Security Trends and Advances in Manufacturing Systems in the Era of Industry 4.0

Sujit Rokka Chhetri, Nafiul Rashid, Sina Faezi, Mohammad Abdullah Al Faruque
{schhetri, nafiulr, sfaezi, alfaruqu}@uci.edu
Department of Electrical Engineering and Computer Science
University of California, Irvine, California, USA

ABSTRACT

The next industrial revolution will incorporate various enabling technologies. These technologies will make the product lifecycle of the manufacturing system *efficient*, *decentralized*, and *well-connected*. However, these technologies have various security issues, and when integrated in the product lifecycle of manufacturing systems can pose various challenges for maintaining the security requirements such as *confidentiality*, *integrity*, and *availability*. In this paper, we will present the various trends and advances in the security of the product lifecycle of the manufacturing system while highlighting the roles played by the major enabling components of Industry 4.0.

1. INTRODUCTION

The fourth industrial revolution is transforming the next generation of manufacturing systems by making it *smarter*, *well-connected*, *self-organized*, *decentralized*, and *flexible*. This is made possible by the incorporation of Cyber-Physical Systems (CPS) for monitoring and controlling the machines, and the use of Internet of Things (IoT) for connecting various components of the manufacturing plant to the Internet, which are two of the major enabling technologies. This transformation is happening at a rapid pace and industrial sectors are already planning to commit US$ 907 billion per annum to Industry 4.0 [1], also known as *Smart Factory*, *Industrial Internet of Things*, etc. Furthermore, 85% of the companies are estimated to implement Industry 4.0 solutions in their businesses [2]. It is estimated that the early adopters of Industry 4.0 concepts will see both revenue gain and cost reduction of the process by 30% [1]. The major and exciting change brought upon by the Industry 4.0 will be a complete end-to-end digitization and re-organization of vertical and horizontal value chains of the manufacturing supply chain and product lifecycle [3]. Moreover, Gartner predicts that digitization will be a major trend, where almost all the physical part of the industry will have a virtual representation [4]. This will be made possible by an influx of Industrial IoTs, making large amount of data available for analysis.

The rosy prospects forecasted by the adoption of various technologies for the Industry 4.0, however, comes laden with various challenges, one of them being the security of the manufacturing systems. Due to the heavy automation and monitoring using CPS, end-to-end digitization, distributed and well-connected components using IoT, to name a few, the challenge for securing manufacturing systems will also rise [1]. The product lifecycle of manufacturing systems has always been challenged by various threats (such as *product tampering*, *service interruption*, *infiltraion*, *intellectual property loss*, etc.) [5]. In fact, manufacturing has consistently been among the top three industries to be targeted by spear phishing attacks [6]. On average 20.1% of industrial computers are attacked by a malware every month [7]. Furthermore, incidents such as attack on German steel mill [8], Maroochy water breach [9], Stuxent [10], to name few have highlighted the crippling effects of attacks on industrial sectors.

Integrating the new technologies will make the infrastructure of the manufacturing system more susceptible to new forms of attacks [11, 12]. Researchers have started highlighting these issues and providing some solutions to secure smart manufacturing [13]. In earlier works, security has been analyzed either in terms of individual enabling components [14–16], highlighted as just one of the challenges for Industry 4.0 [17, 18]); presented without the context of enabling technologies for Industry 4.0 [19, 20]; and analyzed in terms of the standardization frameworks [21, 22]. In our work, we present the current trends and advances to highlight the challenges and solutions associated with securing the manufacturing systems in the context of Industry 4.0. To achieve this, we will present the security challenges and proposed solutions in the context of the enabling technologies and the product lifecycle of the manufacturing system. In Section 2, we will present some of the enabling technologies, in Section 3, we will present the stages of the next generation of the product lifecycle, and the corresponding risks associated with each of the stage. In Section 4, we will present the various security solutions that industry, researchers, and various organizations have proposed to secure the next generation of manufacturing product lifecycle, and finally we provide concluding remarks in Section 5.

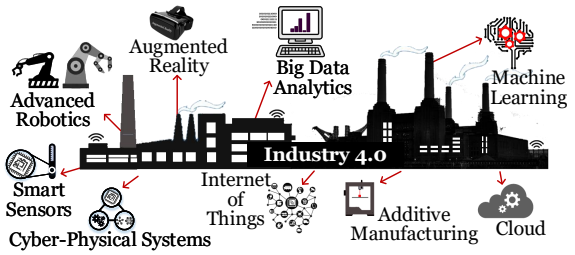

Figure 1: Major Enabling Components of Industry 4.0.

2. INDUSTRY 4.0

Industry 4.0 consists of various enabling components and concepts (see Figure 1). In this section, some of the core technologies and concepts are briefly described and their corresponding security issues are highlighted.

2.1 Enabling Components of Industry 4.0

Cyber-Physical Systems: Cyber-Physical Systems are a new generation of automated systems that provide a tight

integration of the physical world (real systems) with cyberspace (computing and communication infrastructure). Among numerous applications of CPS, few of the noteworthy examples are smart grid, autonomous driving, health care, industrial process control systems, robotics, and aerospace. In Industry 4.0, CPS will be heavily utilized for monitoring and actuating various components.

Internet of Things: CPS connected to the Internet is often referred to as the "Internet of Things (IoT)" [23]. The IoT is an inter-networking of physical objects (sensors, machines, cars, buildings, and other items) that allows interaction and cooperation of these objects to collect and exchange data over the Internet [24]. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications [25] in the context of Industry 4.0.

