Journal of Hardware and Systems Security (2018) 2:51–68
https://doi.org/10.1007/s41635-017-0031-0

Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0

Sujit Rokka Chhetri[1] · Sina Faezi[2] · Nafiul Rashid[2] · Mohammad Abdullah Al Faruque[2]

Received: 30 September 2017 / Accepted: 29 November 2017 / Published online: 15 December 2017

Abstract

The next generation of smart manufacturing systems will incorporate various recent enabling technologies. These technologies will aid in ushering the era of the fourth industrial revolution. They will make the supply chain and the product lifecycle of the manufacturing system *efficient*, *decentralized*, and *well-connected*. However, these technologies have various security issues and, when integrated in the supply chain and 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 supply chain and product lifecycle of the manufacturing system while highlighting the roles played by the major enabling components of Industry 4.0.

Keywords Supply chain · Security · Information · Industry 4.0 · Product lifecycle

1 Introduction

The fourth industrial revolution (Industry 4.0) is transforming the next generation of manufacturing systems by making it *smarter*, *well-connected*, *self-organized*, *decentralized*, and *flexible*. To accelerate this transformation, industrial sectors have planned to commit US$ 907 billion per annum to Industry 4.0 [1]. Furthermore, there is a positive reception toward the Industry 4.0 by companies, with 85% of them estimated to implement Industry 4.0 solutions in their businesses [2]. The early adopters of the Industry 4.0 concepts are estimated to have both revenue gain and cost reduction of the process by 30% [1]. Among these positive changes, one of the major changes 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]. In fact, Gartner predicts that digitization will be a major trend, where almost all the physical part of the industry will have a virtual representation [4].

The rosy prospects forecasted for Industry 4.0, however, comes laden with various challenges, one of them being the security of the manufacturing systems [5]. Due to the heavy automation and monitoring, end-to-end digitization, and distributed and well-connected components, to name a few, the challenge for securing manufacturing systems will also rise [1]. The product lifecycle and the supply chain of manufacturing systems has always been challenged by various threats (such as *product tampering*, *service interruption*, *infiltration*, and *intellectual property loss*) [6], and on average, 20.1% of industrial computers are attacked by a malware every month [7]. Furthermore, manufacturing has consistently been among the top three industries to be targeted by spear phishing attacks [8]. Incidents such as attack on German steel mill [9], Maroochy water breach [10], and Stuxent [11], to name few, have already highlighted the crippling effects of attacks on industrial sectors. To add to this, with the incorporation of Industry 4.0, the cyber-risk to the manufacturing systems is estimated to increase [2].

The major security risk will arise due to the integration of new technologies, as it will introduce new forms of attacks [12, 13]. Researchers have started highlighting these

✉ Sujit Rokka Chhetri
schhetri@uci.edu

[1] Department of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA

[2] University of California, Irvine, CA, USA

issues and provided some solutions to secure manufacturing systems [14]. In earlier works, security has been considered in different ways: analyzed in terms of individual enabling components [15–17], highlighted as just one of the challenges for Industry 4.0 [18, 19], presented without the context of enabling technologies for Industry 4.0 [20, 21], or analyzed in terms of the standardization frameworks [22, 23]. Various works have also considered security of supply chain by providing overview [24], developing topology of risks in the supply chain[25], and classifying supply chain management practices based on intents and analyzing the effectiveness of various practices on supply chain security performance [26]. However, these works do not highlight the effects of the enabling technologies on security of manufacturing systems. In [27], security has been analyzed with just product lifecycle in mind. In this work, we extend [27] to 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, with not only product lifecycle in mind but also the supply chain.

To achieve this, we will present the security challenges and proposed solutions in the context of the enabling technologies and the supply chain along with product lifecycle of the manufacturing system. First, we will present the background in Section 2. Then, in Section 3, we will present security concerns with respect to the major enabling technologies of industry 4.0. In Section 4, we present the stages of the next generation of the product lifecycle and the supply chain, and the corresponding risks associated with each of the stages. In Section 5, we present the various security solutions that industry, researchers, and various organizations have proposed to secure the next generation of manufacturing supply chain and product lifecycle. Finally, we will provide some promising technologies for securing the next generation of manufacturing systems before concluding in Section 8.

2 Background

2.1 Industry 4.0

Industry 4.0, a German government initiative, is a fourth industrial revolution which focuses on advancing the next generation of smart manufacturing systems, with heavy incorporation of enabling technologies such as cyber-physical systems (CPS) for monitoring and automation, Internet of Things (IoT) for connectivity, machine learning for advanced cognition, advanced robotics for actuation, additive manufacturing for rapid prototyping, and cloud for computation and storage to name few. Compared to the third industrial revolution, which achieved automation using computer, in the fourth industrial revolution (happening now), the focus of design principles are on *interconnection*, *information transparency*, *decentralized decision*, and *technical assistance* [28].

2.2 Supply Chain and Product Lifecycle

In Fig. 2, the traditional automation pyramid for manufacturing is presented. This automation pyramid handles both the product and the supply chain of the manufacturing at various stages. There are mainly five levels in the automation pyramid [29]: *company level* at the top layer, *plant level* with the manufacturing execution systems, *process level* with all the material flow management computers, *control level* with the programmable logic controllers (PLCs), and the *field level* with the physical devices. This contemporary automation is limited in connection across the horizontal and the vertical layer. Along horizontal layers, the various distributed field devices, PLCs, and material flow computers almost have no communication path among themselves. On the vertical layer, the automation pyramid has limited connection with the immediate contiguous layer. Although this form of automation level reduces the complexity for maintaining the security [29], it also limits the productivity and efficiency that can be achieved.

The automation pyramid is responsible for managing the supply chain and the product lifecycle. Supply chain is concerned with maintaining the resources necessary for the product design to product delivery [30], and these resources go through various connections, such as the *supplier*, *enterprise* (where the product is designed and developed), *warehouse* (after the product is ready), *transporter*, and finally to the *customer*. On the other hand, product lifecycle is concerned with how the product traverses across various stages of its life, such as *design*, *prototype*, *ordering*, *industrial processing*, *sales* to the customer, and *maintenance*. The product lifecycle for Industry 4.0 along with the proposed decentralized and interconnected automation hierarchy [31] is shown in Fig. 1. Compared to the traditional automation pyramid (Fig. 2), 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 automation more dynamic in performance. However, it will also introduce various security issues [32] due to increased system complexity.

2.3 Security Fundamentals

The next generation of smart manufacturing will require to be *secure* from known risks, *vigilant* against new threats, and *resilient* against the zero-day attacks[13]. Moreover, the security system for Industry 4.0 needs to *identify* risk, implement appropriate safeguards to *protect*

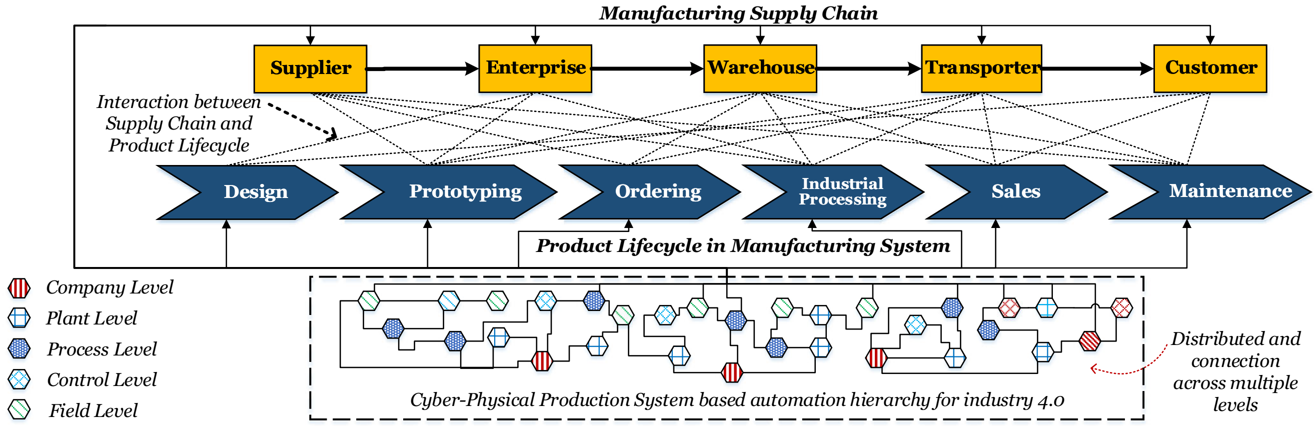

Manufacturing Supply Chain
Supplier
Enterprise
Warehouse
Transporter
Customer
Interaction between Supply Chain and Product Lifecycle
Design
Prototyping
Ordering
Industrial Processing
Sales
Maintenance
Product Lifecycle in Manufacturing System
Company Level
Plant Level
Process Level
Control Level
Field Level
Cyber-Physical Production System based automation hierarchy for industry 4.0
Distributed and connection across multiple levels

Fig. 1 Product lifecycle and supply chain in the context of Industry 4.0 based automation hierarchy

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] and 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 supply chain and the product lifecycle. To do so, we will present three fundamental security requirements for the next generation of smart manufacturing.

