Summer 7-16-2021

Mitigating Insider Threat Risks in Cyber-physical Manufacturing Systems

Jinwoo Song
Syracuse University

ABSTRACT

Cyber-Physical Manufacturing System (CPMS)—a next generation manufacturing system—seamlessly integrates digital and physical domains via the internet or computer networks. It will enable drastic improvements in production flexibility, capacity, and cost-efficiency. However, enlarged connectivity and accessibility from the integration can yield unintended security concerns. The major concern arises from cyber-physical attacks, which can cause damages to the physical domain while attacks originate in the digital domain. Especially, such attacks can be performed by insiders easily but in a more critical manner: Insider Threats.

Insiders can be defined as anyone who is or has been affiliated with a system. Insiders have knowledge and access authentications of the system's properties, therefore, can perform more serious attacks than outsiders. Furthermore, it is hard to detect or prevent insider threats in CPMS in a timely manner, since they can easily bypass or incapacitate general defensive mechanisms of the system by exploiting their physical access, security clearance, and knowledge of the system vulnerabilities.

This thesis seeks to address the above issues by developing an insider threat tolerant CPMS, enhanced by a service-oriented blockchain augmentation and conducting experiments & analysis. The aim of the research is to identify insider threat vulnerabilities and improve the security of CPMS.

Blockchain's unique distributed system approach is adopted to mitigate the insider threat risks in CPMS. However, the blockchain limits the system performance due to the arbitrary block generation time and block occurrence frequency. The service-oriented blockchain augmentation is providing physical and digital entities with the blockchain communication protocol through a

service layer. In this way, multiple entities are integrated by the service layer, which enables the services with less arbitrary delays while retaining their strong security from the blockchain. Also, multiple independent service applications in the service layer can ensure the flexibility and productivity of the CPMS.

To study the effectiveness of the blockchain augmentation against insider threats, two example models of the proposed system have been developed: Layer Image Auditing System (LIAS) and Secure Programmable Logic Controller (SPLC). Also, four case studies are designed and presented based on the two models and evaluated by an Insider Attack Scenario Assessment Framework. The framework investigates the system's security vulnerabilities and practically evaluates the insider attack scenarios.

The research contributes to the understanding of insider threats and blockchain implementations in CPMS by addressing key issues that have been identified in the literature. The issues are addressed by EBIS (Establish, Build, Identify, Simulation) validation process with numerical experiments and the results, which are in turn used towards mitigating insider threat risks in CPMS.

MITIGATING INSIDER THREAT RISKS

IN CYBER-PHYSICAL MANUFACTURING SYSTEMS

by

Jinwoo Song

B.S., Dongguk University, 2015

M.S., Syracuse University, 2018

Dissertation

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Mechanical and Aerospace Engineering.

Syracuse University

July 2021

ACKNOWLEDGEMENT

I would like to express my sincere gratitude by thanking my advisor, Dr. Young Bai Moon for all the guidance during my master and doctoral degree program at Syracuse University. His enthusiasm and passion for academic research and education greatly inspired me in my Ph.D. study. Most importantly, I appreciate him for being a supporter of my research, rather than mere advisor. Without his unconditional support and encouragement, I would not be able to achieve all my accomplishments.

I thank Dr. Xiyuan Liu, Dr. Bing Dong, Dr. Victor Duenas, and Dr. Yuzhe Tang for agreeing to join my dissertation committee. Their helpful reviews and comments enabled me to further make improvements on my dissertation. Also, I truly appreciate Dr. Fanxin Kong for accepting my request for taking the oral examination chair. I am grateful to my dissertation committee members and the chair for their time and effort given to my dissertation defense.

Also, there are many undergraduate and graduate students who helped in my research projects: Mathew Swanson, Emily Greaney, Chunxi Wang, Harika Bandaru, Xinyu He, Zhenyang Qiu, and Jinbo Wang. It was absolutely invaluable to interact and work with them, and I appreciate their efforts and time to my research. I also want to specially thank Dr. Mingtao Wu, who was my doctoral colleague and helped me in finding my research subject and learning fundamental research skills.

Lastly, I would like to thank my family. I was able to study at Syracuse University due to their endless trust and support. This dissertation could not be completed without their love and encouragement. I present my Ph.D. dissertation thesis to my father, mother, my little sister, and my little brother.

Table of Contents

Table List

Figure List

List of Abbreviation

Additive Manufacturing	AM
Automated Guided Vehicle	AGV
Carnegie Mellon's Software Engineering Institute	SEI
Cloud Manufacturing	CM
Convolutional Neural Networks	CNN
Cyber-Manufacturing System	CMS
Cyber-Physical Manufacturing System	CPMS
Cyber-Physical System	CPS
Decentralized-Denial-of-Services	DDOS
Denial-of-Services	DOS
Distributed Control System	DCS
Domain Name System	DNS
Establish, Build, Identify, and Simulation	EBIS
False-Negative	FN
False-Negative-Rate	FNR
False-Positive	FP
False-Positive-Rate	FPR
Information and Communications Technology	ICT
Input/Output	I/O
Insider Attack Scenario Assessment Framework	IASAF
Insider Attack Tree	IAT
Insider Threat Tolerant Cyber-Physical Manufacturing System	ITTCPMS
Internet of Things	IOT
Intrusion Detection System	IDS
Layer Image Auditing System	LIAS
Local Area Network	LAN
Machine-to-Machine	M2M
Malicious Item by Insider	MII

Man in the Middle	MITM
Mean Absolute Percentage Error	MAPE
Minimum Mean Absolute Percentage Error	MMAPE
Multilayer Perceptron Neural Network	MLP
National Insider Threat Task Force	NITTF
Programmable Logic Controller	PLC
Radio Frequency Identification	RFID
Receiver Operating Characteristic	ROC
Rectified Linear Unit	ReLU
Secure Programmable Logic Controller	SPLC
Service-Oriented Architecture	SOA
Service-Oriented Blockchain	SOB
Simplified Convolutional Neural Network	SCNN
Supervisory Control And Data Acquisition	SCADA
Supply Chain Management	SCM
Technology Acceptance Model	TAM
The Intelligence and National Security Alliance	INSA
Threat Score	TS
True-Negative	TN
True-Positive	TP
True-Positive-Rate	TPR

Chapter 1. Introduction

In this chapter, the motivation of the research is discussed by introducing the overview of Cyber-Physical Manufacturing System and its security. The scope of the research is also presented by defining three main key words: Cyber-Physical Manufacturing System, Insider Threats, and Blockchain. Next, the problem statement, hypothesis, and objective of the research are presented and discussed. Finally, a dissertation overview is provided.

1.1 Motivation

The realization of fully automated manufacturing has been accelerated by recent technological advances. In particular, a future generation manufacturing system, such as Cyber-Physical Manufacturing System (CPMS) in which digital and physical domains are seamlessly integrated via the internet or computer networks, will enable drastic improvements in production flexibility, capacity, and cost-efficiency (Monostori et al., 2016).

However, such a manufacturing system necessitates adequate security before it can be safely operated. CPMS ushers in the unique security challenges from the sheer volume and pervasiveness of exchanged data, and increased accessibility of the system by its outsiders and insiders. CPMS becomes a target by attackers because it involves a myriad of confidential and valuable data—such as manufacturing details and product specifications—over numerous connected physical components (Song et al., 2020). Additionally, the fully integrated system structure of CPMS is vulnerable to Cyber-Physical Attacks, which can cause damages in the physical domain due to attacks originating in the cyber domain (Chhetri et al., 2016). Specifically, such attacks can be performed by insiders more easily than outsiders. Insiders are anyone who has been or is affiliated with a system. Since insiders already have physical access, security clearance, and knowledge of the system vulnerabilities, they can bypass or incapacitate general defensive mechanisms of the system to manipulate manufacturing information without being discovered (Song et al., 2020).

Research on insider threats started emerging in manufacturing systems only recently—around 2018. However, a myriad of security organizations has raised their concerns about the seriousness of insider threats in manufacturing systems. According to the survey conducted at the 2019 RSA conference by Gurucul (GURUCUL, 2019), the manufacturing industry is the most

vulnerable industry against insider threats. Furthermore, 40% of insider threats in the sector could not be detected initially, nor detected after the data had been breached. The Intelligence and National Security Alliance (INSA) confirmed these difficulties in their 2018 reports: only 8% of survey respondents have independent defensive preparations for insider threats, and the majority of respondents answered that developing skilled labor and defensive preparations remain elusive because it is difficult to detect and predict insider threats (INSA, 2018a, 2018b). Additionally, IBM reported interesting statistics regarding the insiders (IBM, 2020b, 2020c). According to the investigation on their customer companies, the number of incidents by misconfigurations surged in 2019, but there was actually a decrease in the number of reported incidents from misconfigurations. Regarding this issue, IBM stated that when the misconfiguration incident did occur, the damage was significantly greater than before. This implies that insiders can also unintentionally compromise the system, but the consequences become more serious. In addition, social engineering and malicious insiders are the highest threat vectors based on the average cost of data breaches per the percentage of malicious breaches among 524 organizations, from August 2019 to April 2020.

In spite of the gravity of insider security, there has been negligible research progress. Because of varied human motivations and limited understanding of human psychology in this subject, it is difficult to predict insider attacks in advance (Moore, 2016). Many attacks caused by insiders are stealthier than those by outsiders because insider's trails are easy to hide (Sinclair & Smith, 2008). Also, insiders create a dilemma in the system: additional flexibility in authorized access results in less supervised control over the process, which in turn decreases the security of the system (Bishop et al., 2014). Therefore, it is arduous to thwart insiders by using hierarchical and centralized approaches.

Meanwhile, blockchain technology has gained traction with many researchers as a means to enhance the security of systems in various industry sectors over the past few years. Blockchain's uniqueness as a decentralization-based defensive mechanism has been considered in order to shift the existing paradigm in general security measurements of manufacturing systems. The core mechanism of the blockchain is to store the exact same data in all the machines in the connected network, as well as to link the old data and new data to maintain the entire data integrity. In this way, the blockchain can ensure an unprecedented level of security against outsiders and even insiders.

However, many gaps in understanding of insiders in manufacturing systems and practical implementations of the blockchain to manufacturing systems still remain. Specifically, a blockchain communication protocol has seldom been discussed from the viewpoint of insiders in manufacturing systems. Furthermore, blockchain-based systems have limited system performances due to the arbitrary block generation time and block occurrence frequency. As yet, there has been no systematic investigation of the use of blockchain technology concepts and techniques for security against insider threats.

The understanding of insider threats and blockchain implementation in CPMS may lead to a more consistent method of detecting or preventing insiders, mitigating an insider threat risk, efficient control of blockchain networks, and greater effectiveness in blockchain communication protocols in manufacturing systems.

1.2 Scope of the research

1.2.1 Cyber-Physical Manufacturing System

Cyber-Physical Manufacturing System (CPMS) originated from Cyber-Physical System (CPS), which is an automated and distributed system that integrates digital and physical assets with communication networks and computing infrastructures (Acatech, 2011; Wang et al., 2015). CPMS can be distinguished from CPS by including production activities into key operational processes. As CPS is equipped with advanced artificial intelligence and improved communication capabilities, CPMS will render production activities more sustainable by reducing the need, time, and cost for rebuilding and reprogramming manufacturing lines (Ribeiro & Björkman, 2018). Therefore, CPMS can enable a more effective production process in terms of flexibility, reliability, functionality, usability, and efficiency than traditional embedded systems.

Table 1 5-C Structure

5C-Level	Description
Smart connection	Integration of the physical devices connected in a communication network.
Data to Information Conversion	Conversion from monitored device data to information, in order to understand them and apply to the physical world.
Cybernetic	Use of information for the device virtualization. It is also the level responsible for the communication among assets.
Cognition	Functions of monitoring and prognostics for failure prediction and maintenance optimization.
Configuration	Transmission from the virtual to the physical world, making the machines self-adjusting and self-adaptive.

As a basic architecture model guideline for developing CPS for manufacturing applications, the 5C architecture is proposed. The 5C architecture clarifies how to construct a CPS from the initial data acquisition to analytics, as well as to the final value creation by using a sequential workflow manner (Lee et al., 2015). The details of the 5C architecture can be found in Table 1.

1.2.2 Insider Threats

Insider threats are considered one of the most challenging cyber security issues because they are hardly detected or prevented by commonly employed security mechanisms. Insiders are individuals who have access to and knowledge of a system, and they are also trusted within the security perimeter. Accordingly, insider threats refer to actions that these insiders intentionally or unintentionally misuse or abuse access/knowledge to violate the security policies of the system (Homoliak et al., 2019).

The definition of insider threats differs depending on insiders' intentions. For example, some definitions—such as “harmful acts that trusted insiders might carry out” and “the intentional misuse of computer systems by users who are authorized to access those systems and networks”—limit the scope of insider threats to intentional insiders. On the other hand, other definitions—such as “threats originating from people that have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organization” and “an individual with privileges who misuse them or whose access results in misuse”—include both intentional and unintentional insiders (Greitzer et al., 2011; Hunker & Probst, 2011; Schultz & Shumway, 2001; Theoharidou et al., 2005).

However, unintentional insider threats cannot be ignored from manufacturing system security because these can damage the system as much as intentional insider attacks. Also, it is plausible that insiders become a bridge between outside attackers, thus compromising confidential system domains (Sinclair & Smith, 2008). Moreover, anyone who is able to access the systems—such as suppliers, outsourcing human resources, or even third-party vendors—could turn into a malicious insider. According to the 2016 California Data Breach Report, Target, the eighth-largest retailer in the United States, was hit with a credit card data breach by a third-party vendor, which resulted in 7.5 million customers' credit card information leakage in 2013 (Bishop et al., 2014). The attacker obtained access to Target's customer service database by using credentials stolen from the third-party vendor.

In this research, an insider is defined as "anyone who has been or is affiliated with a system but can intentionally or unintentionally compromise the system security."

Table 2 Insider Category

Intention	Title	Motivation
Voluntary	Malicious Destructor	To gain financial profit
		To express revenge
	Hazardous Misuser	To express boredom
		To express disgruntlement
Involuntary	Dangerous Tinker	To obtain unauthorized software
		To check the system weakness
	Naïve Mistaker	Unintentional mistake
		Ignorance

Accordingly, insiders can be categorized into voluntary insiders and involuntary insiders. Furthermore, each category can be delineated by their motivations: malicious destructor, hazardous misuser, dangerous tinker, and naive mistaker. Different kinds of insiders and their motivations are presented in Table 2 (Pfleeger, 2008; Stanton et al., 2005).

1.2.3 Blockchain

The blockchain is a way to store data in a distributed system in which the system components have connected each other and form a Peer-To-Peer network. The main function of the blockchain is to store the exact same data to all the components in the network, as well as link the old data and new data to maintain the entire data integrity. Because of the connection between old and new data, the modification of the old data in the specific node affects its new data integrity, so any changes in the data could be readily detected by other components and prevented by using consensus algorithms, without inspecting the entire stored data. However, it is inefficient to store the data itself in all the components, because the cumulative data size would be enormous with the given time, while the component's storage size is limited. Therefore, when the node is received, generating, and transferring data, it automatically creates a transaction hash, which consists of 64 digits (Bitcoin) or 66 digits (Ethereum) of a random series of letters and numbers. The transaction hash is a cryptonized identification of the data based on the data’s value, timestamps, creator information etc. The transaction hash will not be directly distributed to the system components, but it will be distributed as a block form that contains many other transaction hashes. The block also has a block hash, which is an identification of the block, and it is distributed to the components. This distributed block will be chained with the previous distributed block by involving the previous block hash, and this is called the blockchain.

1.3 The Problem

Insider threats can be considered as one of the most challenging security issues in CPMS because it is hardly detected or prevented by commonly employed security mechanisms. Furthermore, a fully integrated system structure of CPMS's digital and physical domains will allow insiders to inflict massive damage by manipulating small changes in manufacturing parameters. Therefore, insider threats must be addressed and resolved prior to fully manifesting CPMS in the real world. The main problem that this research address is stated as follows:

An insider threat risk in CPMS is enlarged due to the increased accessibility and connectivity, and it is difficult to detect or prevent in a timely fashion.

The consequences of insider attacks can be enlarged from the sheer volume and pervasiveness of exchanged data and increased accessibility of the system (Song & Moon, 2020c). Moreover, a cross-domain integration between digital data and physical domains enables certain attacks such as cyber-physical attacks—that are initiated from the digital format but result in physical damages. This type of attack can be easily exploited by insiders since they have legitimate access authentications to the digital domains.

Besides, legitimate access authentications enable insiders to hide their digital footprint, such as event logs, browsing histories, and any surveillance history data (Song & Moon, 2020a). Additionally, since insiders are knowledgeable about the system, they can easily bypass or incapacitate any security process and compromise the system without being discovered.

Also, it is plausible that insiders unintentionally become a bridge between outside attackers, thus compromising confidential system domains. Social engineering attacks—such as phishing, SMSishing, baiting, fake software—are deceiving individuals or enterprises to accomplish certain actions that benefit attackers (Greitzer et al., 2014; Salahdine & Kaabouch, 2019).

Furthermore, the growth of collaborative business in the manufacturing industry blurs the boundary between insiders and outsiders (Schultz, 2002). Thus, it is now difficult to decide who are insiders in the system.

Lastly, merely increasing supervised control and restrictions of the systems can result in less flexibility, which can contribute to decreasing productivity (Sinclair & Smith, 2008).

1.4 Hypothesis & Objectives

To overcome gaps in the literature and advance the understanding of insider threats, as well as blockchain implementations in manufacturing systems, the research hypothesis of this thesis is as follows:

A service-oriented blockchain augmentation can reduce insider threat risks in Cyber-Physical Manufacturing System, while remaining its flexibility and productivity.

Systems based on the blockchain have a limited system performance due to the arbitrary block generation time and block occurrence frequency. The service-oriented blockchain augmentation provides physical and digital entities with the blockchain communication protocol through a service layer. In this way, multiple entities will be integrated by the service layer, which will provide the services with less arbitrary delays, while retaining its strong security from the blockchain.

Accordingly, all of the insiders' digital footprints will be retained in the blockchain and continuously validated by other participants. Thus, the blockchain communication protocol can help prevent insiders from hiding their digital footprints.

Also, it is hard to exploit social engineering attacks to compromise the system protected by the blockchain. To damage the system with the attacks, outsiders require computing power

more than 50% of the power of entire blockchain participants' machines, or need to compromise and manipulate more than half number of the machines' blockchain repository. However, such an attempt is not practical, so it is fruitless.

For the ambiguity between insiders and outsiders, since all the services of the digital and physical entities will be provided through the service layer, the system can be protected from anyone who can access the systems.

Lastly, multiple independent service applications can be enabled and customized in the service layer, hence the flexibility and productivity of the CPMS can be ensured.

To validate this hypothesis, the objectives of the proposed work are:

i) To investigate the influence of insiders, their potential threats, attack motives, and vulnerabilities in CPMS.

ii) To develop and validate a physical testbed that represents a small-scaled CPMS augmented by blockchain technology.

iii) To design and evaluate insider attack scenarios via the physical testbed and an assessment framework.

iv) To quantify systematic differences between CPMS's operations with non-blockchain and blockchain to isolate the effectiveness of the distributed system against insider threats.

1.5 Dissertation Overview

The remainder of this dissertation is organized as follows. Chapter 2 reviews the literatures related works on CPMS, insider threats, and blockchain. Chapter 3 presents a survey regarding blockchain applications for manufacturing systems. Chapter 4 proposes and describes an Insider Threat Tolerant Cyber-Physical Manufacturing System (ITTCPMS). Chapter 5 introduces two example models for simulations: Layer Image Auditing System (LIAS) and Secure Programmable Logic

Controller (SPLC). Chapter 6 discuss insider attack scenarios by developing Insider Attack Tree (IAT). Chapter 7 provides an Insider Attack Scenario Assessment Framework (IASAF) and four case studies. Chapter 8 summarizes the dissertation and outlines the limitations and future work.

Chapter 2. Review of Literature

The review of literature consists of three key topics and presents the recent acknowledgments and findings in this interdisciplinary research. For Cyber-Physical Manufacturing System, its overview is introduced including definitions as well as technical and security challenges. Next, insider threats are reviewed by examining reports, regarding insider threats in the manufacturing industry, from various security organizations. After that, the efforts to identify insiders in the systems are presented. Finally, blockchain's basic concept and its applications in the manufacturing industry with advantages and challenges are provided.

2.1 Cyber-Physical Manufacturing System

2.1.1 Definition

In recent years, the development of new paradigms for manufacturing systems has been accelerated by the increased demand for more personalized, smart, and sustainable products with the rapid growth of the industrial internet and cyber-physical technologies (Moghaddam et al., 2018). For example, Cyber-Physical System (CPS) that integrates the computational entities within intensive connections of the surrounding physical world provides data-accessing and data-processing services available on the internet (Acatech, 2011). CPS differs from traditional embedded systems with wireless sensor networks because it is a heterogeneous system that contains diverse networks, which integrate interconnected sensors, actuators, and controllers (Yu et al., 2017).

Accordingly, as a fundamental base for an intelligent manufacturing environment, CPS is introduced to a shop floor of a manufacturing system to provide numerous advantages in the manufacturing process (Liu & Jiang, 2016). Furthermore, today's manufacturing systems can be transformed into the systems of Industry 4.0 with significant economic potential by integrating CPS with production, logistics, and services within the current industrial practices (Lee et al., 2013). Consequently, research and applications of CPS for manufacturing systems have been active, which has positively affected the manufacturing industry in the form of Cyber-Physical Manufacturing Systems (CPMS) in process automation and control (Wang et al., 2015).

CPMS is a vision of Industry 4.0 in which digital and physical domains are seamlessly integrated via internet or computer networks (Song & Moon, 2020c). Thus, all the necessary manufacturing entities in CPMS—such as production facilities, warehousing systems, logistics,

and even social requirements—can be integrated to establish the global value creation via advanced networks (Frazzon et al., 2013).

In order to achieve the goal of Industry 4.0, CPMS should follow three key features: (i) horizontal integration of manufacturing processes, (ii) vertical integration of different hierarchical levels, and (iii) end-to-end digital integration across the system's value chain (Wang et al., 2016). CPMS will enable improved flexibility and robustness with the highest quality standards in the entire production process, including engineering, planning, manufacturing, as well as operational and logistics processes (Kagermann et al., 2013). This will lead to the development of a total of five intelligent functions of CPMS: Self-monitoring, Self-awareness, Self-prediction, Self-optimization, and Self-configuration (Song & Moon, 2019a). As a result, CPMS allows direct communications within the system, thereby solving problems and making adaptive decisions in a timely manner (Zhong et al., 2017).

2.1.2 Challenges

Many researchers have devoted time to develop and advance CPMS for Industry 4.0; however, there are still technical and security challenges to be solved.

2.1.2.1 Technical Challenges

For CPMS's operation, all of the manufacturing-related data—such as system elements, flow, and business specifications—are required to be collected. In the actual production process, a sheer volume of images and information from automation systems and control systems are created and gathered to be analyzed and processed. Particularly, the most complex and cumbersome information data is returned from the overall production management, such as the quality management, process monitoring, fault detection, etc. (Cheng et al., 2018). Therefore, data

analytics in CPMS faces great challenges in the scalability, because of the strict requirements on computation, speed, and variety with regard to the vast amount of data (Bi & Cochran, 2014). This challenge necessitates Big-Data storage that is decentralized, scalable, elastic, and fault-tolerant (Kambatla et al., 2014).

Also, there are technical challenges in integrating the physical domain based on Internet of Things (IoT). IoT requires complicated heterogeneous networks, which include the connection between various types of communication technologies (Xu et al., 2014). However, the lack of powerful tools still poses a major hindrance to accommodate the variety of communication technologies and applications in the network (Xu, 2011). Besides, in order to examine the massive volume of data generated from the physical domain in a timely manner, it is important to develop and improve data analytic techniques (Chen, 2017). Moreover, merely collecting data from a lot of IoT devices efficiently is challenging due to the uncertainty and randomness of the network distribution (Liu et al., 2008). The numerous different links and interactions between the devices makes it a more complex system (Li et al., 2014). The IoT's visions in CPMS has great potential, but many technical, social, and economic questions remain unaddressed (Hodges et al., 2013).

2.1.2.2 Security Challenges

CPMS promises great benefits in production flexibility, capability, and cost efficiency, but realizing CPMS fully is not feasible without tackling security issues accompanying the higher level of connectivity and accessibility (Wu & Moon, 2018). Particularly, Cyber-Physical Attack—that originates from the cyber domain but induces physical damages—has become an emerging serious threat to the manufacturing industry (Chhetri et al., 2016).

The most well-known Cyber-Physical Attack occurred in 2010. Iran's nuclear facilities identified the Stuxnet computer worm, which was specifically targeting the Siemens control

system and re-configuring PLC's programming-language-layer directly (Langner, 2011). In Germany in 2014, the access authority of German Steel Mill's industrial control system was compromised by multiple attackers. The attackers used malicious attachments in emails to manipulate the access authority. The attack imperiled the blast furnace control system, which resulted in access denial for all users, ultimately causing significant damages (Oueslati et al., 2019). Lastly, Norsk Hydro, the largest aluminum producer in Scandinavia, experienced a production halt due to a ransomware attack on the 19th of March 2019. These malware programs are designed to compromise access control of the system and encrypt sensitive data on infected devices to stop the manufacturing operation (Aoyama et al., 2020).

Apart from the Cyber-Physical Attack, the new technologies and requirements of CPMS create new demand for standardization, which is the significant feature to improve security and safety across different regions and communities. However, existing approaches regarding security, safety, and legal standards are insufficient to meet the requirements charged by CPMS (Bicaku et al., 2018). Furthermore, there is no standard communication protocols for the industrial devices commonly employed. Therefore, their manufacturing operations tend to be inflexible and inefficient, and this leads to limiting the full potential of CPMS implementation (Pereira et al., 2017). To secure the use of new technologies and services, information security and data privacy protection are thoroughly examined and investigated; particularly the difficult security issues resulting from IoT implementation are inherent in IoT deployment, mobility, and complexity (Li, 2017). For instance, a tremendous amount of personal and private information would be automatically collected when IoT is fully implemented into CPMS. Thus, protecting privacy in the network environments becomes a more critical issue because the number of attack vectors and surfaces on CPMS is much larger (Xu et al., 2018).

Notably, insider threats are severely hazardous to any manufacturing system's security, but their risks are even more exacerbated against CPMS's security (Song et al., 2020). Insiders are one of the most difficult attackers to deal within CPMS because Insider threat is a complex problem, which involves computational and physical elements with human factors (Chinchani et al., 2005). This means insiders can exploit the advantages of CPMS to maliciously compromise or manipulate a system, which can result in deleterious consequences to the manufacturing system. More details of insider threats are discussed in the following section.

2.2 Insider Threats

The ancient Roman's question—Who will guard the guards themselves?—alludes to the notion that insider threats are perpetual problems in all aspects of real-world system security (Bishop et al., 2014). In the past, insider threats have mainly been discussed among information and computer system communities, who found that intentional insider misuse of information systems resources can be a significant threat to organizations (D'Arcy et al., 2009). As developments of modern global economic and technological infrastructure contribute to an increasingly turbulent and dynamic environment for organizations, the use of information systems has been widespread (Warkentin & Willison, 2009). However, at the same time, their internet-based mechanisms for global interactions introduced a greater vulnerability to the information systems. Researchers of the information security area evaluated that nearly half of intrusions and security violations occur by insiders (Crossler et al., 2013).

Meanwhile, advances in automation and network technologies have enabled the manufacturing industry to take a step forward towards Industry 4.0, and its manufacturing system has become a newcomer in recognizing the gravity of insider threats (Song & Moon, 2020a).

2.2.1 Reports from security organizations

In this section, security reports regarding insider threats in the manufacturing industry are presented.

2.2.1.1 National Insider Threat Task Force (NITTF)

National Insider Threat Task Force (NITTF) was established to forge insider threat detection and prevention programs and to assist federal agencies in developing and implementing these programs in October 2011. In their report, entitled "Protect Your Organization from the Inside Out: Government Best Practices," NITTF defines insider threats not only in terms of information assets or technology but also physical assets as follows: "The insider threat is the risk an insider will use their authorized access, wittingly or unwittingly, to harm their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practices (NIFFT, 2016)."

Also, to provide executive branch departments and agencies with guidance handling insider threats in organizations, NIFFT published "Insider Threat Guide 2017" that offers direction in implementing the basic building blocks of insider threat programs with major categories of the minimum standards, including: i) Designation of Senior Officials, ii) Program Personnel, iii) Access to Information, iv) Employee Training and Awareness, v) Monitoring User Activity on Networks, and vi) Information Integration, Analysis, and Response (NIFFT, 2017).

2.2.1.2 CERT National Insider Threat Center

CERT, the national insider threat center, at Carnegie Mellon's Software Engineering Institute (SEI) focuses on the following items: incident response, network situational awareness,

malicious code analysis, secure coding, resilience management, insider threats, digital investigations and intelligence, workforce development, DevOps, forensics, software assurance, vulnerability discovery and analysis, and risk management (CERT, 2017).

CERT also perceived insider threats from two points of view. To identify the organizational management practices that impact the frequency of cyber-related information theft and physical-related sabotage, CERT conducted an organizational survey. The samples that were used to derive the survey of perceived organizational support are from employees, workers, and clerks from various industries as well as manufacturing. From the survey, CERT shows that there is a negative correlation between perceived organizational support and intentional (primarily malicious) counterproductive work behaviors (Moore et al., 2016).

To inspect the problem of insider threats that impact organizations across all industries, the above effort was extended in "The Common Sense Guide to Mitigating Insider Threats" (CERT, 2019). These guidelines are based on over 1,500 cases of insider threats from their database.

2.2.1.3 IBM

IBM has been publishing annual security reports based on their client information since 2015 (IBM, 2015, 2016, 2017, 2018, 2019, 2020b), and insider threats have always been discussed in these reports. IBM defines an insider as anyone, who has physical or remote access to a company's assets; they could be employees of the company but also be third parties, such as business partners, clients, or maintenance contractors (IBM, 2016).

Particularly, inadvertent insiders, who are unknowingly the primary source of a security incident through their unaware or negligent actions, are focused on because they were responsible for more than two-thirds of total security incidents in 2017 (IBM, 2017). There are three representative malicious behaviors from the inadvertent insiders: i) falling for phishing scams or

social engineering, ii) improperly configuring systems, servers, and cloud environments, and iii) foregoing or sharing passwords (IBM, 2019). Moreover, According to the survey among 204 benchmarked organizations from 2019 to 2020, insider threats by inadvertent insiders take 63 percent of the total number of incidents, and the annualized cost was $4.58 million (IBM, 2020a).

2.2.1.4 GURUCUL

GURUCUL, which is a global cybersecurity company, started publishing insider threat reports beginning in 2019. According to the survey at the 2019 RSA conference, the manufacturing industry is the most vulnerable industry against insider threats, and 40% of insider threats in the sector could not be detected initially, nor detected after the data had been breached (GURUCUL, 2019). In the 2020 survey, more than 68 percent of respondents from various industries answered that their organizational systems are vulnerable to insider attacks, and also, they confirmed that insider attacks are becoming more frequent compared to the past 12 months (GURUCUL, 2020). These results show a significant increase in the 2021 survey with the same respondent demographics; Almost all respondents answered that they experienced insider attacks in the past 12 months and consider increasing access control with unified visibility across all organizational entities (GURUCUL, 2021).

2.2.2 Insider Threat Risk Assessment Models

In an early stage, to tackle the risk of insider threats in a manufacturing system, risk assessment frameworks have been a focus of increased attention by researchers. Since the appropriate countermeasures can be established by identifying tactics and strategies of an adversary, many insider threat risk assessment models have been proposed (Chinchani et al., 2005).

To identify a method that effectively analyzes threats for any organization, the author (Hashim et al., 2018) analyzed the features of various insider assessment frameworks, including NIST, FRAP, OCTAVE, and CRAMM. According to the paper, NIST assesses the risk of insider threats in qualitative and quantitative ways, which is more dynamic and suitable for organizations to estimate the impact of risk (Nostro et al., 2014).

Furthermore, when an access control system examines access requests, threat likelihood is also one of the important elements that should be taken into consideration. To compare and calculate the likelihoods of insider threats, a new approach that can qualitatively and quantitatively evaluate the security and integrity of the subjects has been proposed (Boulares et al., 2017). To validate the approach, the author defined formulas by summarizing and comparing examples, which take different variables.

Although proposed methods have been used to detect insider threats, they can be discovered after the damage occurred. To address this drawback, a risk assessment methodology that evaluates the level of insider threats before the attack occurs has been proposed (Ahmad et al., 2014). Compared with previous works, it assesses the risk of insider threats in a practical and quantitative way. In this methodology, companies are able to compute a Threat Score (TS) based on the attributes and behaviors of each employee and the vulnerability of an employee's equipment. Moreover, due to the increasing number of insider attacks that have been launched by disgruntled or unsatisfied employees, the methodology creatively adds psychological indicators into the behavior assessment.

Also, it is pointed out that a severe challenge exists in Information and Communications Technology (ICT) organizations (Nostro et al., 2014, 2013). To identify insiders and mitigate the

possible threats, the author proposed a methodology, which considers socio-economical aspects, an attack's impact on the entire system, and possible countermeasures into consideration.

2.3 Blockchain

Blockchain technology's innovative defensive mechanism has been widely publicized after Satoshi Nakamoto proposed bitcoin in 2008 (Nakamoto, 2009). However, the foundational concept of the blockchain, a distributed database, was proposed in the late 1970s (Sherman et al., 2018). Specifically, the concept includes the idea of conserving all transactions with all the modification histories to the collected data, which is the core algorithm principle of the modern blockchain. Ralph C. Merkle proposed a *Merkle Hash Tree*, which can immutably chain blocks of information with a cryptographic hash function; it becomes a blockchain's cryptographic technique (Merkle, 1988).

Recently, blockchain technology has received significant attention in manufacturing industry because it has a great potential to sustainably augment future manufacturing systems and eliminate security challenges related to it (Lee et al., 2019). In this section, the proposed blockchain applications for manufacturing systems are presented, and advantages of the blockchain implementation into manufacturing systems are described as well as its challenges.

2.3.1 Advantages

One of the most significant merits of the blockchain implementation in manufacturing systems is that blockchain can guarantee the production credit and the balance of profits without a highly trustworthy third party (Liu et al., 2017). Particularly, blockchain can be used to establish a secure Machine-to-Machine (M2M) communication (Yin et al., 2017). In CPMS, M2M communication, including Machine-to-Cluster(M2C), are both key technologies to realize CPMS's

innovative features, and it is vulnerable to Cyber-Attacks (Kim et al., 2010). Although the communication can be less efficient if its form is changed from a centralized system architecture to a decentralized system architecture, M2M communication can be trusted within the system areas—public networks area, device area, and private area (Yin et al., 2017).

Moreover, by developing systems based on the decentralized system architecture, CPMS makes further improvements in service value and maximizes the benefits of all stakeholders in the value chain of manufacturing, as well as manifests the integration of decentralized manufacturing resources (Zhang et al., 2017). Accordingly, the vision of industry 4.0 indicates that a majority of manufacturing systems is changing from integrated and centralized systems to shared and distributed systems (Li et al., 2018).

The blockchain can help manufacturing systems by overcoming critical challenges regarding the data exchange among system entities and eventually supporting a consistent data flow along the production chain (Frey et al., 2019). Recent developments in blockchain technology show that it can support the development of sharing economy use cases and provide a promising solution for establishing and maintaining trust by storing production information in an immutable, distributed ledger (Geiger et al., 2019).

2.3.2 Challenges

However, implementing blockchain in manufacturing systems presents many challenges due to the systematical differences between existing blockchain platforms and manufacturing system architecture (Song & Moon, 2020c). The main challenges of applying the blockchain to CPMS can be learned from the actual implementation in the industry (Dorri et al., 2016). Since the public blockchain cannot be owned by any central authority, the node management on the

network is an issue. For instance, it is difficult to detect and validate malicious external participants. Furthermore, the smart contract structures cannot enforce participants to follow the contract terms and conditions, which is critical to the manufacturing industry (Dorri et al., 2017). Also, implementing the blockchain to the real business logic would not be always feasible, due to legacy equipment still being used in the current manufacturing system (Lee et al., 2019). Besides, there are still attack threats that are specially targeting decentralized systems, such as 51% attack and Decentralized-Denial-of-Services (DDOS) (Natoli & Gramoli, 2016). However, such attacks require much more computing powers and resources to initiate and implement the attacks, and thus may occur less frequently than other Cyber-Attacks; more analysis is required so that countermeasures can be prepared.

Chapter 3. Blockchain Technology in Manufacturing Systems

This chapter covers how manufacturing systems in literatures have adopted blockchain technology while maintaining their production capacity, flexibility, and cost-efficiency. In order to methodically approach the subject matter, five categories of manufacturing systems—Cyber-Manufacturing System, Supply Chain Management, Internet of Things, Cloud Manufacturing, and Additive Manufacturing—all striving to achieve the goal of Industry 4.0 are defined and exploited to provide a system model-based analysis. Also, a technology roadmap—that visualizes the chronological history of the technology—has been adopted to present the research trend and identify opportunities for future studies.

3.1 Blockchain Research Trend in Manufacturing Systems

The development of a new paradigm for manufacturing systems has been accelerated by increasing demand for more personalized, smart, and sustainable products with the rapid adoption of the industrial internet, 3D printing, and cyber-physical technologies (Moghaddam et al., 2018). However, such a system ushers in serious security challenges, due to its enlarged accessibility and connectivity. Also, the sheer volume and pervasiveness of data allow system security more vulnerable against insiders and outsiders (Song & Moon, 2020c; Wu & Moon, 2020).

To address such security issues in manufacturing systems, blockchain technology has been proposed by numerous researchers (Khan & Salah, 2018). Blockchain technology is a new security defensive mechanism based on a decentralized notion that brings new possibilities of security, resiliency, and efficiency of various systems. It can enable manufacturing systems to have more agile value chains, faster product innovations, closer customer relationships, and quicker integration with the Internet of Things and Cloud Technology. In addition, a system can benefit from the blockchain by lowering the cost of trade with a trusted contract monitored without intervention from a third party (Ahram et al., 2017).

However, research regarding the use of blockchain technology in manufacturing systems has only begun in the past few years. At the same time, the scope of related research has been widened as a system architecture requires a different strategy for each unique system. As a result, research results of using blockchain technology in manufacturing systems have been disseminated through a wide range of different outlets. Therefore, it becomes difficult for researchers and practitioners to keep track of all the new findings reported in various publications (Kasten, 2020).

To resolve this issue, a survey was developed and is presented to reveal how blockchain technology has been studied and implemented into manufacturing systems. To methodically

organize the survey, five categories of manufacturing systems striving to achieve the goal of Industry 4.0 are identified. Different approaches using blockchain technology are classified to provide system model-based analyses. Each system model's trend and strategy in employing blockchain technology are discussed. Also, to present the trend of research of blockchain technology in manufacturing systems, a technology roadmap—a visualization of the chronological history of the technology—has been adopted. The technology roadmap can be used to define and present a timeline for the development of future core technologies (Shim et al., 2019). The road map is used to draw a conclusion that explains the research trend and presents opportunities for future studies.

3.2 Literature Selection Methodology and Result

In order to develop a set of source bibliography with highly relevant papers on blockchain applications in manufacturing systems, as well as efficiently perform an analysis of the applications in depth, the three-step selection process was established and utilized in this survey.