Big Data Analytics: Big data consists of high volume, high veracity, and/or high variety of data. In manufacturing systems, there are large, diverse, structured or unstructured data that are produced by smart sensors, devices, log files, video and audio in real time. They are produced in various automation levels and by the manufacturing plant, transaction applications, etc. With incorporation of CPS and IoT, the amount and variety of data produced will be vast. In fact, in Industry 4.0, big data is expected to consist of six major properties (6C):*connection* (sensor and networks), *cloud* (data on demand), *cyber* (model and memory), *content/context* (meaning and correlation), *community* (sharing and collaboration), and *customization* (professionalization and value) [26].

Cloud Computing: National Institute of Standards and Technology (NIST) defines cloud computing as "on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service" [27]. With large amount of data production from the manufacturing system, distributed and decentralized form of manufacturing, the data management in Industry 4.0 will have to traverse locations, countries and even continents. Moreover, the near real time big data analytics will require flexible, efficient, and secure ways of providing the accessibility of data to all components of the smart manufacturing ecosystem.

Additive Manufacturing: Additive manufacturing (or 3D Printing) has recently gained popularity due to its capability to rapidly prototype free-form 3D objects. In Industry 4.0, The value added by 3D printing will be in *decentralized* and *flexible* manufacturing with *mass customization*, *energy optimization*, reduction of product lifecycle from *just-in-time* to *just-in-place* manufacturing, etc.

Smart Sensors: Smart sensors do not just play the role of measurement, but also consist of their own microprocessors, network chip , micro-controllers or digital signal processors to carry out complex signal processing and support some form of edge computing. These sensors will ease the task of sensor fusion by supporting smart plug and play features in an industrial environment to support both new generation of manufacturing systems, and the legacy systems. Currently, 40% of the company do not have visibility to the real-time status of their company [28]. In this scenario, smart sensors will play a crucial role in sensing and digitizing all the components of the manufacturing plant.

Machine Learning (ML): The third industrial revolution started with the automation of systems for production, and elimination/limitation of human labor in the factory floor. The major focus in automation went into hard-coding proper reactions of the manufacturing system under each possible condition. Recently, due to the overwhelming amount of data gathered from different stages of an industrial process, rather than hard-coding automation, various machine learning algorithms and tools have been adopted for performing much needed analysis of the manufacturing systems. In the context of Industry 4.0, big data collected from the industrial plant will be analyzed and various machine learning tools will be used for building a smart manufacturing system.

Advanced Robotics: In recent years, there is a huge amount of advancement in the field of robotics. Smart robots have been proposed to not only handle the complicated tasks but also learn from each other's mistakes and improve their performance [29]. Advanced robotics are already being merged to industry for enabling the required robotic infrastructure for the fourth industrial revolution [30].

Augmented Reality: Augmented Reality (AR) is a promising technology for Industry 4.0. Authors in [31] have proposed a framework for using AR to enhance the maintenance and support procedure of high-end manufactured products. Authors in [32] have introduced a novel approach that combines laser writers with AR to create a human-robot interactions interface which surpasses many limitations of current interfaces of advanced robots.

2.2 Security in Manufacturing Systems

The security system for Industry 4.0 needs to *identify* risk, implement appropriate safeguards to *protect* critical infrastructures, *detect* occurrence of security events, *respond* to threats, and *recover* after an attack has happened [33]. Various standards such as Reference Architecture Model Industry 4.0 (RAMI 4.0) [34], Industrial Internet Reference Architecture (IIRA) [35] provide the framework for Industry 4.0; however, further analysis is required to view security in terms of the enabling technologies in the product lifecycle. In order to do so, we will present three fundamental security requirements for the next generation of smart manufacturing.

Confidentiality: It involves maintaining the privacy of the information flow throughout the horizontal and the vertical value chains of the manufacturing system. In Industry 4.0, there will be a many information flows which could be tapped by attackers. Confidentiality loss can be costly for a company, they could lose customer's data, intellectual property, trade secrets, etc.

Integrity: Compared to the traditional Information Technology (IT) security, due to the Operation Technologies (OT) having tighter integration with the IT infrastructure, the integrity of the manufacturing system can be easily affected by the cyber attacks. Integrity not only involves *consistency,accuracy* and *trustworthiness* of the information flowing through the manufacturing system but also the consistency and trustworthiness of the physical components throughout the product lifecycle.

Availability: Various forms of cyber and physical attacks can cause the manufacturing system to be out of service. In a well-connected Industry 4.0, an attack on the availability may be mitigated due to the distributed architecture. Nonetheless, coordinated denial of service attacks can render various components of the product lifecycle to be disabled at the same time, causing the entire process chain to halt.