2.3.1 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. Hence, proper mechanisms (such as end-to-end encryption and access control) need to be incorporated for ensuring the confidentiality of the system.

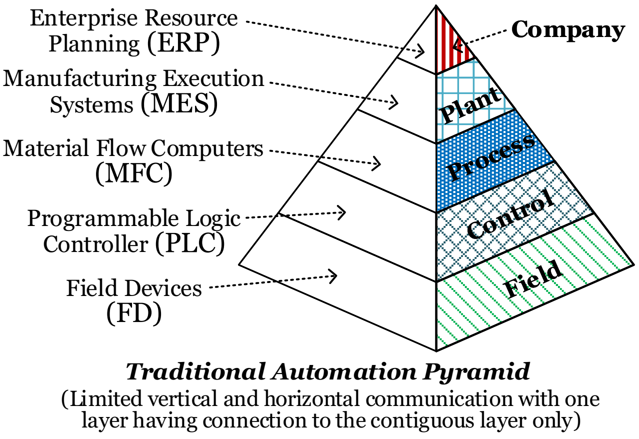

Enterprise Resource Planning (ERP)
Manufacturing Execution Systems (MES)
Material Flow Computers (MFC)
Programmable Logic Controller (PLC)
Field Devices (FD)
Company
Plant
Process
Control
Field
Traditional Automation Pyramid
(Limited vertical and horizontal communication with one layer having connection to the contiguous layer only)

Fig. 2 Traditional automation pyramid

2.3.2 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 supply chain and product lifecycle.

2.3.3 Availability

Various forms of cyber-attacks 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 supply chain and the product lifecycle to be disabled at the same time, causing the entire process chain to halt. Hence, special focus should be given for resiliency and recovery of the next generation of smart manufacturing systems.

3 Security of Enabling Components

The enabling components and concepts of Industry 4.0 are presented in Fig. 3. The list of enabling technologies presented here are not exhaustive; however, these are the major ones that will be incorporated rapidly in coming years [36–38].

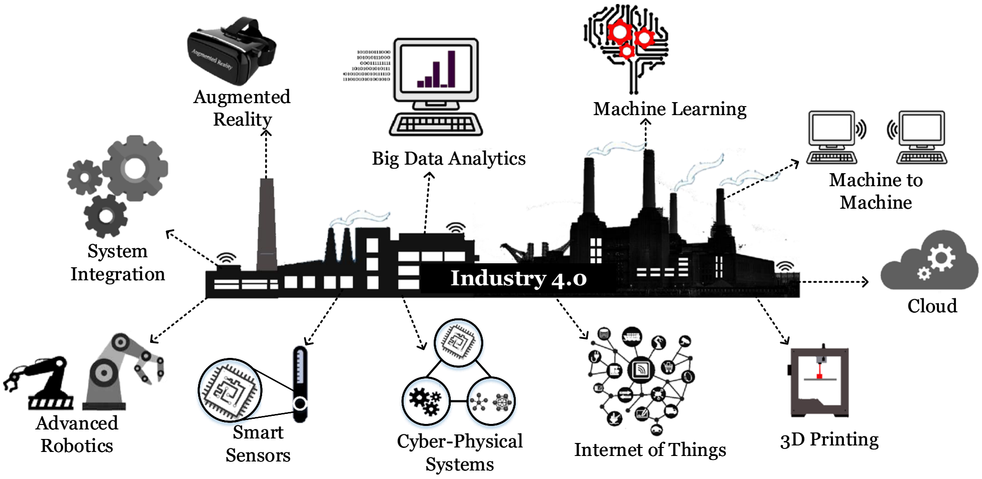


Fig. 3 Major enabling components of industry 4.0

3.1 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 cyber-space (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.

Currently, most of the security challenges in CPS are centered around the Supervisory Control and Data Acquisition (SCADA) security [39]. 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 [40] 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 [41]. ModBUS, which has been the de facto standard since 1979 [42], has no authentication checking and integrity checking built into the protocol [43]. These loopholes in ModBUS protocol will allow the attackers to get easy access into the system through the vulnerable TCP/IP connection. Moreover, CPS faces various challenges in maintaining the confidentiality, integrity, and availability [44].

3.2 Internet of Things

CPS connected to the Internet is often referred to as the "Internet of Things" [45]. The IoT is an inter-networking of physical objects (sensors, machines, cars, buildings, etc.) that allows interaction and cooperation of these objects to collect and exchange data over the Internet [46]. 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 [47] in the context of Industry 4.0. It is estimated that IoT will have an economic impact in between US$ 1.2 to 3.7 Trillion on operations and equipment optimization in factories alone [48].

The advanced connectivity of heterogeneous devices, systems, and services in IoT introduces various security loopholes. Besides, the scalable nature of IoT requires a flexible infrastructure to deal with the security threats. Thus, various security challenges arise in IoT, including authentication and access control, confidentiality, privacy, secure middleware, and trust [49]. As IoT is Internet enabled, it is obvious that the inherent security issues of the Internet will also be prevalent in IoT [50].

3.3 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) [51]. This data will be analyzed using *text analytics*, *machine learning*, *natural language processing*, *statistics*, *data mining*, etc. to extract information for various form of analysis such as *predictive*, *prescriptive*, *diagnostics*, and *descriptive*.

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, and cryptographically enforced access control [52, 53].

3.4 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" [54]. 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.

Since there are already various companies providing cloud-based solutions (Amazon, Google, etc.), it is expected that the next generation of smart manufacturing will rely heavily on the cloud to manage the data. There are various security issues associated with the services provided by cloud computing [55]. Some of the issues are denial of service, data loss, advanced persistent threats, malicious insiders, account hijacking, interface hacking, etc.

3.5 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.

The security of additive manufacturing is spread over the triad of confidentiality, integrity, and availability [56]. Some of the issues are intellectual property theft [57], attack on the integrity of the materials [58], etc.

3.6 Smart Sensors

Smart sensors do not just play the role of measurement but also consist of their own microprocessors, network chips, 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 [59]. In this scenario, smart sensors will play a crucial role in sensing and digitizing all the components of the manufacturing plant.

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.

3.7 System Integration

The system integration along the vertical and the horizontal automation hierarchy of the next-generation smart manufacturing is essential for achieving the goal of visible, flexible, and decentralized manufacturing. This makes it possible for integrated communication along the entire value chain, machine-to-machine interaction, and machine-to-human interaction for mass customization. System integration brings complex system together along the vertical and the horizontal value chain.

The security issues arise in terms of confidentiality as different automation level data in the vertical value chain is now available for access in different levels. Moreover, zero-day exploits in one stage can be used to carry out complex attacks on other stages of the supply chain and the product lifecycle.

3.8 Machine Learning

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.

The lifecycle of machine learning models consists of two stages: training and inference. A machine learning model can be subject to security attacks in any of these two stages [60]. 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 [61].

3.9 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 [62]. Advanced robotics are already being merged to industry for enabling the required robotic infrastructure for the fourth industrial revolution [63].

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 each of the components is prone to conventional cyber-threats, but also the mixture of the components cause new security issues. For instance, spoofing and triggering the system for certain malicious behaviors are possible through sensor manipulation [64].

3.10 Augmented Reality

Augmented reality is a promising technology for Industry 4.0. Authors in [65] have proposed a framework for using augmented reality to enhance the maintenance and support procedure of high-end manufactured products. Authors in [66] have introduced a novel approach that combines laser writers with augmented reality to create a human-robot interaction interface which surpasses many limitations of current interfaces of advanced robots.

