In autonomous driving cars the main feature is parking assistance [29]. We have a lot of transport-related logistics, including supply chain optimization and just-in-time delivery. Due to increasing number of customers ordering through internet, efficient parcel delivery is more important. For this, ICT components are supported to store and retrieval of goods [30].

- **Health**

The health sector includes a vast number of various applications of this integration. New ICT-enabled sensors can be designed. We can have advanced techniques for data and risk analysis (In collaborative research centre SFB 876, these are studied [31]). To identify sources of problems, supply chains can be monitored. After diagnosis is completed, it is also possible to support therapies. Every person (even handicapped patient) can have personalized medication. Result can be monitored by the use of sensors. The detailed information of patient is provided in patient information systems, which avoids redundant information about patient.

- **Structural health monitoring**

Tracking the structural stability of artificial and natural objects is feasible and beneficial. For example, it is possible to predict the risk of falling rocks or collapsing bridges [32].

- **Disaster recovery**

ICT (Information and Computation Technologies) used to provide rescue operations for the disasters, in which communication plays as a key role.

Note that some issues and challenges towards Cyber Physical System (CPS) and Medical Cyber Physical System (MCPS) also have been discussed by Tyagi A. K in [33] and Meghna.N et al., in [34]. Hence in this section we covered different challenges and issues existing in this field. Apart from this we also mentioned the opportunities of the cyber physical system. In the next section we will summarise this work in brief.

7. Conclusions

With the rapid development, we require intelligent maintenance systems to take of manufacturing and many control applications. As we know (discussed), artificial intelligence can help is reduce human work force in detecting vulnerabilities or threat on cyber physical systems/ cyber space. Cyber security is necessary for every business (especially which is connected/ working through web), because today's almost every business is affected by cyber-crimes. Future smart industries will require to optimize not only their own manufacturing processes but also the use of products and manufacturing resources, their maintenance and their recycling. On another side, the integration of Cyber-Physical Systems (CPS) and Intelligent Product (IP) is very needful for two real-world industrial cases, which can cover different phases of the product life-cycle like the production, use and maintenance phases. In summary in near future, the integration of advanced analytics using modern tools can improve manufacturing or industry 4.0 (into manufacturing, products and services). This area is still in growing phase, so require attention from nay research and scientific communities around the world. So, interested people are kindly invited to do their research work on above listed open issues opportunities towards the integration of Cyber Security, Artificial Intelligence (or Machine Learning) and Cyber Physical System.

Acknowledgments

This research work is funded by the Anumit Academy's Research and Innovation Network (AARIN), India. The authors would like to thank AARIN, India, a research network for supporting the project through its financial assistance.