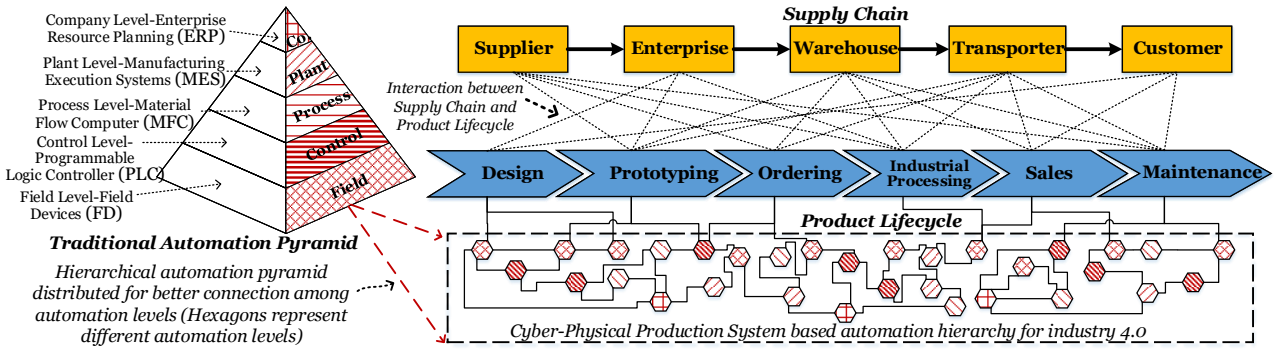

Figure 2: Product Lifecycle for Industry 4.0.

2.3 Security of Enabling Components

Cyber-Physical Systems: Currently, most of the security challenges in CPS are centered around the Supervisory Control And Data Acquisition (SCADA) security [36]. The reason behind this is the architecture of the SCADA system itself. For increased level of productivity in Industry 4.0, the SCADA system is connected to the Internet. These connections are provided over standard protocols, such as Internet Protocol (IP) and Transmission Control Protocol (TCP), which have known vulnerabilities [37] including IP spoofing or man-in-the-middle-attacks. SCADA systems use this TCP/IP protocols without additional protection against this TCP/IP vulnerabilities. Moreover, there are various cross-domain security issues as well [38].

Internet of Things: In IoT, various security challenges arise, including: authentication and access control, confidentiality, privacy, secure middleware, trust. [39]. As IoT is Internet enabled, it is obvious that the inherent security issues of the Internet will also be prevalent in IoT [40].

Big Data Analytics: Big data analytics acquire large amounts of data from customers, designers, suppliers, factory, etc. Due to this, there is an inherent problem of securing it. There are various security challenges associated with big data analytics such as: secure computations in distributed environment, secure data storage and transaction logs, cryptographically enforced access control. [41, 42].

Cloud Computing: There are various security issues associated with the services provided by cloud computing [43]. Some of the issues are denial of service, data loss, advanced persistent threats, malicious insiders, account hijacking, interface hacking, etc.

Additive Manufacturing: The security of additive manufacturing is spread over the triad of confidentiality, integrity and availability [44]. Some of the issues are intellectual property theft [45], attack on the integrity of the materials [46], etc.

Smart Sensors: Smart sensors consist of computation and communication components. Unlike simple sensors which just measure data, smart sensors have a larger attack surface due to the addition of components that make it smart. These extra threats imply better protocols and standards are required to maintain their security.

Machine Learning (ML): The lifecycle of ML models consists of two stages: training and inference. An ML model can be subject to security attacks in any of these two stages [47]. In the training stage, an attack on the integrity of the system may guide the learning process toward a vulnerable model which has hazardous outputs under a particular set of inputs. On the other hand, in the inference stage, an attacker may aim for extracting confidential information embedded in the model (such as training data) or forcing the model to mispredict often by using adversarial samples which in turn, would convince the user to bypass the model because of its poor performance [48].

Advanced Robotics: State-of-the-art robots in industry are cooperative entities. Each entity is a combination of a mechanical structure, actuators, sensors, computation hardware/software, and various types of networks connecting different parts with one another. In this setting, not only is each of the components prone to conventional cyber threats, but also the mixture of the components causes new security issues. For instance, spoofing and triggering the system for certain malicious behaviors is possible through sensor manipulation [49].

Augmented Reality: AR inherits all of the security challenges from smartphones, as it borrows most of its components from them. However, it has a near-eye display with a more comprehensive set of sensors which add new types of security challenges to the system. These new challenges mostly fall into two categories [50]: input and output. A malicious application can gather a user's private information [51] or a company's sensitive data from different sources such as the screens of computers [52] or visible and hearable moving parts of machines running in the surrounding environment.

In summary, each of the enabling technologies consists of various security issues and challenges, listing all of them is out of the scope of this paper. However, in the next section we will highlight how these enabling technologies will fit into the product lifecycle, and what security issues and challenges they will present for the next generation manufacturing product lifecycle.

3. SECURITY AND THE PRODUCT LIFECYCLE

The product lifecycle for Industry 4.0 along with the proposed decentralized and interconnected automation hierarchy [53] is shown in Figure 2. Compared to the traditional automation pyramid, there will be decentralized information flow, which means there will be better connectivity among various levels, and better visibility of the various stages of the product lifecycle. This will make the chains more dynamic in performance, but will introduce various security issues.

Stage 1. Design: This is the first stage of the product lifecycle. It involves taking specification from customers or analyzing the need of the customers, performing research

and development on initial ideas, and tuning the models in various iteration. In the context of enabling components of Industry 4.0, the various security issues associated with this stage of manufacturing system are as follows:
Confidentiality: The design stage will rely heavily on big data and the cloud for gathering and storing information from customers, about the past products, and share initial conceptual ideas to the enterprise. Moreover, Computer Aided Design (CAD) tools are being provided as a service in the cloud. Sharing the CAD designs over the cloud poses a security risk for intellectual property theft [54]. In situations where the CAD tool has already been infected by a worm to infect and steal AutoCAD drawings [55], moving services over the cloud can have big consequences.
Integrity: Work in [56] has demonstrated how the use of 3D designs of CAD models meant for 3D Printing can be surreptitiously modified to compromise the structural integrity of the products.
Availability: Various Ransomwares [57] have already caused denial of service for designers. Moreover, attacks on cloud services can halt the design stage when companies rely on cloud computing.