Augmented reality 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: input and output [67]. A malicious application can gather a user's private information [68] or a company's sensitive data from different sources such as the screens of computers [69] or visible and hearable moving parts of machines running in the surrounding environment. This problem worsens when a user uses augmented reality browsers, such as Junaio and Layar, to load third-party augmented reality content. This is because all requests must go through an augmented reality service provider which has access to the augmented reality peripherals, and it has been proven to be prone to manipulation [70].

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 supply chain and the product lifecycle, and what security issues and challenges they will present for the next generation of smart manufacturing.

4 Supply Chain and Product Lifecycle Security

Industry 4.0 will make the supply chain and the product lifecycle faster (20 to 50% reduction in time to market), flexible (30 to 50% reduction in machine down town), accurate (with forecasting accuracy of up to 85%), and efficient (with productivity increase by 3–5%) [71]. However, the integration of enabling components will also affect the complex supply chain and product lifecycle by introducing various security issues to the *confidentiality*, *integrity*, and *availability* of the manufacturing system. In this section, various such vulnerabilities are highlighted. In order to analyze the security issues that arise due to the enabling components of Industry 4.0, in this section, the various stages of product lifecyle, its relation to the supply chain, and the corresponding security issues in terms of *confidentiality*, *availability*, and *integrity* are presented.

4.1 Design

Design stage of the product lifecycle is shown in Fig. 4. 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. The supplier may provide integrated development environment tools for analyzing the concept design, market demand data, etc. These tools can be provided as a service over the cloud as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS). Moreover, machine learning and big data analytics will play a huge role in better product design [72, 73]. In such scenarios, the various security issues associated with this stage 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. In such scenarios, security vulnerability of cloud may be an easy source for attackers to acquire sensitive information about the customers [74]. Moreover, computer-aided design (CAD) tools are being provided as a service in the cloud. Sharing

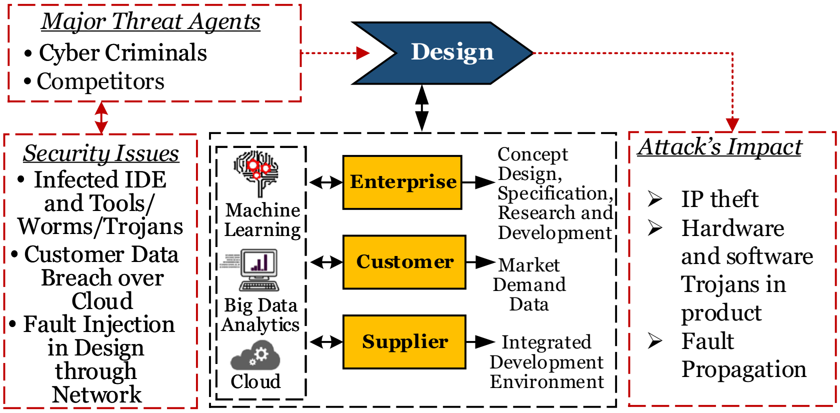

Major Threat Agents
• Cyber Criminals
• Competitors
Design
Security Issues
• Infected IDE and Tools/ Worms/Trojans
• Customer Data Breach over Cloud
• Fault Injection in Design through Network
Machine Learning
Big Data Analytics
Cloud
Enterprise
Customer
Supplier
Concept Design, Specification, Research and Development
Market Demand Data
Integrated Development Environment
Attack's Impact
IP theft
Hardware and software Trojans in product
Fault Propagation

Fig. 4 Design stage of product lifecycle

the CAD designs over the cloud poses a security risk for intellectual property theft [75]. In situations where the CAD tool has already been infected by a worm to infect and steal AutoCAD drawings [76], moving services over the cloud can have big consequences.

Integrity Work in [77] 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. The use of malware-infected CAD tools may introduce structural deformity that are hard to detect during the testing phase, but however may cause massive damage to the critical infrastructures in the long run.

Availability Various ransomwares [78] have already caused denial of service for designers. These malwares encrypt the design files, so that the legitimate users are no longer able to access it. Since Industry 4.0 is moving toward full Internet connectivity, these forms of ransomwares may be highly prevalent during the design stage. Moreover, attacks on the cloud can halt the design stage when companies rely on cloud services.

As shown in Fig. 4, the major threat agents for the design phase of the product lifecycle include the cyber-criminals and the competitors who are interested in stealing the next product design from the company [5].

4.2 Prototyping

The objectives of design prototyping in industry are *testing* and *evaluating* the design for flows, *cost estimation*, *patenting*, etc (see Fig. 5). 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. Supplier may provide computer-aided manufacturing tools and tooling solutions for the product development. Various enabling component will be utilized to assist the prototyping stage, such as additive manufacturing (for rapid prototyping), augmented reality (for creating virtual product development plant and analyzing security [79]), and cyber-physical systems (for monitoring and actuating various systems). Below, we list the security concerns regarding this stage:

Confidentiality In this stage, the designs are vulnerable to conventional cyber-attacks to CAM software, which might be running on cloud [80], the network media connecting the printer to the CAM tool, and the firmware running on the 3D printer [81]. Furthermore, various attack models have been proposed to take advantage of physical structure of CPS. For instance, authors in [82–86] have demonstrated how to utilize acoustic, vibration, electromagnetic, thermal, etc. analog emissions from the 3D printer to reconstruct and steal the geometrical design information of the product.

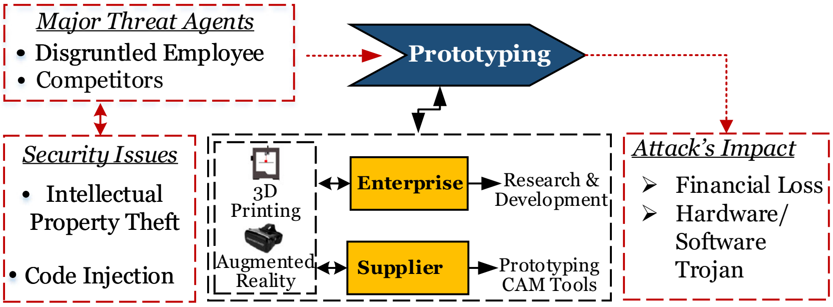


Fig. 5 Prototyping stage of product lifecycle

Integrity Authors in [56, 87] have infected either the CAM tool or firmware of the 3D printer and were able to compromise the integrity of the printed object. These CAM tools and firmwares may be used for prototyping the products and, if infected, may hide various structural deformity in the product.

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.

As shown in Fig. 5, the major threat agents include the competitors interested in stealing the intellectual property, disgruntled employee wanting to sabotage the system, etc.

4.3 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 and deliver them to the right place at the right price (see Fig. 6). The suppliers provide raw materials to the enterprise. Various cloud-based and big data analytics may be used to maintain the constant supply of raw materials for the product development. Some of the security issues in this stage include the following:

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 introduce more confidentiality vulnerabilities [88]. 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 [89] or gets blocked by ransomware attacks [78].

As shown in Fig. 6, the major threat agents include the competitors and unreliable vendors providing counterfeit raw materials for the production [90]. Moreover, the raw materials theft may occur during the transportation of the raw materials to the enterprise [90].

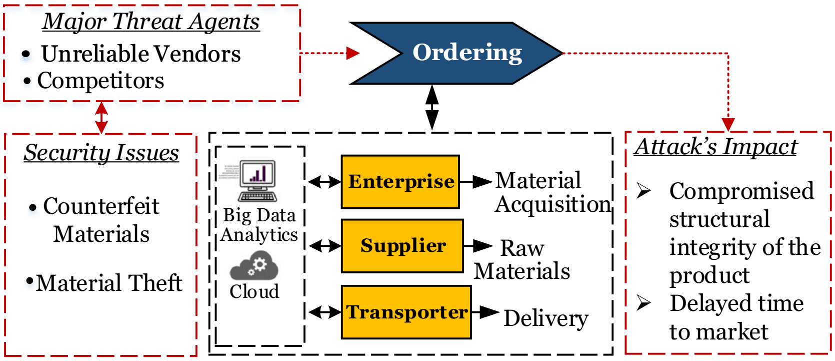
4.4 Industrial Processing

Industrial processing is one of the fundamental stages of product lifecycle (see Fig. 7). This is where the product manifests into actual object that customers end of purchasing. Various enabling technologies will aid the industrial processing stage, ranging from the use of big data analytics and smart sensors for data acquisition and analysis, various heterogeneous system integration, machine-to-machine communication, and advanced robotics.