The first step is a keyword screening, which acquires papers in a wider scope of the subject by using a simplistic combination of keywords. Although this results in including some irrelevant papers that do not concern the actual subject, collecting papers from a wider scope can prevent papers that are highly related to the subject from being overlooked. The second step is a noise screening that removes irrelevant papers generated from the first step. Considering the problem statement and hypothesis of the paper, exclusion criteria based on the subject are applied to make a choice decision in this step. At the same time, citations of the paper are also considered. Finally, to analyze the acquired source bibliography thoroughly and provide a clear technology roadmap, classification is conducted. All the papers in the source bibliography are classified to a

manufacturing system type aiming at industry 4.0. The standards of the classification category are i) a manufacturing domain of the system, ii) objective of the manufacturing system, and iii) manufacturing operation process. From this step, the papers for minor manufacturing systems that cannot form a cluster due to the low sample sizes are screened to highlight the most significant papers connected to major manufacturing systems. The details of each step are described in the following sections.

3.2.1 Step 1: Keyword screening

Two main keywords are applied to obtain a raw paper list regarding the blockchain applications for manufacturing systems: Blockchain and Manufacturing. To collect potential raw papers as much as possible, similar or related keywords—such as Block Chain, Shared Ledger, Decentralized system, Decentralization cryptography, etc.—were also attempted, but did not return distinctive results, and only resulted in noise papers.

For the search engine, Scopus with filtering only journal and conference papers was used, and it resulted in 416 papers published between 2014 and 2021 (up to 5 February 2021).

3.2.2 Step 2: Noise screening

To identify and remove noise papers, the exclusion criteria were established and used for Noise screening. The criteria are as follows:

- Articles are not related to blockchain applications, concepts, techniques, or theories,
- Articles are not related to manufacturing systems aiming at industry 4.0 or vision of the future manufacturing systems,
- Articles are not using blockchain technology to address issues regarding systems' security.

By using the above criteria, a total of 319 noise papers were identified and removed. Afterward, a reference analysis was conducted on the 97 papers, and additional 12 papers were found. Therefore, a total of 109 papers were selected as the source bibliography and used for the survey.

3.2.3 Step 3: Classification

It is important to perform a survey by different categories of manufacturing systems to provide a valid technology roadmap because the timelines for the development of technology differ according to the system domains, objectives, and operation process. Meanwhile, from the classification, a small number of papers that are not enough to represent a chronological history of the technology should be removed. From the 109 papers, four papers were screened due to the small group size, including: two papers about green manufacturing systems, one paper about power grid systems, and one paper about agricultural manufacturing.

Finally, from the classification, five categories of manufacturing systems were identified and used to conduct the analysis and develop the technology roadmap. Their categories and classification results are presented in Table 3.

Table 3 Categories and Classification Result

System	Nomenclature	Paper#
Additive Manufacturing	AM	9
Cloud Manufacturing	CM	12
Cyber-Manufacturing System	CMS	36
Internet of Things	IOT	24
Supply Chain Management	SCM	24

The classification categories were created based on the standard introduced earlier, and each category can be differentiated by the three standards. Details of each category of

manufacturing systems are described in Section 3. Before that, brief quantitative analyses are presented in Figure 1.

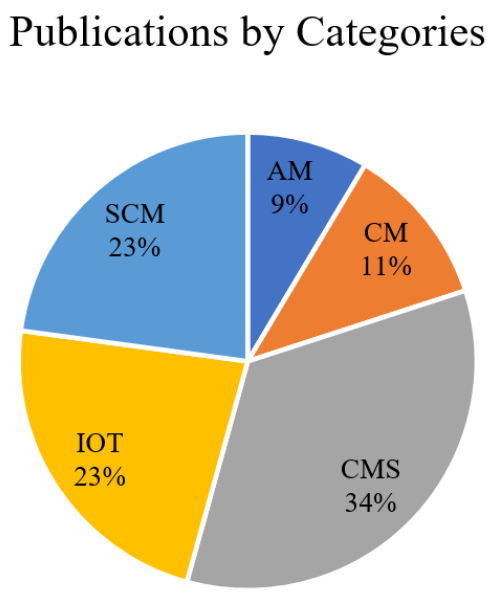
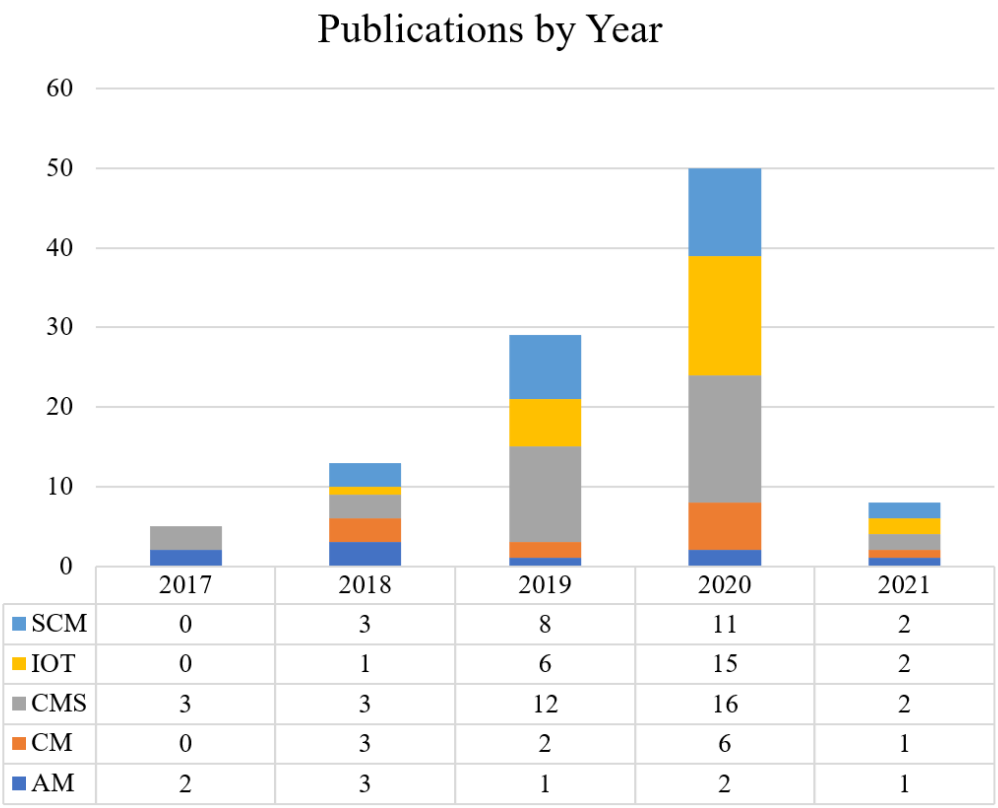


Figure 1 Publications by Categories

The figure shows that 34 percent of the blockchain applications are for Cyber-Manufacturing System (CMS). Supply Chain Management (SCM) and Internet of Things (IOT) take the same value of 23 percent, while Additive Manufacturing (AM) and Cloud Manufacturing (CM) take 9 percent and 11 percent, respectively.



	2017	2018	2019	2020	2021
SCM	0	3	8	11	2
IOT	0	1	6	15	2
CMS	3	3	12	16	2
CM	0	3	2	6	1
AM	2	3	1	2	1

Figure 2 Publications by Year

Seen from Figure 2, the number of publications has increased each year. Considering that the papers were collected up to 5 February 2021, it is expected that the number of publications in 2021 will be more than 2020. The blockchain application for CM was proposed for the first time in 2016, but the number of SCM, IOT, and CMS surpassed CM after 2019.

3.3 Blockchain Implementation Strategies in Manufacturing Systems

3.3.1 Cyber-Manufacturing System (CMS)

CMS is a future vision for the manufacturing system, where physical components that are fully integrated and seamlessly networked with computing processes, resulting in an on-demand, knowledge-rich, communicable repository of manufacturing resource (Kasten, 2020; Shim et al., 2019; Song & Moon, 2019b). Also, capabilities with optimal, sustainable manufacturing solutions

can be enabled. The CMS paradigm was developed in response to recent advances on the Internet of Things, cloud computing, fog computing, service-oriented applications, modeling and simulation, virtual reality, embedded systems, sensor networks, wireless networking, machine learning, data processing, automated manufacturing methods, and so on. By using these technologies, manufacturing resources and capabilities can be sensed and linked directly or through the Internet. Intelligent activities of manufacturing components and processes, such as self-awareness, self-prediction, self-optimization, and self-configuration, are enabled by this degree of interactions and communicative mechanisms (Song & Moon, 2017).

3.3.1.1 Challenges in CMS

However, manifesting fully functioning CMS is delayed due to the many challenges. First, there is lack of standard for connection protocols among legacy manufacturing equipment. Compared to existing internet-based systems in other industries, manufacturing machinery have less connectivity, and even those entities have their own protocols that are not compatible with other protocols, such as Programmable Logic Controller (PLC) (Song & Moon, 2020b). Moreover, the majority of the equipment uses different types of sensors, hardware, and software, which leads to different data formats and acquisition requirements. Also, a sheer volume of data being exchanged in CMS causes other types of connection issues. The volume, velocity, and variety of the generated data from physical and digital entities of CMS become an attractive target for inside or outside intruders due to their pervasiveness (Wu & Moon, 2018). For these reasons, CMS inadvertently ushers in critical cyber security challenges. Cyber-Attacks can exploit CMS's vulnerable connections and enlarged attack surface from the data being exchanged in the system to cause physical damage: Cyber-Physical Attacks (Chhetri et al., 2016; Lee et al., 2016). The cyber security is one of the major hurdles in realizing fully functioning CMS.

3.3.1.2 Strategies for CMS

Due to the lack of a standard for connection protocols, trust issues can occur in establishing reliable partnerships without a highly trustworthy technology (Liu et al., 2017). Current connection protocols are not able to enable secure communications among different heterogeneous physical entities in CMS (Yin et al., 2017). To address this issue, blockchain technology can be implemented to provide transparent and trustworthy standard protocol among organizations, factories, or users (Durán et al., 2020).

Because of the asymmetry in exchanging data in CMS, there are challenges of ensuring the ownership of the data as well as the data integrity by users or physical machinery of the system (Frey et al., 2019). Besides, there is a lack of a secure and trusted digital infrastructure to efficiently integrate entities that have different data format and acquisition requirements, thus it causes further trust issues (Ouyang et al., 2019). Moreover, the continuous-growing diverse manufacturing data hinders a practical and optimal solution to transmit all data via system networks (Leng et al., 2020). Blockchain can help to process the unstructured manufacturing data by enabling transparent sharing of manufacturing data within the CMS (Chung et al., 2019; Ho et al., 2019).

A sheer volume of data that is generated in CMS during the operation process is exchanged in digital format through networks (Zhang et al., 2017). This results in a need for centralized data centers, such as a cloud storage, which are unable to afford the corresponding management tasks (Gu et al., 2019). Also, frequent data requests and provisions among many physical entities of the CMS bring great challenges to the centralized database storage system in terms of storage capacity, processing capabilities, and energy consumption (Li et al., 2019). To solve this issue, the distributed system mechanism can be used to improve the efficiency of value interaction while lower the cost.

There were mainly four strategies used to implement blockchain technology into CMS: Smart contract, Multi-chain, Platform, and Platform with smart contracts.

The smart contract is a set of codified clauses that enables communications with a certain blockchain platform, specifically Ethereum. Ethereum protocol allows to conclude contracts between agents for the execution of program logic, thus the smart contract is trackable, secure, and unalterable (Mohamed & Al-Jaroodi, 2019). By using immutable self-logic codes, the smart contract can be used to implement blockchain technology into CMS (Kapitonov et al., 2018).

The multi-chain structure achieves the data isolation of the system. At the same time, the multichain structure can handle the high concurrent communication requirements of devices belonging to different chains (Li et al., 2019).

An independent platform can exploit the advantage of a blockchain without the modernization of legacy equipment (Chung et al., 2019). It can also be adopted to ensure both the device-level data transmission and the manufacturing service transaction (Lee et al., 2020).

Furthermore, the platform constructed with smart contracts can be a breakthrough for diverse manufacturing systems, where the requirement and resource information are embedded and controlled by the smart contracts' self-logic codes (Yu et al., 2020).

3.3.2 Supply Chain Management (SCM)

Consultants first coined the term Supply Chain Management (SCM) in the early 1980s, and it has been a focus of increased attention (Chen & Paulraj, 2004a). Supply Chain is a set of entities and organizations involved directly or indirectly in the downstream and upstream flows of services, products, information, and finances from source to customer and customer to source (Mentzer et al., 2001). The Global Supply Chain Forum (GSCF) defines SCM as follows: "Supply

Chain Management is the integration of key business processes from end user through original suppliers that provides products, services, and information that add value for customers and other stakeholders (Lambert & Cooper, 2000)." Accordingly, SCM describes both internal and external logistics operations, as well as the preparation and management of materials and information flows within an organization. It has also been used by researchers to explain strategic, interorganizational problems, to explore an alternative organizational form to vertical integration, to define and describe a company's relationship with its suppliers, and to address the purchasing and supply perspective (Chen & Paulraj, 2004b).

3.3.2.1 Challenges in SCM

However, due to the fast and extreme development of advanced technology in communications and operation logistics, SCM has also been undergoing drastic changes from its initial status in manufacturing systems. For this reason, unprecedented new challenges in SCM occurred. For example, there are trust issue in information sharing due to the shortcomings of networked production, including delays, asynchronous data between different parties, a variety of sharing methods, irregularity in control systems, and the risk of shared data being tampered with or hidden (Li et al., 2020). Also, the growth of manufacturing system's components within SCM has resulted in high costs of management or even complete reliance on third-party manufacturers (Bose et al., 2018). Furthermore, because of the lack of transparency, information on their manufacturing processes is not easily shared. This absence of the information could put the supply chain at risk. For these reasons, security of SCM can be weakened, and this will result in increasing the risk of supply chain fraud, such as product counterfeiting, as well as any illegal activity (Maroun et al., 2019).

3.3.2.2 Strategies for SCM

Establishment of trust among supply chain is the most important and challenged task in SCM. Particularly, trust only can be extended to the surface-level visible without transparency (Bhattacharyya & Smith, 2018). For this reason, in an increasingly global environment for manufacturing supply chains, developing trust & transparency can be costly. Moreover, business arrangements within SCM can face an unforeseen complexity and result in disputes between even the most well-intentioned parties (ElMessiry et al., 2019). Therefore, SCM necessitates the implementation of blockchain technology to improve transparency in the business networks. Since the characteristics of blockchain technology can meet the demand for enhanced information sharing and transparency in the networks, it is considered the key technical solution (Xu et al., 2019).

The cost for processing documents and information for SCM is more than twice that of the actual physical transportation. Such problems can be addressed by adopting a blockchain into the supply chain ecosystem, in which event data and document workflows are frequently exchanged (Bose et al., 2018). SCM can effectively reduce the delays and uncertainties in sharing the information by decentralizing important information, including inventory levels, manufacturing performance and operations indicators, as well as order and shipment information (Padalkar et al., 2020).

Traditional SCM are operated in a particular condition that participants are isolated, thus it cannot provide comprehensible provenance information (Appelhanz et al., 2016). This results in shortcomings, including insufficient trust between parties, isolated data storage, and unsatisfactory standardization in communication as well as low traceability in SCM (Abeyratne & Monfared, 2016). Moreover, since the growth of fully automated manufacturing systems requires high

traceability in SCM (Westerkamp et al., 2018), it is important to solve the problem with an adequate solution. Such a problem can be addressed by blockchain technology, which attributes to enhance durability, transparency, immutability, decentralization, and verifiability of the system (Altmann et al., 2020). Accordingly, by implementing blockchain technology in SCM, the traceability of the supply chain can be improved (Westerkamp et al., 2020).

In addition to four main strategies from CMS, Technology Acceptance Model (TAM) is added in SCM. TAM is an information systems theory that models the decision-making process by which users may or may not adopt and implement new technology (Maroun et al., 2019). TAM is based on various behavioral factors, such as cognitive usefulness, cognitive ease of use, user attitudes, and behavioral intentions (Liu et al., 2020). The model can effectively exploit blockchain technology to take advantage of decentralized systems (Bhattacharyya & Smith, 2018).

3.3.3 Internet of Things (IOT)

The term Internet of Things (IOT) was first introduced by Kevin Ashton in 1999 in the context of supply chain management (Gubbi et al., 2013). IOT is a new model that is rapidly gaining popularity in the modern wireless telecommunications scenario. The basic idea of this concept is the pervasive presence around us of a variety of things or objects—such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. By specific addressing schemes, these things or objects are able to communicate with each other and collaborate with their neighbors to achieve common goals (Atzori et al., 2010). The main benefit of the IOT concept is that it will have a high impact on several aspects of the daily life and behavior of potential users. From a private user's point of view, the introduction of the IOT will be felt most clearly in the work and home domains. In this context, robotics, assisted living, e-health and

enhanced learning are just a few examples of application scenarios where new paradigms may play a leading role in the near future. In the same way, from the perspective of manufacturing industry, the most obvious consequences will be seen in the areas of automation of industrial manufacturing, logistics, business/process management, and the intelligent transportation of people and goods (Atzori et al., 2010).

3.3.3.1 Challenges in IOT

However, it necessitates adequate security measurement before it can be fully realized. Current IOT devices have had high-risk vulnerabilities in security for a long time, due to enlarged connections of IOT devices based on a centralized system (Cao et al., 2020). For instance, in 2016, the Mira botnet, a US domain name resolution service provider, launched a DDOS attack on Dyn (Dyn.com). By controlling a large number of IOT devices, this attack caused a large-scale network disconnection in the eastern United States. Such attacks pose a significant risk to the protection of user data and can result in data leakage. Also, because of the large amount of data from independent devices cause the delays in data processing. Moreover, such risk produced a network trust issues. IOT adopters are wary of technical partners that can grant system access and control to authorities (e.g., governments, suppliers, or service providers), allowing them to capture and analyze user data. As a result, the future IOT solutions should prioritize trust and anonymity (Li et al., 2016).

3.3.3.2 Strategies for IOT

For a transparent IOT ecosystem, it is necessary to verify all the connected devices. As the growth of the number of IOT devices within the system boundary, continuous management and verification of these devices will cause a high cost (Bai et al., 2019). Also, to enable efficient computing and communication capabilities among IOT devices, the sensors are connected with

each other and with the manufacturing controllers—such as programmable logic controller and SCADA—through the internet (Bhattacharjee et al., 2020). This makes IOT systems an attractive target for Cyber Attacks. To address this issue, blockchain can be implemented into IOT system to protect the device during its operation by validating its communications (Matheu et al., 2020).

A massive amount of data is constantly generated from IOT devices at high speeds, and it is difficult to meet the processing time requirement (Lallas et al., 2019). Moreover, independent systems that differ from each other can lead to complex integration (Assaqty et al., 2020). By ensuring real-time, accuracy, and effectiveness, blockchain technology can provide privacy preservation in data processing (Lin et al., 2020).

IOT facilitates cloud storage to process information data in a more systematic way, which converts it into real-time actions and information (Díaz et al., 2016). Even though the use of cloud storage is essential in IOT, there is a threat to data security, transparency and privacy (Iqbal et al., 2020). To tackle this issue, data generated from IOT devices can be leveraged through blockchain to reduce the high "trust tax" imposed on global users in IOT networks, including customers, suppliers, distributors, governments, service providers, and other manufacturers that unnecessarily trust each other (Zhang et al., 2019).

3.3.4 Cloud Manufacturing (CM)

Cloud Manufacturing (CM) is a computing and service-oriented manufacturing model that was built from existing advanced manufacturing models and industrial information technology with the help of cloud computing, IOT, virtualization, and service-oriented technologies (Tao et al., 2011). CM aims to achieve maximum sharing and circulation, high usage, and on-demand use of various manufacturing resources and capabilities by providing secure and dependable, high-

quality, low-cost, and on-demand used manufacturing services across the manufacturing lifecycle. More specifically, using IOT technologies—e.g., radio frequency identification (RFID), wired and wireless sensor networks, as well as embedded systems—various manufacturing tools and abilities can be intelligently sensed and linked into the wider internet, and automatically managed and monitored in a CM system. The manufacturing tools and abilities are then virtualized and encapsulated into various manufacturing cloud services (MCSs) that can be accessed, invoked, deployed, used on-demand using virtualization, service-oriented technologies, and cloud computing technologies (Tao et al., 2011).

3.3.4.1 Challenges in CM

However, CM has trust issues to be solved. There is no technical solution to promote trust among users in CM due to its systematical limitation from the centralized network architecture. Existing models commonly use centralized networks and third-party management, which presents a number of drawbacks, including trust issues. The centralized network not only diminishes the CM's efficiency but also introduces shortcomings such as scalability and a fragmented communication model. For this reason, any kind of Cyber-Attack can incur massive damage to the system. Besides, certain physical machines in the manufacturing system could be located in unsecured environments, therefore, they can be easily tampered with by intruders. Furthermore, data is transmitted via a wireless network to a centralized database, which may be a security vulnerability in the system (Li et al., 2018).

3.3.4.2 Strategies for CM

The development of advanced technology in CM allows customers instant pricing and access to a large capacity of manufacturing nodes (Barenji et al., 2018). However, many of CM systems exploit a centralized network with data flowing through an intermediary agent connecting

clients with service providers (Hasan & Starly, 2020). The centralized network not only reduced the productivity of the CM but also bring various flaws, including: scalability issues, a broken communication model expose vulnerabilities against cyber-attack (Tao et al., 2011). In this regard, blockchain technology can provide a potentially viable solution to this issue, thanks to its unique validation process from a decentralized system architecture (Zhu et al., 2020).

3.3.5 Additive Manufacturing (AM)

Additive manufacturing (AM), also known as 3D printing and rapid manufacturing, is a category of manufacturing technologies that can create complex objects by stacking layered material automatically before a three-dimensional object is printed (Baumung & Fomin, 2018). The majority of related AM technologies use powder or wire as a feedstock, which is selectively melted by a concentrated heat source and then consolidated after cooling to form a component (Herzog et al., 2016). Compared to subtractive manufacturing, AM can manufacture complex or custom parts directly from a design without the use of costly tooling or shapes like punches, dies, or casting molds, and it eliminates several machining steps. Also, by removing or reducing the need for multiple component assembly, considerable manufacturing expense reductions can be achieved. Moreover, parts may also be manufactured on demand, eliminating spare parts inventory and reducing lead times for essential or out-of-date replacement parts (DebRoy et al., 2018).

3.3.5.1 Challenges in AM

However, AM's security concerns are growing due to the sheer volume and pervasiveness of data and increased accessibility in the networks. Particularly, Cyber-Physical Attack has become a serious threat to the AM operation. Since the infill structure of the 3D model is usually generated during the conversion process of a CAD file to G-code by the third-party program, the

process can be vulnerable to such attacks. Also, it is hard to detect the attack on infill structure because interior defects can occur without affecting the exterior (DebRoy et al., 2018). Accordingly, the challenges exist in authorized access to product data, assured supply of the agreed quantity, distinction of original parts from counterfeits, as well as protection of intellectual property, product liability, and warranty (Stjepandic & Biahmou, 2016).

3.3.5.2 Strategies for AM

As AM gain attention increasingly in many industries, the need to prevent counterfeiting AM-produced parts increases (Kennedy et al., 2017). The counterfeit AM parts can pose a serious issue because they appear similar to the original parts but have different infill structures. This results in the lack of functionality or tensile strengths in the specific material composition of the object, which may lead to part failure (Campbell & Ivanova, 2013). Blockchain technology can provide a promising solution for acquiring reliability in the additive manufacturing process.

AM improves its production efficiency by remotely sharing digital information, such as construction plans, CAD files, or material specifications to manufacture physical goods (Kurpjuweit et al., 2021). However, significant challenges from compromised access authorizations can cause the breaching of important data, such as product specification, assured supply of the agreed quantity, intellectual property, as well as product liability and warranty (Holland et al., 2017). Blockchain can help AM to overcome authorization issues, allowing them to take advantage of decentralization-based security (Klöckner et al., 2020).

3.4 Technology Roadmap

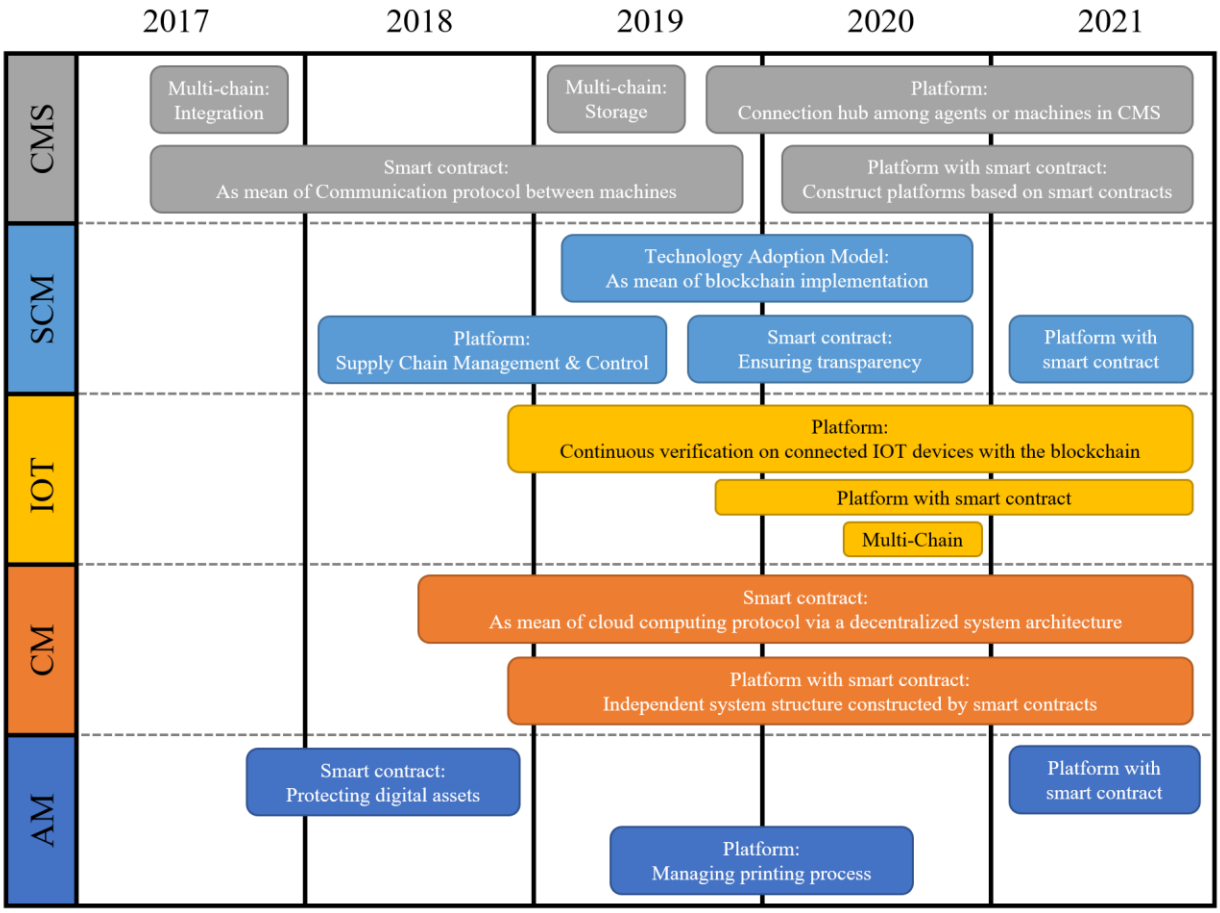


Figure 3 Technology Roadmap

To visualize strategies exploited by manufacturing systems to resolve their unique challenges, a Technology Roadmap was developed. The Technology Roadmap can be helpful in drawing a conclusion that identifies the research trends and opportunities for future studies.

Contract from Ethereum was also tried to manifest secure management systems, and it became a component of a platform to provide more independent and stable services in SCM. Platform development was the mainstream of the blockchain implementation strategies for IOT, because it is efficient to conduct continuous verification on a large number of IOT devices. Also, the smart contract was exploited to tackle data processing issues. Most of the applications for CM

were based on the use of the smart contract. Especially, it was used to play the role of computing protocol to provide more secure cloud service in the manufacturing industry. For AM, the smart contract and platform were proposed to implement blockchain technology to ensure reliability in the additive manufacturing process and access authorization issue.

Overall, manufacturing systems leveraged existing blockchain applications—mainly about a financial trading system—to address their challenges in the early stage. However, these attempts cause many challenges and limitations due to the systematical differences between financial and manufacturing systems. Accordingly, a customizable platform with blockchain technology has been published to handle such issues. In most recent, the smart contract from Ethereum was used to compose and operate a platform to improve data processing efficiency, flexibility, and cost deduction.

In conclusion, more and more blockchain platforms would be considered, developed, and proposed to resolve current issues in the blockchain implementation. Hence, it is essential to understand the effectiveness of the blockchain on reliability and performance in manufacturing systems, and their potentials as manufacturing infrastructures must be properly reviewed. This will contribute to identifying possible solutions for challenges in employing blockchain technology and understanding the impact of various consensus algorithms and programming languages on the blockchain's performance.

Chapter 4. Insider threat tolerant Cyber-Physical Manufacturing System

In this chapter, an insider threat tolerant Cyber-Physical Manufacturing System augmented by a service-oriented blockchain is proposed to overcome security vulnerabilities against insider threats and technical limitations of blockchain technology. First, a discussion of how blockchain technology can mitigate insider threat risks in manufacturing systems is presented. Afterward, a service-oriented architecture (SOA), which motivated the development of a service-oriented blockchain, is reviewed and explained to show how a service-oriented blockchain can enable secure services while reducing redundant connections and optimizing system integration structures. Finally, the insider threat tolerant Cyber-Physical Manufacturing System is introduced with the example to help in understanding how blockchain technology can be implemented into the manufacturing system to secure the system from insider threats.

4.1 Blockchain and Insider Threats

As described in the previous chapter, blockchain technology has been of increased research interest by many researchers to enhance the security of systems in various manufacturing sectors, specifically for manufacturing systems aiming at industry 4.0 (AL-Salman & Salih, 2019). This new paradigm of the security mechanism shows that it is feasible to realize industry 4.0 while ensuring security against intruders. Additionally, blockchain technology can be a technical solution to reduce insider threat risks in manufacturing systems.

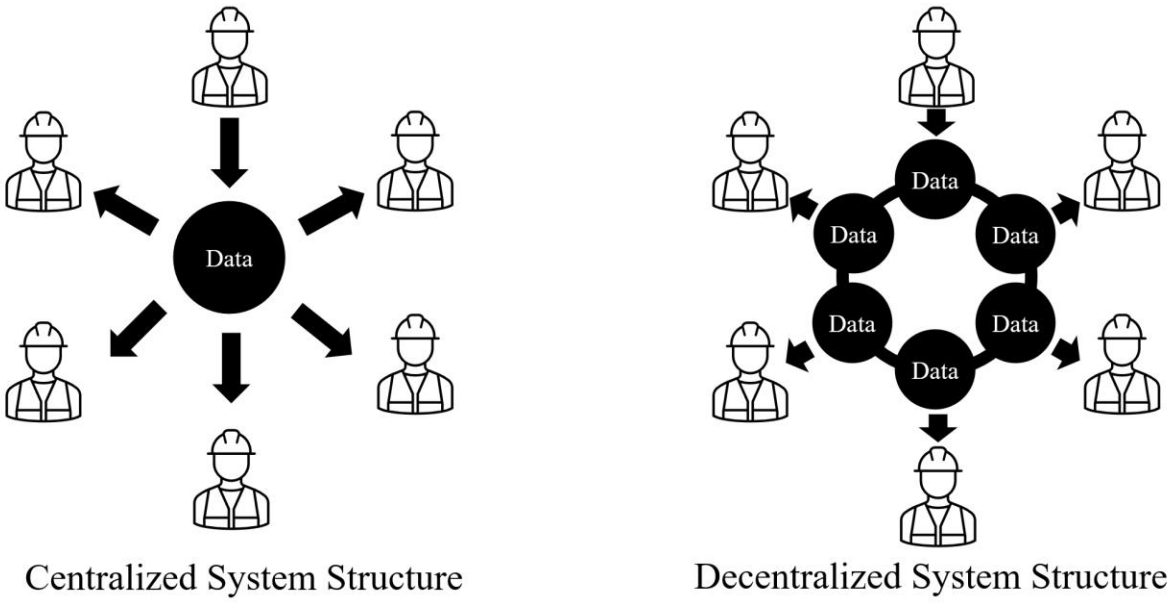


Figure 4 Centralized and Decentralized System Structure

The main reason behind the unprecedented level of security of blockchain technology is a decentralized system structure. Since all the participants in the blockchain networks share identical data and validate each other, the attacker needs massive computing power, time, and resources to successfully launch the attack (Sherman et al., 2018). Accordingly, it is difficult for insiders to inflict insider threats, even though they can bypass or incapacitate the general security mechanisms

by using their legitimate access authentication. For more details, the blockchain's decentralized system structure can be explained by comparing it with a centralized system structure.

For manufacturing systems, the centralized system structure is based on the central control server, which handles system data processing, conversion, storage, and management (Song & Moon, 2020b). Only a limited access authentication for the central control server is allowed and strictly managed because the entire manufacturing operation is configured by the server. Due to its easy configuration, management, and direct control, many manufacturing systems adopt the centralized system structure. Since all manufacturing information and data is controlled and managed by the central control server, a manager or administrator of the system can easily supervise and monitor the manufacturing process. This structure can also provide consistent network environments by enabling stable and predictable communication protocol from the centralization (Hatvany, 1985). Moreover, since every entity in the manufacturing systems is connected and controlled by the server, efficient and optimized integration can be achieved. Thus, it will bring drastic improvements in system performance and response speed.

Meanwhile, the decentralized system structure does not have a server or controller that collectively manages overall system data. Instead, multiple independent entities in the system are functioning as a central control server, and all the entities are connected and establish a decentralized network. In this network, every entity possesses the same data and continuously validates each other to maintain data integrity in the network. As a result, the decentralized system structure's performance is reduced due to the inefficient data management processes. However, such trade-off can be a potential solution for insider threat risks. In lieu of maximizing the system performance, the decentralized based system structure gains reliability. Besides, the stability of the network can be ensured because each entity in the network functions as an independent central

control server. For instance, the attacker cannot incapacitate the system by attacking single target. This can be demonstrated as follows.

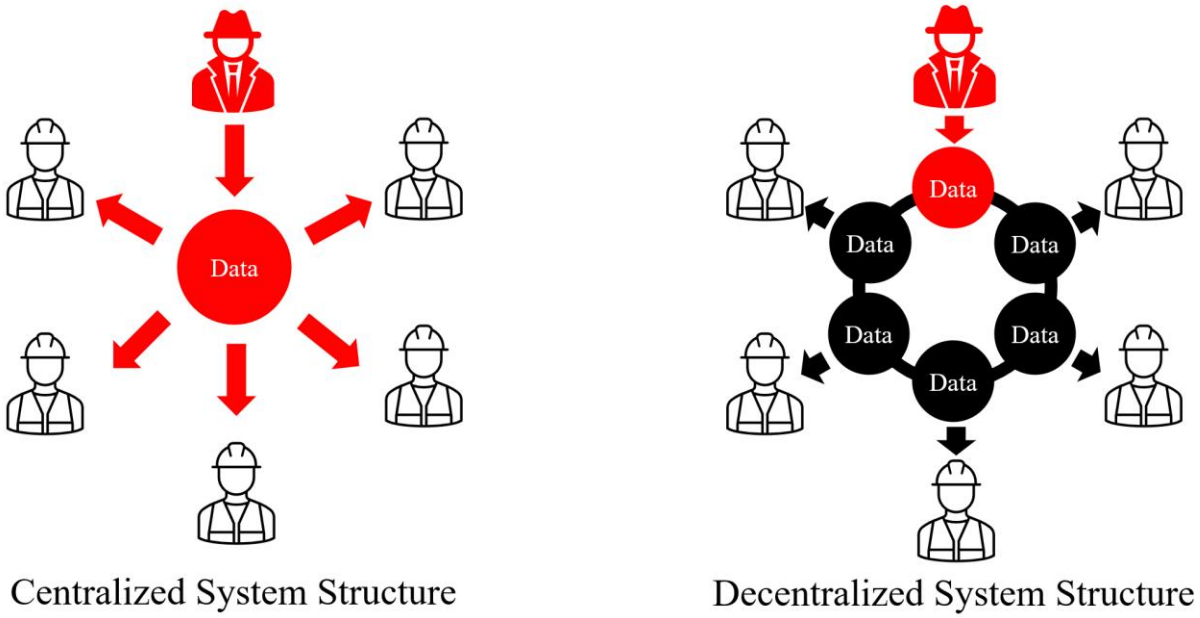


Figure 5 Attack from Insiders

Seen from above, for the centralized system structure, if the malicious insider manipulates the central control server, the data integrity will be compromised without being detected because the insider has the legitimate access authentication or security clearance of the server. Furthermore, this damage will directly affect and harm other entities in the system, because they are seamlessly integrated via the internet and computer networks and always trust the central control server. For this reason, manufacturing systems in industry 4.0 are vulnerable to insider threats, and their risks are increasing.

On the other hand, the decentralized system structure can effectively reduce the damage by using its own systematical architecture. Even though the malicious insider can still manipulate and compromise the data in a certain entity, this damage will not directly be transferred to other entities due to the continuous validation process of blockchain technology. In order to damage this system

structure, the insider would have to attack more than 50% of entire entities simultaneously. Therefore, the attack on the decentralized system structure takes more time, cost, and resources, which enables the system to mitigate insider threat risks.

4.2 Blockchain Implementation

As mentioned earlier in Chapter 4, many researchers have explored blockchain technology to increase the security of manufacturing systems, and a plethora of manufacturing applications with the blockchain have been proposed. According to the survey of manufacturing applications with the blockchain, numerous proposed systems adopted existing blockchain applications to address their challenges. However, such implementations result in other problems because the nature of manufacturing systems is based on the distributed system architecture, not decentralized system architecture.

The decentralized system and distributed system are often used to indicate the same system based on blockchain technology. However, the terms "decentralized' and " distributed" define different system architectures.

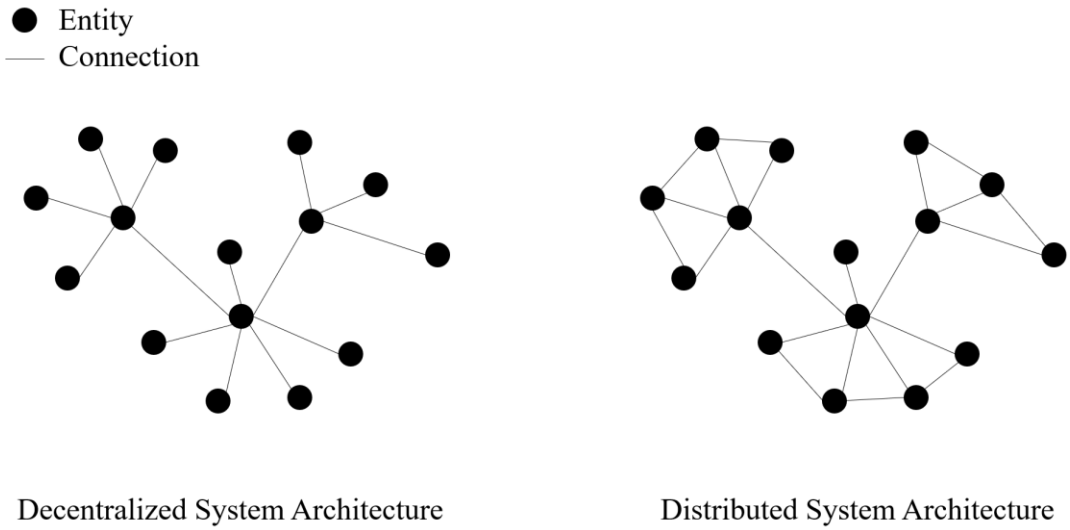


Figure 6 Decentralized and Distributed System Architecture

Seen from Figure 6, in the decentralized system, there is no single entity, which makes the decision for the system operation. Instead, each entity decides its own behavior and actions, which results in the entire system's behavior and performance. Also, since the connection among entities is generally dynamic, it is easy to add a new entity to the system or remove the entity from the system.