Stage 2. Prototyping: The objectives of design prototyping in industry are: *testing* and *evaluating* the design for flows, *cost estimation*, *patenting*, etc. In this stage, the virtual model is converted into machine instructions by Computer Aided Manufacturing (CAM) tools to be realized by a rapid manufacturing technology such as 3D printing. Below, we list the security concerns regarding this stage in terms of CIA:
Confidentiality: In this stage, the designs are vulnerable to conventional cyber attacks to CAM software, which might be running on cloud [58], the network media connecting the printer to the CAM tool, and the firmware running on the 3D printer [59]. Furthermore, various attack models have been proposed to take advantage of physical structure of CPS. For instance, authors in [60–64] have demonstrated how to utilize acoustic, vibration, electromagnetic, and thermal, etc., analog emissions from the 3D printer to reconstruct and steal the geometrical design information of the product.
Integrity: Authors in [44, 65] have infected either the CAM tool or firmware of the 3D printer, and were able to compromise the integrity of the printed object.
Availability: In rapid prototyping, a failure to create the object (when using 3D printing, for example) may occur due to various reasons such as flaws in the designed object, and errors in parameters of the manufacturing system. An attacker can utilize these flaws to surreptitiously infect the system and cause it to be unavailable.

Stage 3. Ordering: Ordering is defined as the process to obtain materials and/or services of the right quality in the right quantity from the right source, deliver them to the right place at the right price. Some of the security issues in this stage include:
Confidentiality: Intelligent attackers use the less secured third party suppliers and vendors as a gateway to get access to the host organizations. Enabling components like cloud computing and IoT introduces more confidentiality vulnerabilities [66]. Once breached, the attackers gain access to the organization's sensitive data, therefore violating the confidentiality. Various confidential information-like quotations from different vendors for a particular contract may then get leaked and hamper the whole ordering process.
Integrity: The attackers, sometimes even malicious vendors, might manipulate the ordered services or replace original materials with a counterfeit one to modify the integrity of the ordered products. With the emergence of enabling technologies like cloud computing, many companies rely on the online-based cloud services from third parties or external vendors. These companies are mostly subject to this integrity attack.
Availability: The availability of the ordered cloud-based service might be at stake when the cloud computing infrastructure breaks down due to a DoS attack [67] or gets blocked by ransomware attacks [57].

Stage 4. Industrial Processing: The enabling components of Industry 4.0 like CPS and IoT have contributed a lot to the growing use of information technology in manufacturing/industrial environment. However, to integrate these new components, the existing industrial control processes require additional *communication paths*, *unverified ad-hoc solutions*, and (often) connection to *low level Supervisory Control And Data Acquisition* systems. Thus, the opportunities introduced by Industry 4.0 puts the entire confidentiality, integrity, availability of a system at risk [7].
Confidentiality: With the enabling technologies like CPS, IoT, cloud computing, 3D printing the whole industrial process is now more connected and open. This openness creates a threat to the confidentiality of the system mostly towards the intellectual property theft. Researchers have shown that the digital design of a 3D printed model can be regenerated from acoustic side channel attacks [61] leading to intellectual property theft of a company.
Integrity: The 3D printing can be easily manipulated by code injection to a design file leading to erroneous printing [68]. Factories incorporating advanced robotics or smart sensors for their factory automation are also prone to integrity modifications via different cyber attacks or sensor tampering [49].
Availability: Attacks on enabling technologies like CPS, IoT, smart sensors and cloud computing can cause the manufacturing plant to be unavailable as well [69].

Stage 5. Sales: This stage is closest to the customers and thus can give input about the behavior of the customers, the market segments, the demand patterns per segment, etc. Sales is the stage which determines the future market demand, also known as the forecast. It also encompasses distribution strategy, transportation planning, physical material flows and inventory levels at distribution centers. In short, this stage directly impacts every product lifecycle stages starting from product design to distribution. Therefore, the risk associated with this stage is also higher.
Confidentiality: Confidentiality is the key security concern in this stage as it deals with various sensitive information like: customer feedbacks, market surveys, estimated revenue, annual sales report. If any malicious attackers get access to the sensitive sales information compromising the confidentiality of a company, the company's future might be at stake. Unfortunately, enabling components like big data and cloud computing may open back doors for the attackers [70].
Integrity: If an adversary gets access to the sophisticated data through the loopholes created by cloud computing, big data or IoT, and alter the data, the integrity of the infor-

mation will then be compromised. Any decision or forecast made based on this corrupted information will lead to wrong decisions and predictions by the management. We refer to this situation as "Forecast Avalanche". Thus, the whole supply chain process will suffer just because of a simple alteration of sophisticated data.
Availability: Moreover, there is another kind of cyberattack called 'Ransomware' that affects the confidentiality and availability of the information. Attackers getting access to the victim's data threatens to expose or block access to the data until a ransom is paid [71].