References

1. V. Perez and Alberto, "Applications of AI to Network Security", 2018.doi: 10.13140/RG.2.2.29373. 56803
2. J. Z. Li, H. Gao, and B. Yu, "Concepts, features, challenges, and research progresses of CPSs," Development Report of China Computer Science in 2009, pp. 1-17.
3. R. Rajkumar, "CPS briefing," Carnegie Mellon University, May 2007.
4. B. H. Krogh, "Cyber Physical Systems: the need for new models and design paradigms," Presentation Report, Carnegie Mellon University.
5. B. X. Huang, "Cyber Physical Systems: A survey," Presentation Report, Jun 2008.
6. H. A. Nasser, A. Gasim and P. Shahbaz. "IOT Services Impact as a Driving Force on Future Technologies by Addressing Missing Dots".16th International Conference on Applied Computer Science (ACS '16), Istanbul, Turkey, 15-17 April 2016
7. S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A Comparison of Machine Learning Techniques for Phishing Detection", APWG eCrime Researchers Summit, October 4-5, 2007, Pittsburg**,** PA.
8. W. Zhuang, Y. Ye, Y. Chen, and T. Li, "Ensemble Clustering for Internet Security Applications", in IEEE xplore, December 17, 2012.
9. T. Subbulakshmi, S. M. Shalinie, and A. Ramamoorthi, "Detection and Classification of DDoS Attacks using Machine Learning Algorithms", European Journal of Scientific Research, ISSN 1450216X, Volume 47, No. 3, pp. 334 – 346, 2010.
10. H. Sedjelmaci, and M. Feham, "Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.
11. K. Revett et al., "A machine learning approach to keystroke dynamics-based user authentication", International Journal of Electronic Security and Digital Forensics, Vol. 1, No. 1, 2007.
12. K. Chellapilla and P. Y. Simard, "Using Machine Learning to Break Visual Human Interaction Proofs (HIPs)", in Advances in Neural Information Processing Systems 17, pp. 265-272, 2005.
13. P. Y. Simard, D. Steinkraus and J. Platt. "Best Practice for Convolutional Neural Networks Applied to Visual Document Analysis," in International Conference on Document Analysis and Recognition (ICDAR),2003. pp. 958-962, IEEE Computer Society, Los Alamitos.
14. W. Yu and J. Cao, "Cryptography based on delayed chaotic neural networks", Physics Letters A, Vol. 356, Issues 4–5, pp. 333-338, ISSN 0375-9601, August 14, 2006.
15. W. Kinzel and I. Kanter, "Neural Cryptography", in Proceedings of the 9th International Conference on Neural Information Processing, Vol. 3, pp. 1351-1354, November 18-22, 2002.
16. K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: social honeypots + machine learning", SIGIR'10, July 19-23, 2010, Geneva, Switzerland
17. Mackenzie Gavel,ABI research blog, https://www.prnewswire.com/
18. M. Shamila, K. Vinuthna and T. Amit Kumar." A Review on Several Critical Issues and Challenges in IoT based e-Healthcare System". IEEE
19. Networking and Information Technology Research and Development Subcommittee. The National Artificial Intelligence Research and Development Strategic Plan; Executive Office of the President or the United States: Washington, DC, USA, 2016.
20. M. Törngren and U. Sellgren, "Complexity Challenges in Development of Cyber-Physical Systems", In Principles of Modelling, Springer: Cham, Switzerland, 2018, Volume 10760, doi:10.1007/978-3-319-95246-8_27.

21. M. Zhang, B. Selic, S. Ali, T. Yue, O. Okariz, and R. Norgren, "Understanding Uncertainty in Cyber-Physical Systems: A Conceptual Model", In Proceedings of the 12th European Conference on Modelling Foundations and Applications, Vienna, Austria, 4–8 July 2016,Springer-Verlag: Berlin/Heidelberg, Germany, 2016, Volume 9764, pp. 247–264, doi:10.1007/978-3-319-42061-5_16.

22. L. Bainbridge, "Ironies of automation", Automatica,1983, 19, 775–779, doi:10.1016/B978-0-08-029348-6.50026-9.

23. W. Waymo, "Safety Report: On the road to Fully Self-Driving", 2018, Available online: https://storage. googleapis.com/sdc-prod/v1/safety-report/Safety%20Report%202018.pdf.

24. M. Wagner and P. Koopman, "A Philosophy for Developing Trust in Self-driving cars", In Road Vehicle Automation2, Springer: Cham, Switzerland, 2015, pp. 163–171, doi:10.1007/978-3-319-19078-5_14.

25. D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman and D. Mané, "Concrete Problems in AI Safety", arXiv 2016, arXiv:1606.06565.

26. S. Engells, "European Research Agenda for Cyber-Physical Systems of Systems and Their Engineering Needs", 2015, Available online: http://www.cpsos.eu/wp-content/uploads/2016/06/CPSoS-D3.2-Policy-ProposalEuropean-Research-Agenda-for-CPSoS-and-their-engineering-needs.pdf

27. N. Falliere, L. O. Murchu and E. Chien, W32, stuxnet dossier, White paper, Symantec Corp., Security Response, 2011.

28. D. Potop-Butucaru, R.de Simone and J. P. Talpin, "The synchronous hypothesis and synchronous languages", In Richard, Z. (ed.): Embedded Systems Handbook, CRC Press, 2006.