However, the distributed system's decisions are collaboratively made by multiple entities. To provide the certain service, more than one entity can be digitally or physically connected and integrated within the system. Therefore, the decision making for the system is more centralized than for the decentralized system. For this reason, manufacturing systems are often based on the distributed system architecture, rather than the decentralized system architecture. The digital and physical entities of the system are integrated to provide various services of manufacturing processes, such as production, quality control as well as resource and order management.

Conclusively, to implement blockchain technology into manufacturing systems without systematical issues, a different approach is needed, and a Service-Oriented Architecture (SOA) can be used.

4.2.1 Service-Oriented Architecture (SOA)

In addition to the systematical differences between the decentralized and distributed system architecture, the demands and requirements for the rapid changes in the manufacturing industry make it difficult to realize fully functioning blockchain manufacturing system. To overcome such problems without compromising performances or cost, it is necessary to approach the problem with a systematical viewpoint, and Service-Oriented Architecture (SOA) can be a potential solution.

For integrating heterogeneous systems, SOA has been explored by many researchers to integrate legacy systems' protocol and platform while remaining its flexibility, adaptability, and simplicity (Xu, 2011). To improve the functionality of interoperable services and adaptability for rapidly changing services, SOA is designed to provide services based on the integrated components of the system.

A service can be considered as a process, which represents the functionalities of the system. SOA can ensure adaptability to rapidly changing business needs by reusing and combining existing services and system components (Iacob & Jonkers, 2009). Also, SOA can implement new business applications by decomposing the existing applications into individual functions and reconstructing them as new services. This enables the recursive aggregation of services, which can create new business processes and publications (Unger et al., 2009). For example, discrete components of a system can be re-composited and reconstructed to be reused for other services. Therefore, SOA allows the system to create new services dynamically to satisfy rapidly changing business needs (Quartel et al., 2009).

Accordingly, SOA can be exploited to implement blockchain technology into manufacturing systems. Specifically, SOA can help to optimize and reduce redundant blockchain communications by enabling blockchain protocol to the service. By applying these ideas and concepts, Service-Oriented Blockchain (SOB) is developed to augment CPMS with blockchain technology while remaining its flexibility, productivity, and cost-efficiency.

4.2.2 Service-Oriented Blockchain (SOB)

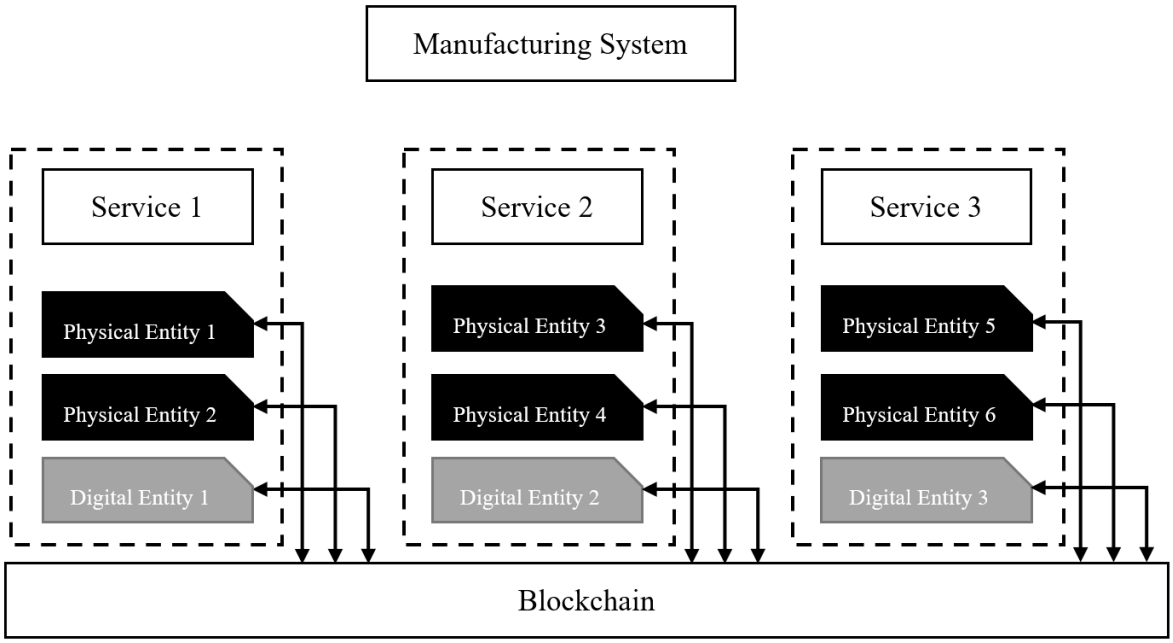


Figure 7 Existing Blockchain Application

The decentralized-based architecture with blockchain technology can be a promising solution to insider threats because it can establish a verifiable communication channel without 3rd party, and insiders will continuously validate each other by using a consensus algorithm. However, since each entity should participate in the blockchain network and communicate via the blockchain protocol, every single data exchange in the system will be delayed due to the arbitrary block generation time and block occurrence frequency. For this reason, the system will have limited system performance. Moreover, since these redundant delays are created from the blockchain's validation process, which cannot be replaced or removed, it is arduous to find technical solutions. Moreover, since all the entities in CPMS are fully connected to enable collaborative manufacturing services, the blockchain augmentation for individual entities is not suitable for the system.

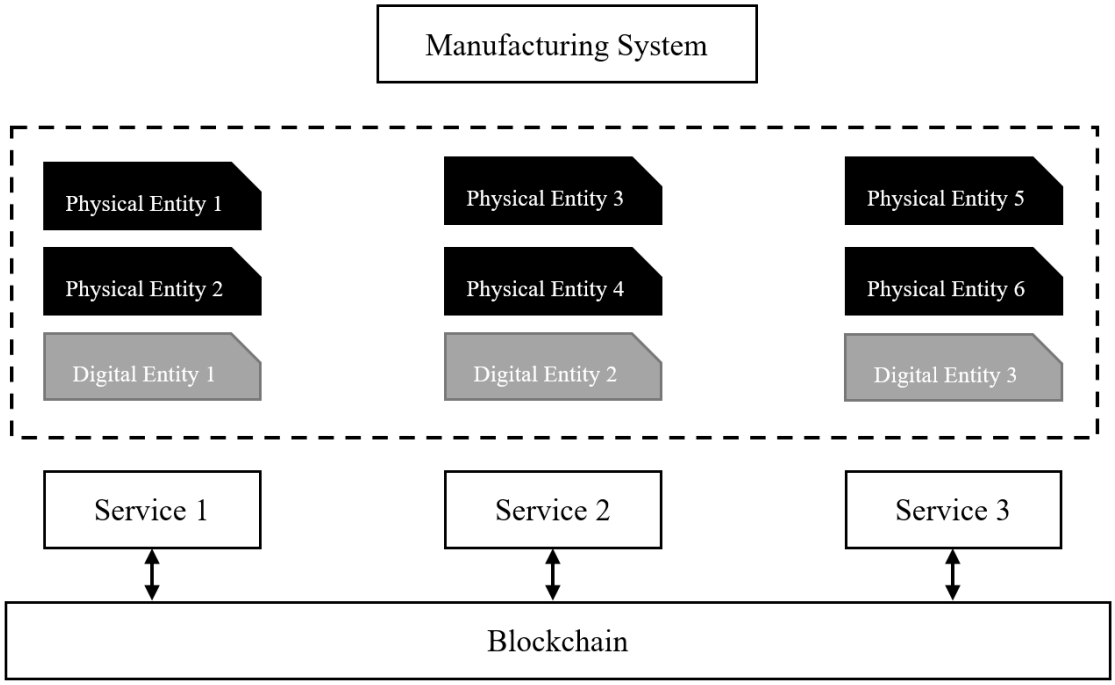


Figure 8 Service-Oriented Blockchain

A Service-Oriented Blockchain (SOB) solves such issues by providing physical and digital entities with the blockchain communication protocol through service applications (Service 1, Service 2, and Service 3), not directly applying the blockchain to individual entities. In this way, multiple entities will be integrated by the service applications, which will enable the services with less arbitrary delays while remaining their strong security from the blockchain. Also, the recursive data transformations between the entities and blockchain can be effectively reduced, and the attack surface is narrowed down to the service layer. Furthermore, new services can be dynamically developed by recomposing, reconstructing, and reusing entities.

4.3 An Insider Threat Tolerant Cyber-Physical Manufacturing System

To overcome security vulnerabilities against insiders and technical limitations of blockchain technology, an insider threat tolerant Cyber-Physical Manufacturing System (ITTCPMS) augmented by a service-oriented blockchain has been proposed. The system consists

of four layers: user layer, entity layer, service layer, and blockchain layer. Details of each layer are discussed in the following sections.

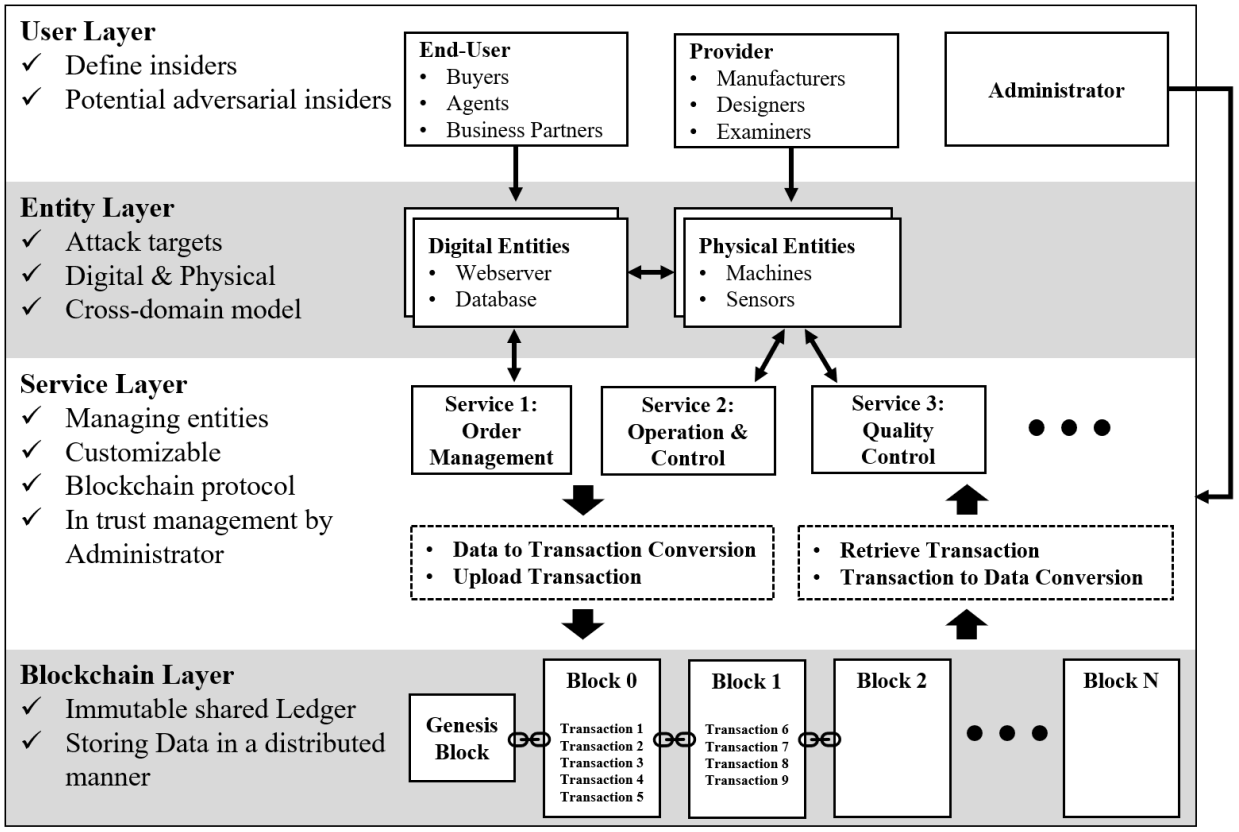


Figure 9 Insider Threat Tolerant Cyber-Physical Manufacturing System

4.3.1 User Layer

Generally, users are not involved in system architectures, but they must be defined in the insider threats research to investigate the influence of insiders and their potential threats. There are three types of users: End-User, Providers, and Administrator. End-User, such as buyers, agents, business partners, can access digital entities in the entity layer, while providers, such as manufacturers, designers, examiners, can access to physical entities. The administrator manages service layer and holds ground truths in the proposed system. It is assumed that all users in the user layers are potential adversarial insiders. They can intentionally manipulate the manufacturing

information or unintentionally reveal the accessible route into the system to outsiders. It is always possible that they can exploit their accessibility and knowledge of the system.

4.3.2 Entity Layer

To investigate vulnerabilities in the system against insiders, a basic model of CPMS must be included. The main system components will be placed in the Entity layer, which is the attack targets for insiders. The entity layer consists of the digital entity and physical entity. The digital entity includes manufacturing specification, operation parameters, resource, and order scheduling management data, while the physical entity represents machines, sensors, and actuators. These entities are seamlessly integrated through the internet and computer network to provide certain services such as order management, production, and quality control.

4.3.3 Service Layer

The service layer is the most important layer in ITTCPMS, and it bridges between the entity layer and the blockchain layer. The main objective of the service layer is to provide physical and digital entities with the blockchain communication protocol through a service layer. In this way, multiple entities will be integrated by the service layer, which will enable the services with less arbitrary delays while remaining its strong security from the blockchain. Also, multiple independent service applications in the service layer can ensure the flexibility and productivity of the CPMS.

Additionally, it is assumed that the service layer is under trust management by the administrator, who manages the service layer and can tailor the layer based on users' needs and entities' requirements.

4.3.4 Blockchain Layer

The blockchain is a way to store data in a distributed system in which the system components have connected each other and form a Peer-To-Peer network. The blockchain's decentralized system structure can offer an innovative decentralized and transparent transaction mechanism (Leng et al., 2020). Figuratively, the blockchain consists of decentralized updated blocks of data. Each block includes various information—such as a timestamp, difficulty, balance, and list of transactions—with a link to a previous block. Also, the blockchain contains connected historical data, which enables every transaction in the database to be traced back to the source (Leng et al., 2021). For this reason, the blockchain can validate the data with each other within the network participants without a third party (Li et al., 2019).

Accordingly, the above decentralized-base validation process makes the blockchain immutable and reliable without a third party. Thus, all sensitive data can be stored in the blockchain layer, and it can only be accessed through the service layer to ensure security against insiders.

4.3.5 Example

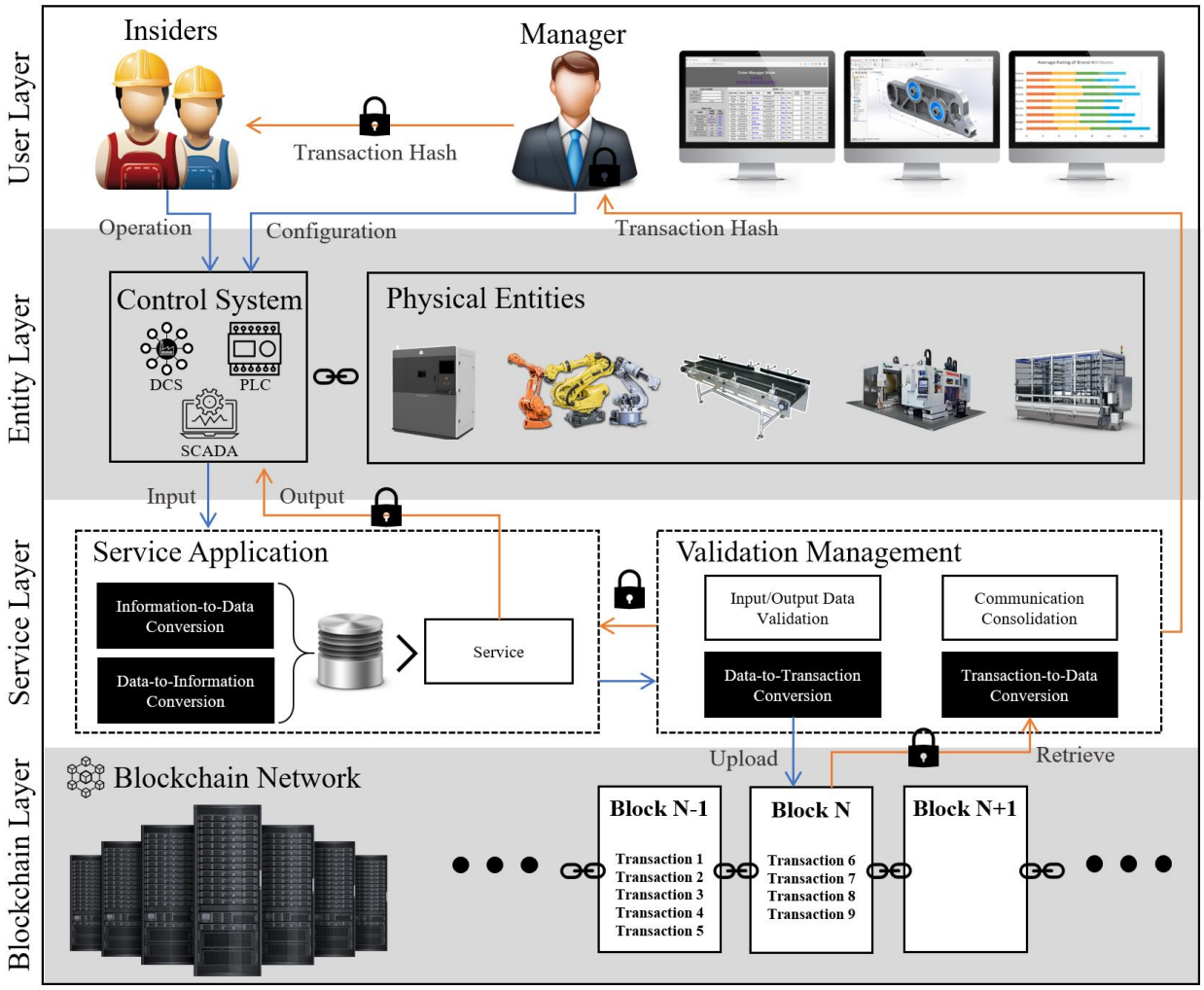


Figure 10 Example of ITTCPMS

To help in understanding the proposed system, an example of ITTCPMS is developed and demonstrated, and its layout can be found in Figure 10. The goal of the system is to operate the manufacturing system in a safe environment established by SOB. The objectives of the system operation are i) to integrate physical entities via a service application, ii) to enable validation management within the service layer, and iii) to allow communications between the service layer and blockchain layer.

Manager—who establishes the system and is an administrator of the system—configures the system entities in the entity layer before operating the system. It is assumed that the security clearance for the configuration process is only limited to the administrator of the system. Insiders, who are potential threats to the system, have a legitimate access authentication to the entity layer. They can only operate the system with a permission from the manager, and all the activities are recorded and monitored by the manager.

In the entity layer, digital entities and physical entities are integrated by the control system, such as Distributed Control System (DCS), Supervisory Control And Data Acquisition (SCADA), and Programmable Logic Controller (PLC). Based on the production goal and purpose of the system, the control system and integrated physical entities can be varied, as well as the scale of the entity layer. On the basis of the number of services required by the system, multiple control systems can exist in the entity layer, and physical entities can be dynamically decomposed and re-organized to provide flexible services. The control system is connected to the service layer to validate input and output data through the blockchain layer.

There are four main conversion functions of the service layer: the information-to-data conversion, data-to-transaction conversion, transaction-to-data conversion, and data-to-information conversion. When configuration information arrives at the service layer, it is first converted to data that can be manipulated and processed for the service. After the data processing and validation for the service, it is converted to a transaction to be uploaded on the blockchain layer. Once it is uploaded on the blockchain layer, the layer returns the transaction hash, which functions like 'a key' to access the uploaded data. This transaction hash is delivered to the manager, and the manager passes to the insiders for the system operation. When the input data with the transaction hash by the insiders arrives at the service layer, the transaction hash is used to retrieve

the corresponding transaction from the blockchain layer, and the transaction is converted to the data to be processed in the service layer. In this way, the entity layer can continuously validate input and output data via the blockchain layer, which is immutable and reliable against insider threats.

Chapter 5. Example Models and Validation

This chapter introduces two example models and their validation process. The two example models of the insider threat tolerant Cyber-Physical Manufacturing System were developed: Layer Image Auditing System (LIAS) and Secure Programmable Logic Controller (SPLC). These models are explained in detail, and the discussion for each model is provided to describe how the blockchain can help to mitigate insider threat risks in the general manufacturing practices.

5.1 LIAS

5.1.1 Motivation

The realization of a fully automated manufacturing system for more productive, flexible, and economical production is accelerated by recent technological advances. Specifically, an unprecedented level of autonomy utilizing Additive Manufacturing (AM) has been adopted by Cyber-Physical Manufacturing System (CPMS) (Lhachemi et al., 2019).

However, cyber-physical attacks—that originate from the cyber domain but result in physical damages—has become a serious threat to the CPMS (Chhetri et al., 2016). Since the cross-domain system structure of CPMS increases the attack surface and vectors, its system properties are vulnerable to such an attack method. Any attackers from inside or outside of the system can exploit this attack to perpetrate their malicious actions through various networks, due to the increased accessibility and connectivity of the CPMS.

Especially in additive manufacturing processes, it is difficult to detect an attack on infill structure because interior defects can occur without the exterior being altered (Sturm et al., 2017). Thus, it is important to establish a defensive mechanism to detect or prevent such kind of attacks. Previously, an Intrusion Detection System (IDS) was developed to identify an abnormality in the cyber domain before physical damages occur. However, its high false alarm rate and long detection timeline have been pointed out as critical limitations. To manage such an issue, augmenting IDS with physical data auditing by correlating physical and cyber data has been proposed (Wu & Moon, 2020). This research showed that physical data auditing in real-time can be an effective solution for preventing or detecting cyber-physical attacks.

To detect the infill defectives by auditing physical data, layer images of the printing objective can be used. Faulty detection systems based on image classification have been explored by several researchers in various fields (Yan et al., 2020; Yue et al., 2020; Zhang et al., 2020), although similar applications to AM have been a few. The main idea of auditing physical data is to classify the layer images to detect defectives by using machine learning techniques.

However, the auditing process in CPMS is not free from cyber-physical attacks. Particularly, machine learning systems themselves are vulnerable to an attacker, who can exploit the adaptability of the system (Barreno et al., 2010). For example, the parameters of defensive mechanisms augmented by machine learning can be exposed to various attack vectors due to the enlarged attack surface of the CPMS. Specifically, such parameters can be easily targeted by insiders, who has been or is being affiliated with the system: Insider Threats.

Insider threats are becoming one of the most difficult security issues for various fields—such as financial, medical, public service, and manufacturing sectors—due to their virulence to the system architecture that is dependent on computers and networks. In fact, the insider threat is a serious problem across all respects of any real-world system where people trusted with access to critical and sensitive information can abuse the access authentication to damage and compromise the information; or collaborate with others to cause failures, losses and serious harms to the system.

To manage such risk, blockchain technology was incorporated into the machine learning process (Song & Moon, 2020c). However, since the size of data being stored in the blockchain is limited and its implementation and operation can cause extra cost, it is not practical to implement the blockchain concept in the entire physical data auditing process.

To address these issues in adopting the blockchain to the auditing process, a Layer Image Auditing System (LIAS) that incorporates a blockchain to protect the auditing process while

maintaining high classification accuracy has been developed. LIAS employs multiple image processing techniques to detect edges and a neural network to classify the layer image. To simplify computations and reduce the machine learning parameters, LIAS equips a new filtering process that does not require any kernels to acquire a clear edge of the layer images. Using the new filtering process, LIAS can be trained by simulated images from 3D printing software and can test physical images that are captured by a camera from the top of a 3D printer. Both training and testing images were collected in different settings: non-defective type (normal) and five defective types (Center, Top-Right, Top-Left, Bottom-Right, and Bottom-Left). The added level of security is ensured by storing the weights and biases for the neural network in a block provided by the blockchain environment.

5.1.2 Background

A layer-by-layer infill image detection system was previously developed to detect malicious infill defects in the 3D printing process (Wu et al., 2017). To demonstrate forged defective infill structure, simulated 3D printing process images were used by capturing the actual printing processes from the top view of the 3D printer. For the experiments, the layer images were captured in two groups: Defect and Non-Defect. For the classification, two machine learning algorithms were used: Naive Bayes Classifier and J48 Decision Trees. Each algorithm classified the images with 85.26% and 95.51% accuracy respectively. This method showed great potential for future additive manufacturing security.

However, it also revealed the limitation of the use of machine learning for attack detection. To train the supervised machine learning algorithm, it required a sheer volume of training data to yield a meaningful classification performance. However, image data collection for training the

algorithm alone is not only wasting resources but also time consuming. Besides, since the layer images can only be collected from the actual printing process, redundancy of data collection is signified.

One way of addressing the problem is to use simulated images for training the machine learning algorithm. However, due to the complex nature of photographs of real objectives, it is difficult to expect high classification accuracy by training simulated images.

To enable simulated images as training data, more advanced machine learning techniques are required, such as Convolutional Neural Networks (CNN). CNN can train the model with the pattern of the image (Farabet et al., 2013; Krizhevsky et al., 2017). It can also assure enough classification performances with simulated images by producing many convolutional layers and conducting sub-sampling processes. However, CNN is an over-sophisticated and complicated algorithm to classify infill layer images. Infill layer images are typically collected in a controlled environment, and these are anticipated to remain in a certain quality.

However, CNN is devised to recognize visual imagery in various sizes of feature maps. Also, CNN tends to remove abnormal patterns in the image to extract the overall pattern of images. Thus, it is not beneficial to use to detect abnormalities in the images. Besides, CNN's pixel-by-pixel filtering process requires many computations with various types of kernels. Accordingly, a myriad of parameters including kernels for the filtering process is required to run it: this can be a critical security issue.

To protect the machine learning process, blockchain technology can be adopted. The blockchain has been widely implemented in various industries to enhance system security (Azaria et al., 2016; Lepoint et al., 2018; Mengelkamp et al., 2018; Nakasumi, 2017). These applications have database structures based on the blockchain communication protocol to enable strong security

in the processes of storing and retrieving data. Furthermore, there was an attempt to augment CPMS's security by implementing the blockchain. The proposed system has a unique system architecture to avoid redundant delay occurring from the blockchain's validation process. The system consists of User Layer, Provider Layer, Service Layer, and Blockchain Layer. By separating storing process from retrieving process in the manufacturing operation, users in the User Layer and providers in the Provider Layer can share the ground truth in a secured way. To show the effectiveness of the proposed system, the author demonstrated three physical data auditing examples by using the proposed system. Even though the algorithm used for the examples is simple, it shows high accuracy rates for attack detection and a quick response time (an average of 0.122 seconds).

Additionally, blockchain technology has shown its potential for security enhancement in machine learning. A Simplified Convolutional Neural Network (SCNN) has been proposed to secure CNN from inside or outside attackers (Song, Shukla, et al., 2020). SCNN enables the blockchain communication protocol in its machine learning process by uploading and retrieving machine learning parameters on the blockchain. Since CNN is a fully connected deep learning network model, a plethora of parameters are required to be stored in the blockchain. The problem is the blockchain has a limited size of data being stored in one block, due to its cryptographic algorithms. Therefore, CNN needs to be simplified to implement the blockchain into the machine learning process. This research demonstrates that the potential of the blockchain application enabling machine learning in a trusted environment.

Nonetheless, the proposed SCNN has critical limitations in terms of classification. Due to the overly simplified algorithm, SCNN can only perform well in certain types of training and test

images. Besides, there is no clear network model and a specific application structure for the blockchain implementation.

5.1.3 Architecture

LIAS consists of pre-processing and a Multilayer Perceptron Neural Network (MLP). Unlike CNN, convolutional layers (CL^1, CL^2) are acquired by simply subtracting the feature x from Padding Layers pd, which are created from x. Since LIAS does not require any kernels and uses padding layers of which size is the same with x, it requires much less computational power than CNN does.

Each of the first padding layers pd^1 of size $500 \times 500 \times 8$ (pixel) filters the feature x^1 and generate the first convolutional layers CL^1. After that, $ReLU$ is applied to the CL^1, and then these eight layers are combined by taking the average value. Max Pooling is then used to produce x^2, and the same steps are followed for x^2, except Average Pooling is used at the end. Finally, 2500 data from the Average Pooling are fed to MLP, which consists of 5 hidden layers and 6 output layers. The architecture scheme of LIAS can be found in Figure 11.

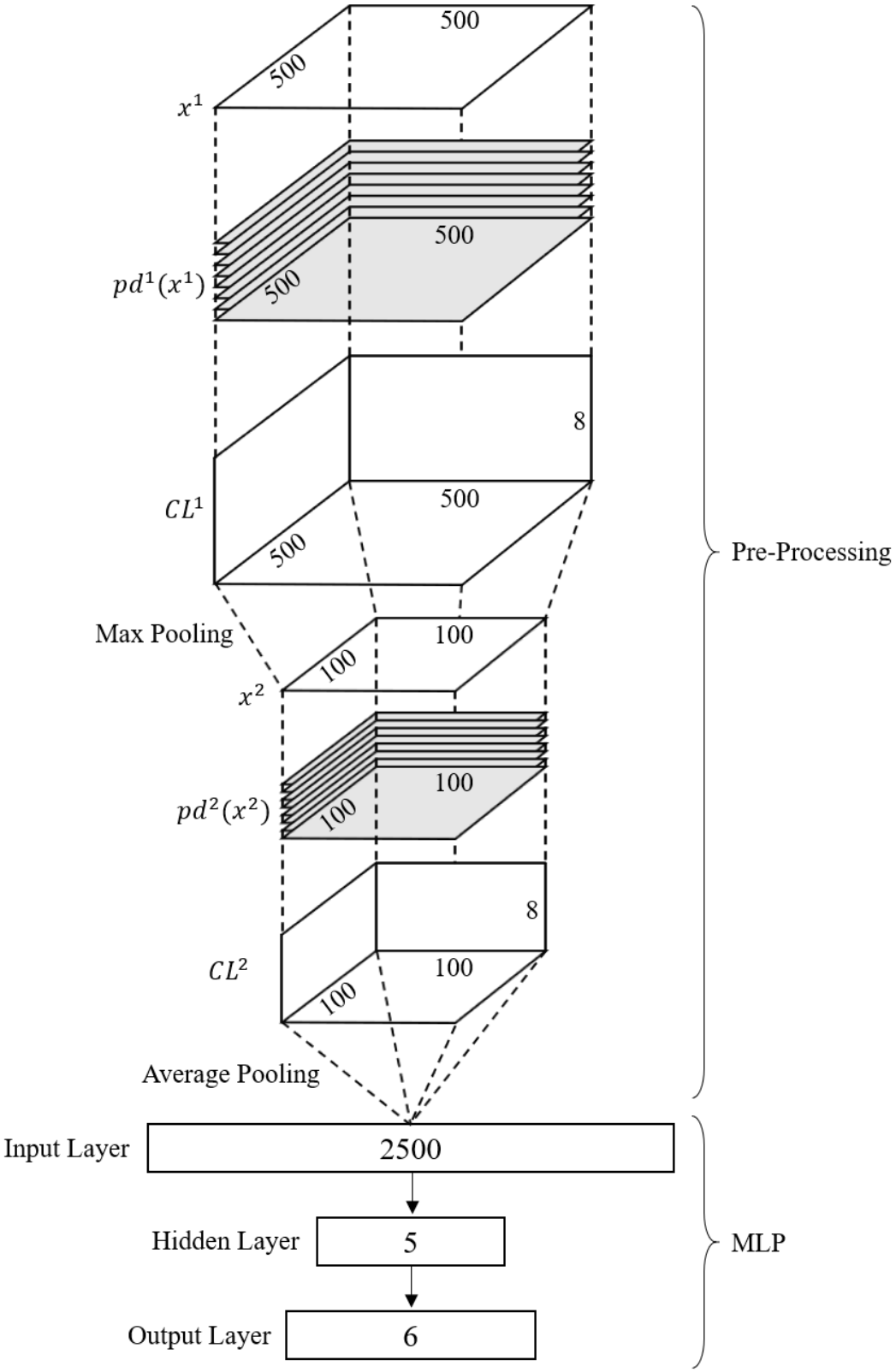


Figure 11 LIAS Architecture

5.1.3.1 Pre-processing

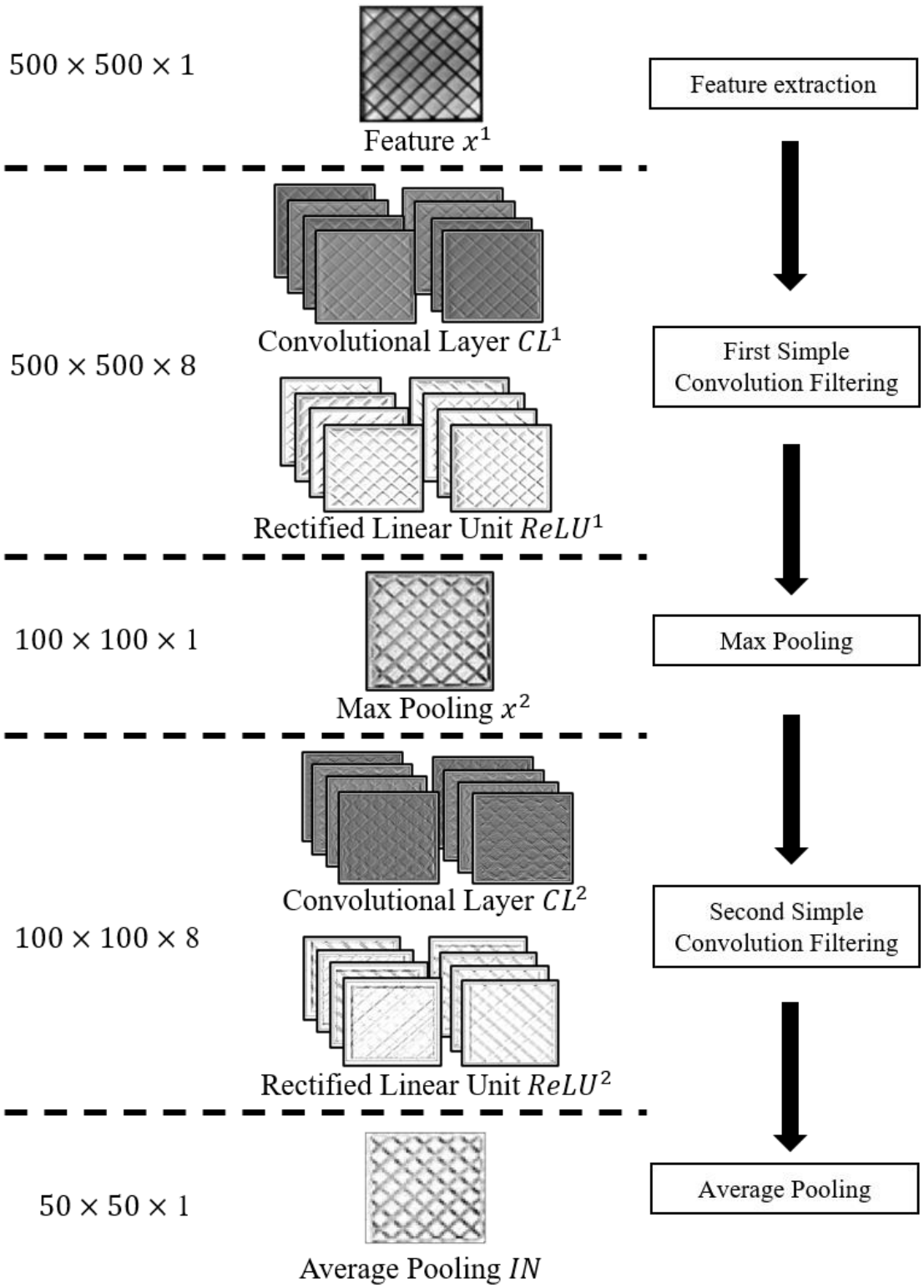


Figure 12 Pre-processing Structure

As shown in Figure 12, the pre-processing consists of five steps: the feature extraction, first simple convolution filtering, max pooling, second simple convolution filtering, and average pooling. The objectives of the pre-processing in LIAS are to extract outlines of the images and to reduce the data points of the images. The simple convolutional filtering is used to obtain outlines of the feature, and the number of data points is reduced by one-tenth from the max and average pooling process.

In the first stage, the normalized feature is extracted from the image data, and the first simple convolution filtering process will be conducted. The convolutional layer of LIAS is quite different from CNN's because the layer image will always have the same scale of size. Thus, it is not necessary to apply various kernel sizes with the stride values to produce sub-samples. Instead, LIAS convolutional layers are primarily used to detect the edge of the image. More details of the simple convolution filtering process will be explained below.

After the first filtering process, all the convolutional layers will be combined by using Max Pooling image processing techniques and go through the second simple convolution filtering. By conducting two rounds of the filtering process, LIAS can achieve clearer images as well as reduced data volume.

The simple convolution filtering process algorithm is presented in Table 4. Due to the padding layers $pd(x)$, the simple convolution filter produces eight convolutional layers in a very different way from the CNNs' kernel filtering method. The kernel filtering method convolutes an image by using a kernel with many dot product computations, but the simple convolution filtering produces a convolutional layer by using a padding layer with one subtract computation. Since the size of kernels (receptive field) is smaller than the original image to achieve precise filtering results, a large number of the dot product computations are required based on the stride value—the

distance between the receptive field centers of neighboring neurons in a kernel map. However, since the padding layer has the same size as the original image, it enables only one subtract computation to acquire the outlines of the original image. To accomplish this, padding layers are constructed by: i) moving the feature's values as many as offset value pixel by pixel to 8 inverse directions, ii) filling zero values in an empty row or column, and iii) trimming the feature values, which are out of the original feature range.

Table 4 Simple Convolution Filtering Process Algorithm

Given:
Feature, $x \in \mathbb{R}^{m \times n}$
Upper diagonal matrix $d_{n \times n}$ and Lower diagonal matrix $d'_{n \times n}$,

$$d = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix} \text{ and } d' = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

Padding Layer $pd(x)$:

$$\begin{aligned} pd_T(x) &= d \cdot x, & pd_{TR}(x) &= d \cdot x \cdot d, \\ pd_B(x) &= d' \cdot x, & pd_{TL}(x) &= d \cdot x \cdot d', \\ pd_R(x) &= x \cdot d, & pd_{BR}(x) &= d' \cdot x \cdot d, \\ pd_L(x) &= x \cdot d', & pd_{BL}(x) &= d' \cdot x \cdot d'. \end{aligned}$$

Convolutional Layer CL:

$$CL = x - pd(x)$$

Rectified Linear Unit $ReLU$:

$$ReLU = \max(0, CL)$$

Average $mean$:

$$mean = \frac{1}{8} \sum_{i=1}^{8} ReLU_i$$

By using the padding layers, eight convolutional layers CL are generated by subtracting the feature (x) from eight Padding Layers (pd). CL includes: CL_1 (highlight a top side outliner), CL_2 (highlight a bottom side outliner), CL_3 (highlight a right-side outliner), CL_4 (highlight a left side outliner), CL_5 (highlight a top and right side outliner), CL_6 (highlight a top and left side outliner), CL_7 (highlight a bottom and right side outliner), and CL_8 (highlight a bottom and left side outliner).

Rectified Linear Unit ($ReLU$) is then applied for all the layers to acquire clear outliners in the images. To help understanding the concept, four samples of convolutional layers (Top, Bottom, Right, and Left) are compared under two conditions: Before $ReLU$ and After $ReLU$. The result can be found in Figure 13.