Stage 6. Maintenance: Maintenance is the process which ensures that a system performs its required functions at the standard level of safety and reliability. Due to the decentralized nature of Industry 4.0, various security issues can arise in this stage.
Confidentiality: In this stage, there is a strong possibility of the costumer's confidential information being leaked when the company uses enabling technologies such as IoT or Augmented Reality for maintenance. For instance, the use of cameras on AR devices to snoop over private data has previously been highlighted [52]. Attackers could attack these enabling technologies to breach the confidentiality. In addition, machine learning models created from the data collected from the users may be attacked to extract information using adversarial samples [48].
Integrity: Companies need to choose a right and reliable partner for outsourcing maintenance work to ensure that the replaced parts are genuine. If the partner company is not reliable, they might replace the piece with a defected part to gain extra profit and, effectively, compromise the integrity [72].
Availability: In case of outsourcing, the outsource company has access to the parameters of the product under maintenance. A change in these parameters might increase the maintenance requirements of the product which leads to less availability of the product and more profit for the outsource company. Industry 4.0 also tries to use a network maintenance system instead of technicians, but this ends up increasing the DoS attacks. These attacks can make the maintenance service become unavailable for a long time.

4. SECURITY TRENDS

In order to tackle the security issues associated with the incorporation of the enabling technologies for the product lifecycle, various security solutions have also been proposed. In this section, we will highlight the advances made in securing the product lifecycle with the incorporation of the enabling technologies.

Stage 1. Design: Beside the standard protocols and framework from ISO, IEC, ASME, etc., that provide frameworks for best practices of design modeling for manufacturing systems, there are various works that also consider securing designs when various enabling technologies are used.
Confidentiality: Work in [73] describe methods to maintain the confidentiality of the designs and use 3D printing as a method for validation. Standards such as ISO/ASTM 52915, describe a framework for sharing design information for 3D printing. [74] propose method for transferring data securely in cloud computing environment. Solutions such as AutoDesk vault [75] are providing access control to secure the CAD files in the cloud.
Integrity: There are various works [76], which aim at making sure the designs shared through the network or cloud maintain their integrity.
Availability: Works such as [77] describe methods to make sure that cloud sources are protected from denial of service attacks.

Stage 2. Prototyping: The prototyping stage is a tight integration of cyber components such as CAM tools, embedded software/hardware, network systems, IoT, and also physical components such as mechanical parts and actuators. Various works have been conducted to provide security solutions while considering this tight coupling.
Confidentiality: Authors in [78] have evaluated the possibilities for increasing trustworthiness of software, network, embedded software/hardware, and IoT, respectively. Authors in [79] have shown how a novel CPS approach embedded in the CAM tool using machine learning can significantly decrease the amount of information leaked from the 3D printers while prototyping.
Integrity: Various approaches have been suggested to assure the integrity of the printed object in the prototyping stage. Authors in [80] have used visible light sensing for verification of the printed object, while authors of [46] and [81] have suggested monitoring the 3D printer via analog sidechannels to assure the structural integrity of the product. Also, authors in [82] have proposed a reverse engineering methodology for validation of the printed objects that can also be utilized for integrity assurance of the system.
Availability: Besides the commonly known tools such as [83] designed to help improve the availability of web-based services, authors in [84] have suggested using six tools to evaluate vulnerabilities and demonstrated them with code from open source projects.

Stage 3. Ordering: The various measures taken to defend the ordering stage from the known security challenges include:
Confidentiality: To protect the confidentiality of the information, the vendors must be aligned to follow a specific set of rules provided by the host organizations. Companies that are using various cloud-based services should especially impose or adapt strict rules to protect them from cloud-based threats [74].
Integrity: To maintain the integrity of the products supplied by the vendors, organizations can initiate vendor management programs that will include identifying the most critical vendors, selecting a primary contact, establishing guidelines and controls, and finally integrating them with the organization's practices [5].
Availability: Various initiatives have been taken to guard the cloud-based services against DoS [77] or ransomware attacks [57].

Stage 4. Industrial Processing: The International Society of Automations ISA99 committee has been working to define security standards for industrial automation and control systems since 2007. In 2010, these standards were aligned with the corresponding International Electrotechnical Commission (IEC) standards to become the ISA/IEC 62443 series. However, these standards are not yet fully sufficient for Industry 4.0. Meanwhile, responsible automation hardware/software suppliers have taken initiatives in developing innovative solutions to the problems of cyber-physical

production system security, and have addressed the issues in a variety of ways.

Confidentiality: To protect the industrial control systems from threats, different organizations have undertaken projects such as uTRUSTit (Usable Trust in the Internet of Things) [85] and the iCore project [86] for IoT and CPS, to maintain the confidentiality of the system.

Integrity: For maintaining the integrity, works such as [87] discuss how to protect CPS, IoT or 3D printing against various side channel attacks.

Availability: The availability of a system can be achieved by guarding the system against various DoS attacks. [88] shows some ways to defend against these attacks.

Stage 5. Sales: This stage is mostly vulnerable to information security attacks. However, other issues regarding security have also been studied.

Confidentiality: The confidentiality in this stage is mostly vulnerable due to the cloud-based services handling different sophisticated information.

Integrity: To preserve the integrity, organizations should prepare more robust defense. A small breach to the information can have terrible consequences. Different solutions [89] proposed by the researchers should be adapted to preserve the integrity of critical information.