29. R. Okuda, Y. Kajiwara and K. Terashima, "A survey of technical trend of ADAS and autonomous driving", In: Proceedings of Technical Program, 2014, International Symposium on VLSI Technology, Systems and Application (VLSI-TSA), pp. 1–4 (2014). doi:10.1109/ VLSI-TSA.2014.6839646

30. C. Auffermann, A. Kamagaev, A. Nettsträter, M. tenHompel, A. Vastag, K. Verbeek and O. Wolf, "Cyber physical systems in logistics", http://www.effizienzcluster.de/files/9/5/938_ scientific_paper_cyber_physical_systems_in_logistics.pdf

31. K. Morik, et al., "Collaborative research centre on resource constrained machine learning", 2015, http://www.sfb876.tu-dortmund.de

32. "National Instruments: Overview of structural health monitoring solutions", 2014, www.ni. com/white-paper/8426/en/pdf

33. Tyagi. Amit Kumar, "Cyber physical systems (cpss) â [euro]" opportunities and challenges for improving cyber security", International Journal of Computer Applications, 2016,137 (14).

34. Meghna Manoj Nair, Tyagi Amit Kumar, Richa Goyal, "Medical Cyber Physical Systems and Its Issues, International Conference on Recent Trends in Advanced Computing 2019, ICRTAC 2019, Procedia Computer Science 00 (2019) 000–000, 2019.

35. Shah Ahsanul Haque,Syed Mahfuzul Aziz, Mustafizur Rahman,"Review of Cyber-Physical System in Healthcare", International Journal of Distributed SensorNetworks, 2014.

36. Chunxiao Li, A. Raghunathan, and N.K. Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on, pages 150–156, June 2011.

37. D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zeropowerdefenses. In Security and Privacy, 2008. SP 2008. IEEE Symposium on, pages 129–142, May 2008.

38. Chun-Hao Lo and Nirwan Ansari, "The Progressive Smart Grid System from Both Power and Communications Aspects", IEEE Communications Surveys & Tutorials, Vol. 14, No. 3, Third Quarter 2012.

39. Zhuo Lu, Xiang Lu, Wenye Wang, and Cliff Wang. Review and evaluation of security threats on the communication networks in the smart grid. In MILITARY COMMUNICATIONS CONFERENCE, 2010- MILCOM 2010, pages 1830–1835. IEEE, 2010.

40. Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC), 14(1):13, 2011.

41. Andres Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel ´ Cecchet, and David Irwin. Private memoirs of a smart meter. In Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building, pages 61–66. ACM, 2010.

42. Eric Byres and Justin Lowe. The myths and facts behind cyber security risks for industrial control systems. In Proceedings of the VDE Kongress, volume 116, 2004.

43. Ellen Nakashima and Steven Mufson. Hackers have attacked foreign utilities, cia analyst says. Washington Post, 19, 2008.

44. FOX News Network. Threat to the grid? details emerge of sniper attack on power station. http://www.foxnews.com/politics/2014/02/06/ 2013- sniper-attack- on- power- grid- still-concern-in-washington-andfor-utilities/, 2014.

45. InvestmentWatch. First time in history, a terrorist attack on the electric power grid has blacked-out an entire nation in this case yemen. http: //investmentwatchblog.com/first-time-in-history-a-terrorist-attack-onthe - electric - power- grid - has - blacked - out - an - entire - nation - in - this - case-yemen, 2014.

46. https://auto.economictimes.indiatimes.com/news/industry/the-future-of-autonomous-vehicles-in-india-steering-the-legal-issues/64985989.

47. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, HovavShacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In USENIX Security Symposium, 2011.

48. Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. Security threats to automotive can networks — practical examples and selected short-term countermeasures. In Proceedings of the 27th International Conference on Computer Safety, Reliability, and Security, SAFECOMP '08, pages 235–248, Berlin, Heidelberg, 2011. Springer-Verlag.

49. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In Security and Privacy (SP), 2010 IEEE Symposium on, pages 447–462, May 2010.

50. Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In Cryptographic Hardware and Embedded Systems-CHES 2013, pages 55–72. Springer, 2013.

51. D. Mourtzis, "Challenges and future perspectives for the life cycle of manufacturing networks in the mass customisation era", Springer Berlin Heidelberg,2016.

52. Symantec Security Response. Dragonfly: Western energy companies under sabotage threat. http://www. symantec.com/connect/ blogs/ dragonfly-western-energy-companies-under-sabotage-threat, 2014.

53. Alvaro A Cardenas, Saurabh Amin, and Shankar Sastry. Research ´ challenges for the security of control systems. In HotSec, 2008.

54. Cristina Alcaraz and SheraliZeadally. Critical control system protection in the 21st century: Threats and solutions. 2013.