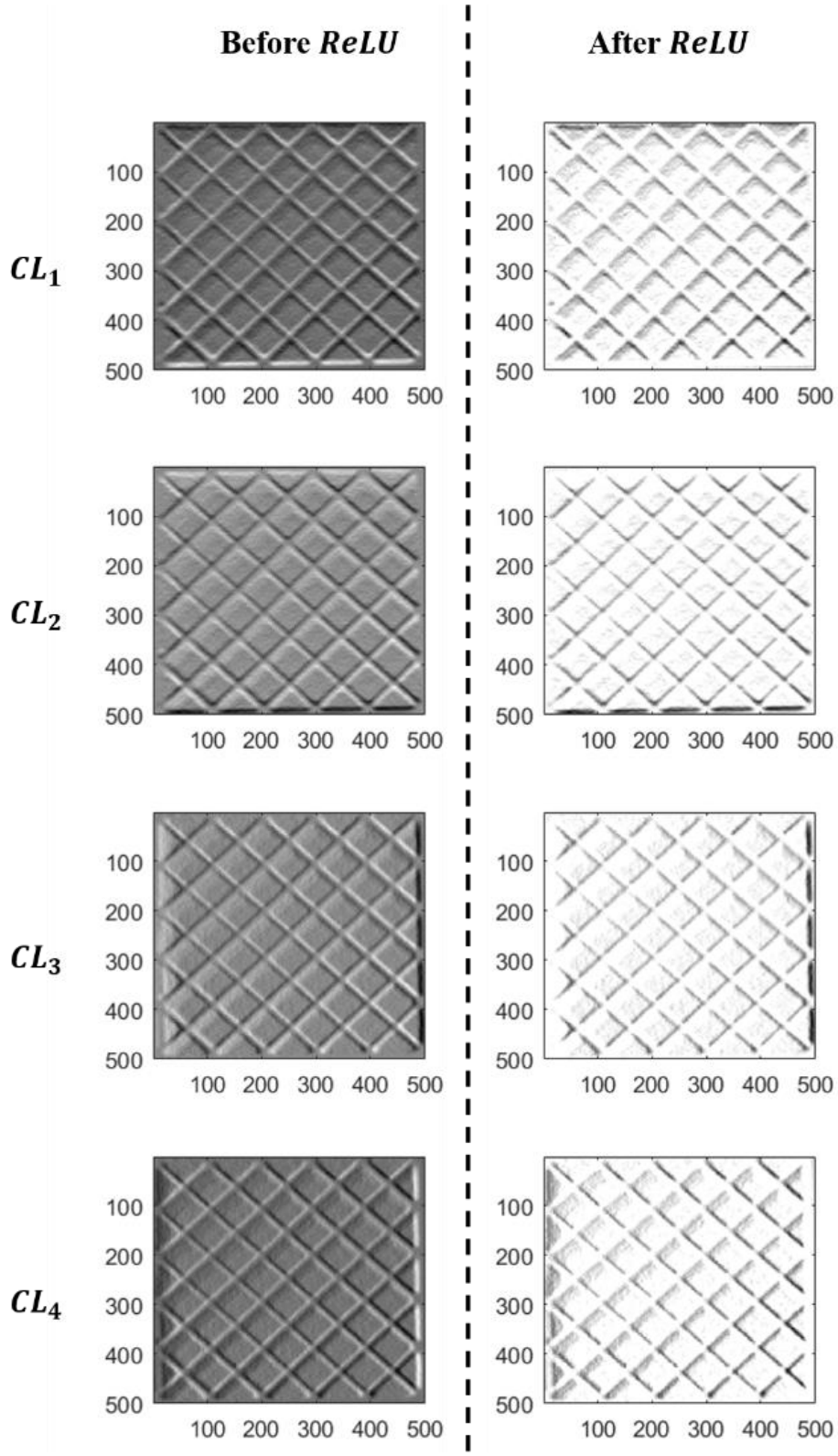


Figure 13 ReLU Result

For the pooling layers, a max-pooling is used after the first simple convolutional filtering, and an average-pooling is used to feed MLP after the second simple convolutional filtering. For both pooling layers, there is no overlap among adjacent pooling units. Hence, the stride values for the pooling layers are always the same as the pooling kernel size.

For the max-pooling defined as equation (1), the pooling kernel size 5×5 with the stride value 5.

$$MaxPooling(x) = \max_{i,j} x_{i,j} \tag{1}$$

The average pooling that takes the pooling kernel size of 2×2 with the stride value 2, is defined by the equation (2), where s is the stride value.

$$AveragePooling(x) = \frac{1}{s}\sum_{i=1}^{s} x_i \tag{2}$$

Each step's results from the simulated image and physical image are provided below. Pre-processing reduces the data dimensions from 500 x 500 x 1 to 50 x 50 x 1, while clearly extracting outlines of features of the infill images. Each step of the pre-processing samples can be found in Figure 14.

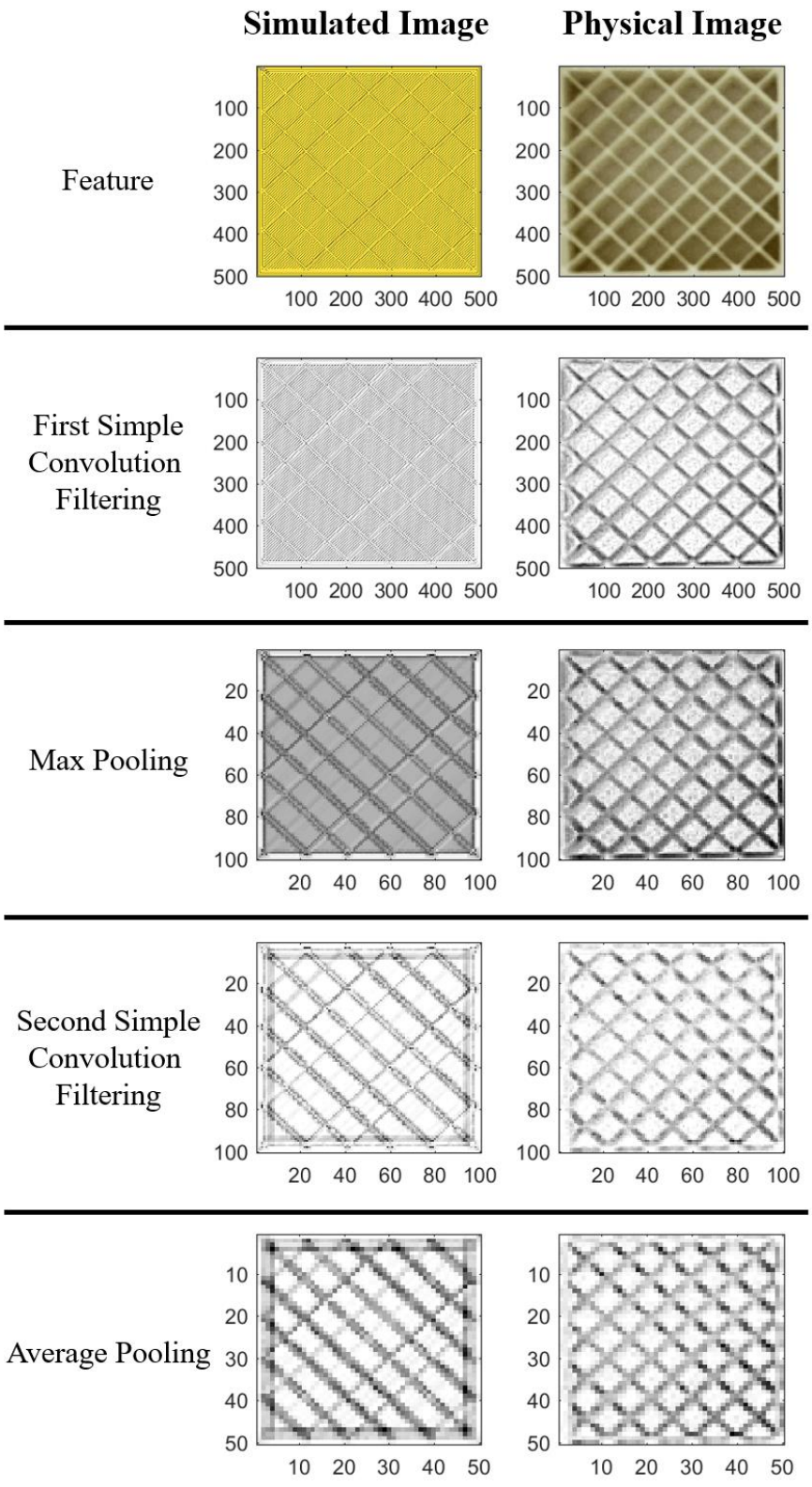


Figure 14 Pre-processing Samples

5.1.3.2 Multilayer Perceptron Neural Network

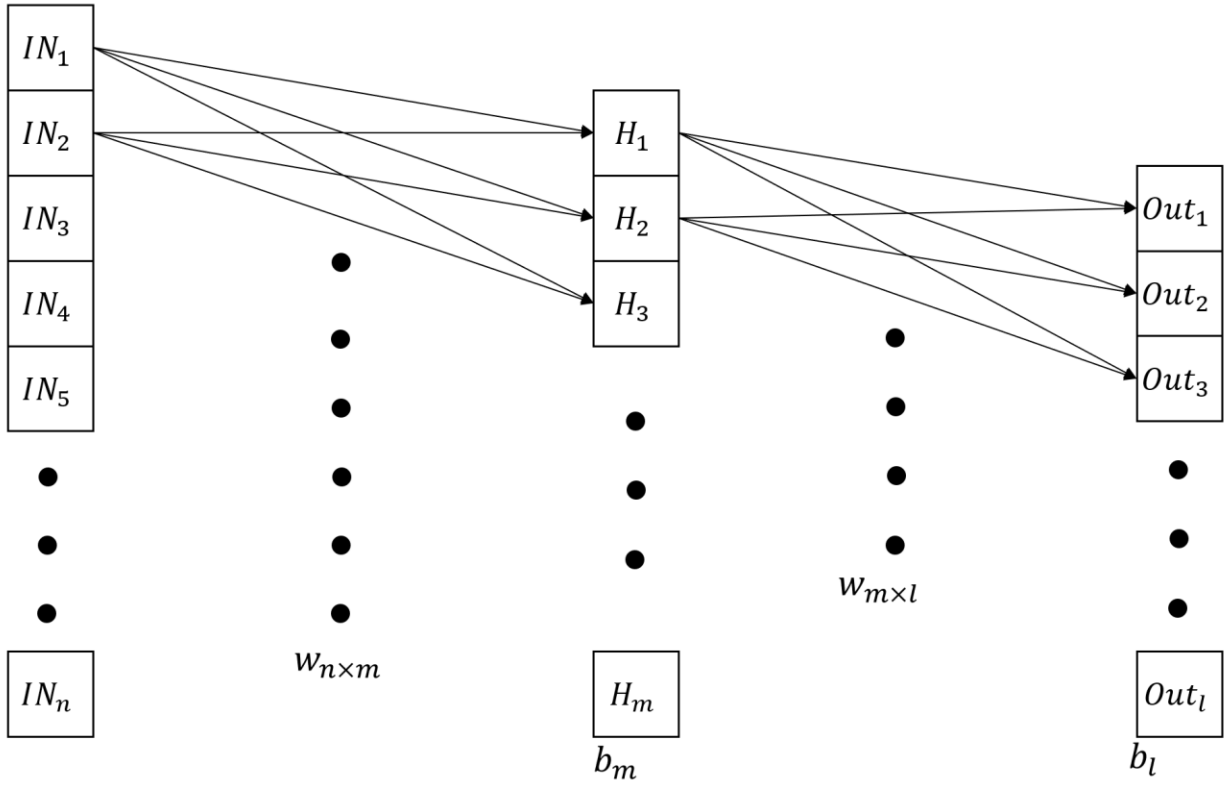


Figure 15 Multilayer Perceptron Neural Network

After creating final input values for training and testing layer images, a multilayer perceptron (MLP) neural network is used to proceed with the input values. The neural network consists of input nodes, hidden nodes, and output nodes. The number of the output nodes can be decided based on the prepared image data set.

Propagation and back-propagation algorithms based on stochastic gradient descent are implemented in the neural network process. Also, the sigmoid function is used for an activation function in the network. For the propagation, equations (3) and (4) are used.

$$H_m = f\left(\sum_{k=1}^{n}\left(IN_k \cdot w_{k+n(m-1)}\right) + b_m\right) \quad (3)$$

$$Out_l = f\left(\sum_{k=1}^{m}\left(H_k \cdot w_{k+m(l-1)}\right) + b_l\right) \quad (4)$$

For the back-propagation algorithm, equations (5) and (6) are used for updating each weight (w) and bias (b). The learning rate (η) is used to train the model was 0.1. Finally, a loss function with logistic regression was used to validate the training process.

$$w^{+}_{m(n\times l)} = w_{m(n\times l)} - \eta \cdot \frac{\partial E_l}{\partial w_{m(n\times l)}} \tag{5}$$

$$b^{+}_{m+l} = b_{m+l} - \eta \cdot \frac{\partial E_l}{\partial b_{m+l}} \tag{6}$$

5.1.3.3 Blockchain Implementation

To enable LIAS as an infill defective detection system in the additive manufacturing industry from the viewpoint of ITTCPMS, LIAS's weights and biases can be available through the system's network. In this way, training and testing layer images can be separated, so the manufacturing operation process can avoid unnecessary delays, which include generating simulated images and training these for LIAS. However, the weights and biases on the network can easily be a target for attackers due to their sensitivity to the detection system and enlarged attack surfaces. To prevent the weights and biases from unintended and malicious manipulations, the blockchain can be integrated to securely store and transfer machine learning parameters. For this reason, the algorithms for training and auditing of LIAS were developed by using Python 3 with the web3 package for blockchain communication. The algorithms used for testing LIAS are shown in Figure 16 and Figure 17.

INPUT: Feature Vectors x_α, where α = Number of features
OUTPUT: Transaction Hash tx

$InputNode_\alpha = Read\_Images(x_\alpha)$
$w_k, b_l = Initialize\_Weight\_Bias()$
$Target = Initialize\_Target()$

for i **in** $range(\alpha)$
    $HiddenNode = Propagation(InputNode_i, w_k, b_l)$
    $OutputNode = Propagation(HiddenNode, w_k, b_l)$
    $ErrorTotal = (OutputNode - Target) \times \{OutputNode \times (1 - OutputNode)\}$
    $w_k, b_l = BackPropagation(w_k, b_l, ErrorTotal)$
$tx = Issue\_Transaction(w_k, b_l)$

Return tx

Figure 16 Training Algorithm

INPUT: Feature Vectors x_α, Transaction Hash tx
OUTPUT: Prediction Result $FinalResult$

$InputNode_\alpha = Read\_Images(x_\alpha)$
$w_k, b_l = Retrieve\_Transaction(tx)$

for i **in** $range(\alpha)$
    $HiddenNode = Propagation(InputNode_i, w_k, b_l)$
    $OutputNode = Propagation(HiddenNode, w_k, b_l)$
    $FinalResult.append(OutputNode)$

Return $FinalResult$

Figure 17 Auditing Algorithm

5.1.3.4 ITTCPMS Implementation

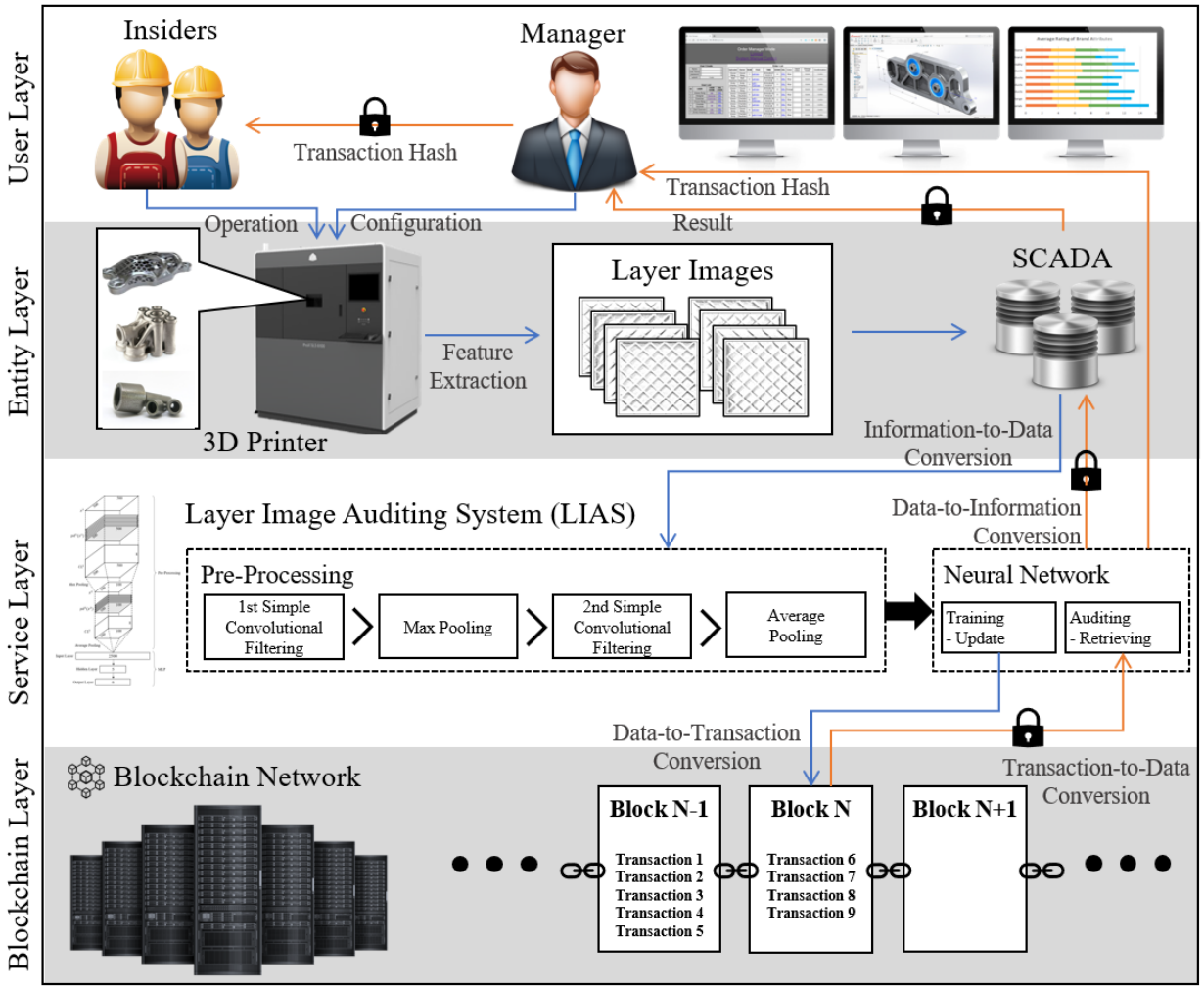


Figure 18 ITTCPMS with LIAS

Figure 18 shows the ITTCPMS when LIAS is applied. In the entity layer, the main physical entity is a 3D printer, and SCADA is utilized to manage layer images from the printer. The inspection result is also handled in SCADA.

The system operation starts from the manager's configuration. The simulated original and defective layer images can be generated by the manager and trained by LIAS. This results in the trained weights and biases, which are uploaded on the blockchain layer. When the data-to-

transaction conversion is executed by the service layer, the blockchain layer returns the transaction hash, which is corresponding to the uploaded data, to the service layer. Then the service layer delivers the transaction hash to the manager. This transaction hash is the key to access and run the LIAS's auditing process. By accessing LIAS with the transaction hash and protecting the machine learning parameters in the blockchain layer, the manager of the system can trust LIAS's result, but also insiders can ensure the legitimacy of the inspection process.

5.1.4 Validation

To validate and evaluate LIAS, experiments were designed to provide a comparative performance analysis of the classification. Since the main objective of LIAS's classification is to detect defective infill layer images, a normal type of physical images was paired with each of the defective types for testing. However, the experiments under the condition that various defective types need continuously be developed over layers were not considered. Additive manufacturing fabricates objects by continuously adding material layer by layer from bottom to top, hence early defective detection in the low layer could enable to prevent other defectives in the higher layers.

To design the experiments, five different infill defective types were developed. The same defective shape at different locations was used to differentiate defective types to evaluate LIAS in an unbiased condition. Simulated images were created by CURA 4.1.0 SOFTWARE. A total of 12,000 simulated images were generated for the experiments, and the image data type and the number are summarized in Table 5.

Table 5 Simulated Layer Images

Type	Image	#Number
Normal		2000
Defective; Center		2000
Defective; Top-Right		2000
Defective; Top-Left		2000
Defective; Bottom-Right		2000
Defective; Bottom-Left		2000

For the physical image data, MP Select Mini 3D printer V2 and Logitech C525 camera were used. The camera was placed above the 3D printer to take a photo from the top view of the printing sample layer by layer, and the photo was edited 500 pixels by 500 pixels. The summary of physical image data is in Table 6.

Table 6 Physical Layer Images

Type	Image	#Number
Normal		70
Defective; Center		70
Defective; Top-Right		52
Defective; Top-Left		47
Defective; Bottom-Right		48
Defective; Bottom-Left		47

The experiment setups were as follows. First, pre-processing was conducted for all the collected data using MATLAB. The MLP was constructed with 2,500 input nodes, 5 hidden nodes, and 6 output nodes programmed by Python. Accordingly, a total of 12,530 weights and 11 biases were initialized with random values. Also, the target value 0.99, and the non-target value 0.01 were set to train six types of infill layers: normal, defective center, defective top-right, defective top-left, defective bottom-right, and defective bottom-left. 100 replications of training were set to make sure the gradient descent process was completed. A desktop computer with i7-4790 CPU and Intel graphic card was used to train the neural network. Total training time took around two hours, and

updated weights and biases were uploaded to the blockchain by using web3 package of Python. After uploading weights and biases, its transaction hash was returned, and it was entered to retrieve the weight and biases for predictions.

Finally, five data sets—normal type physical images with each of defective types—were tested by the LIAS. For the predictions, output nodes' normal class and defective class scores were analyzed. For the defective score, the highest score among 5 classes were chosen. Figure 19 shows the five data sets' final score results.

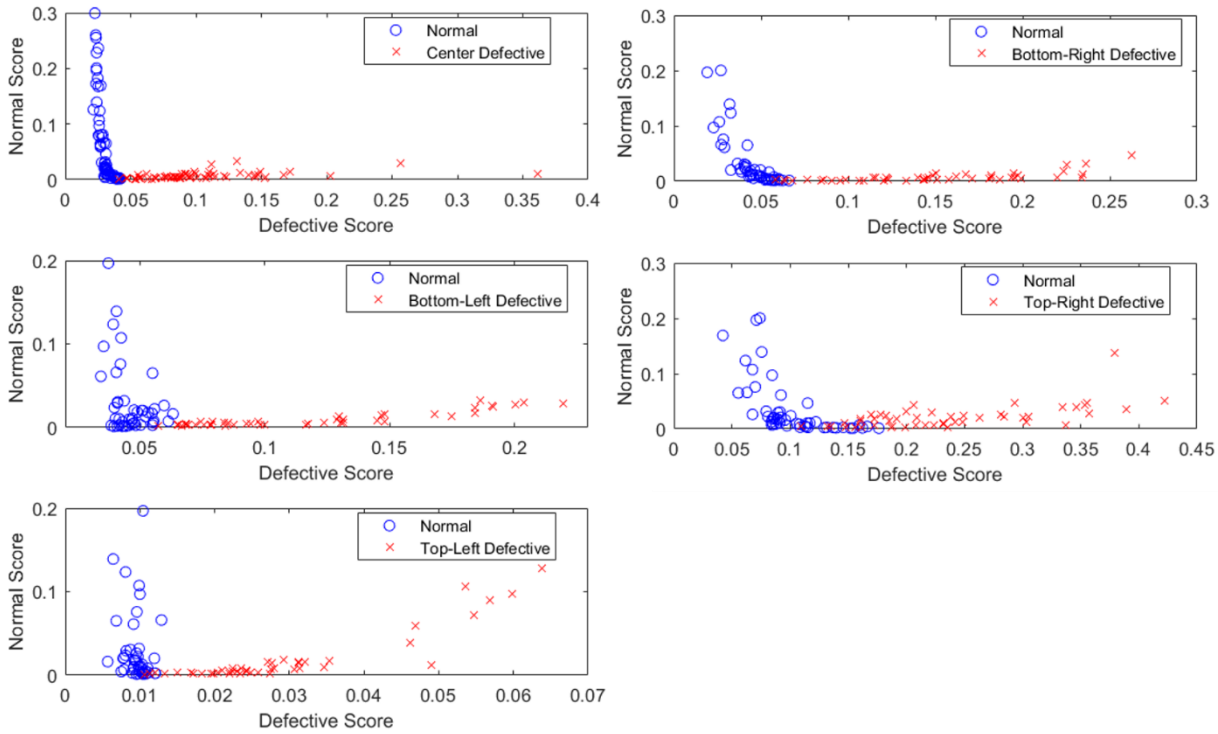


Figure 19 Final Score Results

Seen from Figure 19, LIAS effectively classified the normal class and defective classes. Although the normal score itself hardly differentiates the classes, the defective score clearly shows enough distinction between the normal class and the defective class. To acquire certain accuracy values from the results, a Receiver Operating Characteristic (ROC) curve was exploited to find the optimized threshold that maximizes True-Positive-Rate (TPR) for each result.

A classification accuracy, False-Positive-Rate (FPR), and False-Negative-Rate (FNR) were measured by equations (7), (8), and (9), where True-Positive is TN, True-Negative is TN, False-Positive is FP, and False-Negative is FN.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{7}$$

$$FPR = \frac{FP}{FP+TN} \tag{8}$$

$$FNR = \frac{FN}{TP+FN} \tag{9}$$

Table 7 Prediction Results

Condition	Classification Results		Accuracy	FPR	FNR
Defective; Center	TP	70	0.992857	0.014286	0.0
	TN	69			
	FP	1			
	FN	0			
Defective; Top-right	TP	45	0.892157	0.098039	0.117647
	TN	46			
	FP	5			
	FN	6			
Defective; Top-Left	TP	47	0.968085	0.063830	0.0
	TN	44			
	FP	3			
	FN	0			
Defective; Bottom-Right	TP	48	0.968750	0.062500	0.0
	TN	45			
	FP	3			
	FN	0			
Defective; Bottom-Left	TP	44	0.957447	0.021277	0.063830
	TN	46			
	FP	1			
	FN	3			
Total	TP	254	0.958175	0.049430	0.034221
	TN	250			
	FP	13			
	FN	9			

The results shown in Table 7 illustrate that the pre-processing is effective. Compared with other labels, the Top-right defective shows the lowest accuracy with 89%. It turns out there was a lighting issue that causes the low quality of the few images. However, the overall accuracy still shows more than 90% for entire experiment conditions with a low level of FNR.

To evaluate how the blockchain affects the test response time, it was measured in two different conditions: implementations with the blockchain and without the blockchain. The blockchain provides a sufficient guarantee of security against attackers, but it also causes redundant delays from the uncontrollable and arbitrary block generation time and block occurrence frequency. This issue has been already resolved in LIAS by separating the auditing process from the training process. Because the delays occur only for uploading the weights and biases to the blockchain, not for retrieving the data from the blockchain. However, since the data have to be passed through the blockchain, some delays still happen.

To objectively measure these delays, the response times for auditing physical images when the weights and biases are locally retrieved (without blockchain) were recorded and compared with the response time when the weights and biases are retrieved from the blockchain (with blockchain). The average response time for implementation with the blockchain and without the blockchain were 0.46285 and 0.15801 seconds, respectively. Although the result shows that the implementation without the blockchain was faster than the implementation with the blockchain, 0.46285 second is still acceptable for real time inspection.

5.1.5 Discussion

The compromised parameters of machine learning algorithms can cause the detection system to fail. In other words, the machine learning process itself is not safe from cyber-attacks. It

can be corrupted by an attacker who tries to exploit the vulnerability of the system. For example, an Adversarial Example Attack can pose serious threats to security-sensitive applications by simply injecting small perturbations to correctly classified inputs (Lecuyer et al., 2019). Especially, in the case of Deep Neural Networks (DNNs), only a small amount of malicious input data can induce a flawed classification that can result in increased False Positive Rates (FPR) and False Negative Rates (FNR).

To address such an issue, ITTCPMS employs the blockchain layer as a database for machine learning parameters. The blockchain can provide better security than the general database management system for the machine learning parameters since the old parameters remain in the blockchain and are tightly linked to the new parameter to maintain data integrity. Therefore, it is difficult to manipulate machine learning parameters without being discovered. All the processes required for updating data, uploading data, or retrieving data will be recorded by the blockchain layer, and these cannot be easily modified or removed.

However, adopting blockchain technology to the machine learning process is still in the early stage. Since the size of data being stored in the blockchain is limited and can cause extra cost, it is impossible to merely adopt the original blockchain concept for complicated and sophisticated machine learning algorithms. To show and prove the concept of ITTCPMS with LIAS, the pre-processing—simplified filtering process—was forced for the machine learning algorithm. To adopt blockchain technology for the wide range of machine learning applications, it is essential to improve and optimize the blockchain itself.

5.2 SPLC

5.2.1 Motivation

Insider threats are becoming more serious in the manufacturing industry as an automated manufacturing system is being deployed and developed further. Particularly, when Industrial Control Systems (ICS) for manufacturing process automation is employed, security vulnerabilities by insiders increase. ICS—such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control System (DCS), and Process Control Systems (PCS)—have been employed in various industries to monitor and control data transmission in facilities. In general, ICS uses the Programmable Logic Controller (PLC) as a control device, which is operating physical machines based on Input/Output (I/O) data of a system. PLCs are typically located on the shop floor to form a network environment. Furthermore, in CPMS, since they are integrated into the system via the internet and computer networks, insiders have physical and digital access to the PLCs (Ghaleb et al., 2018; Nicholson et al., 2012). As a result, insiders can intentionally or unintentionally pose serious threats to the entire manufacturing process security through PLC.

To reduce the severity of insider threats, blockchain technology can be adopted for PLC operation. However, attempts to utilize the blockchain to secure PLC have been few. Although numerous researchers have explored the security of PLC communication, most of them have focused on intruders from outside of the system.

As the first step to manage insider threats for PLC, a Secure Programmable Logic Controller (SPLC) has been developed to validate input and output data for the manufacturing process via blockchain technology. In order to validate SPLC in a practical manner and to assist future research, a testbed was developed and is presented in this section.

5.2.2 Background

PLC is a device to control physical machines in the shop floor. PLC controls the machines based on input and output data and uses Boolean values. Typically, PLC requires an operating system with the software for configuration. So it can be considered as a small computer that collects data from sensors or user input, operates the physical machines, and returns its operation result to the software or main operating system. The ladder logic is a graphical programming language that enables PLC engineers to write, read, or modify the program code easily. The steps for embedding the ladder logic code in PLC devices are: i) engineers write or modify code, ii) a software compiles the ladder logic code to binary code for PLC devices, and iii) a software uploads the code to the PLC device and embeds it to the system.

Since PLC is an important and dominant system component in the automation of manufacturing systems, it is likely that the controller would still be considered as a control device in CMS. However, PLC should meet new requirements and overcome security challenges to be adopted to the systems. Langmann et al. (Langmann & Stiller, 2019) proposed a new type of a PLC—Smart Industrial Control Services (SICS)—to fulfill the new conditions resulting from the new operation processes. The PLC enables the separated control function to the related equipment through a cloud server. SICS is powered by IEC6113

1-3 standard control program and can be run in two different modes: Server-Based Mixed Mode and Server-Based Mode. There is another study about extracting sensing data from PLC for CMS. The proposed method involves many approaches to identify useful data from the PLC devices. Conclusively, multithreading and HashSet algorithms improved the data extraction performance dramatically when these are applied to filter out the memory address (Leang et al., 2019).

Security vulnerabilities of PLC devices in Supervisory Control and Data Acquisition (SCADA) systems have been analyzed. The communication between PLC and engineering station—which is in charge of configuration of the PLC—can be interfered or compromised by the attackers in three attack methods: replay attack, man-in-the-middle-attack, and stealth command modification attack (Ghaleb et al., 2018). There are two more attack methods—bypass logic attack and brute-force output attack—oriented from legacy PLC protocols such as ModBus, Ethernet/IP, DNP 317 and Iso-TSAP. To address such attacks, five solutions have been proposed: protocol modification, protection via special filtering units, intrusion detection system, creation of demilitarized zones, and practices for securing PLC systems (Sandaruwan et al., 2013).

PLC has been deployed for several decades without adopting any effective security defensive mechanism. Even though various security policies, restrictions, and traditional IT security such as firewalls have been adopted to prevent PLC program code from unauthorized configuration; the validation process for input data has been minimal. In 2000, Maroochy Shire—Queensland computerized waste management system—was hacked by a former employee. He had installed the malicious program in the sewage control system and attacked the system after his job application was rejected by the area's council. His laptop and a wireless radio were used to inject unauthorized commands to the system to dump a large amount of sewage into the public area in the city.

Also, PLC's high availability requirements can yield another security vulnerability. In 2010, Iran's nuclear facilities identified the Stuxnet computer worm, which was specifically targeting the Siemens control system and re-configuring PLC's programming-language-layer directly. Although it is unknown how the facilities became infected, this could happen because of the po1tential

threats that insiders can voluntarily or involuntarily reveal accessible routes into the system to outsiders without being discovered (Langner, 2011).

5.2.3 Architecture

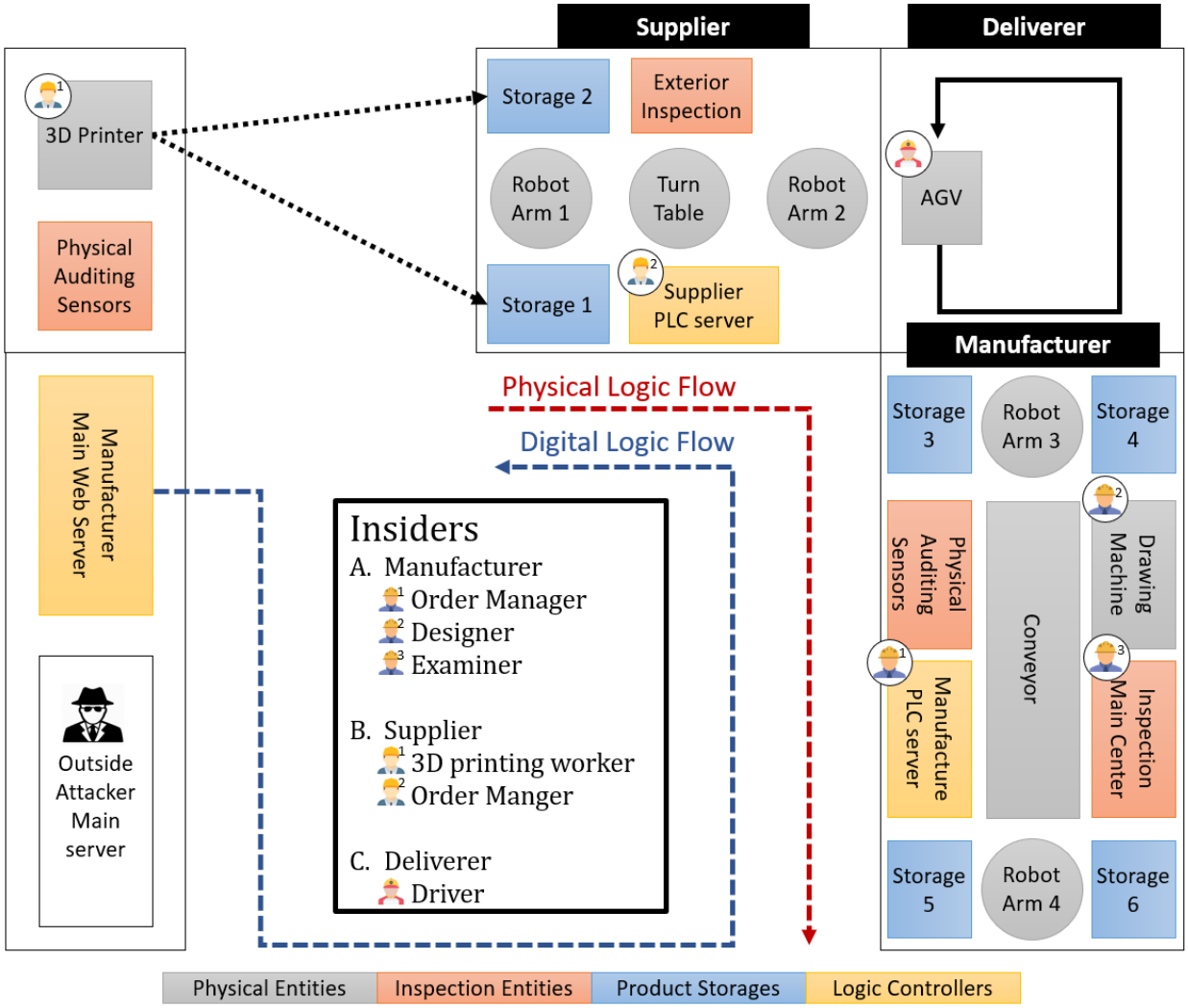


Figure 20 Physical Testbed Layout

The physical testbed was prepared to validate SPLC in a practical manner and to assist future research. Figure 20 shows the layout of the testbed. The testbed is based on a virtual manufacturing scenario to represent the general manufacturing practice. The additive manufacturing supply chain was chosen for the basic model of the testbed, which comprises three

main actors—Manufacturer, Supplier, and Deliverer—to provide 3D-printing services to customers. To help understanding in the testbed layout, the photographs are provided in Figure 21.

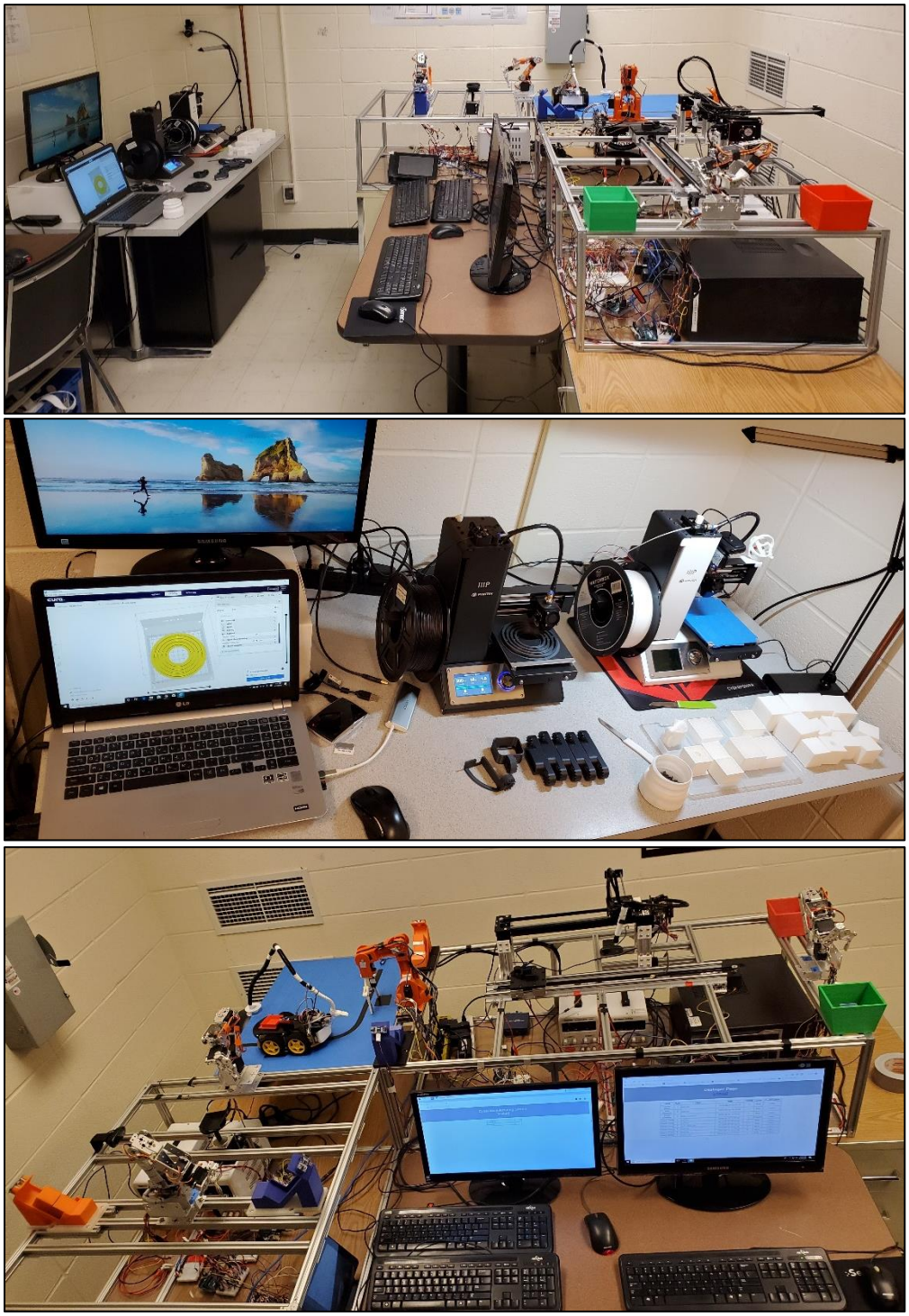


Figure 21 Physical Testbed Photographs

5.2.3.1 Actors

The manufacturer receives an order from the customer and sends its raw material order to the supplier. The manufacturer represents the end manufacturer in the manufacturing industry. The main task of the manufacturer is putting a design on a cube (1.5 x 1.5 x 1.5 inches), which can be interpreted as a final manufacturing process, such as packaging, welding, assembly, and painting. Three insiders were defined for the manufacturer in order to conduct insider threat analyses: order manager, designer, and examiner.