Morever, 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, and availability of a system at risk [7].

Confidentiality With the enabling technologies like CPS, IoT, cloud computing, and 3D printing, the whole industrial

Fig. 6 Ordering stage of product lifecycle



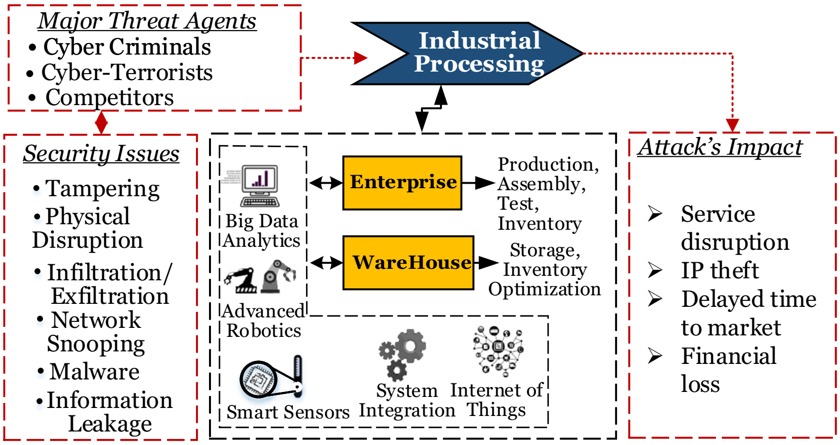


Fig. 7 Industrial processing stage of product lifecycle

process is now more connected and open. This openness creates a threat to the confidentiality of the system mostly toward the intellectual property theft. Researchers have shown that the digital design of a 3D-printed model can be regenerated from acoustic side channel attacks [83] leading to intellectual property theft of a company.

Integrity 3D printing can be easily manipulated by code injection to a design file leading to erroneous printing [91]. Factories incorporating advanced robotics or smart sensors for their factory automation are also prone to integrity modifications via different cyber-attacks or sensor tampering [64].

Availability Attacks on enabling technologies like CPS, IoT, smart sensors, and cloud computing can cause the manufacturing plant to be unavailable as well [92]. Authors in [93] have demonstrated how different cyber-attacks impact the cooling system of an engine making the system unstable and even unavailable for some time.

The major threat agents include the competitors, cyber-criminals, and cyber-terrorists. (see Fig. 7), who can cause various security issues such as tampering, physical disruption, and infiltration.

4.5 Sales

This stage is the closest to the customers (see Fig. 8) 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 stage starting from product design to distribution. Therefore, the risk associated with this stage is also higher. Various cloud, IoT, and big data analytics will aid next-generation inventory optimization and customer data acquisition for feedback to the design stage.

Confidentiality Confidentiality is the key security concern in this stage as it deals with various sensitive information like customer feedbacks, market surveys, estimated revenue, and annual sales reports. 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 [94].

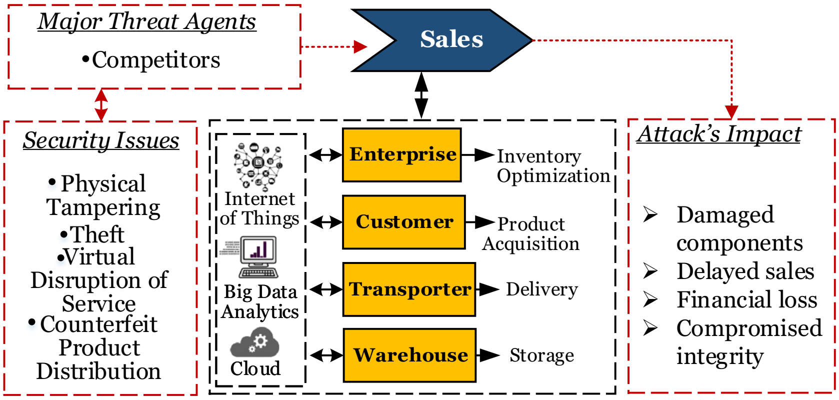


Fig. 8 Sales stage of product lifecycle

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 information 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 cyber-attack 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 [99]. Few examples of the very recent ransomware attacks include “WannaCry” in May 2017 [99] and “Petya” in June 2017 [98]. “WannaCry” affected almost 230,000 computers in over 150 countries including the UK National Health Service [99]. “Petya” originated from Ukarine and infected many of the airlines, banks, and utilities across Europe [98].

As shown in Fig. 8, the major threat agents include the competitors, who can tamper the physical product during transportation stage, steal the product, create virtual distribution of the sales by performing denial of service in the cloud, and destroy company reputation with influx of counterfeit products in the market.

4.6 Maintenance

Maintenance is the process which ensures that a system performs its required functions at the standard level of safety and reliability. The product used by customers are transported back to the enterprise. The spare parts stored in the warehouse might also need to be transported for the repair of the products. Enabling technologies such as augmented reality will be used for visualizing the faults in the products. Cloud, big data, and Internet of Things will also aid in gathering more data about the product for its maintenance. Due to the decentralized nature of Industry 4.0, various security issues may arise in this stage.

Confidentiality In this stage, there is a strong possibility of the customer’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 augmented reality devices to snoop over private data has previously been highlighted [69]. 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 [61].

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 [96].

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.

As shown in Fig. 9, the major threat agents include the competitors and counterfeit vendors, who can cause product theft, counterfeit part placement, infiltration of malwares, etc. Summary of the security issues in the supply chain and the product lifecycle of the manufacturing in the era of Industry 4.0 is shown in Table 1.

Adversaries As shown in Figs. 4, 5, 6, 7, 8 and 9, there are various threat agents acting on utilizing the vulnerabilities of

Fig. 9 Maintenance stage of product lifecycle

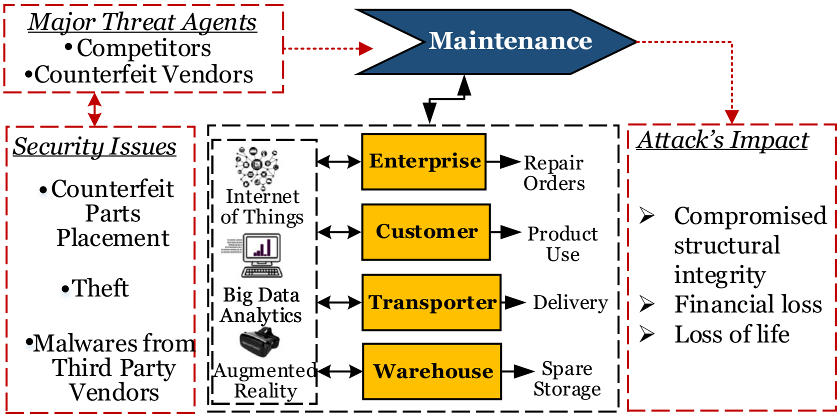


Table 1 Summary of security vulnerabilities in product lifecycle and supply chain due to enabling components

Product lifecycle →	Design	Prototyping	Ordering	Industrial processing	Sales	Maintenance
Confidentiality	Customer data breach from cloud [74], CAD design theft from cloud [75], worm-infected service over cloud [76]	Information leakage from additive manufacturing systems [82, 83]	Customer data breach in cloud [88]	Intellectual property theft [83]	Sales data theft [94]	Customer's data breach through augmented reality devices [69]
Integrity	Deformity injection in CAD [77]	Attack on CAM tool for fault injection [56, 87]	Counterfeit product supply [95] injection [91]	Product tampering through code	–	Replacement with counterfeit parts [96]
Availability	Ransomwares on data [78]	DDoS Attacks on IoT [97]	Material flow obstruction [90]	DoS on sensors [92]	Ransomware affecting sale data [98]	–
Supply chain affected	Enterprise, supplier, customer	Enterprise, supplier	Enterprise, supplier, transporter	Enterprise, warehouse	Enterprise, warehouse, transporter, customer	Enterprise, warehouse, transporter, customer

the supply chain and the product lifecycle. The adversaries can be a disgruntled employee who has access to high-level data. It can be competitors with large resources (computing power and domain knowledge). Some cyber-criminals have large domain knowledge regarding the IoT, CPS, and other enabling components. Which they can utilize at their disposal for breaching the confidentiality, integrity, and availability of the manufacturing system.