Availability: As mentioned earlier, availability in this stage is mostly related to various DoS and ransomware attacks on cloud computing infrastructure. Works in [77] provide ways to secure the cloud, which could lead to avoiding DoS and ransomware attacks.

Stage 6. Maintenance: The shift in the maintenance stage toward using new technologies such as big data, smart sensors, cloud computing, machine learning, IoT, and AR has raised many new security concerns as it is discussed in Section 3. Various advances in solving these issues are as follows:

Confidentiality: Securing the cloud [90] can ensure confidentiality of the user side data gathered in the maintenance phase over the cloud. New operating systems for augmented reality devices such as [91] can limit the access of the system to the surrounding environment of the user. This limitation on access will eliminate the chance of a malicious program from misusing private information from the root. Machine learning models as presented in [92] can also protect user information.

Integrity: Work presented in [93], provide a mechanism for ensuring that the procedure displayed on the screen of the augmented reality device is the same as in the physical world. Works presented in [94] help in protecting the machine learning models from external manipulation and can aid in securing the system and product health monitoring in maintenance stages to prevent faulty analysis. Works in [95] address the issues regarding the trustworthiness of the parts replaced in the product.

Availability: Similar to other stages, once the maintenance phase immigrates over the cloud and network, the availability concerns can be tested and addressed by [77]. Also, it is worth mentioning that using the enabling technologies such as AR and machine learning would shorten the required maintenance time, which in turn would improve the availability of the product.

5. CONCLUSION

In summary, the fourth industrial revolution will bring about various changes to the manufacturing system. However, it will also add various security challenges to the product lifecycle of the manufacturing system. In this paper, we presented various enabling technologies for Industry 4.0, explained their respective security issues, presented security issues in the product lifecycle in terms of enabling components, and highlighted the advances made in securing the enabling components for the product lifecycle of the manufacturing system. By presenting the current issues and solutions for securing the the product lifecycle, this paper aims to highlight the current efforts in securing the next generation of manufacturing systems.

6. REFERENCES

[1] R. Geissbauer, J. Vedso, and S. Schrauf, "Industry 4.0: building the digital enterprise: 2016 global industry 4.0 survey," *PwC, Munich*, 2016.

[2] I. Deloitte, "Industry 4.0–challenges and solutions for the digital transformation and use of exponential technologies," *White Paper*, 2014.

[3] S. Schrauf and P. Berttram, "Industry 4.0 and how digitization makes the supply chain more efficient, agile, and customer-focused." www.strategyand.pwc.com, 2016.

[4] K. Panetta, "Gartner top 10 strategic technology trends for 2017." http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/, 2016.

[5] D. Shackleford, "Combatting cyber risks in the supply chain," *SANS. org*, 2015.

[6] Symantec, "Internet security threat report," 2016.

[7] K. Lab, "Threat landscape for industrial automation systems in the second half of 2016," 2016.

[8] R. M. Lee, M. J. Assante, and T. Conway, "German steel mill cyber attack," *Industrial Control Systems*, vol. 30, 2014.

[9] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *Critical infrastructure protection*, 2007.

[10] C. E. Falliere N, Murchu LO, "W32.stuxnet dossier. symantec security response.." https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2011. [Accessed August 06, 2017].

[11] RadarServices, "Competence series: Industry 4.0 = security 4.0?," *RadarServices Smart IT-Security GmbH*, 2015.

[12] R. Waslo and L. a. Tyler, "Industry 4.0 and cybersecurity: Managing risk in an age of connected production," *Deloitte. University Press*, 2017.

[13] L. Thames and D. E. Schaefer, *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing.* Springer, 2017.

[14] G. Manogaran, C. Thota, *et al.*, "Big data security intelligence for healthcare industry 4.0," in *Cybersecurity for Industry 4.0*, Springer, 2017.

[15] D. Glavach, J. LaSalle-DeSantis, *et al.*, "Applying and assessing cybersecurity controls for direct digital manufacturing (ddm) systems," in *Cybersecurity for Industry 4.0*, Springer, 2017.

[16] Y. Wang, O. Anokhin, *et al.*, "Concept and use case driven approach for mapping it security requirements

on system assets and processes in industrie 4.0," *Procedia CIRP*, 2017.

[17] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *Journal of Industrial Information Integration*, 2017.

[18] I. D. L. Bogle, "A perspective on smart process manufacturing research challenges for process systems engineers," *Engineering*, 2017.

[19] D. Prokop, *Global Supply Chain Security and Management: Appraising Programs, Preventing Crimes*. Butterworth-Heinemann, 2017.

[20] J. Smith and J. Teuton, "What do you mean, supply chain security? a taxonomy and framework for knowledge sharing," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[21] H. Flatt and S. a. Schriegel, "Analysis of the cyber-security of industry 4.0 technologies based on rami 4.0 and identification of requirements," in *International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, 2016.

[22] Z. Ma, A. Hudic, *et al.*, "Security viewpoint in a reference architecture model for cyber-physical production systems," in *European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2017.

[23] N. Jazdi, "Cyber physical systems in the context of industry 4.0," in *Automation, Quality and Testing, Robotics*, IEEE, 2014.

[24] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, 2010.

[25] J. HÃűller, V. Tsiatsis, *et al.*, *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Elsevier, 2014.