The supplier who represents a raw material producer in the testbed receives the order from the manufacturer and produces cubes from a 3D printer. Two attributes were defined for the cube. But for the sake of simplicity, two attributes were distinguished by colors only. Two insiders were defined for the supplier: 3D printing worker and order manager.

The deliverer stands for transportation between the manufacturer and the supplier; it transfers the cube from the supplier to the manufacturer. In the testbed, the deliverer indicates the geographical distance between the manufacturer and the supplier.

The manufacturer and the supplier can communicate through the internet network. Particularly, since automated programmable logic controllers for the manufacturer and the supplier are operated based on internet communication, the entire testbed operation can be controlled by the testbed user interface remotely.

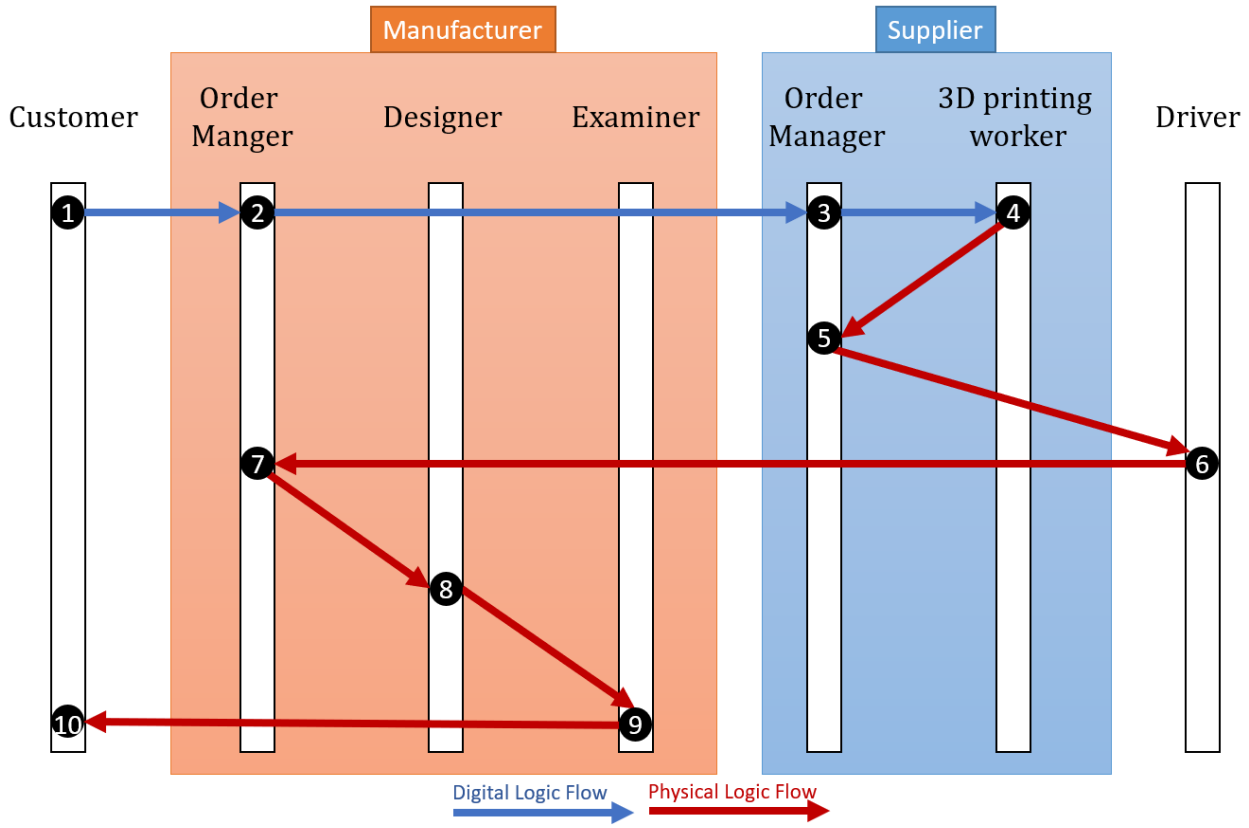


Figure 22 Interactions among Actors

Figure 22 shows that the insiders of the manufacturer, the supplier, and the deliverer are seemingly interacting with each other by sharing digital and physical assets. The order manager of the manufacturer acquires digital assets—manufacturing specification, graphical designs, orders—from its main webserver, creates the order based on the inventory status and sends it to the supplier's order manager. And then, the 3D printing worker receives the order from the order manager of the supplier and produces a cube. The cube is transferred from the supplier to the driver, who delivers the cube to the manufacturer's order manager. The order manager of the manufacturer passes the cube through the designer and the examiner in order. The designer operates a drawing machine to apply the corresponding graphical designs, and the examiner performs a quality inspection.

5.2.3.2 Entities

The manufacturer consists of two robotic arms, two cube storages with ultrasonic sensors, one CNC Drawing Machine, and one linear slide conveyor powered by Biopolar stepper motor. These physical entities are controlled by six Arduino UNO boards, which are under the control of Raspberry Pi 3.

The supplier consists of two robotic arms, one turntable operated by Bipolar stepper motor, and two 3D-printers. One Raspberry Pi 3 with OpenPLC server and three Arduino UNO boards are used to integrate physical entities of the supplier, except two 3D printers. In the case of the deliverer, an automated guided vehicle (AGV) powered by the Arduino board is used. Additionally, five avoidance sensors are used to guide the AGV and detect the cube on the AGV.

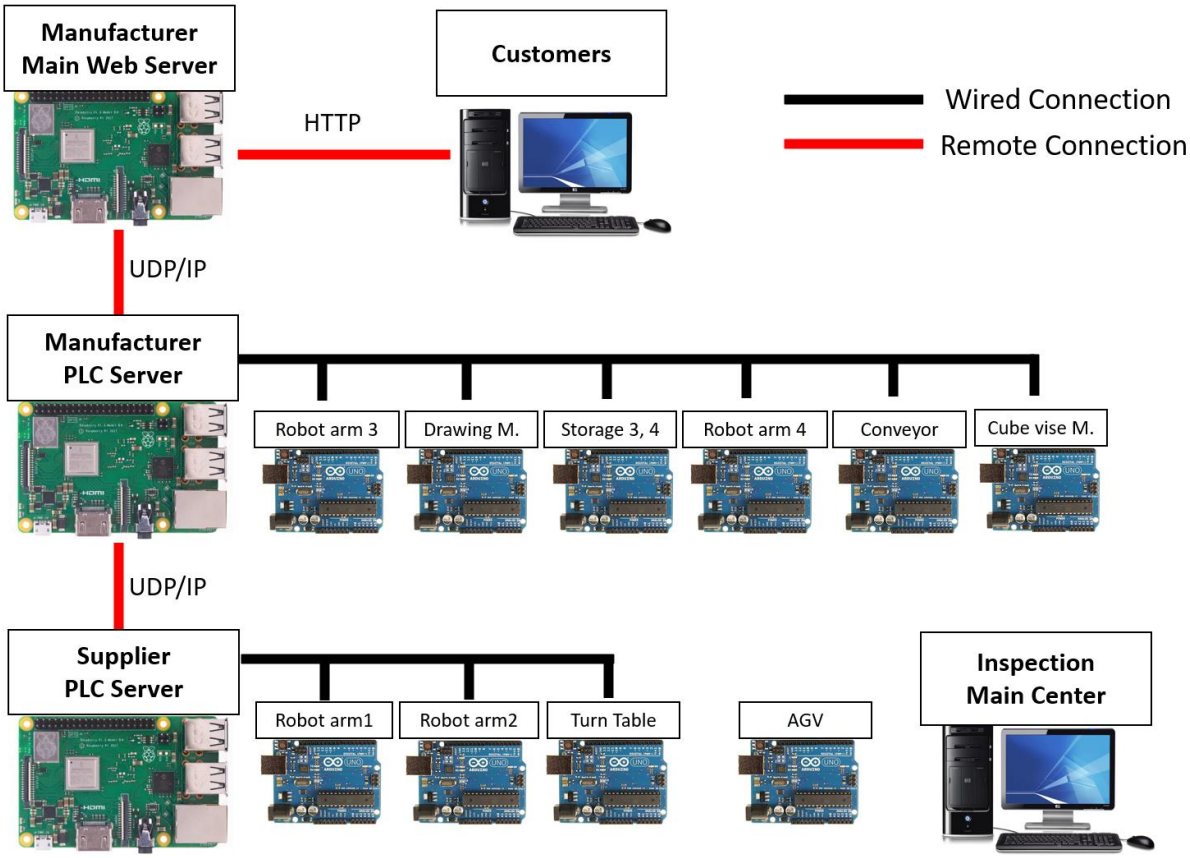


Figure 23 Physical Entity Connections

In addition, another Raspberry Pi 3 is used to maintain the manufacturer's webserver to enable communication between the customers and the manufacturers and store all the original digital assets. Four DC power supplies are used to power the stepper motors and servo motors comprising robotic arms. Lastly, the entire testbed's frame consists of $20 \times 20\ mm$ T-slotted aluminum bars with joiners, nuts, and bolts. A layout of the components and connections can be found in Figure 23.

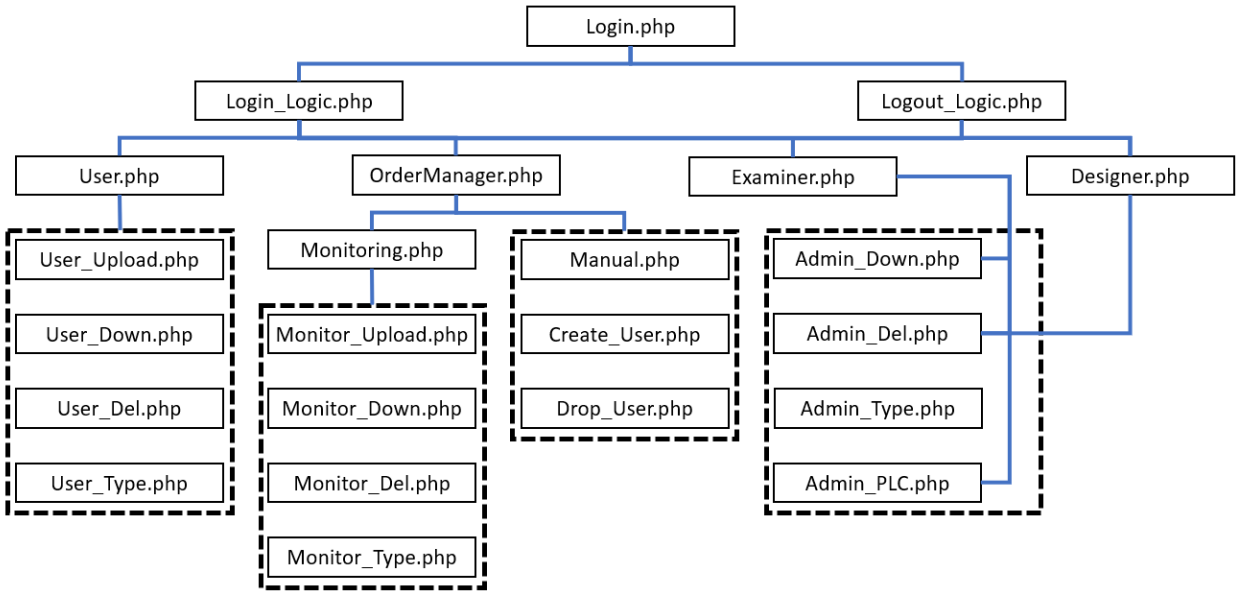


Figure 24 Front-End Structure

The manufacturer's webserver, the manufacturer's PLC server, and the supplier's PLC server are remotely connected via the UDP/IP protocol. The communication is done by sending/receiving packets, which are created by the C-programming language with the raw socket library. Each PLC server and physical entities' controller are connected by 24 gauge silicone wires. Customers can access the webserver with the user interface front-end through HTTP protocol. Details of the front-end structure can be found in Figure 24.

The user interface front-end was built by PHP 5.0, JavaScript, and MySQL database. The webserver's access authentication is managed by ID & password login system with the database, and it limits the access to the certain PHP documents based on the authentication. Data transmission between PHP documents are done by POST & GET method, and basic security method such as cookie and special character filtering were applied. Each php documents interacts with the MySQL database. The structure of the database can be found below.

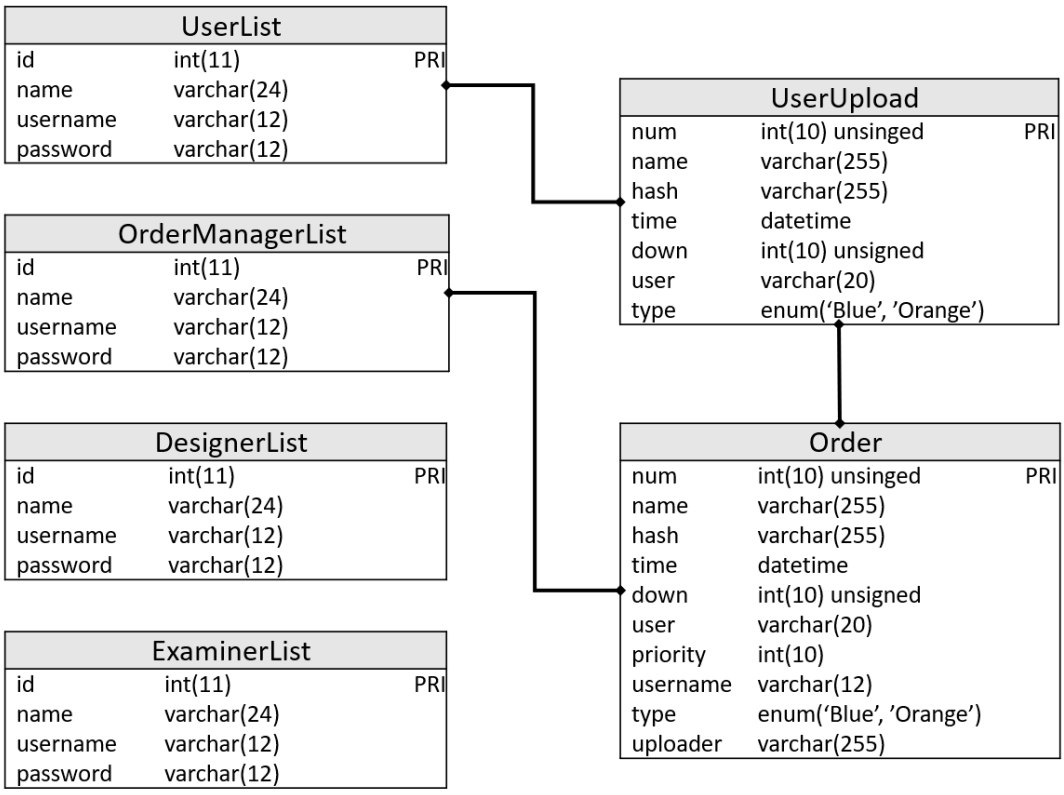
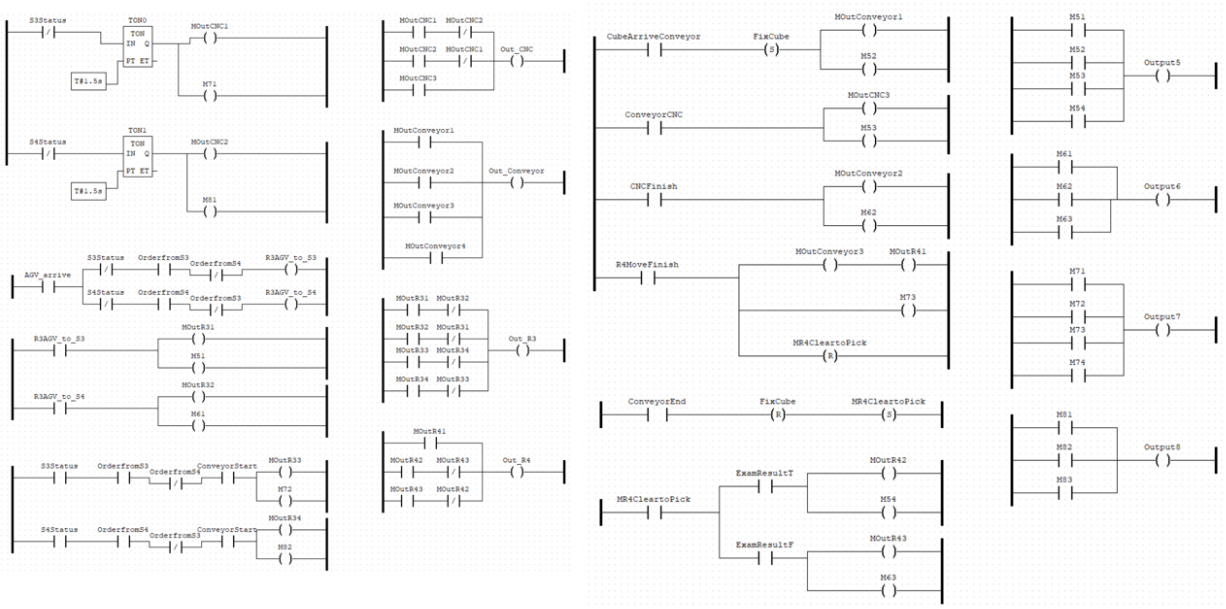


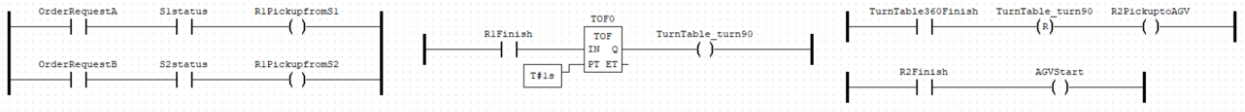
Figure 25 Database Structure

Open-sourced Programmable Logic Controller (OpenPLC) with IEC 61131-3 standard was installed to integrate all the physical entities. Two different ladder logics were written for the manufacturer and the supplier, and those were embedded in the manufacturer's PLC server and the supplier's PLC server.

Manufacturer



Supplier



The entire flow chart of testbed operating simulation is presented in Figure 27. The manufacturer PLC server and the supplier PLC server are running the OpenPLC server at 8080 port to manage each other's physical entities and Python SCAPY script at 9090 port to receive packets that are generated by C-programing. The number of simulation replications is assigned as present number of orders (PO), and the simulation will be terminated after PO reaches 0.

This logic starts from the webserver. Sending an order to Manufacturer PLC server and check the inventory status. After that, if there is no stock in the Manufacturer’s inventory, the order is generated and send to supplier. Similarly, if there is no raw material in the supplier’s inventory, 3D printing worker produce the material, and then processed. Once Manufacturer’s inventory is filled, Manufacturer’s PLC server proceeds the product by following the programmed ladder logic.

PO	Present number of Order
ILI	Initial Level of Inventory
SI, MI	Supplier Inventory, Manufacturer Inventory
NRO	Number of Requested Order
MWS	Manufacturer Main Web Server
MPLC, SPLC	Manufacturer PLC Server, Supplier PLC server
R1, R2, R3, R4	Robot arm 1, 2, 3, 4
TT	Turn Table
AGV	Automated Guided Vehicle
C	Conveyor
CVM, DM	Cube Vise Machine, Drawing Machine
->	Trigger a signal (e.g. A -> B = A trigger B to operate)

Figure 26 Nomenclature for the Flowchart

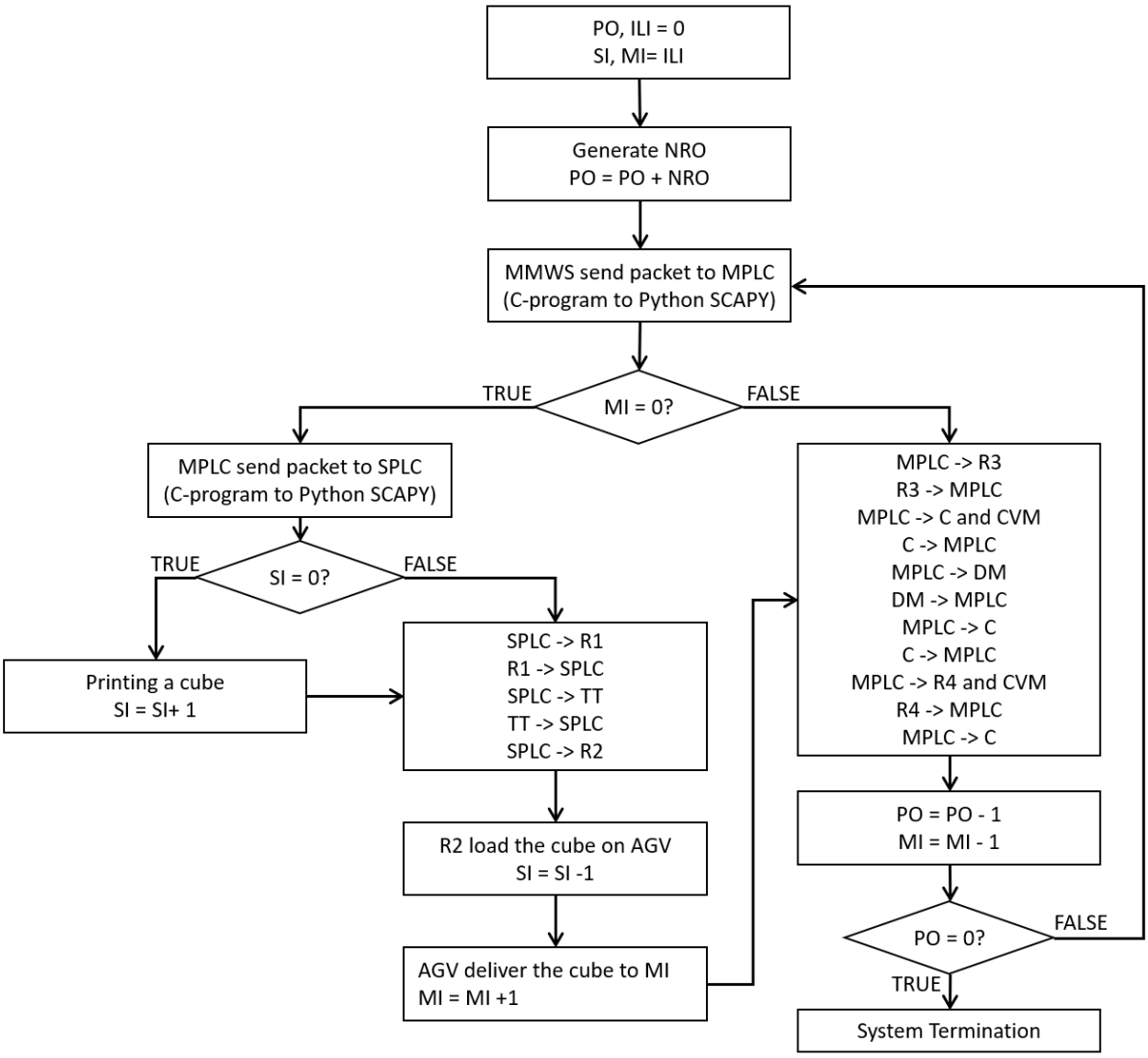


Figure 27 Testbed Operation Flowchart

5.2.3.3 Blockchain Implementation

To implement the blockchain layer into SPLC, three programs are run in the PLC devices simultaneously: OpenPLC software, Python, and GETH client. OpenPLC and Python's GPIO package with WiringPi are interacting by I/O data. Uploaded input data in the blockchain layer is transferred by Python's web3 package through GETH client to be utilized for PLC operations. Also, a new I/O data can be uploaded in the same way. The algorithms for retrieving data and uploading data can be found in Figure 28 and Figure 29, respectively.

```
1   Import socket, time, Web3
2   Import RPi.GPIO as GPIO
3
4   url = "http://127.0.0.1:8545"
5   web3 = Web3(Web3.HTTPProvider(url))
6   GPIO.setmode(GPIO.BCM)
7   IP = "PLC IP"
8   PORT = Port Number
9   sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
10  sock.bind((IP, PORT))
11  while True:
12      Transaction, Server_addr = sock.recvfrom(1024)
13      INPUT = web3.eth.getTransaction(Transaction).input
14      if INPUT ! = None:
15          continue
16      elif INPUT == "Inp00":
17          GPIO.output(2, GPIO.HIGH)
18          sleep(1)
19          GPIO.output(2, GPIO.LOW)
20      elif INPUT == "Inp01":
21          GPIO.output(3, GPIO.HIGH)
22          sleep(1)
23          GPIO.output(3, GPIO.LOW)
```

Figure 28 Retrieving Data

```
1   Import socket, Web3
2
3   url = “http://127.0.0.1:8545”
4   web3 = Web3(Web3.HTTPProvider(url))
5   INPUT = Generate_Input()
6   Transaction = web3.eth.sendTransaction({‘from’:
    web3.eth.coinbase, ‘data’: INPUT, ‘gas’: Gas value}))
7   IP = “PLC IP”
8   PORT = Port Number
9   sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
10  sock.sendto(MESSAGE, (IP, PORT))
```

Figure 29 Uploading Data

As a result, PLC can have a two-way communication channel with the blockchain by employing Python as an intermediary. The channel's algorithms and architecture are presented as follows.

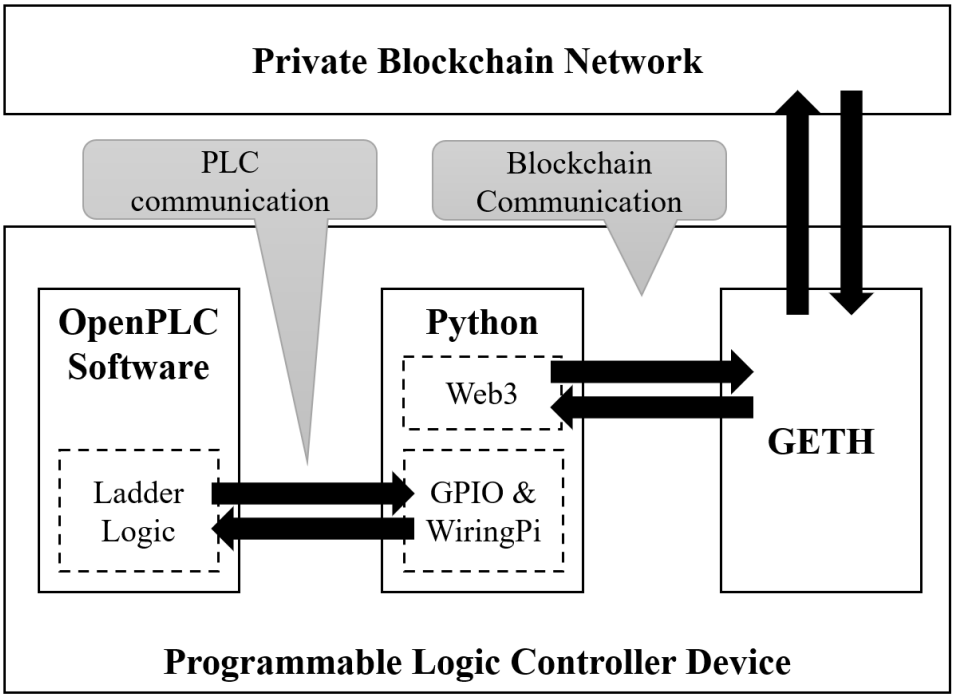


Figure 30 Communication Channel for SPLC

In this way, input data for PLC operations only can be accessed by entering a transaction hash that is returned when the input data is uploaded. Also, the input data is retrieved and temporarily existed in the memory of the PLC device when the valid transaction hash is entered, while the input data is permanently and immutably stored in the blockchain. Hence, insiders only can operate the PLC device based on pre-uploaded input data and cannot modify the data without attacking the blockchain. This means that PLC can now have a strong validation process for the input data.

5.2.3.4 ITTCPMS Implementation

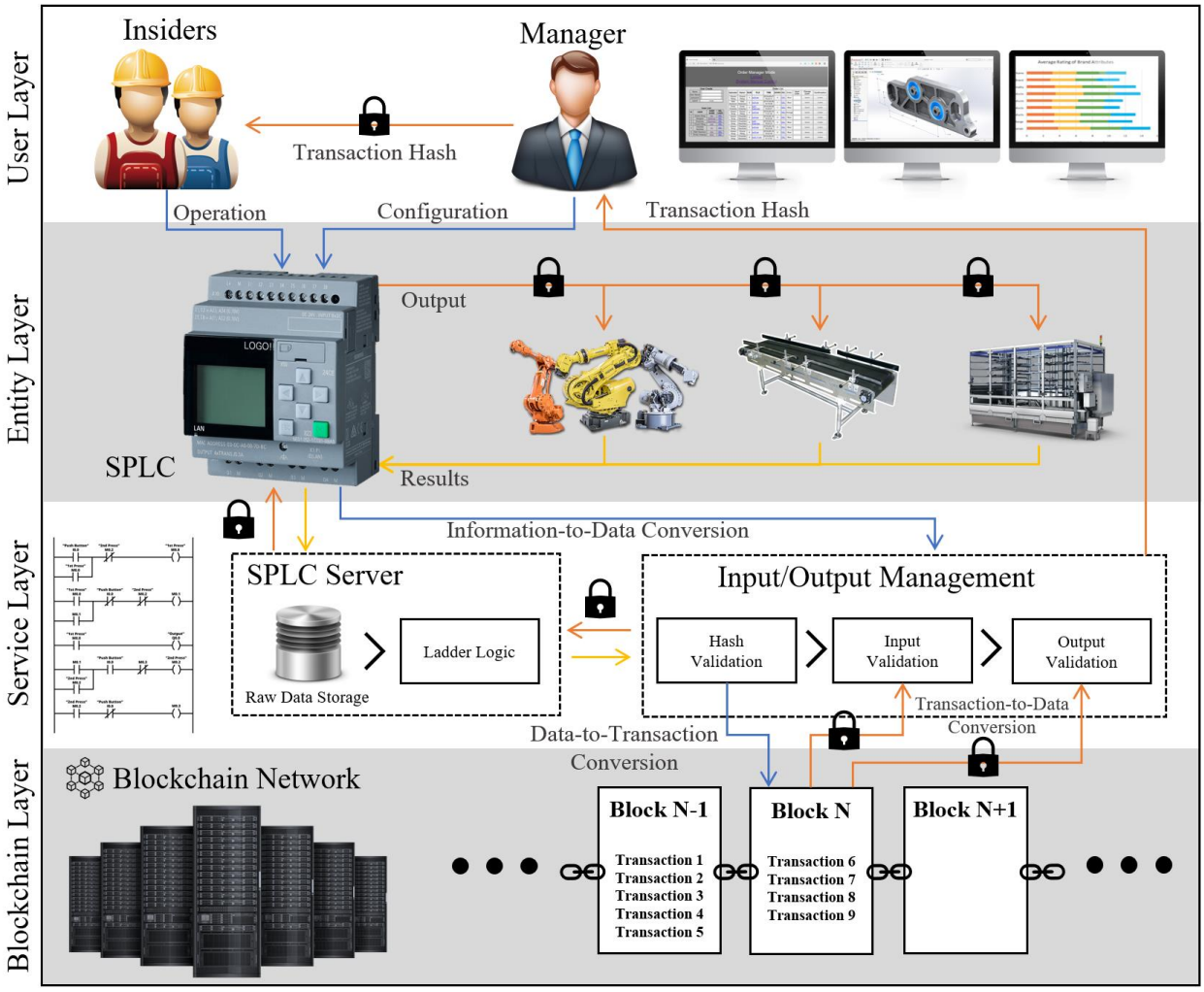


Figure 31 ITTCPMS with SPLC

Figure 31 shows how SPLC can be applied to ITTCPMS. SPLC devices with the multiple physical entities are placed in the entity layer. The SPLC server is in the service layer, communicating with SPLC and managing the ladder logic.

From the manager's configuration process, the verified Input and Output data will be organized and uploaded on the blockchain layer via the service layer. As explained for the LIAS operation process, the generated transaction hash will be delivered to the insiders and used to access the uploaded data.

5.2.4 Discussion

Insiders can make modifications that can result in serious damage to the physical machines in the system. For example, insiders can change the sensitive manufacturing specifications by modifying input values such as heating treatment temperature, nozzle travels the speed of 3D-printer, and a spindle speed of CNC machines (Wu & Moon, 2018). In the PLC testbed, it is assumed that the largest shareholder—a manufacturer in the manufacturer's factory—of the system is holding a ground truth while potential insiders could be PLC engineers, shop floor workers, or production managers (Song, Shukla, et al., 2020).

However, the blockchain can effectively prevent the data from insiders' malicious modification. The blockchain can reduce the insider threats risk by adding a validation process for input data. PLC can only proceed with legitimate input data by entering the transaction hash to retrieve corresponding data, which is already validated by the blockchain. Now, insiders need to find out the exact transaction hash value of false order and alter the embedded legitimate transaction hash to false order's transaction hash to attack the system, which is only available for the limited number of insiders. Also, since input data's transaction hash will be renewed every time

when the main control server is sending the input data, it is not easy to identify the legitimate input data from the transaction hash. In another way, insiders can add new input data to the blockchain and acquire a malicious transaction hash. But insiders need to access the private blockchain, which allows only a limited number of insiders to join. Lastly, modifying the blockchain itself can be another way to directly modify input data. To do this, insiders require computing power more than 50% of the power of entire blockchain node machines or need to compromise and manipulate more than half number of entire the node machines' blockchain repository. However, such an attempt is not practical, so it is fruitless (Afanasev et al., 2018).

Chapter 6. Insider Attack Tree

In this chapter, insider threats in Cyber-Physical Manufacturing System (CPMS) are examined in depth. In order to better understand different ways in which a system can be attacked by insiders, Insider Attack Tree (IAT) is presented. The IAT consists of four parts: Root, Branch, Sub-Branch, and Leaf. The Root is the eventual attack target for insiders, and the Branches represent three different assets in CPMS. Sub-branches indicate the attack targets of assets while the Leaf represents attack vectors.

6.1 Insider Threats

Advances in automation and network technologies have enabled the manufacturing industry to take a step forward towards the realization of the vision of Cyber-Manufacturing Physical System (CPMS). The manufacturing industry can take advantage of CPMS to increase productivity, enhance quality, and reduce manufacturing costs (Hutchins et al., 2015).

However, CPMS ushers in unseen security challenges from the sheer volume and pervasiveness of exchanged data along with the enlarged attack surface for both outside and inside attackers. Particularly, insiders who have been or are affiliated with a system can pose more sever threats than outsiders, and their threats are especially enlarged in CPMS. For example, CPMS's cross-domain structure's physical domain and the digital domain will enlarge insider attack consequences because insiders in the system will have more extended control and access to the system properties (Song & Moon, 2020b). Also, they can easily hide their digital footprint because they have legitimate access authentications to manipulate or remove their digital records, such as event logs, browsing history, and any surveillance history data. Moreover, insiders can unintentionally become a bridge to the system for outsiders by social engineering attacks, such as phishing, scam, and misconfiguration (Greitzer et al., 2011; Salahdine & Kaabouch, 2019). Besides, since the growth of collaborative business in the manufacturing industry blurs the boundary between insiders and outsiders, it is hard to decide who insiders are in the system (Schultz, 2002). Finally, there is a critical contradictory problem between security and flexibility. Merely increasing restrictions on the system will definitely improve system security. However, it also reduces system flexibility (Sinclair & Smith, 2008).

Accordingly, concerns about security in manufacturing systems have been reported by many security organizations. In 2017 CERT and 2018 IBM reports, manufacturing is found to be

the second most industry that experienced cyber-attacks (IBM, 2018). Among those attacks, 23 percent of cyber-attacks were suspected to be caused by insiders. 45 percent of survey respondents agreed that the damage from insider attacks was more critical than the damage from outsider attacks (CERT, 2019). However, while some research about insider threats has been performed in the information system community, such research in CPMS has not been conducted or at least not reported.

The consequences of insider attacks can affect the dramatic physical domain in CPMS. Insiders may end up with serious damages in CPMS not only through information leakage or intellectual property theft, but also by damaging facilities, sabotaging manufacturing operations, and perpetrating acts of security policy violation. The attacks that begin in digital format may result in malfunctioning manufacturing equipment, defective products, or any other unintended changes (Wu & Moon, 2018). Insiders can exacerbate or provoke Cyber-Physical Attacks in a shifty way. Insiders who are knowledgeable of the system can easily bypass or incapacitate the security process and compromise the system to induce physical damage. The growth of outsourcing and subcontracting in the manufacturing industry can also increase the number of insider attacks in a supply chain and contribute to diversifying the attack methods.

Despite the severity of insider threats in CPMS, in the manufacturing community, understanding of its significance is limited. According to the Intelligence and National Security Alliance (INSA), only 8% of survey respondents in 2018 are acquiring internal identity data to warn of an impending attack. Respondents also answered that it is difficult to develop skilled labor and adequate defensive preparation due to the lack of known threats to their organizations. Without being aware of potential threats, they often make inappropriate decisions that can yield wasteful expenditures (INSA, 2018a, 2018b).

6.2 Insider Attack Tree

As the first step to systematically understand different ways insiders can compromise CPMS, an Attack Tree can be utilized. Attack Tree systematically classifies different ways in which a system can be attacked (Audinot et al., 2018). The Attack Tree's nodes consist of the root node, children of a node, and leaves. Each node represents the main goal of an attacker, refinements of the goal, attacks that cannot be refined, and those that can be used to analyze attributes of the system security (Mauw & Oostdijk, 2006). The Attack Tree can be used to investigate system security in various ways. Saini et al. (Saini et al., 2008) use the Attack Tree to develop the concept of threat modeling, which provides practical and high-level guidance. Also, to design the attacker's behavior, the Attack Tree can be extended by adopting the temporal order of the attacker's decision-making process (Jürgenson & Willemson, 2010). Moreover, a particularly refined form of the Attack Tree has been employed to develop a simple risk-analysis-based method (Buldas et al., 2006). However, insider threats have never been analyzed by using the Attack Tree.

In order to better understand different ways in which a system can be attacked by insiders, Insider Attack Tree (IAT) is developed and presented. The IAT consists of four components: Root, Branch, Sub-Branch, and Leaf. The Root represents an ultimate attack target while the Branch indicates domains of CPMS's asset: physical asset, digital asset, and access authorization. The Sub-Branch is the attack target for each Branch, whereas the Leaf refers to a specific attack vector to compromise its Sub-Branch.