5 Security Trends

To tackle the security issues associated with the incorporation of the enabling technologies for the supply chain and the product lifecycle, various security solutions have also been proposed. Protocols such as ISO 28000 [100] provide standards for maintaining the supply chain security, and ISO/IEC 20243:2015 [101] provide standards for preventing counterfeits products from being introduced in the supply chain. However, research on strengthening the security of supply chain and product lifecycle in the era of Industry 4.0 is still at its infancy. In this section, we will highlight the advances made in securing the supply chain and the product lifecycle.

5.1 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 [102] describes methods to maintain the confidentiality of the designs and uses 3D printing as a method for validation. Standards such as ISO/ASTM 52915 describe a framework for sharing design information for 3D printing. [103] propose method for transferring data securely in cloud computing environment. Solutions such as AutoDesk vault [104] are providing access control to secure the CAD files in the cloud. Software such as [105] provides one-time password mechanism to secure the cloud-based application, whereas some provide solutions to secure the drawing files from being modified or copied without permission [106].

Integrity Maintaining the integrity of the product in the design phase is crucial as the design flaws which may be ignored by the infected CAD tools can propagate through the product lifecycle and the supply chain and cause massive damage to critical infrastructure. There are various works [107], which aim at making sure that the designs shared through the network or cloud maintain their integrity.

Moreover, work in [108] proposes a integrity layer for data storage in the cloud.

Availability Works such as [109] describe methods to make sure that cloud sources are protected from denial of service attacks. Works in [108] propose a high availability layer for cloud storage services. This can be crucial for designers as designers will be using various cloud services for not only designing their products but also storing them in the cloud.

5.2 Prototyping

The prototyping stage is a tight integration of cyber-components such as CAM tools, embedded software/hardware, network systems, IoT, and 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 [110] have evaluated the possibilities for increasing trustworthiness of software, network, embedded software/hardware, and IoT, respectively. Authors in [111] 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 [112] have used visible light sensing for verification of the printed object, while authors in [58] and [113] have suggested monitoring the 3D printer via analog side channels to assure the structural integrity of the product. Also, authors in [114] 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 [115] designed to help improve the availability of web-based services, authors in [116] have suggested using six tools to evaluate vulnerabilities and demonstrated them with code from open source projects.

5.3 Ordering

Various organizations are trying set of specific standards like FDIC [127] and PCI DSS [128] to deal with the supply chain security issues associated with the third party. The various measures taken to defend the ordering stage from the known security challenges include the following:

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[103].

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 [6].

Availability This is imperative for making sure that the manufacturers are able to manage the supply of raw materials to maintain regular flow of products in the supply chain. Customs-Trade Partner Against Terrorism (C-TPAT) [124] suggests that documentation and verification of the business vendors, access controls, personnel security, and container security are the key to availability in the ordering process [125].

5.4 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. Work in [129] have highlighted the importance of security when IoT is incorporated in the Industry 4.0.

Confidentiality To protect the industrial control systems from threats, different organizations have undertaken projects such as uTRUSTit (Usable Trust in the Internet of Things) [117] and the iCore project [118] for IoT and CPS, to maintain the confidentiality of the system.

Integrity For maintaining the integrity, works such as [121] discuss how to protect CPS, IoT, or 3D printing against various side channel attacks. Integrity of IoT devices, heterogeneous systems, during industrial processing is crucial. Any damage to the to the integrity of the these enabling technologies can halt the whole process chain.

Availability The availability of a system can be achieved by guarding the system against various DoS attacks. [126] shows some ways to defend against these attacks. Work in

[130] presents framework for maintaining the availability of CPS.

5.5 Sales

This stage is mostly vulnerable to information security attacks. However, other issues regarding security have also been studied. Security during the sales stage mostly involves securing the transportation of product from the warehouse to the customers.

Confidentiality The confidentiality in this stage is mostly vulnerable due to the cloud-based services handling different sophisticated information. Since most of the manufacturing industry will rely on using information and communication technology for maintaining their transportation and logistics, attack on the services (such as cloud) can leak valuable transportation information to attackers [119].

Integrity To preserve the integrity, organizations should prepare more robust defense. A small breach to the information can have terrible consequences. Different solutions [131] proposed by the researchers should be adapted to preserve the integrity of critical information. [119] provide various data to secure the transportation of product in the supply chain. This logistics should be followed to reduce the risk of product tampering and theft during the sales stage of the product lifecycle.

Availability As mentioned earlier, availability in this stage is mostly related to various DoS and ransomware attacks on cloud computing infrastructure. Works in [109] provide ways to secure the cloud, which could lead to avoiding DoS and ransomware attacks. Moreover, securing the transportation by securing the data in the cloud about transportation routes can maintain the steady flow of product in the supply chain [119].

5.6 Maintenance

The shift in the maintenance stage toward using new technologies such as big data, smart sensors, cloud computing, machine learning, IoT, and augmented reality has raised many new security concerns as it is discussed in Section 4.6. Various advances in solving these issues are as follows:

Confidentiality Securing the cloud [132] 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 [120] 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 [133] can also protect user information.

Integrity Work presented in [122] provides 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 [134] 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 [123] 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 [109]. Also, it is worth mentioning that using the enabling technologies such as augmented reality and machine learning would shorten the required maintenance time, which in turn would improve the availability of the product.

Summary of the security advances in the supply chain and the product lifecycle is shown in Table 2. For maintaining the confidentiality, various authentication schemes, access control, etc. have been proposed. For maintaining the integrity, intrusion detection, integrity layer, etc. have been proposed. For confidentiality, secure cloud services, routing protocols, etc. have been proposed. Moreover, services have currently been made available [135] for data center security, embedded security, anomaly detection, endpoint protection, email and web security, data loss prevention, encryption, etc., for various enabling components such as cloud, IoT, and CPS. Given the fact that the enabling components will reduce the cost of manufacturing itself [3] and that patching security is costlier in the end than a secure by design system [136], these defense mechanisms, although they require large research efforts, are necessary for next generation of smart manufacturing.

6 Hardware Security and Manufacturing Supply Chain

Hardware security can tremendously influence the security of the processing components used in the manufacturing supply chain. Hardware trojans implanted in chips during various stage [137, 138] of its supply chain can lead to information leakage [139], operational failure [137] leading to denial of service, and breach in the integrity of the data [140]. IoT, Smart Sensors, and CPS in general have various resource constraint which makes the task of securing the hardware challenging [141]. There have been various efforts to secure the hardware [142–144]. Next generation

Table 2 Summary of security advances/defense in product lifecycle and supply chain due to enabling components

Product lifecycle →	Design	Prototyping	Ordering	Industrial processing	Sales	Maintenance
Confidentiality	Framework for maintaining IP during outsourcing [102], encryption for cloud data [103, 105], secure vault for CAD files [104]	Trustworthy IoT [110], secure CAM [111]	Cloud user data security [103]	Trust protocols for IoT and CPS [117, 118]	Transportation route security [119]	Operating system for secure augmented reality [120]
Integrity	Integrity layer for cloud data storage [108]	Product verification [112, 114], trojan detection [113]	Vendor management [6] detection methods [121]	Integrity attack augmented reality	–	Maintain integrity in data integrity [122], integrity assessment of replaced parts [123]
Availability	High availability cloud [108], cloud security against DDoS [109]	High availability server [115], secure 3D printer [116]	Protocols for access control [124, 125]	Routing protocols against DDoS on IoT [126]	Secure route data in cloud [119]	Protocols against DDoS on Cloud [109]

of manufacturing systems using various IoT, CPS, etc. can only be secured if the underlying hardware is secured [145].

7 Promising Technologies and Guidelines

Block Chain Block chain has recently gained much attention due to its capability to maintain a large distributed record, which are time stamped and cannot be modified [146]. In the context of supply chain and the product lifecycle, this technology would help in maintaining a secure data about all the steps in the vertical and the horizontal value chain.

Digital Twin Digital twin is a virtual/digital representation of a physical entity or system. While the concept of a digital twin has been around since 2002 [147], it came into reality because of the various enabling technologies of Industry 4.0 like IoT, cloud computing, big data analytics, and augmented reality. Gartner [4] named it as one of the top 10 strategic technology trends for 2017 because of its tremendous potential in today's business. Digital twin allows the analysis of data and monitoring of systems to forecast problems even before they occur [148], thus preventing downtime and providing better efficiency. It helps to understand how a projected change to a manufacturing process might impact the whole supply chain of the product including the cost and time to delivery. More importantly, various vulnerabilities may be predicted along the product lifecycle and the supply chain.