[26] J. Lee, B. Bagheri, *et al.*, "Recent advances and trends of cyber-physical systems and big data analytics in industrial informatics," in *International Proceeding of Int Conference on Industrial Informatics (INDIN)*, 2014.

[27] P. Mell, T. Grance, *et al.*, "The nist definition of cloud computing," 2011.

[28] G. Johnson, "Intelligent sensor technology and the cloud," 2016.

[29] S. Nolfi, J. C. Bongard, P. Husbands, and D. Floreano, "Evolutionary robotics.," 2016.

[30] M. A. K. Bahrin and M. F. o. Othman, "Industry 4.0: a review on industrial automation and robotic," *Jurnal Teknologi*, 2016.

[31] D. Mourtzis, V. Zogopoulos, and E. Vlachou, "Augmented reality application to support remote maintenance as a service in the robotics industry," *Procedia CIRP*, 2017.

[32] D. Q. Huy, I. Vietcheslav, and G. S. G. Lee, "See-through and spatial augmented reality-a novel framework for human-robot interaction," in *International Conference on Control, Automation and Robotics (ICCAR)*, IEEE, 2017.

[33] N. I. of standards and technology, "Manufacturing profile: Nist cybersecurity framework," 2016.

[34] M. Hankel and B. Rexroth, "The reference architectural model industrie 4.0 (rami 4.0)," *ZVEI*, 2015.

[35] I. I. Consortium, "Industrial internet reference architecture (iira)," *[Online], Available: http://www.iiconsortium.org*, 2015.

[36] J. Giraldo, E. Sarkar, *et al.*, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design & Test*, 2017.

[37] S. M. Bellovin, "Security problems in the tcp/ip protocol suite," *ACM SIGCOMM Computer Communication Review*, 1989.

[38] S. R. Chhetri, J. Wan, and M. A. Al Faruque, "Cross-domain security of cyber-physical systems," in *Design Automation Conference (ASP-DAC), 2017 22nd Asia and South Pacific*, pp. 200–205, IEEE, 2017.

[39] S. Sicari, A. Rizzardi, *et al.*, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, 2015.

[40] Q. Jing, A. V. Vasilakos, *et al.*, "Security of the internet of things: Perspectives and challenges," *Wireless Networks*, 2014.

[41] C. S. Alliance, "Top ten big data security and privacy challenges," *[Online], Available: http://www.isaca.org*, 2012.

[42] Y. Gahi, M. Guennoun, *et al.*, "Big data analytics: Security and privacy challenges," in *Symposium on Computers and Communication (ISCC)*, IEEE, 2016.

[43] K. Hamlen, M. Kantarcioglu, *et al.*, "Security issues for cloud computing," *Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies*, 2012.

[44] S. E. Zeltmann, N. Gupta, *et al.*, "Manufacturing and security challenges in 3d printing," *Jom*, 2016.

[45] S. R. Chhetri *et al.*, "Side-channels of cyber-physical systems: Case study in additive manufacturing," *IEEE Design & Test*, 2017.

[46] S. R. Chhetri, A. Canedo, and M. A. Al Faruque, "Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems," in *International Conference on Computer-Aided Design (ICCAD)*, IEEE, 2016.

[47] N. Papernot, P. McDaniel, *et al.*, "Towards the science of security and privacy in machine learning," *arXiv preprint arXiv:1611.03814*, 2016.

[48] N. Papernot *et al.*, "Practical black-box attacks against machine learning," in *Asia Conference on Computer and Communications Security*, 2017.

[49] J. McClean, C. Stull, *et al.*, "A preliminary cyber-physical security assessment of the robot operating system (ros)," *SPIE Defense, Security, and Sensing*, 2013.

[50] F. Roesner, T. Kohno, and D. Molnar, "Security and privacy for augmented reality systems," *Communications of the ACM*, 2014.

[51] R. Templeman, M. Korayem, *et al.*, "Placeavoider: Steering first-person cameras away from sensitive spaces.," in *NDSS*, 2014.

[52] H. Kim, H. Kim, *et al.*, "A new technique using a shuffling method to protect confidential documents from shoulder surfers," in *International Conference on Software Security and Assurance (ICSSA)*, IEEE, 2015.

[53] Y. Lu, K. C. Morris, *et al.*, "Current standards landscape for smart manufacturing systems," *National Institute of Standards and Technology, NISTIR*, 2016.

[54] C. Jackson, "Is cad in the cloud truly terrifying?," *http://www.engineering.com*, 2013.

[55] ESET, "Acad/medre.a, eset whitepaper," Retrieved: 2017.

[56] S. Belikovetsky, M. Yampolskiy, *et al.*, "dr0wned-cyber-physical attack with additive

manufacturing," *arXiv preprint arXiv:1609.00133*, 2016.

[57] G. O'Gorman and G. McDonald, *Ransomware: A growing menace*. Symantec Corporation, 2012.

[58] L. Zhang, Y. Luo, *et al.*, "Cloud manufacturing: a new manufacturing paradigm," *Enterprise Information Systems*, 2014.

[59] S. Ravi, A. Raghunathan, *et al.*, "Security in embedded systems: Design challenges," *Transactions on Embedded Computing Systems (TECS)*, 2004.

[60] A. Hojjati, A. Adhikari, *et al.*, "Leave your phone at the door: Side channels that reveal factory floor secrets," in *ACM Conference on Computer and Communications Security*, 2016.