In the Branch, access authorization can be viewed as digital asset. However, access authorization is different from digital asset in many respects. Access authorization is a part of the system to manage access to CPMS's assets. On the other hand, digital assets such as manufacturing information, product specification, supply chain management, and design are highly related to the

manufacturing process and can affect the process in various ways. Also, access authorization is subject to be an attack target to access CPMS's asset, but digital asset is attacked to compromise the manufacturing process itself. Therefore, attack scenarios and the scope of insiders for access authorization should be separated from digital assets.

The main objectives of the IAT are: i) to analyze insider threats across cyber and physical domains in CPMS; ii) to identify possible insider attack scenarios; iii) to diagnose system vulnerabilities against insiders, and iv) to help design technical countermeasures.

The Insider Attack Tree can be found in Figure 32.

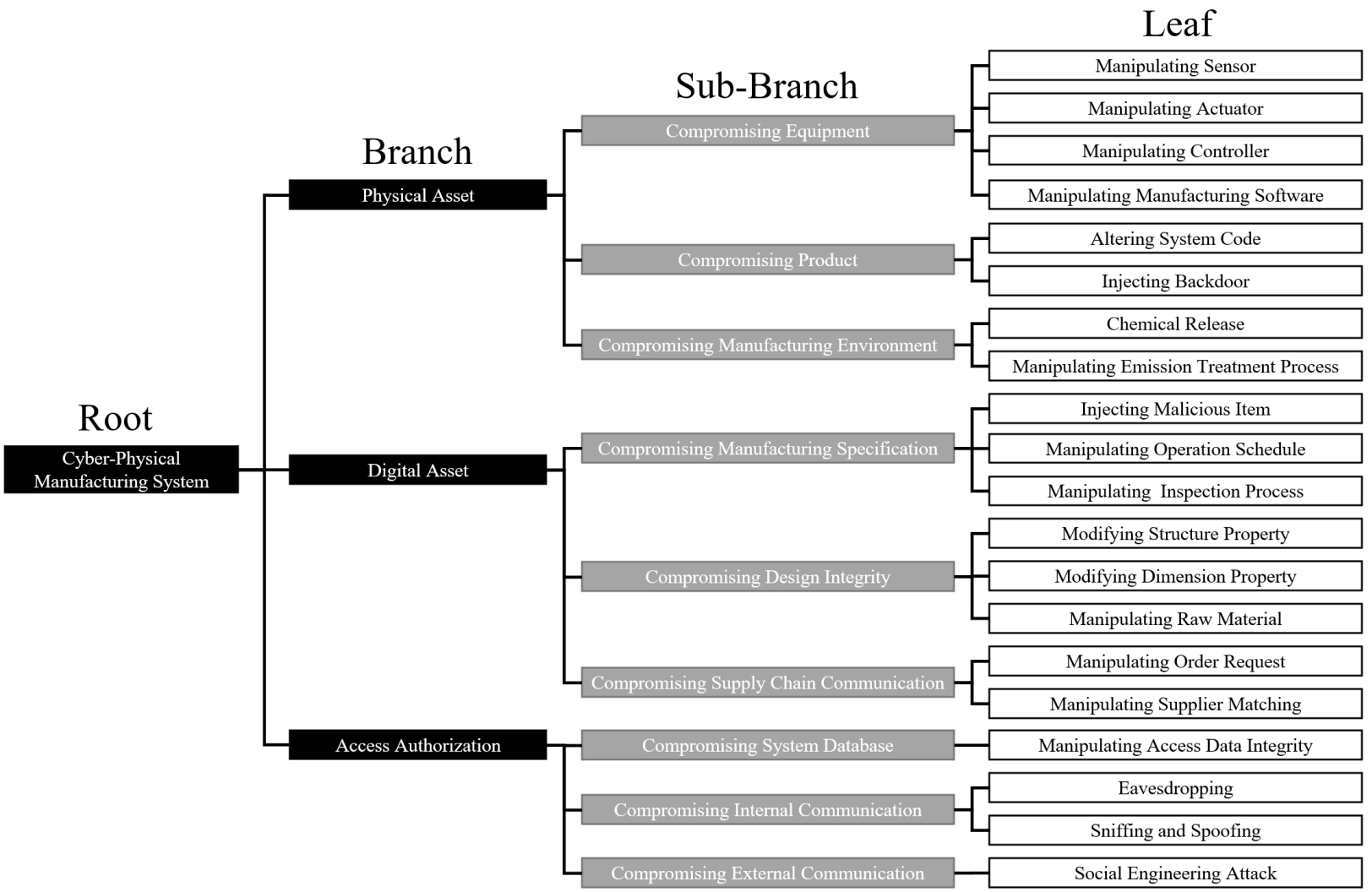


Figure 32 Insider Attack Tree

6.2.1 Physical Asset

Physical asset in CPMS can be categorized into Equipment, Product, and Manufacturing Environment. Insiders working in a shop floor or having access authorization can intentionally or unintentionally imperil the physical asset with eight possibilities.

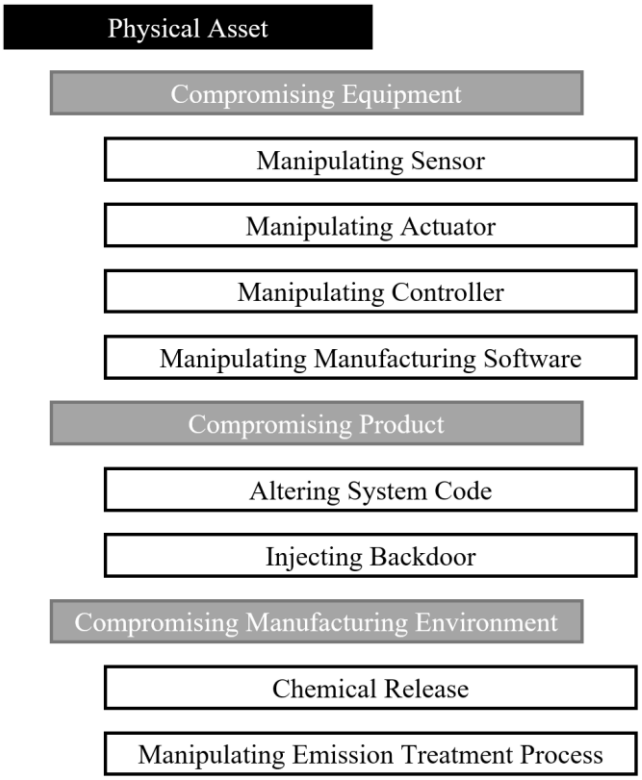


Figure 33 Physical Asset

6.2.1.1 Compromising Equipment

Manipulating Sensor: Sensors attached to machineries such as temperature, motion, or acoustic sensors can be manipulated by insiders. Insiders can directly inflict physical damages on sensors or alter operation codes to corrupt data integrity. Sensor manipulation can result in malfunctions in manufacturing processes and cause production accidents (Wu & Moon, 2019).

Manipulating Actuator: Actuators including hydraulic, pneumatic, and electric types are susceptible to insider manipulation. Even unintended subtle changes can immediately cause a failure of a machine and destruction of the entire system.

Manipulating Controller: Programmable Logic Controller (PLC) that is commonly used in the manufacturing industry can be compromised by insiders. PLC manipulation can cause an unintended series of machine operations and induce production accidents.

Manipulating Manufacturing Software: A software that operates manufacturing equipment such as a 3D-printer or robotic arm can be altered by insiders. For example, a CNC milling machine software can be changed to increase the spindle speed, which may result in over-wearing of the end mill tool (Wu & Moon, 2019).

6.2.1.2 Compromising Product

Altering System Code: System codes embedded in the product can be modified by insiders. Insiders knowledgeable of product specification can alter the code that would pass Quality Control (QC) but eventually fail when the product is operated by end-users (Sturm et al., 2017). It can also result in malfunction or a reduced lifecycle of a product.

Injecting Backdoor: A backdoor is an intended malicious code structure within a system that provides unauthorized access to the privileged functionality of the system. Insiders can inject the backdoor into the product's software or hardware, which allows outside attackers to access the product's administrative control (Thomas & Francillon, 2018).

6.2.1.3 Compromising Manufacturing Environment

Chemical Release: Insiders can voluntarily or involuntarily release chemical substances such as oil, ammonia, chlorine, etc. According to the United States Chemical Safety and Hazard

Investigation Board (CSB), the chemical release was the most frequent incident during 2005–2006 (Gomez et al., 2008).

Manipulating Emission Treatment Process: The emission treatment process can be manipulated by insiders. The malfunctioned emission treatment process may yield a serious worker health hazard. For example, high concentrations of nanoparticles have been observed from industrial-scale 3D-printer operations without proper ventilation in the facility (Davis et al., 2019).

6.2.2 Digital Asset

Digital assets can be jeopardized by compromising manufacturing specifications, design integrity, and supply chain communication. Insiders who are in the security parameter of a system can intentionally or unintentionally attack the Digital Asset with eight possibilities.

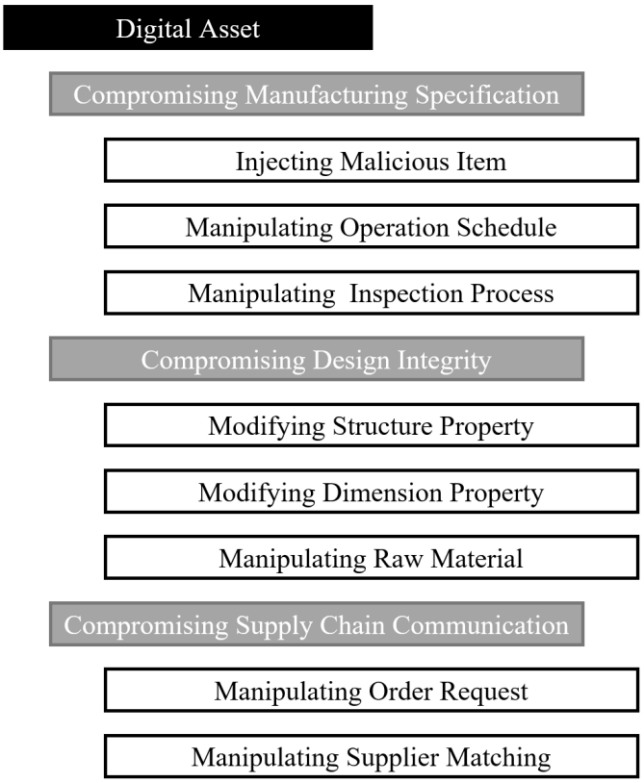


Figure 34 Digital Asset

6.2.2.1 Compromising Manufacturing Specification

Injecting Malicious Item: Malicious Item can be injected by insiders bypassing the inspection process. For instance, a 3D-model design that involves infill defectives can be injected, which does not affect the exterior (Wu et al., 2017).

Manipulating Operation Schedule: The operation schedule is one of the important assets in digital form, and it can be manipulated by insiders, especially involuntary insiders. For example, an insider might mismatch operation schedules due to a miscommunication.

Manipulating Inspection Process: Inspection processes in the manufacturing system cannot be free from the attack by insiders. Insiders can manipulate inspection parameters such as threshold or inspection programming code to compromise inspection processes (Song & Moon, 2020c).

6.2.2.2 Compromising Design Integrity

Modifying Structure Property: The structure of the design can be manipulated by insiders to compromise the physical specifications of the product such as tension or strain, as well as design features.

Modifying Dimension Property: Insiders can change the dimension property of the design, which can yield improper assembly processes. This attack can be accomplished stealthily. For instance, if the insider scales the design slightly while keeping the design's overall shape, it would be hard to detect the changes and can cause a product quality issue.

Manipulating Raw Material: The raw material can be changed by insiders. This attack may occur in a business-to-business relationship. For example, a supplier would replace the raw material for the part if it is cheaper but can pass the quality control required by a manufacturer. However, it can result in various side effects after some time.

6.2.2.3 Compromising Supply Chain Communication

*Manipulating Order Reques*t: Insiders can manipulate order requests between manufacturers and suppliers to compromise inventory control or manufacturing processes. Insiders can manipulate the communication with Man-In-The-Middle-Attack (MITMA), which exploits internet network vulnerabilities.

Manipulating Supplier Matching: The supplier for a manufacturer is determined by various factors such as availability, production capacity and quality, cost, and distance. So it can also be manipulated by insiders. The compromised factors may increase the manufacturing expenses and decrease the product quality.

6.2.3 Access Authorization

Access authorization requires a high level of confidentiality since it controls access to CPMS's assets. At the same time, access authorization is subject to an attack target by not only insiders but also outsiders. Access authorization can be attacked by compromising the system database, internal communication, and external communication.

Access authorization can be viewed as the digital asset. However, access authorization is different from the digital asset in many respects. Access authorization is a part of the system to manage access to CPMS's assets. On the other hand, digital assets such as manufacturing information, product specification, supply chain management, and design are highly related to the manufacturing process and can affect the process in various ways. Also, access authorization is subject to be an attack target to access CPMS's asset, but the digital asset is attacked to compromise the manufacturing process itself. Therefore, attack scenarios and the scope of insiders for access authorization should be separated from digital assets.

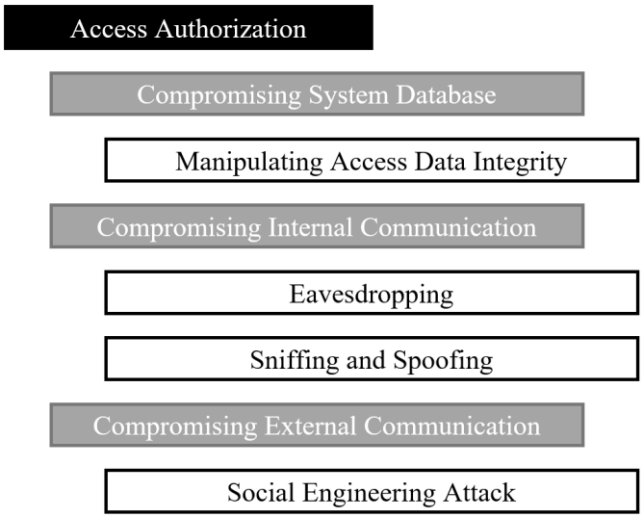


Figure 35 Access Authorization

6.2.3.1 Compromising System Database

Manipulating Access Data Integrity: Insiders can directly manipulate access data by using their authorizations. Also, breaching their access authorization data may cause impersonating attacks by outsiders: an attacker who acquires a legitimate insider's access authorization impersonates another user for malicious purposes (Salem et al., 2008).

6.2.3.2 Compromising Internal Communication

Eavesdropping: Insiders may become careless in managing their access authorization, which can violate the security policies of the system. It can also be eavesdropped on or picked up by voluntary insiders to be used for malicious purposes.

Sniffing and Spoofing: Insiders who are knowledgeable of the IT network structure of the system can use sniffing and spoofing code to steal or breach access authorization. Since the insiders are in the same network environment, it is easy to use the internet network vulnerabilities to succeed in the attack such as DNS server attacks.

6.2.3.3 Compromising External Communication

Social Engineering Attack: Social Engineering Attacks—such as phishing, SMSishing, baiting, fake software—are deceiving individuals or enterprises to accomplish certain actions that benefit attackers (Salahdine & Kaabouch, 2019). Social engineering attack is one of the critical insider threats because it reveals accessible routes into the system to outsiders, although involuntarily sometimes. Generally, social engineering attack utilizes mediums that are used for external communication such as phone, email, webpage, etc. For example, Target, the eighth-largest retailer in the United States, was attacked with a credit card data breach by a third-party vendor, which resulted in 7.5 million dollars worth of customers' credit card information leaking in 2013 (Harris, 2016).

Chapter 7. Assessment and Case Studies

To validate and evaluate the insider threat tolerant Cyber-Physical Manufacturing System (CPMS) augmented by the service-oriented blockchain, this chapter presents an Insider Attack Scenario Assessment Framework (IASAF) to evaluate vulnerabilities of manufacturing systems against insiders. The framework investigates pitfalls from insiders by evaluating potential insider attack scenarios within five domains: Actor, Preparation, Implementation, Consequence, and Recovery. The proposed framework is used to evaluate four attack scenarios generated using the Insider Attack Tree: Manipulating Inspection Process, Sniffing and Spoofing, Injecting Malicious Item, and Social Engineering. Each attack scenario is explained and developed as a case study. To demonstrate the effectiveness of the blockchain, two simulation models (LIAS and SPLC) without the blockchain layer were used for the case studies.

7.1 Insider Attack Scenario Assessment Framework

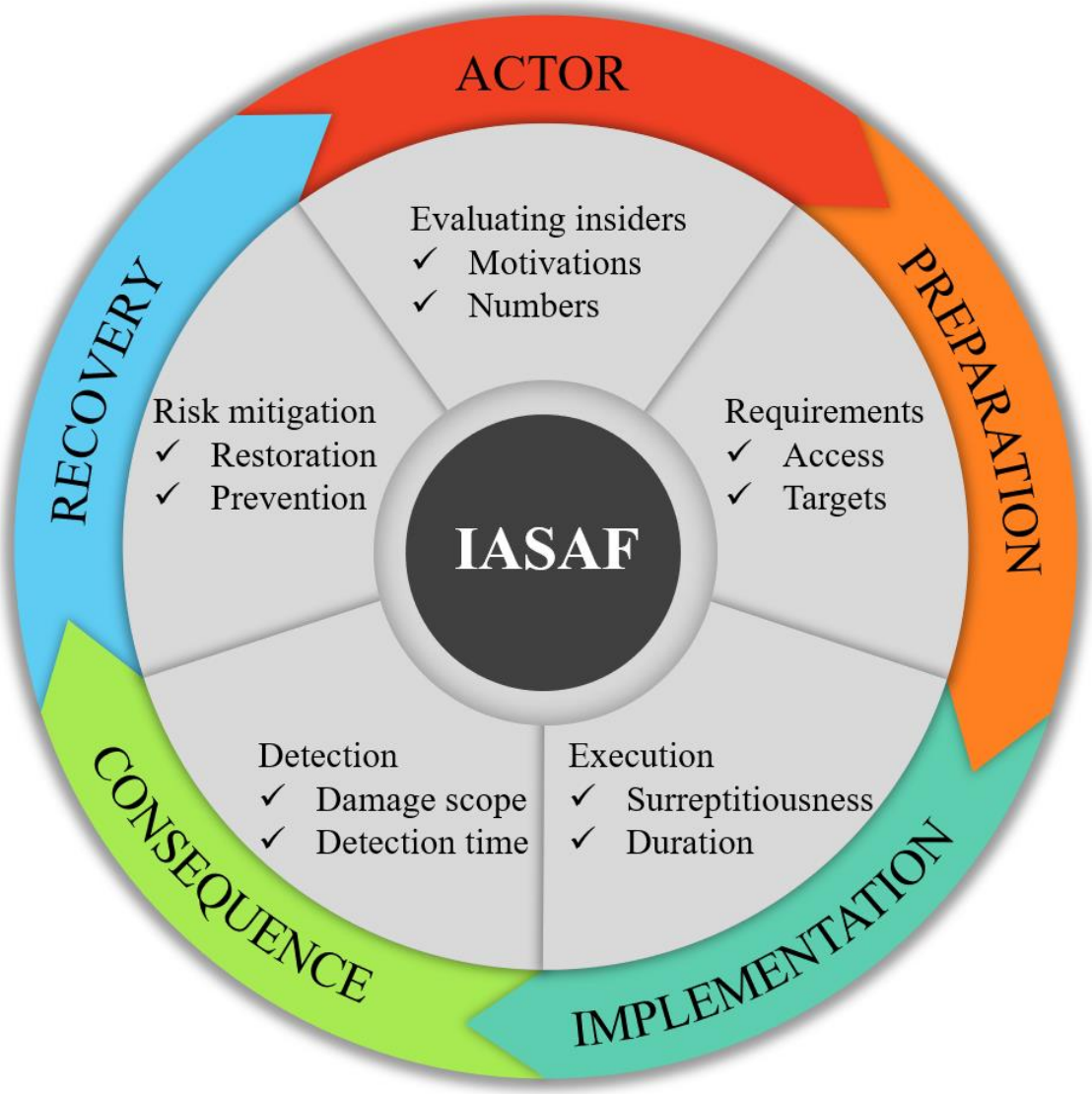


Figure 36 Insider Attack Scenario Assessment Framework

As the growth of fully automated manufacturing systems and the complexity of these systems has been developed, a diverse and complicated problem arises concerning conditions associated with system compositions, operating configurations, and behaviors. As a result, an assessment framework of existing methods barely affords necessary information about the various conditions of problems in manufacturing systems (Primova et al., 2018). Besides, it is not adequate

to assess a system to analyze attacks from insiders—who are in a security perimeter of a system—because they are parts of the system and can elude and deceive the assessment process.

To address such issues, a new approach to assess systems from the viewpoint of attack methodology has been developed: An Insider Attack Scenario Assessment Framework (IASAF). IASAF can help to analyze system vulnerabilities by assessing attacks. IASAF examines an attack by five domains in order: Actor, Preparation, Implementation, Consequence, and Recovery. Each domain consists of a set of questions that evaluates the attack in terms of two key factors of the domain. The domains, key factors, and its indicator are organized in Table 8.

Table 8 Key Factor and Indicator

Domain	Key Factor	Indicator
Actor	Motivations	A1
	Numbers	A2
Preparation	Access	P1
	Targets	P2
Implementation	Surreptitiousness	I1
	Duration	I2
Consequence	Damage Scope	C1
	Detection Time	C2
Recovery	Restoration	R1
	Prevention	R2

7.1.1 Actor

In Actor domain, the quantitative evaluation will be processed by assessing attack motivations and the number of insiders. Motivation is one of the most difficult factors of IASAF, because it is elusive to predict insider attacks in advance, due to the varied human motivations and limited understanding of human psychology with regard to this subject (Moore, 2016). However, by categorizing the attack's intention and the degree of its intensity, the motivation can be objectively evaluated.

7.1.2 Preparation

This domain will check the requirements of the attack implementation based on two key factors: Access and Targets. It is essential to identify required entities to successfully implement the attack, such as sensors, controllers, and servers. For the evaluation, i) security clearance level, ii) position, and iii) policies to access the entities can be considered as well as the number of the entities. The target is defined as the attack target, which is necessary to be compromised or manipulated for the attack implementation. Since physical and digital entities of a system are varied by different manufacturing systems, a customized checklist for the domain is inevitable.

7.1.3 Implementation

The attack timeline for this domain is before the damage has occurred. Surreptitiousness and duration of the attacks will be measured and evaluated. Accessing and compromising system entities must leave digital traces, such as event logs, browsing history, and any surveillance history data. However, insiders can easily hide their digital footprint because they have legitimate access authentications to manipulate or remove their digital records. Therefore, these records that need to

be erased are considered for the surreptitiousness. Also, the duration to execute the attack—including a preparation phase—is checked.

7.1.4 Consequence

For Consequence, the attack timeline is after the damage has occurred. The attack consequences will be checked in terms of the scope of the damage and detection time. For the scope of the damage, a significance of the entities based on hierarchical system structure will be considered alone with the number of the entities. The detection time can be measured based on the systems operation process.

7.1.5 Recovery

Finally, in the recovery, the level of the required restoration process and attack prevention will be evaluated. The length of the restoration process is the main measurement of this domain. Also, potential technical countermeasures for the attack and its cost and efficacy are also considered.

7.2 Case Study Design

This section presents case studies with IASAF implementation. The attack scenarios from the Insider Attack Tree (IAT) were chosen for the case studies, and three different attack methods are used to simulate the scenarios. For the attack scenario selection, since LIAS and SPLC have different manufacturing objectives and purposes with the service layer, Manipulating Inspection Process and Social Engineering were chosen for LIAS, and SPLC was tested with two other attack scenarios: Injecting Malicious Item and Sniffing and Spoofing. These are organized in the following Table 9.

Table 9 Attack Scenario and Target Model

Case	Attack Scenario	Target Model
Case Study 1	Manipulating Inspection Process	LIAS
Case Study 2	Social Engineering	LIAS
Case Study 3	Injecting Malicious Item	SPLC
Case Study 4	Sniffing and Spoofing	SPLC

7.2.1 Testbeds for the case studies

To demonstrate the effectiveness of the blockchain implementation, the attack scenarios should be simulated under the condition without the blockchain layer. Therefore, for the testbeds of the case studies, the blockchain layer was removed from LIAS and SPLC while remaining their functionalities. The testbeds consist of three layers: user Layer, entity Layer, and service Layer. The architecture of the testbeds for LIAS and SPLC can be found in Figure 37 and Figure 38, respectively.

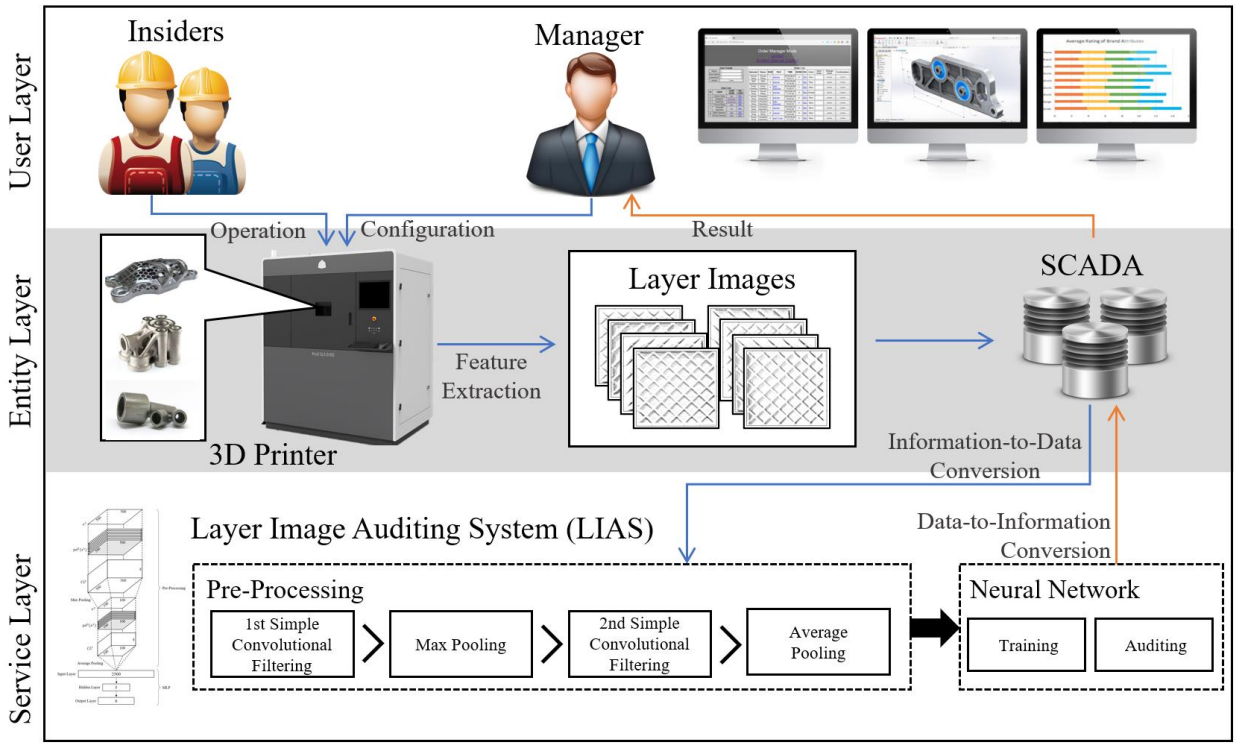


Figure 37 Testbed for LIAS

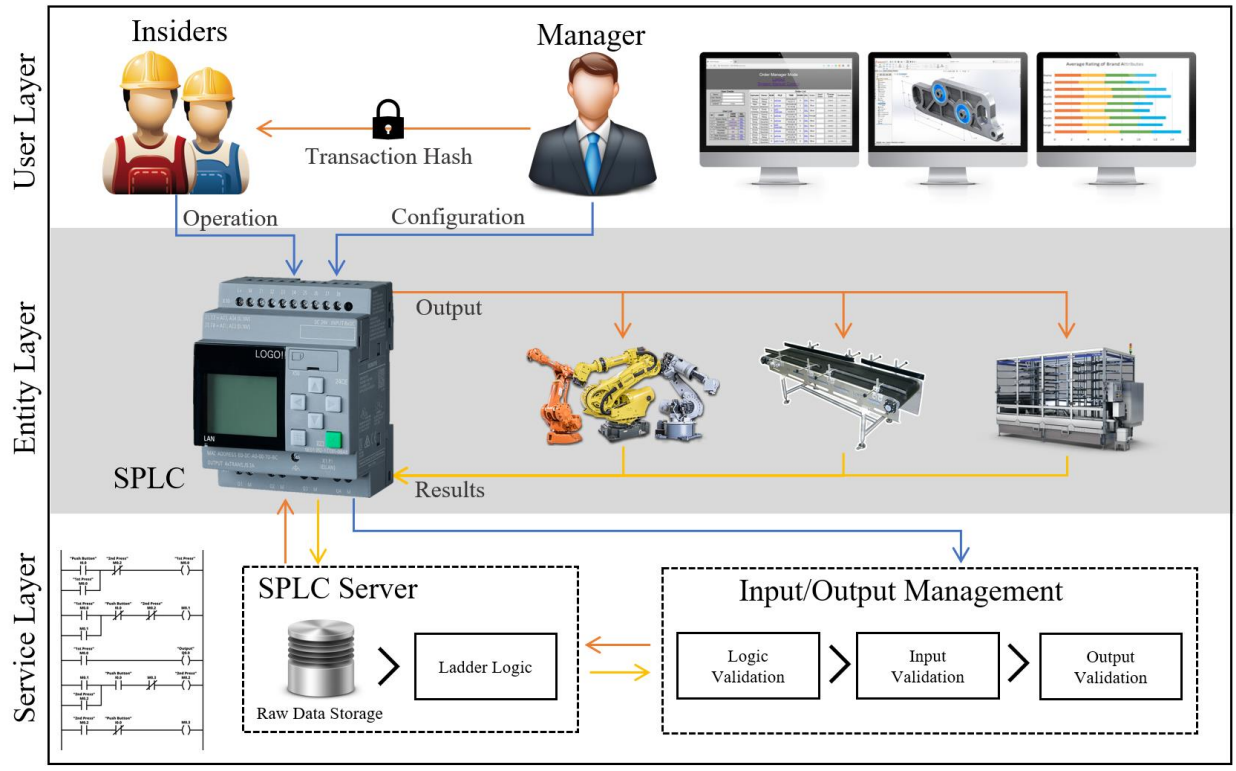


Figure 38 Testbed for SPLC

7.2.2 Questionnaires for IASAF

To evaluate attack scenarios from the case studies, questionnaires for five domains of IASAF were created. The evaluation is made for each key factor of the domain, and the key factors are evaluated by three levels of the degree of posing threat risks: moderate (*), significant (**), and critical (***).

For Actor domain, the questionnaire for the motivation and numbers are created. Two major motivations of insiders (Voluntary and Involuntary) were used to comprise the questionnaire for the motivation. For the numbers, two categories of the insiders (Skilled and Layperson) were also included in the questionnaire to consider the quality as well as the quantity of the insiders. The questionnaires for Actor domain in Table 10.

Table 10 Actor Questionnaire

Key Factor	Indicator	Degree	Questionnaire
Motivations	A1	Moderate (*)	Can either voluntary or involuntary insiders be motivated to the scenario?
		Significant (**)	Can both voluntary and involuntary insiders be motivated to the scenario?
		Critical (***)	Is it hard to determine the motivation of the scenario?
Numbers	A2	Moderate (*)	Are more than two insiders, who are layperson or skilled or on a high position, involved?
		Significant (**)	Is only one insider, who is skilled or on a high position, involved in the scenario?
		Critical (***)	Is only one insider, who is a layperson, involved in the scenario?

Preparation domain has two key factors: Access and Targets. The access was evaluated whether the insiders have the access authority to the entities for the attack scenario. For the target, the access to the digital entities and physical entities are separated. Also, the questionnaire for the target considers the number of the targets, because some attack scenarios may require attacking more than two targets to successfully compromise the system. The questionnaires for Preparation domain in Table 11.

Table 11 Preparation Questionnaire

Key Factor	Indicator	Degree	Questionnaire
Access	P1	Moderate (*)	Do insiders have no access authority to the entities required for the attack scenario?
		Significant (**)	Do insiders have partial access authority to the entities required for the attack scenario?
		Critical (***)	Do insiders have access authority to all the entities required for the attack scenario?
Targets	P2	Moderate (*)	Are more than two digital or physical entities required to be accessed to implement the attack?
		Significant (**)	Are both the digital and physical entities required to be accessed to implement the attack?
		Critical (***)	Is either a single digital or physical entity required to be accessed to implement the attack?

For Implementation domain, the questionnaires for the surreptitiousness and duration key factors are created. Mainly, a digital footprint and surveillance record were used to evaluate the surreptitiousness. For the duration, to objectively evaluate the attack duration, a TAKT time was introduced. The TAKT time is a manufacturing terminology to describe the required production

timeline, which can satisfy the demand (Moorthi et al., 2011). The questionnaires for Implementation domain in Table 12.

Table 12 Implementation Questionnaire

Key Factor	Indicator	Degree	Questionnaire
Surreptitiousness	I1	Moderate (*)	Does the attack leave a digital footprint or any surveillance record, but insiders cannot delete it?
		Significant (**)	Does the attack leave a digital footprint or any surveillance record, but insiders can delete it?
		Critical (***)	Does the attack leave no digital footprint or any surveillance record?
Duration	I2	Moderate (*)	Can the attack only be implemented with a long time period?
		Significant (**)	Can the attack be shortly implemented within a takt time?
		Critical (***)	Can the attack be instantly implemented without any delay?

There are two key factors in Consequence domain: the damage scope and detection time. The scope of the damage is highly dependent on the systems and services. Therefore, entities' functionality and performances were focused on for the questionnaire. The takt time is used again for the detection time to objectively assess the key factor. The questionnaires for Consequence domain in Table 13.

Table 13 Consequence Questionnaire

Key Factor	Indicator	Degree	Questionnaire
Damage Scope	C1	Moderate (*)	Is the attack damage not affecting other entities' functionality or performances at all?
		Significant (**)	Can the attack affect other entities' functionality or performances?
		Critical (***)	Is the attack damage transferable to other entities that are not targeted in the attack scenario?
Detection Time	C2	Moderate (*)	Will the attack consequences be detected instantly after damaging the system?
		Significant (**)	Will the attack consequences be detected within a takt time?
		Critical (***)	Is the attack detection time unpredictable and taking a long time period?

Finally, Recovery domain is evaluated by two key factors, the restoration and prevention. The degree of the restoration is decided based on whether the system is operational after the restoration process. For the prevention, limiting insiders' authority or manufacturing process was mainly focused. These solutions can absolutely prevent the insider attacks but it also decreases the manufacturing productivity, capacity, and efficiency. Therefore, the attack can pose moderate threats to the system if the attack can be prevented by merely changing existing security policy or system configuration.

Table 14 Recovery Questionnaire.

Key Factor	Indicator	Degree	Questionnaire
Restoration	R1	Moderate (*)	Can the system be restored and operated after detecting the attack?
		Significant (**)	Can the system be restored and operated within a takt time after detecting the attack?
		Critical (***)	Is the system permanently damaged, and it cannot be restored and operated within a takt time?
Prevention	R2	Moderate (*)	Can the attack be prevented by changing the existing security policy or system configuration?
		Significant (**)	Can the attack be prevented without limiting insiders' authority or manufacturing process?
		Critical (***)	Can the attack only be prevented by limiting insiders' authority or manufacturing process?

7.2.3 Case Study 1: Manipulating Inspection Process

An inspection process is one of the important manufacturing processes to maintain the quality of the production and detect malicious behavior of the system. To follow a vision of the future manufacturing systems, the inspection process can be also integrated into the autonomous manufacturing process. As a result, insiders can easily access to the process and control the parameters with their legitimate access authentication. Thus, it cannot be free from the attack by insiders, and its risk is enlarged due to the connectivity and availability of the system.

Case study 1 describes how insiders can manipulate the inspection process in CPMS environments. The attack target for the case study is LIAS. Insider will manually modify the parameter of the neural network to manipulate the results of the layer image inspection. One of the weights trained by the manager of LIAS was changed to demonstrate the attack, and its results are

presented and explained. The attack was analyzed by using IASAF, and it is compared with the system with the blockchain layer to explain how blockchain technology can prevent this attack from insiders.

7.2.3.1 Attack Description

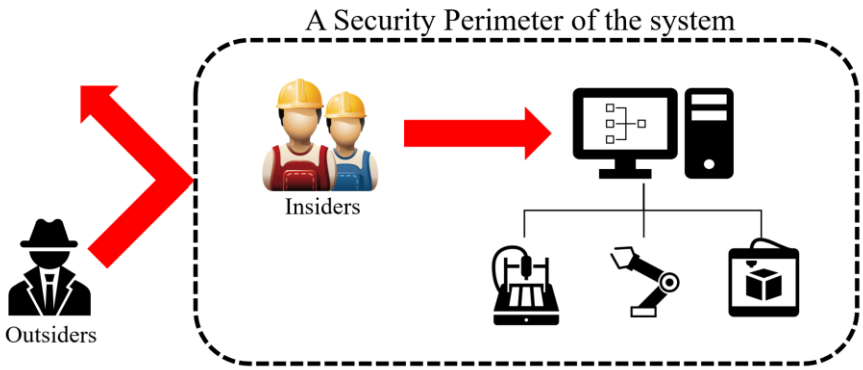


Figure 39 Direct Modification

The major difference between insiders and outsiders is that only insiders can access a system. The attack method "Direct Modification" can only be implemented by insiders, especially, who have legitimate access authentication to the system. Therefore, this attack method does not require any special techniques or skills to compromise system entities. Furthermore, Direct Modification is not limited to intentional insider threats. According to IBM's annual security report, the number of security incidents in the operational technology industry has been dramatically increased, and the major reason for this significant rise was misconfigurations by insiders. The number of incidents from the misconfiguration made up 86 percent of the records reported in 2019 (IBM, 2020b).

LIAS utilizes a Multilayer Perceptron Neural Network (MLP) to train the pattern of the normal and defective layer images. The back-propagation algorithm enables MLP to find optimized weight (w) and bias (b), which are used to calculate the similarity of the images.

Therefore, compromising just one of the weights and biases can cause spurious results. Besides, the results can be fabricated by compromising a certain weight or bias to deceive the manager (Seibold et al., 2020). By changing certain area's weights or biases, all the true positive (TP) can be classified as negative, thus it will result in a false negative (FN). Similarly, all the true negative (TN) can be classified as positive, which results in a false positive (FP). Moreover, by changing random weights and biases, the result can be stochastically compromised. Four attack forms—False-Positive Attack, False-Negative Attack, False-Inverse Attack, and False-Random attack—are defined and tested with a total of 107 samples, the results can be found in Table 15.

Table 15 Manipulated Inspection Result

	TP	**TN**	**FP**	**FN**
Original	72	35	0	0
False-Positive Attack	72	0	35*	0
False-Negative Attack	0	35	0	72*
False-Inverse Attack	0	0	35*	72*
False-Random Attack	34	17	18*	28*

*compromised result

Seen from above table, insiders can manipulate inspection results in a variety of forms. Especially, False-Random Attack is a critical attack form because it can be activated after a long-term period without being discovered, but eventually causing a considerable amount of extra manufacturing expenses.

7.2.3.2 Attack Simulation

To simulate the attack, a total of 140 samples (Normal: 70, Defective-Center: 70) was chosen from the validation experiments of LIAS in chapter 5. The target digital entity in this

simulation is the uploaded weights and biases, which are trained by 12,000 simulated images. Originally, LIAS stores such machine learning parameters in the blockchain layer, but the testbed used in this attack simulation stores the digital entity in the local database. Therefore, it is assumed that insiders can easily access the parameter and compromise it. To test the samples with the compromised parameters, just one value from the trained weights was manually changed to a random value and tested. The result is shown in Table 16.