Digital Thread Digital thread is a communication framework that will help in maintaining a constant data flow throughout the, otherwise isolated, manufacturing processes [149]. Through this data flow, digital thread will provide an integrated view of the manufacturing system and the product throughout the product lifecycle and the supply chain. One of the biggest challenges in Industry 4.0 is to devise a new way of sharing data throughout the entire supply chain and the product lifecycle. Digital thread can connect various isolated components to enhance data exchange among disparate software systems, such as computer-aided design and computer-aided manufacturing tools and real-time product status [150]. In terms of securing next generation of manufacturing systems, digital thread can improve transparency in information flow among system components (thus helping to maintain confidentiality) and allow easier system integration (in turn minimizing hidden security vulnerabilities arising from complex system interactions), etc.

Security Guidelines and Protocols Various works have started providing guidelines for securing the next generation of smart manufacturing. [151, 152] present various guidelines for securing the product lifecycle, authenticating and authorizing legitimate users, monitoring and identifying attacks, recovering from an attacks, etc., in the context of Industry 4.0. Security company Symantec [135], Kaspersky [153], Cisco[154], Rohde and Schwarz Cybersecurity [155], etc. have provided solutions for cyber-security in the era of Industry 4.0. These guidelines will form a basis for the next iteration of security protocols and architecture for smart manufacturing. There also has been efforts to devise new protocols and architectures to improve the security of enabling components of the Industry 4.0. Authors in [156] discuss and highlight the security solutions for IoT in the protocol level. National Institute of Standards and Technology (NIST) has provided cyber-security framework for improving the security and reducing the risk in manufacturing environment [157].

8 Conclusion

In summary, the fourth industrial revolution is paving the way for efficient and smart manufacturing systems. Various developments in the technologies have enabled this transformation from the third industrial revolution to the Industry 4.0. While these enabling technologies offer many advantages, it will also present various security challenges to the supply chain and the product lifecyle of the manufacturing systems. To highlight these issues, in this paper, we presented the security issues present in the current major enabling technologies. Then, we discussed about the supply chain and the product lifecycle and the various security issues introduced by the enabling technologies. Then, we presented recent research and trends in securing the supply chain and the product lifecycle when the major enabling technologies are incorporated in them. Finally, we discussed some promising technologies and guidelines that, if incorporated in the current manufacturing systems, will help in securing the next generation of manufacturing systems.

Acknowledgments The views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF.

Funding Information This work was partially supported by NSF CPS grant CNS-1546993.

References

1. Geissbauer R, Vedso J, Schrauf S (2016) Industry 4.0: building the digital enterprise: 2016 global industry 4.0 survey, PwC Munich
2. Industry Deloitte (2014) Industry 4.0—challenges and solutions for the digital transformation and use of exponential technologies. White Paper
3. Schrauf S, Berttram P (2016) Industry 4.0 and how digitization makes the supply chain more efficient, agile, and customer-focused. www.strategyand.pwc.com
4. Panetta K (2016) Gartner top 10 strategic technology trends for 2017. http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/
5. Berger R (2015) Cyber-security–managing threat scenarios in manufacturing companies. Accessed April 20:2016
6. Shackleford D (2015) Combatting cyber risks in the supply chain, White Paper. SANS.org. https://goo.gl/LqKX1G
7. Kaspersky Lab (2016) Threat landscape for industrial automation systems in the second half of 2016. https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/
8. Symantec (2016) Internet security threat report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
9. Lee RM, Assante MJ, Conway T (2014) German steel mill cyber attack. Industrial Control Systems, vol 30
10. Slay J, Miller M (2007) Lessons learned from the maroochy water breach. Critical infrastructure protection. Springer
11. Falliere N, Murchu LO, Chien E (2011) W32 stuxnet dossier, symantec security response, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. [Accessed August 06, 2017]
12. RadarServices Competenceseries (2015) Industry 4.0 = security 4.0? RadarServices Smart IT-security GmbH
13. Waslo R, Tyler LA (2017) Industry 4.0 and cybersecurity: managing risk in an age of connected production. University Press, Deloitte
14. Thames L, Schaefer DE (2017) Cybersecurity for industry 4.0: analysis for design and manufacturing. Springer
15. Manogaran G, Thota C et al (2017) Big data security intelligence for healthcare industry 4.0. In: Cybersecurity for industry 4.0. Springer
16. Glavach D, LaSalle-DeSantis J et al (2017) Applying and assessing cybersecurity controls for direct digital manufacturing (ddm) systems. In: Cybersecurity for industry 4.0. Springer
17. Wang Y, Anokhin O et al (2017) Concept and use case driven approach for mapping it security requirements on system assets and processes in industrie 4.0. System, Elsevier
18. Lu Y (2017) Industry 4.0: a survey on technologies, applications and open research issues. Journal of Industrial Information Integration, Elsevier
19. Bogle IDL (2017) A perspective on smart process manufacturing research challenges for process systems engineers. Engineering Journal, Elsevier
20. Prokop D (2017) Global supply chain security and management: appraising programs, preventing crimes. Butterworth-Heinemann
21. Smith J, Teuton J (2017) 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
22. Flatt H, Schriegel SA (2016) 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
23. Ma Z, Hudic A et al (2017) Security viewpoint in a reference architecture model for cyber-physical production systems. In: European symposium on security and privacy workshops (euros&PW). IEEE
24. Hintsa J, Gutierrez X, Wieser P, Hameri A-P (2009) Supply chain security management: an overview. International Journal of Logistics Systems and Management 5(3-4):344–355