[61] A. Faruque, M. Abdullah, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in *Proceedings of the 7th International Conference on Cyber-Physical Systems*, p. 19, IEEE Press, 2016.

[62] M. A. Faruque, S. Chhetri, S. Faezi, and A. Canedo, "Forensics of thermal side-channel in additive manufacturing systems-semantic scholar," *Irvine, CA*, 2016.

[63] S. R. Chhetri, *Novel Side-Channel Attack Model for Cyber-Physical Additive Manufacturing Systems*. PhD thesis, University of California, Irvine, 2016.

[64] S. R. Chhetri, A. Canedo, and M. Al Faruque, "Confidentiality breach through acoustic side-channel in cyber-physical additive manufacturing systems," *ACM Transactions on Cyber-Physical Systems (TCPS)*, 2016.

[65] H. Turner, J. White, *et al.*, "Bad parts: Are our manufacturing systems at risk of silent cyberattacks?," *Security & Privacy*, 2015.

[66] R. Gellman, "Privacy in the clouds: risks to privacy and confidentiality from cloud computing.," in *Proceedings of the World privacy forum,*, 2012.

[67] M. Armbrust, A. Fox, *et al.*, "Above the clouds: A berkeley view of cloud computing," tech. rep., Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

[68] L. Sturm, C. Williams, *et al.*, "Cyber-physical vunerabilities in additive manufacturing systems," *Context*, 2014.

[69] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *Pervasive Computing*, 2008.

[70] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of network and computer applications*, 2011.

[71] J. Kastrenakes, R. Brandom, *et al.*, "Wannacry ransomware: all the updates on the cyberattack," 2017. [Accessed August 06, 2017].

[72] W. Wilson, "Counterfeit parts: Dangerous and costly." http://www.maintenancetechnology.com/2017/06/counterfeit-parts-dangerous-costly/, April 2017. [Accessed August 10, 2017].

[73] M. Yampolskiy and T. R. a. Andel, "Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing," in *Proceedings of the 4th Program Protection and Reverse Engineering Workshop*, ACM, 2014.

[74] R. Arora, A. Parashar, *et al.*, "Secure user data in cloud computing using encryption algorithms," *International journal of engineering research and applications*, 2013.

[75] Autodesk, "Autodesk vault," https://www.autodesk.co.uk, 2017.

[76] Intel, "Understanding and implementing intel transparent supply chain," *https://www.intel.com/*, 2015.

[77] B. Joshi *et al.*, "Securing cloud computing environment against ddos attacks," in *Computer Communication and Informatics*, IEEE, 2012.

[78] S. Li and L. Da Xu, *Securing the Internet of Things*. Syngress, 2017.

[79] S. R. Chhetri, S. Faezi, *et al.*, "Fix the leak! an information leakage aware secured cyber-physical manufacturing system," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2017.

[80] J. Straub, "Identifying positioning-based attacks against 3d printed objects and the 3d printing process," in *SPIE Defense+ Security*, International Society for Optics and Photonics, 2017.

[81] H. Vincent, L. Wells, *et al.*, "Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems," *Procedia Manufacturing*, 2015.

[82] N. G. Tsoutsos and H. o. Gamil, "Secure 3d printing: Reconstructing and validating solid geometries using toolpath reverse engineering," in *Workshop on Cyber-Physical System Security*, ACM, 2017.

[83] M. C. Rinard, C. Cadar, *et al.*, "Enhancing server availability and security through failure-oblivious computing.," in *OSDI*, 2004.

[84] S. Moore, P. Armstrong, *et al.*, "Vulnerability analysis of desktop 3d printer software," in *Resilience Week (RWS)*, IEEE, 2016.

[85] "Usable trust in the internet of things." http://www.utrustit.eu/. [Accessed August 08, 2017].

[86] "icore project.." http://www.iot-icore.eu. [Accessed August 08, 2017].

[87] S. Crane, A. Homescu, *et al.*, "Thwarting cache side-channel attacks through dynamic software diversity.," in *NDSS*, 2015.

[88] S. Alanazi, J. Al-Muhtadi, *et al.*, "On resilience of wireless mesh routing protocol against dos attacks in iot-based ambient assisted living applications," in *International Conference on E-health Networking, Application & Services (HealthCom)*, IEEE, 2015.

[89] C. Wang and Q. a. Wang, "Privacy-preserving public auditing for data storage security in cloud computing," in *Infocom*, Ieee, 2010.

[90] F. Zhao, C. Li, *et al.*, "A cloud computing security solution based on fully homomorphic encryption," in *International Conference on Advanced Communication Technology (ICACT)*, IEEE, 2014.

[91] L. D'Antoni *et al.*, "Operating system support for augmented reality applications.," in *HotOS*, vol. 13, pp. 21–21, 2013.

[92] K. Xu, T. Cao, *et al.*, "Cleaning the null space: A privacy mechanism for predictors.," in *AAAI*, 2017.

[93] K. Lebeck and K. a. Ruth, "Securing augmented reality output," in *Symposium on Security and Privacy (SP)*, IEEE, 2017.

[94] D. Amodei, C. Olah, *et al.*, "Concrete problems in AI safety," *arXiv preprint arXiv:1606.06565*, 2016.

[95] P. K. Rao *et al.*, "Three dimensional point cloud measurement based dimensional integrity assessment for additive manufactured parts using spectral graph theory," in *International Manufacturing Science and Engineering Conference*, 2016.