Table 16 Attack Result

Condition	Classification Results		Accuracy	FPR	FNR
Defective; Center with legitimate weight and bias	TP	70	0.992857	0.014286	0.0
	TN	69			
	FP	1			
	FN	0			
Defective; Center with compromised weight and bias	TP	46	0.607143	0.409091	0.378378
	TN	39			
	FP	27			
	FN	28			

Seen from the result, only one weight out of 125,530 weights was compromised but the classification result was largely affected. The accuracy was dropped from 99% to 61%, and FPR was increased by 41% as well as FNR.

7.2.3.3 IASAF Analysis

Based on the attack description and attack simulation of the case study, IASAF analysis was conducted by answering the questionnaires for IASAF. The analysis results are provided by a

table with each factor's risk degree and a radar chart with the summation of the number of the star (*) within the same domain. The results are presented in Table 17.

Table 17 IASAF Result for Case Study 1

Domain	Key Factor	Indicator	Risk Degree
Actor	Motivations	A1	**
	Numbers	A2	**
Preparation	Access	P1	***
	Targets	P2	***
Implementation	Surreptitiousness	I1	*
	Duration	I2	**
Consequence	Damage Scope	C1	*
	Detection Time	C2	***
Recovery	Restoration	R1	**
	Prevention	R2	***

Moderate (*), Significant (**), Critical (***)

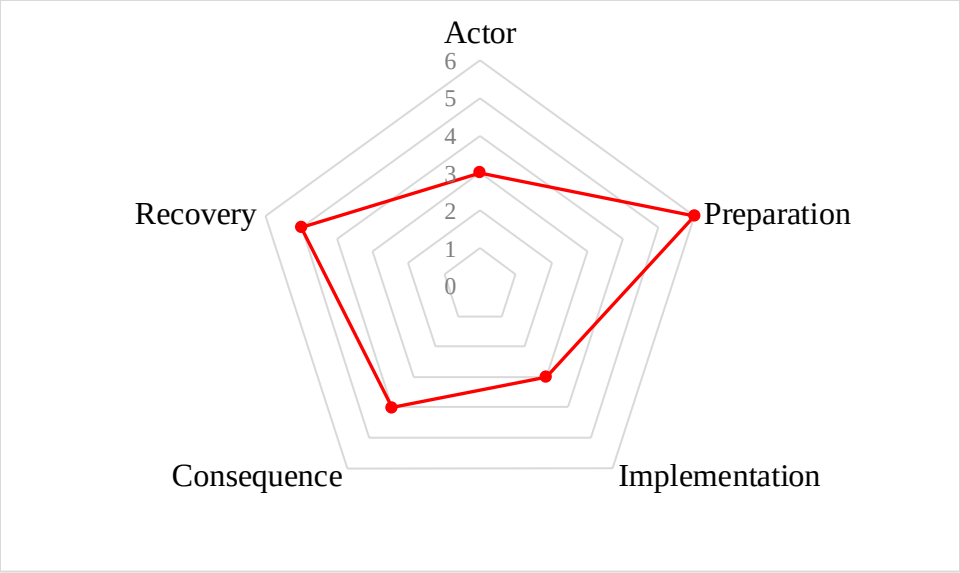


Figure 40 Radar Chart Analysis for Case Study 1

Since it is assumed that the insider has the access authority to the specific digital entity, trained weights and biases, the number of potential insiders is limited. Also, the motivation of the attack was quite clear, the posed threat risks from Actor domain were comparably low. Meanwhile, Preparation domain shows the highest threat risks, because the attack scenario has only one target, the machine learning parameter, and the insider's access and manipulation were legitimate. For this reason, this attack scenario has moderate surreptitiousness. However, since the inspection results can be controlled randomly by the False-Random Attack, which makes the attack is hardly detected for a long time period. For Consequence domain, the damage scope was only limited to the single digital entity, and the detection time can be unpredictable. Finally, since there is no way to protect the parameter data from insiders who have access authority, the threat risks from the prevention are critical.

7.2.3.4 Summary

Case study 1 explains how insiders can manipulate inspection results by compromising the digital entity of the system. According to the IASAF analysis, this attack scenario poses less threat risks from Actor and Implementation domains, but Preparation domain. This means that the attack scenario highly depends on the insider's ability and authority to implement the attack successfully.

The LIAS, the system including the blockchain layer, can easily counter this attack. Even though insiders have the access authority to the machine learning parameters, they only can access and use it with the transaction hash through the service layer, which is protected by the blockchain communication protocol. If the machine learning parameters are needed to be changed, the change must be announced to the entire system components. Besides, the digital footprint will remain in the blockchain layer, which is immutable and impossible to manipulate without any validation process.

7.2.4 Case Study 2: Social Engineering Attack

Social engineering attack can be considered as involuntary insider attack because it makes insiders reveal accessible routes into the system to outsiders without their intention. By accessing malicious websites or spam mail, naïve insiders can accidentally install malware, which can incapacitate network security mechanisms, such as a firewall, for outside attackers (Salahdine & Kaabouch, 2019).

For Case study 2, it is assumed that one of the insiders' devices in LIAS is already compromised due to the social engineering attack. Thus, outside attackers are able to conduct Denial of Service (DOS) attacks on the system. DOS attack is the most common network attack vector in the world (Zhang et al., 2016). DOS attack disturbs information exchanges by making

network resources consume a sheer volume of invalid data. This case study shows how DOS attack can disturb LIAS's inspection process. Also, the response time in retrieving the machine learning parameter data is presented and explained to demonstrate the attack.

7.2.4.1 Attack Description

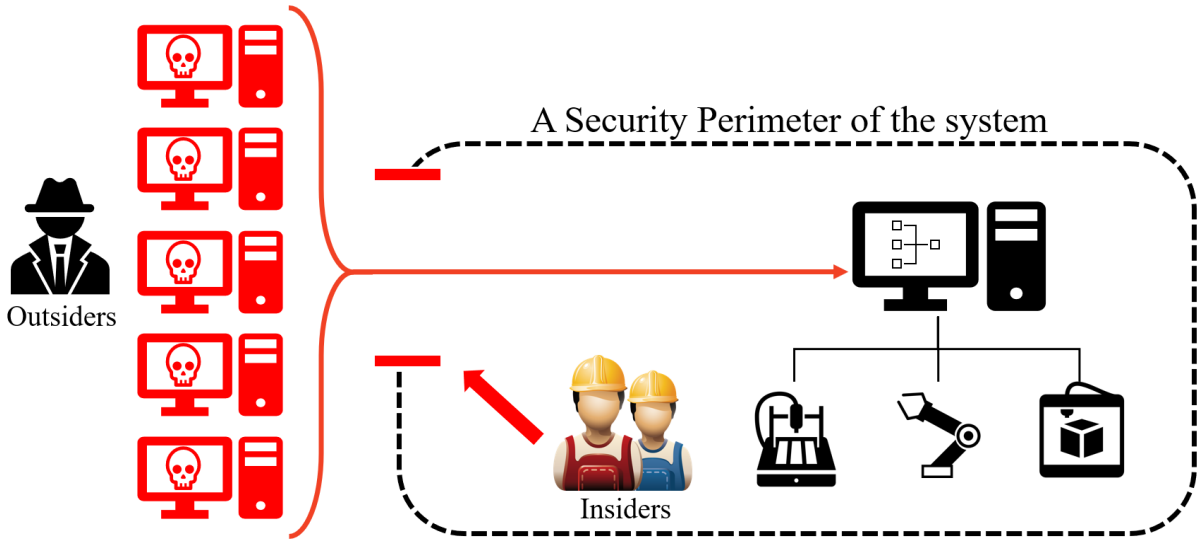


Figure 41 Denial of Service Attack

Denial of Service Attack (DOS) attack exploits a limitation in the capacity of processing data for the target system. By creating and sending a large amount of invalid data, the target system’s data processing can be interrupted. For this attack, the attacker must have the target's IP address and need access to the target's LAN. However, since DOS attack does not require any pre-manipulation to launch the attack, social engineering attacks have been used to initiate the attacks. If a naïve insider unintentionally installs malicious malware via clicking spam mail or uncertified webpages, the route to the target system can be opened via the insider's machine that is used to implement DOS attack.

7.2.4.2 Attack Simulation

To simulate DOS attack on the LIAS, Kali Linux's hping3 tool was used. For the attack parameters, five packets per second with one-hundred bytes invalid data, which is very light attack intensity, was used to attack, because the tool was too strong enough to crush the program. For the experiment purpose, LIAS continuously retrieves the trained weight and bias data with 100 iterations. The attack was inflicted on the LIAS after the 50th iteration to compare with the ideal state. Finally, the response time of retrieving data from the local storage to LIAS was measured for the experiment result. The result can be found in Figure 42.

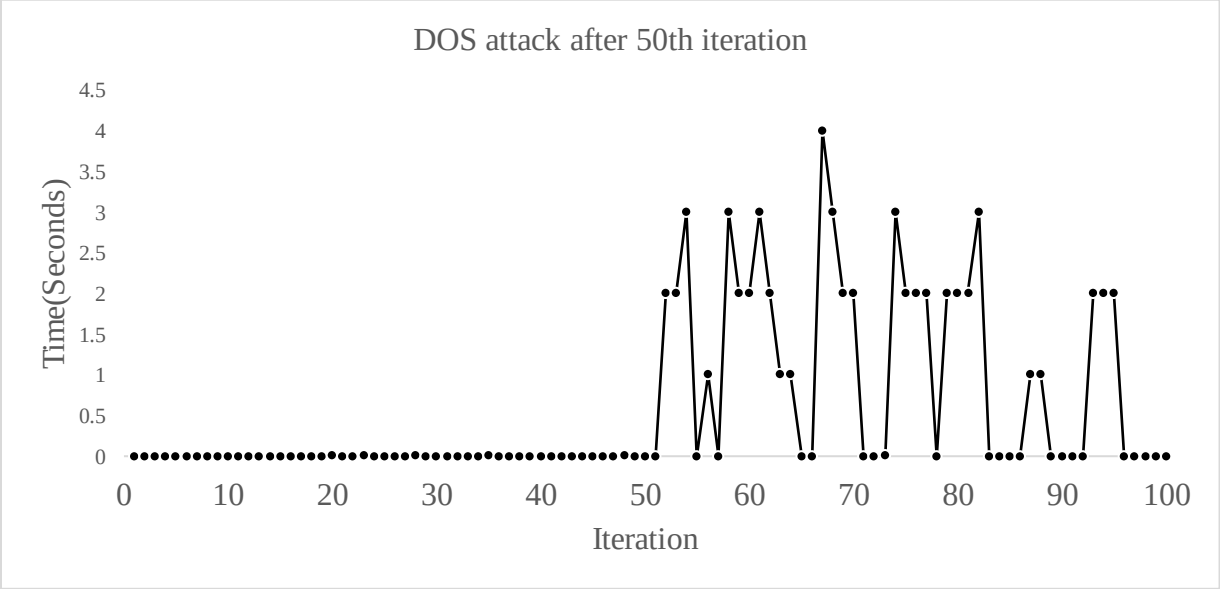


Figure 42 DOS Attack Result

Seen from above, the response time shows irregularities after the 50th iteration. A total 28 iterations out of 50 were affected by the simulated DOS attack. However, it is likely that the communication will be totally halted if the real UDP DoS attack was implemented. From the

empirical experiments, DOS attack with more than fifty packets per second was enough to crush the communication.

7.2.4.3 IASAF Analysis

The IASAF analysis was conducted in the same way as case study 1, and the results are presented in Table 18.

Table 18 IASAF Result for Case Study 2

Domain	Key Factor	Indicator	Risk Degree
Actor	Motivations	A1	***
	Numbers	A2	***
Preparation	Access	P1	**
	Targets	P2	*
Implementation	Surreptitiousness	I1	*
	Duration	I2	*
Consequence	Damage Scope	C1	***
	Detection Time	C2	*
Recovery	Restoration	R1	**
	Prevention	R2	***

Moderate (*), Significant (**), Critical (***)

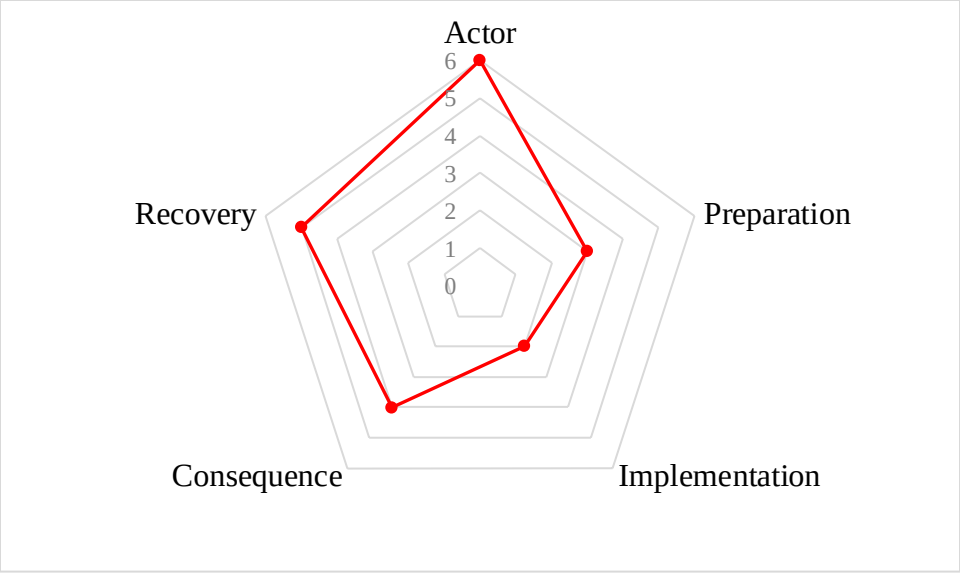


Figure 43 Radar Chart Analysis for Case Study 2

Since the attack for case study 2 is based on the social engineering attack, the motivation from the insiders in the system is unpredictable and unknown. Furthermore, the attack could target the uncertain number of the insiders, the treat risks from Actor domain is very critical. However, since launching DOS attack requires many resources and power with multiple targets to disturb the system operation, Preparation domain shows low threat risks. Also, DOS attack will remain a myriad of digital footprints because it is based on the network activity. Besides, the attack could take a long time period from gathering enough information about the attack target. Since DOS attack is basically interrupting communications among devices, its damage scope would be comparably enlarged. But the attack will be discovered shortly because the abnormal behavior of the entities in the system can be observed immediately.

7.2.4.4 Summary

Case study 2 illustrates DOS attack scenario on the system when the insiders are under social engineering attack and reveal the system vulnerabilities against outside attackers. Since an uncertain number of insiders without specific motivations can be involved in this attack, Actor

domain poses significant threat risks to the system. But the risks from Preparation and Implementation domains are negligible because DOS attack created digital footprints from the sheer volume of the network activity and takes a long time to actually launch the attack.

For the LIAS with the blockchain layer, the communication will not be disturbed at all because the blockchain network is formed in a decentralized structure. Thus, to affect the blockchain communication, all the nodes should be attacked at the same time, which is called Distributed Denial of Service (DDOS) attack (Mahjabin et al., 2017). Since DDOS attack requires tremendous volume of network resources from outside of the system, the attack could be fruitless (Mirkin et al., 2020).

7.2.5 Case Study 3: Injecting Malicious Item

Additive Manufacturing (AM) fabricates three-dimensional objects by continuously adding material layer by layer from a computer-aided design (CAD) model. In recent years, an unprecedented level of autonomy in AM has been enabled by CPMS. AM's machines can have constant interactions with each other through the internet or other computer networks.

However, insider threat risks in AM are growing due to the sheer volume and pervasiveness of data and increased accessibility in the networks. Particularly, since the infill structure of the 3D model is usually generated during the conversion process of a CAD file to G-code by the third-party program, the malicious item can be easily injected by insiders. Also, it is hard to detect the attack on infill structure because interior defects can occur without affecting the exterior (Wu et al., 2017).

Case study 3 illustrates how insiders can inject malicious item, which can bypass or incapacitate the existing security mechanism. The testbed based on SPLC was used for this case study. The insider will manually change the G-code file, which has the lower infill density, but the same exterior, to deceive the existing security mechanism of the testbed. The Minimum Mean Absolute Percentage Error (MMAPE) was developed and used to simulate the existing security mechanism. MMAPE will be utilized to demonstrate the attack. The attack scenario was analyzed by using IASAF, and it is compared with the system with the blockchain layer to explain how blockchain technology can prevent this attack from insiders.

7.2.5.1 Attack Description

This attack scenario includes specific motivation for the attack. A 3D printer worker for the supplier wants to decrease manufacturing cost and 3D printing process time by decreasing the infill density of the products. The percentage of infill density of the product decides the amount of filament printed inside the products, which affects the strength and duration of the product. Thus, it can yield serious quality issues if the infill density is lowered. However, infill defectives do not affect the exterior of the product, so it is hard to be detected after printing. Thus, layer-by-layer inspection is required to monitor the infill defectives.

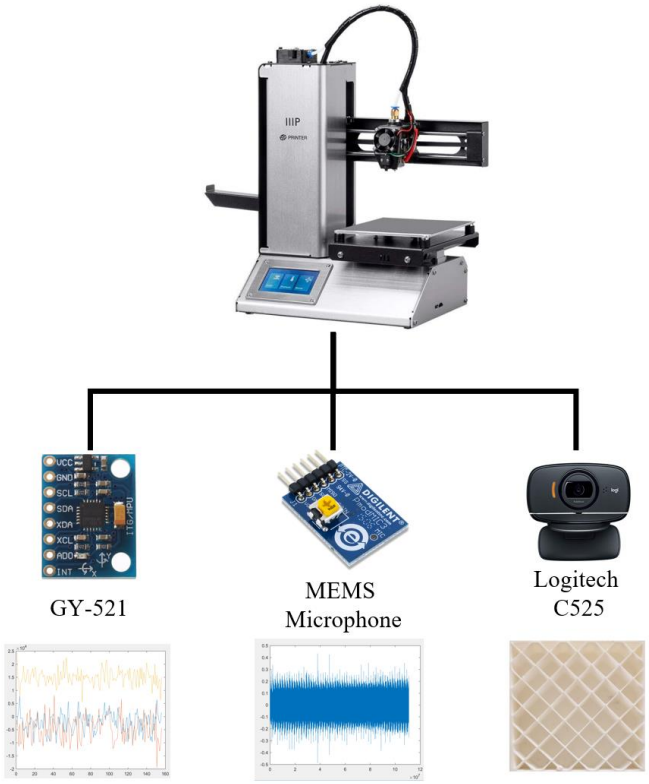


Figure 44 Physical Auditing

Currently, a physical auditing was adopted to the testbed. The physical auditing is collecting physical data, which are obtained from the physical machine by using multiple sensors, to verify machine operation. Seen from Figure 44, the physical auditing consists of three physical data inspections: acceleration, acoustic, and image.

Accelerometer data, acoustic data, and image data can be collected for the physical auditing by using the GY-521 sensor, MEMS microphone, and Logitech C525, respectively. To verify the machine operation in a timely manner, the physical auditing system requires a simplistic classification algorithm to avoid redundant delays. In this case, average pooling (AP) and mean absolute percentage error (MAPE) can be used to reduce the data dimensions while the data originality remains for the classification (Yu et al., 2017). However, this classification model is an under-fitted model to validate the AIM, which yields subtle errors that might be ignored. Also,

each collected data set likely starts at a different point (beginning of the machine operation) due to the low-quality sensors. Thus, MMAPE classification was developed to increase the classification sensitivity. MMAPE is provided in Figure 45.

Given:$(a_1, b_1), \dots, (a_m, b_m)\ where\ a_m, b_m \in \mathbb{R}$

Offset k:

$k = \{-p+1, -p+2, \dots, p-2, p-1\},\ where\ p = pooling\ dimension$

Average Pooling $AP(x_l, y_l)$:

$For\ \ l = \frac{m}{p}\ and\ \ i = \{1, 1+p, 1+2p, \dots, 1+(l-1)p\},$

$x_l = \frac{1}{P}\sum_{i=1-k}^{i+P-k} a_i,\ \ y_l = \frac{1}{P}\sum_{i=1-k}^{i+P-k} b_i,$

Minimum Mean Absolute Percentage Error $mmape$:

$mmape(z_k) = Minimum\left\{\frac{100\%}{l}\sum_{j=1}^{l}\left|\frac{x_j - y_j}{x_j}\right|\right\}$

Prediction:

$Prediction = \begin{cases} 0, & if\ mmape(z_k) < threshold \\ 1, & otherwise \end{cases}$

Figure 45 MMAPE

Mean Absolute Percentage Error (MAPE) is generally used for the prediction model, comparing two data sets by calculating absolute distance values. However, due to the low-accurate sensor, each collected data set likely starts at a different point. Thus, MAPE applies an offset value

k to the Average Pooling $AP(x_l, y_l)$ to find the certain value that makes minimized mean absolute percentage error. In this way, the asymmetry between the data points can be solved.

7.2.5.2 Attack Simulation

In this attack scenario, there are three groups of samples. The first group is "Original," which is the intended manufacturing production with the legitimate manufacturing specification. The second group is "Defective." This group is well known defective type, and the physical auditing system was designed to detect such defectives. Finally, the last group is Malicious Item by Insider (MII). This group is fabricated by insiders, who want to decrease manufacturing cost and 3D printing process time for their own benefit.

To design the samples of three groups, a 3D model of $1.5 \times 1.5 \times 1.5$ inches cube was generated as a G-code file. For the defective group, a cylinder shape defective (0.5 inches diameters with 1.5 inches height) was injected. In the case of MII group, the original group's design was used, but the infill density was modified by the 3D printer software (CURA 4.2.1). A total of 108 layers were generated from each design, and some images of the 54th layer for each group are shown below.

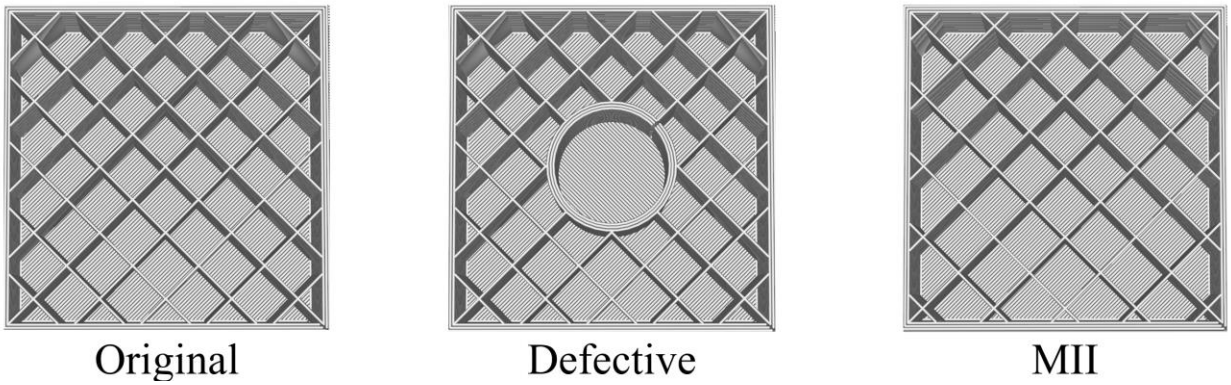


Figure 46 Experiment Designs

The amount of filament is reduced by the percentage of the infill density. According to the CURA, 13% infill density requires 6.77m of filament while 6.44m of filament for 12% infill density. The printing time is also reduced from 59 minutes to 41 minutes. GY-521, MEMS microphone, and Logitech C521 were attached to the Monoprice MP Select Mini 3D printer V1 to collect the data. The classification result is prepared in Table 19.

Table 19 Classification Result

Physical Data	Sample	Average of $mape$	Prediction
Accelerometer (Threshold: 0.30)	Original	0.1085	True
	Defective	0.3665	False
	MII	0.2243	True
Acoustic (Threshold: 0.40)	Original	0.2571	True
	Defective	0.4879	False
	MII	0.3861	True
Image (Threshold: 0.02)	Original	0	True
	Defective	0.0386	False
	MII	0.0167	True

Seen from above, the MII was able to bypass the physical auditing system. The important difference from image manipulation is that insiders do not have to modify the digital assets, but the physical assets need to compromise the manufacturing process without being discovered.

7.2.5.3 IASAF Analysis

Table 20 IASAF Result for Case Study 3

Domain	Key Factor	Indicator	Risk Degree
Actor	Motivations	A1	**
	Numbers	A2	**
Preparation	Access	P1	***
	Targets	P2	***
Implementation	Surreptitiousness	I1	***
	Duration	I2	***
Consequence	Damage Scope	C1	*
	Detection Time	C2	***
Recovery	Restoration	R1	*
	Prevention	R2	***

Moderate (*), Significant (**), Critical (***)

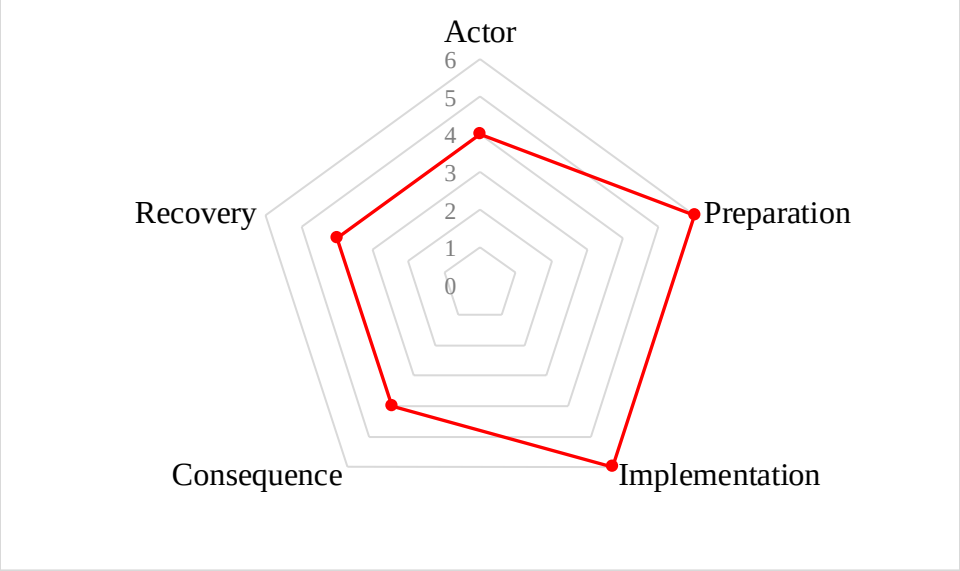


Figure 47 Radar Chart Analysis for Case Study 3

In accordance with case study 1, it is assumed that the insider can legitimately access the specific digital entity, in this case, a G-code file. For the same reason, potential insiders for this attack are limited due to the access authority. Therefore, the posed threat risks from the Actor domain are low. However, Preparation and Implementation domain shows the high degree of the posed threat risks. The insider already has the security clearance to the necessary entities, and there is only a single target for the attack: the infill density. Moreover, since injecting malicious items can be seen as a legitimate activity for the insider, it is difficult to detect the attack. Also, the attack damage occurs immediately after injecting the item.

7.2.5.4 Summary

Case study 3 illustrates how insiders can inject malicious items, which can bypass the physical auditing process of the system. Due to the requirements and nature of the attack scenario, there are critical threat risks posed from Preparation and Implementation domains.

The SPLC with the blockchain layer can be an effective countermeasure against attacks. The G-code file can be uploaded on the blockchain layer by the manager, and insiders can only access the G-code file via the service layer. Also, the 3D printing machine can only be operated by inputting the transaction hash of the G-code file. In this way, the G-code file can be free from malicious manipulation, and the malicious item injection also can be prevented.

7.2.6 Case Study 4: Sniffing and Spoofing

Insiders who are knowledgeable of the IT network structure of the system can use sniffing and spoofing codes to breach or manipulate manufacturing information. Since insiders are in the same network environment, it is easy to use the internet network vulnerabilities to succeed in the attack such as Domain Name System (DNS) server attacks.

Case study 4 demonstrates how insiders can manipulate the communications among manufacturing entities by exploiting Man in the Middle (MITM) attack. MITM attack exploits the victim's communication channel. By redirecting data flow to the attacker, it can be easily manipulated and sent to the victim. Usually, a redirecting step requires sensitive information such as a main server's IP address as well as physical access to connect to the target's Local Area Network (LAN). For these reasons, insiders can play an important role to successfully implement MITM attack because they have legitimate access authentications for these. Thus, they can simply compromise DNS server, which will redirect the communication channel.

7.2.6.1 Attack Description

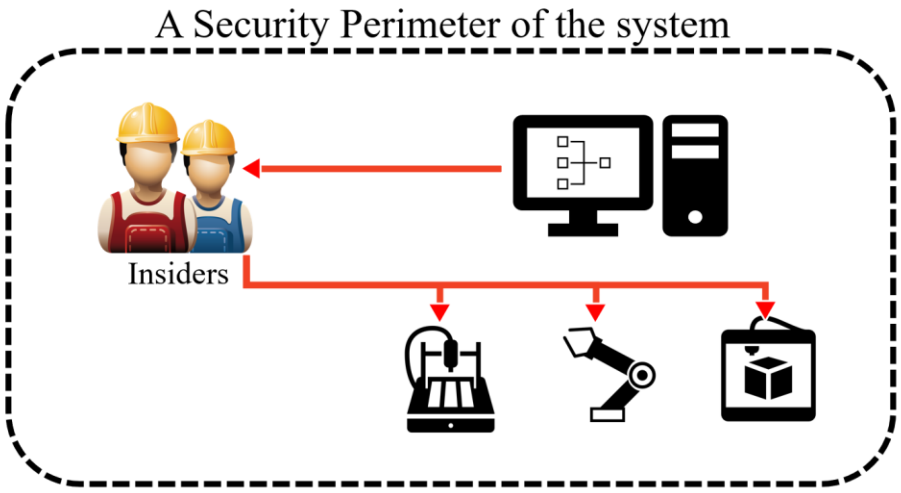


Figure 48 Man In the Middle Attack

The main idea of MITM attack is redirecting the victim's communication channel to attackers and manipulating or injecting malicious communication. Generally, a redirecting step needs a lot of efforts and conditions. For example, the Kaminsky Attack, which is one of the remote DNS cache poisoning attacks, is required to guess 16-bit transaction number to succeed in the

attack (Hmood et al., 2015). The chance is one out of 2^{32}. However, in regard to insiders, a simple modification of DNS server with their access authentication enables to redirect the communication channel. Furthermore, this attack can be a stealthy and critical attack method because insiders can control the frequency of malicious output results.

7.2.6.2 Attack Simulation

To simulate the attack to the testbed, one virtual machine (attacker) in the same LAN was used to run MITM algorithm using SCAPY package of Python. By using SCAPY function send() and sniff(), the communication between PLC device and the service application can be easily altered. For example, an insider operates the machine with input value 0, but it is changed to 1 before it arrives at the service application. Therefore, eventually, the machine will be operated with the input value 1, which is the compromised value by MITM attack.

For the test, the main control server sent out input data with Input value 0, which is expected to activate the output value 0. Meanwhile, the attacker's virtual machine will send out input value 1 to the PLC device whenever it detects a legitimate packet from the main control server. The test was conducted for 100 seconds, which represents 100 iterations, and the attack was implemented after the 50th iteration. The result is in below.

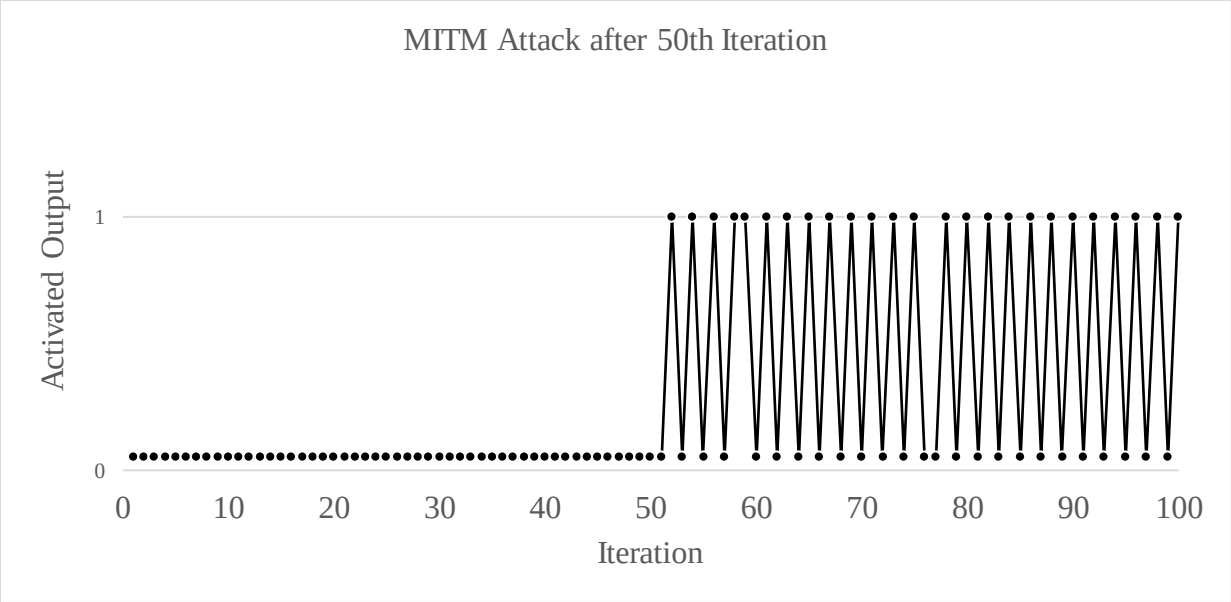


Figure 49 MITM Attack Result

In the testbed, the attack won the race condition at a rate of 50%, which can easily be modified by changing the number of sending input data.

7.2.6.3 IASAF Analysis

Table 21 IASAF Result for Case Study 4

Domain	Key Factor	Indicator	Risk Degree
Actor	Motivations	A1	*
	Numbers	A2	**
Preparation	Access	P1	***
	Targets	P2	**
Implementation	Surreptitiousness	I1	**
	Duration	I2	***
Consequence	Damage Scope	C1	*
	Detection Time	C2	***
Recovery	Restoration	R1	**
	Prevention	R2	**

Moderate (*), Significant (**), Critical (***)

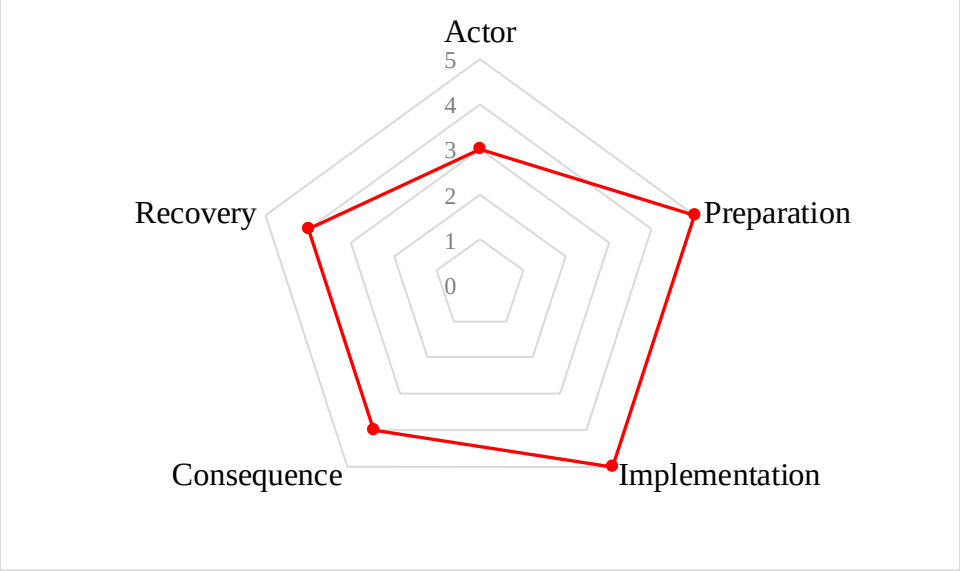


Figure 50 Radar Chart Analysis for Case Study 4

MITM attack necessitates IT knowledge and skills and physical access to the local LAN. Therefore, only a small group of insiders could be an actor for this attack scenario. This is the reason why Actor domain poses low threat risks. However, for the same reason of case study 3, Preparation and Implementation domains pose high threat risks. Since the main objectives of MITM attack are to breach the manufacturing information and to manipulate manufacturing operation, it does not directly harm the physical entities. But the attack detection timeline is unpredictable, the detection time from Consequence domain poses high threat risks.

7.2.6.4 Summary

Case study 4 demonstrates how insiders can launch MITM attack on the PLC network environments. Due to the difficulty of the attack, the posed threat risks from Actor domain are low, but Preparation and Implementation domains show high threat risks.

In the case of the SPLC with the blockchain layer, MITM attack would not work because it uses a different network communication protocol. Since the blockchain delivers the transaction data through a peer-to-peer network, it is arduous to sneak into the network. Therefore, blockchain technology provides an effective security enhancement against MITM attack. Although the transaction hash itself can be exploited to launch the attack, such as Replay Attack, the data in the transaction cannot be modified due to its decentralized data management system. Moreover, the private blockchain system can limit and manage the network nodes, so it can help to trace and identify insiders effectively.

Chapter 8. Conclusion and Future works

This dissertation proposes an insider threat tolerant Cyber-Physical Manufacturing System, and it is validated by a four-step process: Establish, Build, Identify, and Simulation (EBIS). In this chapter, the summary and conclusion of the dissertation are presented, and its contributions and impact on the field are described. Finally, the limitation of this research and future works are presented.

8.1 Summary

This dissertation seeks to address insider threat issues in manufacturing systems by developing an insider threat tolerant Cyber-Physical Manufacturing System enhanced by a Service-Oriented Blockchain (SOB) augmentation. Insiders are anyone who has been or is being affiliated with a system. Since insiders have knowledge and access authentications of the system's properties, they can perform more serious attacks than outsiders. To reduce threat risks from insiders, SOB makes physical and digital entities reusable and interoperable via a service application, which enables the blockchain communication protocol over the entities. In this way, services for the manufacturing process can be available with less arbitrary delays while remaining its strong security from the blockchain.