25. Rao S, Goldsby TJ (2009) Supply chain risks: a review and typology. Int J Logist Manag 20(1):97–123
26. Lu G, Koufteros X, Lucianetti L (2017) Supply chain security: a classification of practices and an empirical study of differential effects and complementarity. IEEE Trans Eng Manag 64(2):234–248
27. Chhetri SR, Rashid N, Faezi S, Al Faruque MA (2017) Security trends and advances in manufacturing systems in the era of industry 4.0. In: IEEE/ACM international conference on computer aided design
28. Hermann M, Pentek T, Otto B (2016) Design principles for industrie 4.0 scenarios. In: 49th Hawaii international conference on system sciences (HICSS), 2016. IEEE
29. Sauter T (2007) The continuing evolution of integration in manufacturing automation. IEEE Ind Electron Mag 1(1):10–19
30. Hugos MH (2011) Essentials of supply chain management, vol 62. Wiley, New York
31. Lu Y, Morris KC et al (2016) Current standards landscape for smart manufacturing systems. National Institute of Standards and Technology, NISTIR
32. Monostori L (2014) Cyber-physical production systems: roots, expectations and r&d challenges. Procedia CIRP 17:9–13
33. National institute of standards and technology. Manufacturing profile: Nist Cybersecurity Framework (2016)
34. Hankel M, Rexroth B (2015) The reference architectural model industrie 4.0 (rami 4.0) ZVEI
35. Industrial Internet Consortium (2015) Industrial internet reference architecture (iira). [Online], Available: http://www.iiconsortium.org
36. Li J-Q, Yu FR, Deng G, Luo C, Ming Z, Yan Q (2017) Industrial internet: a survey on the enabling technologies, applications, and challenges. IEEE Communications Surveys and Tutorials
37. Wan J, Cai H, Zhou K (2015) Industrie 4.0: enabling technologies. In: International conference on intelligent computing and internet of things (ICIT), 2014. IEEE, pp 135–140
38. Wang S, Wan J, Li D, Zhang C (2016) Implementing smart factory of industrie 4.0: an outlook. International Journal of Distributed Sensor Networks. SAGE Publications Sage UK. London, England
39. Giraldo J, Sarkar E et al (2017) Security and privacy in cyber-physical systems: a survey of surveys. IEEE Design & Test
40. Bellovin SM (1989) Security problems in the TCP/IP protocol suite. In: ACM SIGCOMM computer communication review
41. Chhetri S, Wan J, Al Faruque M (2017) Cross-domain security of cyber-physical systems. In: Design automation conference (ASP-DAC), 2017 22nd asia and south pacific. IEEE, pp 200–205
42. Modbus application protocol specification v1.1, http://www.modbus.org/docs/modbus_application_protocol_v1_1b.pdf, 2006
43. Byres EJ, Franz M et al (2004) The use of attack trees in assessing vulnerabilities in SCADA systems. In: Proceedings of the international infrastructure survivability workshop
44. Chattopadhyay A, Prakash A, Shafique M (2017) Secure cyber-physical systems: current trends, tools and open research problems. In: 2017 Design, automation & test in Europe conference & exhibition (DATE). IEEE
45. Jazdi N (2014) Cyber physical systems in the context of industry 4.0. In: Automation, quality and testing, robotics. IEEE
46. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Computer Networks Journal, Elsevier
47. Höller J, Tsiatsis V et al (2014) From machine-to-machine to the internet of things: introduction to a new age of intelligence. Elsevier
48. James M, Chui M et al (2015) The internet of things: mapping the value beyond the hype. McKinsey Global Institute
49. Sicari S, Rizzardi A et al (2015) Security, privacy and trust in internet of things: the road ahead. Computer Networks Journal, Elsevier
50. Jing Q, Vasilakos AV et al (2014) Security of the internet of things: perspectives and challenges. Wireless Networks Journal, Springer
51. Lee J, Bagheri B et al (2014) 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)
52. Cloud Security Alliance (2012) Top ten big data security and privacy challenges. [Online], Available: http://www.isaca.org
53. Gahi Y, Guennoun M et al (2016) Big data analytics: security and privacy challenges. In: Symposium on computers and communication (ISCC). IEEE
54. Mell P, Grance T et al (2011) The NIST definition of cloud computing. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST) Gaithersburg
55. Hamlen K, Kantarcioglu M et al (2012) Security issues for cloud computing. Optimizing information security and advancing privacy assurance: new technologies: new technologies
56. Zeltmann SE, Gupta N et al (2016) Manufacturing and security challenges in 3D printing. The Journal of The Minerals, Metals & Materials Society (JOM), Springer
57. Rokka Chhetri S et al (2017) Side-channels of cyber-physical systems: case study in additive manufacturing. IEEE Design & Test
58. Chhetri SR, Canedo A, Al Faruque MA (2016) KCAD: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems. In: International conference on computer-aided design (ICCAD). IEEE
59. Johnson G (2016) Intelligent sensor technology and the cloud. Process Technology magazine. https://goo.gl/ZMt4hY
60. Papernot N, McDaniel P et al (2016) Towards the science of security and privacy in machine learning. arXiv:1611:03814
61. Papernot N et al (2017) Practical black-box attacks against machine learning. In: Asia conference on computer and communications security
62. Nolfi S, Bongard JC, Husbands P, Floreano D (2016) Evolutionary robotics: the biology, intelligence, and technology of self-organizing machines. MIT Press
63. Bahrin MAK, Othman MFO (2016) Industry 4.0: a review on industrial automation and robotic. Jurnal Teknologi (Sciences and Engineering)
64. McClean J, Stull C et al (2013) A preliminary cyber-physical security assessment of the robot operating system (ROS). SPIE Defense, Security, and Sensing
65. Mourtzis D, Zogopoulos V, Vlachou E (2017) Augmented reality application to support remote maintenance as a service in the robotics industry. Procedia CIRP, Elsevier
66. Huy DQ, Vietcheslav I, Lee GSG (2017) See-through and spatial augmented reality—a novel framework for human-robot interaction. In: International conference on control, automation and robotics (ICCAR). IEEE
67. Roesner F, Kohno T, Molnar D (2014) Security and privacy for augmented reality systems. Communications of the ACM
68. Templeman R, Korayem M et al (2014) Placeavoider: steering first-person cameras away from sensitive spaces. In: NDSS
69. Kim H, Kim H et al (2015) A new technique using a shuffling method to protect confidential documents from shoulder surfers. In: International conference on software security and assurance (ICSSA). IEEE
70. McPherson R, Jana S et al (2015) No escape from reality: security and privacy of augmented reality browsers. In: Proceedings

of the 24th international conference on world wide web. International world wide web conferences steering committee

71. Bauer H, Baur C et al (2015) Industry 4.0: how to navigate digitization of the manufacturing sector. Tech. Rep., McKinsey Digital
72. Autodesk (2017) Generative design. [Accessed September 25, 2017]. https://www.autodesk.com/solutions/generative-design
73. Li J, Tao F et al (2015) Big data in product lifecycle management. The International Journal of Advanced Manufacturing Technology, Springer
74. King NJ, Raja V (2012) Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review Journal, Elsevier
75. Jackson C (2013) Is CAD in the cloud truly terrifying? http://www.engineering.com
76. ESET (2017) ACAD/Medre.a, eset whitepaper. Retrieved
77. Belikovetsky S, Yampolskiy M et al (2016) Dr0wned-cyber-physical attack with additive manufacturing, arXiv:1609.00133
78. O'Gorman G, McDonald G (2012) Ransomware: a growing menace. Symantec Corporation
79. Fruth J, Münder R, Gruschinski H, Dittmann J, Karpuschewski B, Findeisen R (2011) Sensitising to security risks in manufacturing engineering: an exemplary VR prototype. In: Second international workshop on digital engineering, pp 39–44
80. Zhang L, Luo Y et al (2014) Cloud manufacturing: a new manufacturing paradigm. Journal of Enterprise Information Systems, Taylor and Francis
81. Ravi S, Raghunathan A et al (2004) Security in embedded systems: design challenges. ACM Transactions on Embedded Computing Systems (TECS)
82. Hojjati A, Adhikari A et al (2016) Leave your phone at the door: side channels that reveal factory floor secrets. In: ACM conference on computer and communications security
83. Faruque A, Abdullah M, Rokka Chhetri S, Canedo A, Wan J (2016) Acoustic side-channel attacks on additive manufacturing systems. In: Proceedings of the 7th international conference on cyber-physical systems. IEEE Press, p 19
84. Faruque MA, Chhetri S, Faezi S, Canedo A (2016) Forensics of thermal side-channel in additive manufacturing systems. Center for Embedded and Cyber-Physical Systems (CECS) Technical Report 16-01, University of California Irvine. https://goo.gl/u41QFu
85. Rokka Chhetri S (2016) Novel side-channel attack model for cyber-physical additive manufacturing systems, Ph.D. Dissertation, University of California, Irvine
86. Rokka Chhetri S, Canedo A, Al Faruque M (2016) Confidentiality breach through acoustic side-channel in cyber-physical additive manufacturing systems. ACM Transactions on Cyber-Physical Systems (TCPS)
87. Turner H, White J et al (2015) Bad parts: are our manufacturing systems at risk of silent cyberattacks? IEEE Journal on Security and Privacy
88. Gellman R (2012) Privacy in the clouds: risks to privacy and confidentiality from cloud computing. In: Proceedings of the world privacy forum
89. Armbrust M, Fox A et al (2009) Above the clouds: a Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Tech. Rep.
90. Zhang S, Hepashi K, Wynn M (2010) Security issues associated with material flow in supply chain of manufacturing industry. In: The conference on web based business management
91. Sturm L, Williams C et al (2014) Cyber-physical vunerabilities in additive manufacturing systems: a case study attack on the. STL file with human subjects. Journal of Manufacturing Systems, Elsevier
92. Raymond DR, Midkiff SF (2008) Denial-of-service in wireless sensor networks: attacks and defenses. IEEE Journal on Pervasive Computing
93. Rashid N, Wan J, Quirós G, Canedo A, Faruque MAA (2017) Modeling and simulation of cyberattacks for resilient cyber-physical systems. In: 13th IEEE conference on automation science and engineering (CASE), Elsevier
94. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, Elsevier
95. Guin U, Huang K, DiMase D, Carulli JM, Tehranipoor M, Makris Y (2014) Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proceedings of the IEEE
96. Wilson W (2017) Counterfeit parts: dangerous and costly. [Accessed August 10, 2017]. http://www.maintenancetechnology.com/2017/06/counterfeit-parts-dangerous-costly/
97. Kolias C, Kambourakis G, Stavrou A, Voas J (2017) DDoS in the IoT: Mirai and other botnets. Computer
98. Rothwell J, Titcomb J, McGoogan C (2017) Petya cyber attack: ransomware spreads across europe with firms in ukraine, britain and Spain shut down. [Accessed August 06, 2017]. http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/
99. Kastrenakes J, Brandom R et al (2017) Wannacry ransomware: all the updates on the cyberattack. [Accessed August 06, 2017]. [Online]. Available: https://www.theverge.com/2017/5/14/15638026/wannacry-ransomware-updates-cyberattack-cybersecurity
100. International Organization for Standardization (2007) Specification for security management systems for the supply chain. [Accessed September 25, 2017]. https://www.iso.org/standard/44641.html
101. ISO (2015) ISO/IEC 20243:2015: information technology – open trusted technology providertm standard (O-TTPS) – mitigating maliciously tainted and counterfeit products. [Accessed September 25, 2017]. https://www.iso.org/standard/67394.html
102. Yampolskiy M, Andel TRA (2014) Intellectual property protection in additive layer manufacturing: requirements for secure outsourcing. In: Proceedings of the 4th program protection and reverse engineering workshop. ACM
103. Arora R, Parashar A et al (2013) Secure user data in cloud computing using encryption algorithms. Int J Eng Res Appl 3(4): 1922–1926
104. Autodesk (2017) Autodesk vault. https://www.autodesk.co.uk
105. Onshape (2017) Onshape security. https://www.onshape.com/
106. AutoDWG (2017) Autodwg locker. http://www.autodwg.com/dwglock/
107. Intel (2015) Understanding and implementing intel transparent supply chain. https://www.intel.com/
108. Bowers KD, Juels A, Oprea A (2009) Hail: a high-availability and integrity layer for cloud storage. In: Proceedings of the 16th ACM conference on computer and communications security. ACM
109. Joshi B et al (2012) Securing cloud computing environment against DDoS attacks. In: Computer communication and informatics. IEEE
110. Li S, Da Xu L (2017) Securing the internet of things. Syngress, Elsevier
111. Chhetri SR, Faezi S et al (2017) Fix the leak! An information leakage aware secured cyber-physical manufacturing system. In: Design, automation & test in Europe conference & exhibition (DATE)
112. Straub J (2017) Identifying positioning-based attacks against 3D printed objects and the 3D printing process. In: SPIE Defense+ security. International society for optics and photonics