55. Igor NaiFovino, Andrea Carcano, Marcelo Masera, and Alberto Trombetta. An experimental investigation of malware attacks on scada systems. International Journal of Critical Infrastructure Protection, 2(4):139–145, 2009.

56. M.Khalil, Ahmad Yousef, Anas AlMajali,Salah Abu Ghalyon,Waleed Dweik,and Bassam J. Mohd1 "Analyzing Cyber-Physical Threats on Robotic Platforms", Sensors (Basel, Switzerland), vol. 18,5 1643, 21 May. 2018, doi:10.3390/s18051643

57. Chowdhury, Abdullahi, GourKarmakar and JoarderKamruzzaman. "Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches." Detecting and Mitigating Robotic Cyber Security Risks. IGI Global, 2017. 284-299. Web. 30 Oct. 2019. doi:10.4018/978-1-5225-2154-9.ch019.

58. https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/advanced_avionics_handbook/media/aah_ch04.pdf

A. Vuorio, T. Laukkala, I. Junttila, R. Bor, B. Budowle, E. Pukkala, and A. Sajantila, "Aircraft-Assisted Pilot Suicides in the General Aviation Increased for One-Year Period after 11 September 2001 Attack in the United States", International journal of environmental research and public health, 15(11), 2525, doi:10.3390/ijerph15112525, 2018.

59. Kumar, Kadupukotla Satish and P. S. Ramaiah. "Hazard Analysis and Metrics Identification for Software Safety in Medical Cyber-Physical Systems", 2016.

60. Cyber-Security in Smart Grid: Survey and Challenges Z. Elmrabet1, H. Elghazi1, N. Kaabouch2, H. Elghazi1, https://arxiv.org

61. Amara, Dinesh &Chebrolu, Naga & R, Vinayakumar&Kp, Soman. (2018). A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities.

62. Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, Shankar Sastry, "highAttacks against process control systems: risk assessment, detection, and response", ASIACCS '11 Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security,355-366.

63. Francisco J. Rodríguez Lera, Camino Fernández Llamas, Ángel Manuel Guerrero and Vicente Matellán Olivera, "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety", DOI: 10.5772/intechopen.69796.

64. https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/phak/media/04_phak_ch2.pdf.

APPENDIX

S. No	Cyber Physical Systems	Cyber Security	Artificial Intelligence	Machine Learning	Deep Learning	Future work	Attacks	Severity of risks
1	medical physical systems	yes	yes	yes	yes	In the decision making and feedback field, the control / actuation portion of CPS is still largely dependent on the manual intervention of healthcare professionals.[35]	Replay attacks [36], privacy invasion [36], DoS [37], false data and unauthorized commands injection [36].	Less [60]
2	Smart Grid	yes	yes	yes	yes	IoT devices can be designed to make them compact, cost-effective, energy-efficient and robust. In order to improve performance and security, progressive communications protocols may also be investigated. It is possible to further develop monitoring systems for power generation plants, pumps and turbines.[38]	Denial of Service (DoS) [39], false data injection [40], loss of customer personal information [41], untargeted malware [42], Cyber extortion [43], Vandalism [44], terrorist attacks [45].	Critical [61]
3	autonomous automobile systems	yes	yes	yes	----	Innovation and automation are the future of the automotive sector. This is why most automotive players now focus on driverless /	Malware injection via cellular network [47],malware injection via OBD-II port [48],packet	Medium [62]

						autonomous cars (AVs).[46]	injection [49],malware injection via Bluetooth [47], ABS Spoofing [50], Replay attacks [49],DoS [48,49], false data injection [49],privacy invasion [47].	
4	process control systems	yes	yes	yes	yes	Reduced process and lifecycle acquisition costs, innovative ways for data models.[51]	Dragonfly attack [52], unintentional attack [53], night dragon attack [54], Modbus worm [55].	High [63]
5	distributed robotics	yes	yes	yes	----	Identify the causes of vulnerabilities on adopt mobilerobots platforms of robotics software [56]	DoS attacks, extortapalooza public shaming, extortion attack, impersonation attack, sybil attack [57].	Severe [64]
6	automatic pilot	yes	yes	-----	yes	adopt more precise GPS guided system.[58]	Aircraft attacks, terrorist attacks [59].	Less [65]

Table 1: Different types of attacks occur in various Cyber Physical Systems.