113. Vincent H, Wells L et al (2015) Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. Procedia Manufacturing Journal, Elsevier
114. Tsoutsos NG, Gamil HO (2017) Secure 3D printing: reconstructing and validating solid geometries using toolpath reverse engineering. In: Workshop on cyber-physical system security. ACM
115. Rinard MC, Cadar C et al (2004) Enhancing server availability and security through failure-oblivious computing. In: OSDI
116. Moore S, Armstrong P et al (2016) Vulnerability analysis of desktop 3D printer software. In: Resilience week (RWS). IEEE
117. Usable trust in the internet of things, http://www.utrustit.eu/, [Accessed August 08, 2017]
118. Icore project. http://www.iot-icore.eu, [Accessed August 08, 2017]
119. PwC (2011) Transportation and logistics 2030- volume 4: securing the supply chain. [Accessed September 15, 2017]
120. D'Antoni L et al (2013) Operating system support for augmented reality applications. In: HotOS, vol 13, pp 21–21
121. Crane S, Homescu A et al (2015) Thwarting cache side-channel attacks through dynamic software diversity. In: NDSS
122. Lebeck K, Ruth KA (2017) Securing augmented reality output. In: Symposium on security and privacy (SP). IEEE
123. Rao PK et al (2016) Three dimensional point cloud measurement based dimensional integrity assessment for additive manufactured parts using spectral graph theory. In: International manufacturing science and engineering conference
124. C-TPAT: Customs-Trade Partnership Against Terrorism, https://goo.gl/bgxyzc
125. Supply chain security best practices - ppai, http://www.ppai.org/media/1724/scs_bp_supplychainsecuritytransportation.pdf
126. Alanazi S, Al-Muhtadi J et al (2015) 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
127. FDIC Federal deposit insurance corporation (fdic). https://goo.gl/JM4oe9, [Accessed August 08, 2017]
128. PCI Payment card industry data security standard (pci dss). https://goo.gl/a47EuQ, [Accessed August 08, 2017]
129. Bligh-Wall S (2017) Industry 4.0: security imperatives for IoT—converging networks, increasing risks. Cyber Security: A Peer-Reviewed Journal 1(1):61–68
130. Parvin S, Hussain FK, Hussain OK, Thein T, Park JS (2013) Multi-cyber framework for availability enhancement of cyber physical systems. Computing Journal, Springer
131. Wang C, Wang QA (2010) Privacy-preserving public auditing for data storage security in cloud computing. In: Infocom. IEEE
132. Zhao F, Li C et al (2014) A cloud computing security solution based on fully homomorphic encryption. In: International conference on advanced communication technology (ICACT). IEEE
133. Xu K, Cao T et al (2017) Cleaning the null space: a privacy mechanism for predictors. In: AAAI
134. Amodei D, Olah C et al (2016) Concrete problems in AI safety. arXiv:1606.06565
135. Symantec (2016) Smarter security for manufacturing in the industry 4.0 era. Accessed 18 Sept 2017. https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf
136. Sniderman B, Gorman G et al (2016) The design of things: building in IoT connectivity. https://goo.gl/n5fGif
137. Bhunia S, Hsiao MS, Banga M, Narasimhan S (2014) Hardware trojan attacks: threat analysis and countermeasures. Proceedings of the IEEE
138. Forte D, Perez R, Kim Y, Bhunia S (2016) Supply-chain security for cyberinfrastructure [guest editors' introduction]. IEEE Computer Society
139. Hu N, Ye M, Wei S (2017) Surviving information leakage hardware trojan attacks using hardware isolation. IEEE Transactions on Emerging Topics in Computing
140. Bhasin S, Regazzoni F (2015) A survey on hardware trojan detection techniques. In: IEEE international symposium on circuits and systems (ISCAS), 2015. IEEE
141. Kanuparthi A, Karri R, Addepalli S (2013) Hardware and embedded security in the context of internet of things. In: Proceedings of the 2013 ACM workshop on security, privacy & dependability for cyber vehicles. ACM
142. Regazzoni F, Polian I (2017) Securing the hardware of cyber-physical systems. In: Design automation conference (ASP-DAC), 2017 22nd Asia and South Pacific. IEEE
143. Rostami M, Koushanfar F, Karri R (2014) A primer on hardware security: models, methods, and metrics. Proceedings of the IEEE Journal
144. Tehranipoor M, Wang C (2011) Introduction to hardware security and trust. Springer Science & Business Media
145. Dofe J, Frey J, Yu Q (2016) Hardware security assurance in emerging IoT applications. In: IEEE International symposium on circuits and systems (ISCAS), 2016. IEEE
146. Pilkington M (2015) Blockchain technology: principles and applications. Browser Download This Paper
147. Glaessgen EH, Stargel D (2012) The digital twin paradigm for future NASA and US air force vehicles. In: 53rd struct. Dyn. Mater. Conf. Special session: digital twin, Honolulu, HI, US, pp 1–14
148. Grieves M, Vickers J (2017) Digital twin: mitigating unpredictable, undesirable emergent behavior in complex systems. In: Transdisciplinary perspectives on complex systems. Springer, pp 85–113
149. TechTarget. Digital thread, https://goo.gl/L3sjx5, [Accessed September 28, 2017]
150. Proto Labs Data, digital threads, and industry 4.0. https://goo.gl/C4tRZC, [Accessed September 28, 2017]
151. Bokämper W (2016) Industrie 4.0 security guidelines: Recommendations for actions. [Accessed September 25, 2017]. http://www.vdmashop.de/refs/Leitf_I40_Security_En_LR_neu.pdf
152. Industrial Internet Consortium (2016). Accessed September 25, 2017
153. Kaspersky (2017) Industrial cybersecurity: solution overview. Accessed 18 Sept 2017. https://media.kaspersky.com/en/business-security/enterprise/KICS_Technology_Overview_v1.pdf
154. Cisco (2016) Communication structures for industry 4.0. Accessed September 10, 2017
155. Rohde and Schwarz Cybersecurity GmbH (2017) Security solutions for industry 4.0: detect, analyze and protect proactively. Accessed September 25, 2017
156. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials
157. Stouffer K, Zimmerman T, Tang C, Lubell J, Cichonski J, McCarthy J (2017) Cybersecurity framework manufacturing profile. NIST Interagency/Internal Report (NISTIR)-8183