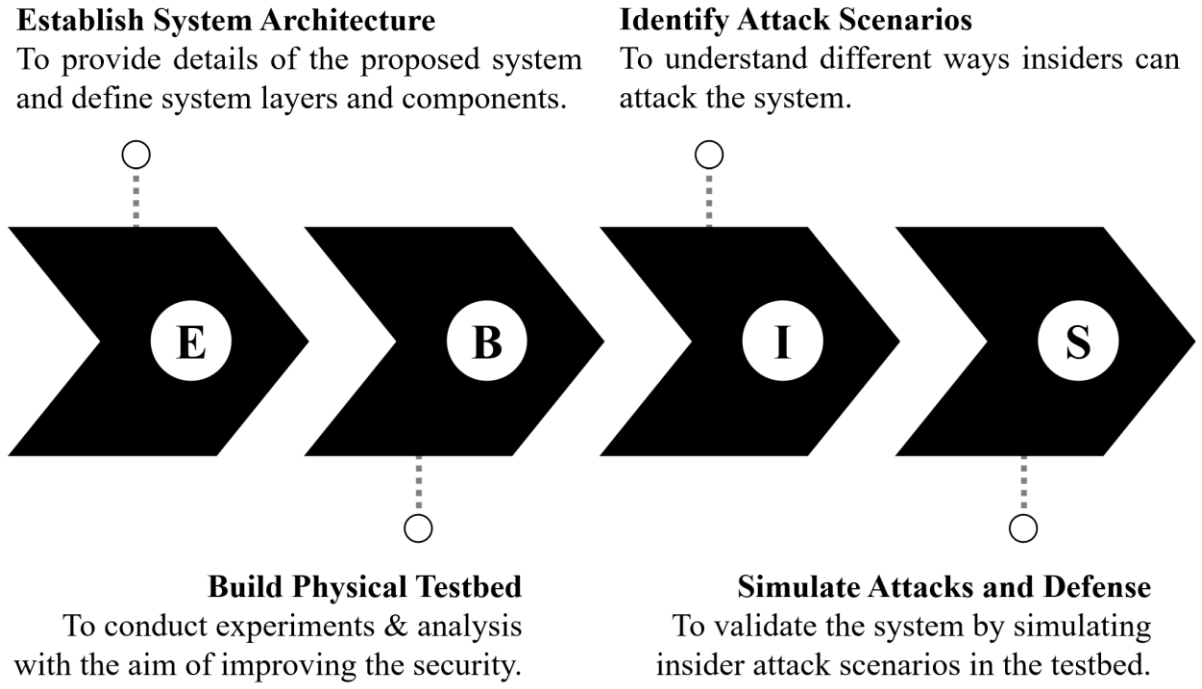


Figure 51 EBIS Validation Process

To validate the insider threat tolerant Cyber-Physical Manufacturing System with SOB augmentation, EBIS validation process was employed to strike a balance between well-principled

formal security guarantees and empirical security enhancement from practical approaches. The EBIS validation process consists of a series of steps in developing and performing security analysis processes to improve and validate the system's security. The four steps of the EBIS are as follows: **Establish** system architecture, **Build** a physical testbed, **Identify** attack scenarios, and **Simulate** attacks and defense.

To establish system architecture, first, a survey was conducted on blockchain applications in manufacturing systems. Various approaches using blockchain technology were investigated to identify technical challenges in blockchain implementation into the manufacturing systems. Accordingly, differences between the centralized system structure and decentralized system structure are discussed as well as the differences between the decentralized system architecture and distributed system architecture. Finally, an insider threat tolerant Cyber-Physical Manufacturing System augmented by a service-oriented blockchain was proposed to overcome security vulnerabilities against insiders and technical limitations of blockchain technology. The system consists of four layers: user layer, entity layer, service layer, and blockchain layer, and each layer's details were explained with the example.

To build the physical testbed, two simulation models were designed and developed from the established system architecture: Layer Image Auditing System (LIAS) and Secure Programmable Logic Controller (SPLC). The testbeds for each model were built and validated with the experiments with the physical data. These models are explained in detail, and the discussion for each model is provided to describe how the blockchain can help to mitigate insider threat risks in the system.

To identify insider attack scenarios, insider threats in CPMS are examined in depth. In order to better understand different ways in which a system can be attacked by insiders, Insider

Attack Tree (IAT) was developed and presented. The IAT consists of four parts: Root, Branch, Sub-Branch, and Leaf. The Root is the eventual attack target for insiders, and the Branches represent three different assets in CPMS. Sub-branches indicate the attack targets of assets while the Leaf represents attack vectors.

To simulate attacks and defenses, four attack scenarios were chosen from the Insider Attack Tree: Manipulating Inspection Process, Sniffing and Spoofing, Injecting Malicious Item, and Social Engineering. Each attack scenario is explained and developed as a case study. Therefore, a total of four case studies were presented. To demonstrate the effectiveness of the blockchain, two simulation models (LIAS and SPLC) without the blockchain layer were built and used for the case studies. Furthermore, each case study was analyzed by using an Insider Attack Scenario Assessment Framework (IASAF), which is proposed to evaluate the attack scenarios within five domains: Actor, Preparation, Implementation, Consequence, and Recovery. The proposed framework was used to evaluate four attack scenarios.

In conclusion, insiders can pose critical threats to CPMS due to their trusted access authentication and knowledge of the systems. According to the case studies and analysis from IASAF, blockchain technology provides a security enhancement against insiders. Also, SOB augmentation to the system reduces redundant and arbitrary delays in the system's communications while maintaining the flexibility and connectivity among digital and physical entities of the system. By storing data in a decentralized way with the validation process, the blockchain can provide decision-makers with higher trust in their manufacturing processes. It also enables the vision of CPMS without entirely modernizing legacy systems.

8.2 Contribution

This dissertation advances the understanding of insider threats and blockchain implementations in CPMS by presenting key issues remaining in the literature. In support of this statement, this dissertation describes the following contributions:

Insider threats in the manufacturing industry have been identified and analyzed. To disclose insider threat risks in manufacturing systems, the dissertation investigated the influence of insiders, their potential threats, and vulnerabilities in CPMS. As a result, Insider Attack Tree (IAT) was designed and utilized to identify potential insider threat scenarios in the proposed system. IAT can be widely used to identify attack scenarios in an intuitive manner, appropriately conveying security information to even layperson (Song & Moon, 2020a).

Blockchain applications for manufacturing systems in the literature have been investigated and analyzed. To discuss how manufacturing systems can effectively adopt blockchain technology, a survey was conducted. To investigate a recent and relevant analysis of the research trend, this survey consists of 148 articles of major relevance were selected from 380 publications, presented between 2018 and 2021. Also, to help to understand the trend history of research for blockchain technology in manufacturing systems, the dissertation presents a Technology Roadmap, which is visualized the chronological history of the technology to support a flexible and long-range plan.

Technical challenges in the blockchain implementation have been resolved by developing the Service-Oriented Blockchain (SOB). To solve the technical challenges identified from the survey, this dissertation introduced a Service-Oriented Architecture (SOA), which could be a potential solution for the challenges. SOA can recomposite and reconstruct discrete components of a system to reuse them for other services. SOB was inspired by these ideas and

concepts. SOB enables smart and collaborative services with less arbitrary delays while remaining its strong security from the blockchain. By retaining manufacturing data in the blockchain and continuously validating the digital entities with the blockchain communication protocol, the data integrity of digital entities will be assured.

An assessment framework from the viewpoint of the insider attack scenario has been developed and presented. To investigate the system's security vulnerabilities and evaluate the insider attack scenarios in a practical manner, this dissertation proposed Insider Attack Scenario Assessment Framework (IASAF). Details of IASAF were explained, and it is demonstrated via four case studies analysis. The example of questionnaires was also presented.

8.3 Limitation and Future works

In spite of the promising security improvement provided, there are still unaddressed limitations and further possible improvements for future work.

The disadvantages of employing the blockchain should be thoroughly examined before it can be fully utilized. It is essential to overcome the lack of privacy, standardization, scalability, and inefficiency to integrate existing security architectures with blockchain's security mechanisms. So far, many blockchain platforms have been developed and proposed with various consensus algorithms and programming languages to resolve such issues, but their potentials as manufacturing infrastructures have not been properly reviewed. Thus, it is necessary to develop the evaluation methodology to understand the effectiveness of the blockchain on reliability and performance in manufacturing systems. This work can contribute to identifying possible solutions for challenges in employing blockchain technology and understanding the impact of various consensus algorithms and programming languages on the blockchain's performance.

As the manufacturing industry is moving toward CPMS, many manufacturing systems have adopted new technology from computer systems and internet networks to improve and optimize their manufacturing logistics. Despite the vital advantages of these adoptions, it is not ideal to fully incorporate the new technology due to the attack risk from many cyber-attacks that have been developed for decades. The majority of the cyber-attacks were already analyzed and prevented by developing countermeasures, but these attacks could be serious threats to a manufacturing system that includes a physical domain. Thus, it is important to understand existing cyber-attacks and their countermeasures to investigate whether these attacks can be exploited and damage the physical domain in manufacturing systems. SEED Labs is a NSF-funded project, which provides over 30 labs that cover a wide range of topics in computer and information security, including: software security, network security, web security, operating system security, and mobile app security (Du, 2019). Further attack scenarios—which are motivated by SEED Labs—specified in manufacturing systems can be developed for future works. The new attack scenarios can explain how cybersecurity can be extended to manufacturing system security, and this will allow engineers to soundly examine cross-domain system behavior.

References

Abeyratne, S., & Monfared, R. (2016). Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *International Journal of Research in Engineering and Technology*, *05*.

Acatech (Ed.). (2011). Cyber-Physical Systems: Driving force for innovations in mobility, health, energy and production. *Springer-Verlag*. https://doi.org/10.1007/978-3-642-29090-9

Afanasev, M. Y., Krylova, A. A., Shorokhov, S. A., Fedosov, Y. V., & Sidorenko, A. S. (2018). A Design of Cyber-physical Production System Prototype Based on an Ethereum Private Network. *2018 22nd Conference of Open Innovations Association (FRUCT)*, 3–11. https://doi.org/10.23919/FRUCT.2018.8468296

Ahmad, M. B., Saeed-Ur-Rehman, Akram, A., & Asif, M. (2014). Towards a Realistic Risk Assessment Methodology for Insider Threats of Information Misuse. *2014 12th International Conference on Frontiers of Information Technology*, 176–181. https://doi.org/10.1109/FIT.2014.41

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology Engineering Management Conference (TEMSCON)*, 137–141. https://doi.org/10.1109/TEMSCON.2017.7998367

AL-Salman, H. I., & Salih, M. H. (2019). A review Cyber of Industry 4.0 (Cyber-Physical Systems (CPS), the Internet of Things (IoT) and the Internet of Services (IoS)): Components, and Security Challenges. *Journal of Physics: Conference Series*, *1424*, 012029. https://doi.org/10.1088/1742-6596/1424/1/012029

Altmann, P., Abbasi, A. G., Schelen, O., Andersson, K., & Alizadeh, M. (2020). Creating a Traceable Product Story in Manufacturing Supply Chains Using IPFS. https://doi.org/10.1109/NCA51143.2020.9306719

Aoyama, T., Sato, A., Lisi, G., & Watanabe, K. (2020). On the Importance of Agility, Transparency, and Positive Reinforcement in Cyber Incident Crisis Communication. In S. Nadjm-Tehrani (Ed.), *Critical Information Infrastructures Security* (pp. 163–168). Springer International Publishing. https://doi.org/10.1007/978-3-030-37670-3_13

Appelhanz, S., Osburg, V.-S., Toporowski, W., & Schumann, M. (2016). Traceability system for capturing, processing and providing consumer-relevant information about wood products: System solution and its economic feasibility. *Journal of Cleaner Production*, *110*, 132–148. https://doi.org/10.1016/j.jclepro.2015.02.034

Assaqty, M. I. S., Gao, Y., Hu, X., Ning, Z., Leung, V. C. M., Wen, Q., & Chen, Y. (2020). Private-Blockchain-Based Industrial IoT for Material and Product Tracking in Smart Manufacturing. *IEEE Network*, *34*(5), 91–97. https://doi.org/10.1109/MNET.011.1900537

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Audinot, M., Pinchinat, S., & Kordy, B. (2018). Guided Design of Attack Trees: A System-Based Approach. *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, 61–75. https://doi.org/10.1109/CSF.2018.00012

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30. https://doi.org/10.1109/OBD.2016.11

Bai, L., Hu, M., Liu, M., & Wang, J. (2019). BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT. *IEEE Access*, *7*, 58381–58393. https://doi.org/10.1109/ACCESS.2019.2914223

Barenji, A. V., Li, Z., & Wang, W. M. (2018). Blockchain Cloud Manufacturing: Shop Floor and Machine Level. *Smart SysTech 2018; European Conference on Smart Objects, Systems and Technologies*, 1–6.

Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine Learning*, *81*(2), 121–148. https://doi.org/10.1007/s10994-010-5188-5

Baumung, W., & Fomin, V. (2018, July 1). Increasing the Utilization of Additive Manufacturing Resources through the Use of Blockchain Technology for a Production Network.

Bhattacharjee, A., Badsha, S., & Sengupta, S. (2020). Blockchain-based Secure and Reliable Manufacturing System. *2020 International Conferences on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, 228–233. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00052

Bhattacharyya, K., & Smith, N. (2018). Antecedents to the success of block chain technology adoption in manufacturing supply chains. 64–67. https://doi.org/10.1145/3278252.3278273

Bi, Z., & Cochran, D. (2014). Big data analytics with applications. *Journal of Management Analytics*, *1*. https://doi.org/10.1080/23270012.2014.992985

Bicaku, A., Schmittner, C., Tauber, M., & Delsing, J. (2018). Monitoring Industry 4.0 applications for security and safety standard compliance. *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 749–754. https://doi.org/10.1109/ICPHYS.2018.8390801

Bishop, M., Conboy, H. M., Phan, H., Simidchieva, B. I., Avrunin, G. S., Clarke, L. A., Osterweil, L. J., & Peisert, S. (2014). Insider Threat Identification by Process Analysis. *2014 IEEE Security and Privacy Workshops*, 251–264. https://doi.org/10.1109/SPW.2014.40

Bose, S., Raikwar, M., Mukhopadhyay, D., Chattopadhyay, A., & Lam, K.-Y. (2018). BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1326–1335. https://doi.org/10.1109/Cybermatics_2018.2018.00229

Boulares, S., Adi, K., & Logrippo, L. (2017). Insider Threat Likelihood Assessment for Flexible Access Control. In E. Aïmeur, U. Ruhi, & M. Weiss (Eds.), *E-Technologies: Embracing the Internet of Things* (Vol. 289, pp. 77–95). Springer International Publishing. https://doi.org/10.1007/978-3-319-59041-7_5

Buldas, A., Laud, P., Priisalu, J., Saarepera, M., & Willemson, J. (2006). Rational Choice of Security Measures Via Multi-parameter Attack Trees. In J. Lopez (Ed.), *Critical Information Infrastructures Security* (pp. 235–248). Springer. https://doi.org/10.1007/11962977_19

Campbell, T. A., & Ivanova, O. S. (2013). Additive Manufacturing as a Disruptive Technology: Implications of Three-Dimensional Printing. *Technology & Innovation*, *15*(1), 67–79. https://doi.org/10.3727/194982413X13608676060655

Cao, Y., Jia, F., & Manogaran, G. (2020). Efficient Traceability Systems of Steel Products Using Blockchain-Based Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *16*(9), 6004–6012. https://doi.org/10.1109/TII.2019.2942211

CERT. (2017). CERT Insider Threat Center, The CERT Division. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91513

CERT. (2019). Common Sense Guide to Mitigating Insider Threats (CMU/SEI-2018-TR-010; Sixth). Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644

Chen, H. (2017). Applications of Cyber-Physical System: A Literature Review. *Journal of Industrial Integration and Management*, *02*(03), 1750012. https://doi.org/10.1142/S2424862217500129

Chen, I. J., & Paulraj, A. (2004a). Towards a theory of supply chain management: The constructs and measurements. *Journal of Operations Management*, *22*(2), 119–150. https://doi.org/10.1016/j.jom.2003.12.007

Chen, I. J., & Paulraj, A. (2004b). Understanding supply chain management: Critical research and a theoretical framework. *International Journal of Production Research*, *42*(1), 131–163. https://doi.org/10.1080/00207540310001602865

Cheng, Y., Chen, K., Sun, H., Zhang, Y., & Tao, F. (2018). Data and knowledge mining with big data towards smart production. *Journal of Industrial Information Integration*, *9*, 1–13. https://doi.org/10.1016/j.jii.2017.08.001

Chhetri, S. R., Canedo, A., & Faruque, M. A. A. (2016). KCAD: Kinetic Cyber-attack detection method for Cyber-physical additive manufacturing systems. *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 1–8. https://doi.org/10.1145/2966986.2967050

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005). Towards a theory of insider threat assessment. *2005 International Conference on Dependable Systems and Networks (DSN'05)*, 108–117. https://doi.org/10.1109/DSN.2005.94

Chung, K., Yoo, H., Choe, D., & Jung, H. (2019). Blockchain Network Based Topic Mining Process for Cognitive Manufacturing. *Wireless Personal Communications*, *105*(2), 583–597. https://doi.org/10.1007/s11277-018-5979-8

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Davis, A. Y., Zhang, Q., Wong, J. P. S., Weber, R. J., & Black, M. S. (2019). Characterization of volatile organic compound emissions from consumer level material extrusion 3D printers. *Building and Environment*, *160*, 106209. https://doi.org/10.1016/j.buildenv.2019.106209

DebRoy, T., Wei, H. L., Zuback, J. S., Mukherjee, T., Elmer, J. W., Milewski, J. O., Beese, A. M., Wilson-Heid, A., De, A., & Zhang, W. (2018). Additive manufacturing of metallic components – Process, structure and properties. *Progress in Materials Science*, *92*, 112–224. https://doi.org/10.1016/j.pmatsci.2017.10.001

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-Art, Challenges, and Open Issues in the Integration of Internet of Things and Cloud Computing. *J. Netw. Comput. Appl.*, *67*(C), 99–117. https://doi.org/10.1016/j.jnca.2016.01.010

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: Challenges and Solutions. *ArXiv:1608.05187 [Cs]*. http://arxiv.org/abs/1608.05187

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

Du, W. (2019). Computer & Internet Security: A Hands-on Approach (2nd edition). Wenliang Du.

Durán, R. G., Yarlequé-Ruesta, D., Bellés-Muñoz, M., Jimenez-Viguer, A., & Muñoz-Tapia, J. L. (2020). An Architecture for Easy Onboarding and Key Life-Cycle Management in Blockchain Applications. *IEEE Access*, *8*, 115005–115016. https://doi.org/10.1109/ACCESS.2020.3003995

ElMessiry, M., ElMessiry, A., & ElMessiry, M. (2019). Dual Token Blockchain Economy Framework. In J. Joshi, S. Nepal, Q. Zhang, & L.-J. Zhang (Eds.), *Blockchain – ICBC 2019* (pp. 157–170). Springer International Publishing. https://doi.org/10.1007/978-3-030-23404-1_11

Farabet, C., Couprie, C., Najman, L., & LeCun, Y. (2013). Learning Hierarchical Features for Scene Labeling. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *35*(8), 1915–1929. https://doi.org/10.1109/TPAMI.2012.231

Frazzon, E. M., Hartmann, J., Makuschewitz, T., & Scholz-Reiter, B. (2013). Towards Socio-Cyber-Physical Systems in Production Networks. *Procedia CIRP*, *7*, 49–54. https://doi.org/10.1016/j.procir.2013.05.009

Frey, P., Lechner, M., Bauer, T., Shubina, T., Yassin, A., Wituschek, S., Virkus, M., & Merklein, M. (2019). Blockchain for forming technology – tamper-proof exchange of production data.

IOP Conference Series: Materials Science and Engineering, *651*, 012046. https://doi.org/10.1088/1757-899X/651/1/012046

Geiger, S., Schall, D., Meixner, S., & Egger, A. (2019). Process traceability in distributed manufacturing using blockchains. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 417–420. https://doi.org/10.1145/3297280.3297546

Ghaleb, A., Zhioua, S., & Almulhem, A. (2018). On PLC network security. *International Journal of Critical Infrastructure Protection*, *22*, 62–69. https://doi.org/10.1016/j.ijcip.2018.05.004

Gomez, M. R., Casper, S., & Smith, E. A. (2008). The CSB Incident Screening Database: Description, summary statistics and uses. *Journal of Hazardous Materials*, *159*(1), 119–129. https://doi.org/10.1016/j.jhazmat.2007.07.122

Greitzer, F. L., Frincke, D., & Zabriskie, M. (2011). Social/Ethical Issues in Predictive Insider Threat Monitoring. *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*. https://doi.org/10.4018/978-1-61692-245-0.ch007

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. *2014 IEEE Security and Privacy Workshops*, 236–250. https://doi.org/10.1109/SPW.2014.39

Gu, A., Yin, Z., Fan, C., & Xu, F. (2019). Safety Framework Based on Blockchain for Intelligent Manufacturing Cyber Physical System. *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, 1–5. https://doi.org/10.1109/IAI47267.2019.9085328

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

GURUCUL. (2019). Insider Threat Survey: 671 International Information Technology Professionals Surveyed on Insider Threats at RSA Conference 2019. www.gurucul.com

GURUCUL. (2020). 2020 Insider Threat Report. https://gurucul.com

GURUCUL. (2021). 2021 Insider Threat Report. https://gurucul.com

Harris, K. D. (2016). California Data Breach Report 2016. *Attorney General California Department of Justice*. https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

Hasan, M., & Starly, B. (2020). Decentralized cloud manufacturing-as-a-service (CMaaS) platform architecture with configurable digital assets. *Journal of Manufacturing Systems*, *56*, 157–174. https://doi.org/10.1016/j.jmsy.2020.05.017

Hashim, N. A., Abidin, Z. Z., Zakaria, N. A., Ahmad, R., & Puvanasvaran, A. P. (2018). Risk assessment method for insider threats in cyber security: A review. *International Journal of Advanced Computer Science and Applications*, *9*(11), 126–130. Scopus. https://doi.org/10.14569/ijacsa.2018.091119

Hatvany, J. (1985). Intelligence and cooperation in heterarchic manufacturing systems. *Robotics and Computer-Integrated Manufacturing*, *2*(2), 101–104. https://doi.org/10.1016/0736-5845(85)90065-1

Herzog, D., Seyda, V., Wycisk, E., & Emmelmann, C. (2016). Additive manufacturing of metals. *Acta Materialia*, *117*, 371–392. https://doi.org/10.1016/j.actamat.2016.07.019

Hmood, H. S., Li, Z., Abdulwahid, H. K., & Zhang, Y. (2015). Adaptive Caching Approach to Prevent DNS Cache Poisoning Attack. *The Computer Journal*, *58*(4), 973–985. https://doi.org/10.1093/comjnl/bxu023

Ho, N., Wong, P.-M., Soon, R.-J., Chng, C.-B., & Chui, C.-K. (2019). Blockchain for Cyber-Physical System in Manufacturing. *Proceedings of the Tenth International Symposium on Information and Communication Technology*, 385–392. https://doi.org/10.1145/3368926.3369656

Hodges, S., Taylor, S., Villar, N., Scott, J., Bial, D., & Fischer, P. T. (2013). Prototyping Connected Devices for the Internet of Things. *Computer*, *46*(2), 26–34. https://doi.org/10.1109/MC.2012.394

Holland, M., Nigischer, C., & Stjepandic, J. (2017). Copyright Protection in Additive Manufacturing with Blockchain Approach. https://doi.org/10.3233/978-1-61499-779-5-914

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Comput. Surv.*, *52*(2). https://doi.org/10.1145/3303771

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats – an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, 4–27.

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing*, *1*, 47–63. https://doi.org/10.1016/j.promfg.2015.09.060

Iacob, M.-E., & Jonkers, H. (2009). A model-driven perspective on the rule-based specification and analysis of service-based applications. *Enterprise Information Systems*, *3*(3), 279–298. https://doi.org/10.1080/17517570903042762

IBM. (2015). IBM 2015 Cyber Security Intelligence Index. https://www.ibm.com/security/data-breach/threat-intelligence

IBM. (2016). IBM 2016 Cyber Security Intelligence Index-reviewing a year of serious data breaches, major attacks and new vulnerabilities. https://www.ibm.com/security/data-breach/threat-intelligence

IBM. (2017). IBM X-Force Threat Intelligence Index 2017-The year of the mega breach. https://www.ibm.com/security/data-breach/threat-intelligence

IBM. (2018). IBM X-Force Threat Intelligence Index 2018-Notable security events of 2017, and a look ahead. https://www.ibm.com/security/data-breach/threat-intelligence

IBM. (2019). *IBM X-Force Threat Intelligence Index 2019.* https://www.ibm.com/security/data-breach/threat-intelligence

IBM. (2020a). Cost of Insider Threats: Global Report 2020. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

IBM. (2020b). IBM X-Force Threat Intelligence Index 2020. https://www.ibm.com/security/data-breach/threat-intelligence

IBM. (2020c). Cost of a Data Breach Report 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/

INSA. (2018a). An Assessment of Data Analytics Techniques for Insider Threat Programs. https://www.insaonline.org/an-assessment-of-data-analytics-techniques-for-insider-threat-programs/

INSA. (2018b). A Framework for Cyber Indications and Warning. https://www.insaonline.org/a-framework-for-cyber-indications-and-warning/

Iqbal, A., Amir, M., Kumar, V., Alam, A., & Umair, M. (2020). Integration of Next Generation IIoT with Blockchain for the Development of Smart Industries. *Emerging Science Journal*, *4*(0), 1–17. https://doi.org/10.28991/esj-2020-SP1-01

Jürgenson, A., & Willemson, J. (2010). Serial Model for Attack Tree Computations. In D. Lee & S. Hong (Eds.), *Information, Security and Cryptology – ICISC 2009* (pp. 118–128). Springer. https://doi.org/10.1007/978-3-642-14423-3_9

Kagermann, H., Wahlster, W., & Helbig, J. (2013). Securing the future of German manufacturing industry: Recommendations for implementing the strategic initiative Industrie 4.0 (pp. 19–20). https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf

Kambatla, K., Kollias, G., Kumar, V., & Grama, A. (2014). Trends in big data analytics. *Journal of Parallel and Distributed Computing*, *74*(7), 2561–2573. https://doi.org/10.1016/j.jpdc.2014.01.003

Kapitonov, A., Berman, I., Bulatov, V., Lonshakov, S., & Krupenkin, A. (2018). Robonomics Based on Blockchain as a Principle of Creating Smart Factories. *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, 78–85. https://doi.org/10.1109/IoTSMS.2018.8554864

Kasten, J. E. (2020). Engineering and Manufacturing on the Blockchain: A Systematic Review. *IEEE Engineering Management Review*, *48*(1), 31–47. https://doi.org/10.1109/EMR.2020.2964224

Kennedy, Z. C., Stephenson, D. E., Christ, J. F., Pope, T. R., Arey, B. W., Barrett, C. A., & Warner, M. G. (2017). Enhanced anti-counterfeiting measures for additive manufacturing:

Coupling lanthanide nanomaterial chemical signatures with blockchain technology. *Journal of Materials Chemistry C*, *5*(37), 9570–9578. https://doi.org/10.1039/C7TC03348F

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Kim, B. H., Ahn, H.-J., Kim, J. O., Yoo, M., Cho, K., & Choi, D. (2010). Application of M2M technology to manufacturing systems. *2010 International Conference on Information and Communication Technology Convergence (ICTC)*, 519–520. https://doi.org/10.1109/ICTC.2010.5674785

Klöckner, M., Kurpjuweit, S., Velu, C., & Wagner, S. M. (2020). Does Blockchain for 3D Printing Offer Opportunities for Business Model Innovation? *Research-Technology Management*, *63*(4), 18–27. https://doi.org/10.1080/08956308.2020.1762444

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, *60*(6), 84–90. https://doi.org/10.1145/3065386

Kurpjuweit, S., Schmidt, C. G., Klöckner, M., & Wagner, S. M. (2021). Blockchain in Additive Manufacturing and its Impact on Supply Chains. *Journal of Business Logistics*, *42*(1), 46–70. https://doi.org/10.1111/jbl.12231

Lallas, E. N., Xenakis, A., & Stamoulis, G. (2019). A generic framework for a Peer to Peer Blockchain based Fog Architecture in Industrial Automation. *2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media*

Conference (SEEDA-CECNSM), 1–5. https://doi.org/10.1109/SEEDA-CECNSM.2019.8908360

Lambert, D. M., & Cooper, M. C. (2000). Issues in supply chain management. *Industrial Marketing Management*, *29*(1), 65–83. https://doi.org/10.1016/S0019-8501(99)00113-3

Langmann, R., & Stiller, M. (2019). The PLC as a Smart Service in Industry 4.0 Production Systems. *Applied Sciences*, *9*(18), 3815. https://doi.org/10.3390/app9183815

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Leang, B., Ean, S., Kim, R.-W., Chi, S.-Y., & Yoo, K.-H. (2019). Extracting Sensing Data from PLCs in Smart Manufacturing Machines. *2019 International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1249–1250. https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00208

Lecuyer, M., Atlidakis, V., Geambasu, R., Hsu, D., & Jana, S. (2019). Certified Robustness to Adversarial Examples with Differential Privacy. *ArXiv:1802.03471 [Cs, Stat]*. http://arxiv.org/abs/1802.03471

Lee, C. K. M., Huo, Y. Z., Zhang, S. Z., & Ng, K. K. H. (2020). Design of a Smart Manufacturing System with the Application of Multi-Access Edge Computing and Blockchain Technology. *IEEE Access*, *8*, 28659–28667. https://doi.org/10.1109/ACCESS.2020.2972284

Lee, J., Azamfar, M., & Singh, J. (2019). A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. *Manufacturing Letters*, *20*, 34–39. https://doi.org/10.1016/j.mfglet.2019.05.003

Lee, J., Bagheri, B., & Jin, C. (2016). Introduction to cyber manufacturing. *Manufacturing Letters*, *8*, 11–15. https://doi.org/10.1016/j.mfglet.2016.05.002

Lee, J., Bagheri, B., & Kao, H.-A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*, 18–23. Scopus. https://doi.org/10.1016/j.mfglet.2014.12.001

Lee, J., Lapira, E., Yang, S., & Kao, A. (2013). Predictive Manufacturing System—Trends of Next-Generation Production Systems. *IFAC Proceedings Volumes*, *46*(7), 150–156. https://doi.org/10.3182/20130522-3-BR-4036.00107

Leng, J., Ruan, G., Jiang, P., Xu, K., Liu, Q., Zhou, X., & Liu, C. (2020). Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. *Renewable and Sustainable Energy Reviews*, *132*, 110112. https://doi.org/10.1016/j.rser.2020.110112

Leng, J., Yan, D., Liu, Q., Xu, K., Zhao, J. L., Shi, R., Wei, L., Zhang, D., & Chen, X. (2020). ManuChain: Combining Permissioned Blockchain with a Holistic Optimization Model as Bi-Level Intelligence for Smart Manufacturing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 182–192. https://doi.org/10.1109/TSMC.2019.2930418

Leng, J., Ye, S., Zhou, M., Zhao, J. L., Liu, Q., Guo, W., Cao, W., & Fu, L. (2021). Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(1), 237–252. https://doi.org/10.1109/TSMC.2020.3040789

Lepoint, T., Ciocarlie, G., & Eldefrawy, K. (2018). BlockCIS—A Blockchain-Based Cyber Insurance System. 378–384. https://doi.org/10.1109/IC2E.2018.00072

Lhachemi, H., Malik, A., & Shorten, R. (2019). Augmented Reality, Cyber-Physical Systems, and Feedback Control for Additive Manufacturing: A Review. *IEEE Access, 7*, 50119–50135. https://doi.org/10.1109/ACCESS.2019.2907287

Li, J., Maiti, A., Springer, M., & Gray, T. (2020). Blockchain for supply chain quality management: Challenges and opportunities in context of open manufacturing and industrial internet of things. *International Journal of Computer Integrated Manufacturing*, *33*(12), 1321–1355. https://doi.org/10.1080/0951192X.2020.1815853

Li, K., Tang, Y., Kim, B. H., & Xu, J. (2019). Secure Consistency Verification for Untrusted Cloud Storage by Public Blockchains. *ArXiv:1904.06626 [Cs]*. http://arxiv.org/abs/1904.06626

Li, L., Li, S., & Zhao, S. (2014). QoS-Aware Scheduling of Services-Oriented Internet of Things. *IEEE Transactions on Industrial Informatics*, *10*(2), 1497–1505. https://doi.org/10.1109/TII.2014.2306782

Li, L., Liu, M., Shen, W., & Cheng, G. (2016). A Discrete Stress–Strength Interference Theory-Based Dynamic Supplier Selection Model for Maintenance Service Outsourcing. *IEEE Transactions on Engineering Management*, *63*(2), 189–200. https://doi.org/10.1109/TEM.2016.2527684

Li, S. (2017). Chapter 3—Security and Vulnerability in the Internet of Things. In S. Li & L. D. Xu (Eds.), *Securing the Internet of Things* (pp. 49–68). Syngress. https://doi.org/10.1016/B978-0-12-804458-2.00003-2

Li, S., Xiao, H., Wang, H., Wang, T., Qiao, J., & Liu, S. (2019). Blockchain Dividing Based on Node Community Clustering in Intelligent Manufacturing CPS. *2019 IEEE International Conference on Blockchain (Blockchain)*, 124–131. https://doi.org/10.1109/Blockchain.2019.00025

Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-Integrated Manufacturing*, *54*, 133–144. https://doi.org/10.1016/j.rcim.2018.05.011

Li, Z., Wang, W. M., Liu, G., Liu, L., He, J., & Huang, G. Q. (2018). Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing. *Industrial Management & Data Systems*, *118*(1), 303–320. https://doi.org/10.1108/IMDS-04-2017-0142

Lin, H., Hu, J., Xiaoding, W., Alhamid, M. F., & Piran, M. J. (2020). Towards Secure Data Fusion in Industrial IoT using Transfer Learning. *IEEE Transactions on Industrial Informatics*, 1–1. https://doi.org/10.1109/TII.2020.3038780

Liu, C., Ji, H., & Wei, J. (2020). The Impact of Block-Chain on Collaborative Product Innovation of Manufacturing Supply Chain. In G. Salvendy & J. Wei (Eds.), *Design, Operation and Evaluation of Mobile Communications* (pp. 73–83). Springer International Publishing. https://doi.org/10.1007/978-3-030-50350-5_7

Liu, C., & Jiang, P. (2016). A Cyber-physical System Architecture in Shop Floor for Intelligent Manufacturing. *Procedia CIRP*, *56*, 372–377. https://doi.org/10.1016/j.procir.2016.10.059

Liu, J., Jiang, P., & Leng, J. (2017). A framework of credit assurance mechanism for manufacturing services under social manufacturing context. *2017 13th IEEE Conference on Automation Science and Engineering (CASE)*, 36–40. https://doi.org/10.1109/COASE.2017.8256072

Liu, M., Li, Z., Guo, X., & Dutkiewicz, E. (2008). Performance Analysis and Optimization of Handoff Algorithms in Heterogeneous Wireless Networks. *IEEE Transactions on Mobile Computing*, *7*(7), 846–857. https://doi.org/10.1109/TMC.2007.70768

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12), 1550147717741463. https://doi.org/10.1177/1550147717741463

Maroun, E. A., Daniel, J., Zowghi, D., & Talaei-Khoei, A. (2019). *Blockchain in Supply Chain Management: Australian Manufacturer Case Study* (Vol. 367). https://doi.org/10.1007/978-3-030-32242-7_8

Matheu, S. N., Robles Enciso, A., Molina Zarca, A., Garcia-Carrillo, D., Hernández-Ramos, J. L., Bernal Bernabe, J., & Skarmeta, A. F. (2020). Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems. *Sensors*, *20*(7), 1882. https://doi.org/10.3390/s20071882

Mauw, S., & Oostdijk, M. (2006). Foundations of Attack Trees. In D. H. Won & S. Kim (Eds.), *Information Security and Cryptology—ICISC 2005* (pp. 186–198). Springer. https://doi.org/10.1007/11734727_17

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., & Weinhardt, C. (2018). A blockchain-based smart grid: Towards sustainable local energy markets. *Computer Science - Research and Development*, *33*(1), 207–214. https://doi.org/10.1007/s00450-017-0360-9

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining Supply Chain Management. *Journal of Business Logistics*, *22*(2), 1–25. https://doi.org/10.1002/j.2158-1592.2001.tb00001.x

Merkle, R. C. (1988). A Digital Signature Based on a Conventional Encryption Function. In C. Pomerance (Ed.), *Advances in Cryptology—CRYPTO '87* (pp. 369–378). Springer. https://doi.org/10.1007/3-540-48184-2_32

Mirkin, M., Ji, Y., Pang, J., Klages-Mundt, A., Eyal, I., & Juels, A. (2020). BDoS: Blockchain Denial of Service. *ArXiv:1912.07497 [Cs]*. http://arxiv.org/abs/1912.07497

Moghaddam, M., Cadavid, M. N., Kenley, C. R., & Deshmukh, A. V. (2018). Reference architectures for smart manufacturing: A critical review. *Journal of Manufacturing Systems*, *49*, 215–225. https://doi.org/10.1016/j.jmsy.2018.10.006

Mohamed, N., & Al-Jaroodi, J. (2019). Applying Blockchain in Industry 4.0 Applications. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0852–0858. https://doi.org/10.1109/CCWC.2019.8666558

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., & Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals*, *65*(2), 621–641. Scopus. https://doi.org/10.1016/j.cirp.2016.06.005

Moore, A. P., Savinda, J., Monaco, E., Moyes, J., Rousseau, D., Perl, S., Cowley, J., Collins, M., Cassidy, T., VanHoudnos, N., Buttles-Valdez, P., Bauer, D., & Parshall, A. (2016). The Critical Role of Positive Incentives for Reducing Insider Threats. *Carnegie Mellon University. Journal Contribution*. https://doi.org/10.1184/R1/6585104.v1

Moore, M. (2016). Cybersecurity Breaches and Issues Surrounding Online Threat Protection. In *Http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-1941-6*. IGI Global. www.igi-global.com/book/cybersecurity-breaches-issues-surrounding-online/169252

Moorthi, E., Kathiresan, G., Prasad, P., & Mohanram, P. (2011). A survey on lean practices in Indian machine tool industries. *International Journal of Advanced Manufacturing Technology*, *52*, 1091–1101. https://doi.org/10.1007/s00170-010-2788-y

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography Mailing List at Https://Metzdowd.Com*.

Nakasumi, M. (2017). Information Sharing for Supply Chain Management Based on Block Chain Technology. *2017 IEEE 19th Conference on Business Informatics (CBI), 01*, 140–149. https://doi.org/10.1109/CBI.2017.56

Natoli, C., & Gramoli, V. (2016). The Blockchain Anomaly. *ArXiv:1605.05438 [Cs]*. http://arxiv.org/abs/1605.05438

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, *31*(4), 418–436. https://doi.org/10.1016/j.cose.2012.02.009

NIFFT. (2016). Protect Your Organization from the Inside Out: Government Best Practices. https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf

NIFFT. (2017). Insider Threat Guide. https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2014). Insider Threat Assessment: A Model-Based Methodology. *SIGOPS Oper. Syst. Rev.*, *48*(2), 3–12. https://doi.org/10.1145/2694737.2694740

Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2013). A methodology and supporting techniques for the quantitative assessment of insider threats. *Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing*, 1–6. https://doi.org/10.1145/2506155.2506158

Oueslati, N. E., Mrabet, H., Jemai, A., & Alhomoud, A. (2019). Comparative Study of the Common Cyber-physical Attacks in Industry 4.0. *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, 1–7. https://doi.org/10.1109/IINTEC48298.2019.9112097

Ouyang, L., Yuan, Y., & Wang, F.-Y. (2019). A Blockchain-based Framework for Collaborative Production in Distributed and Social Manufacturing. *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 76–81. https://doi.org/10.1109/SOLI48380.2019.8955075

Padalkar, N., Sheikh-Zadeh, A., & Song, J. (2020). Business Value of Smart Contract: Case of Inventory Information Discrepancies. *AMCIS 2020 Proceedings*. https://aisel.aisnet.org/amcis2020/sig_green/sig_green/1

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, *13*, 1253–1260. Scopus. https://doi.org/10.1016/j.promfg.2017.09.047

Pfleeger, C. P. (2008). Reflections on the Insider Threat. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, & S. Sinclair (Eds.), *Insider Attack and Cyber Security: Beyond the Hacker* (pp. 5–16). Springer US. https://doi.org/10.1007/978-0-387-77322-3_2

Primova, H., Sotvoldiev, D., & Safarova, L. (2018). Approaches to solving the problem of risk assessment with fuzzy initial information. *2018 Dynamics of Systems, Mechanisms and Machines (Dynamics)*, 1–5. https://doi.org/10.1109/Dynamics.2018.8601485

Quartel, D. A. C., Pokraev, S., Dirgahayu, T., Pessoa, R. M., Steen, M. W. A., & Sinderen, M. van. (2009). Model-driven development of mediation for business services using COSMO.

Enterprise Information Systems, *3*(3), 319–345. https://doi.org/10.1080/17517570903045591

Ribeiro, L., & Björkman, M. (2018). Transitioning From Standard Automation Solutions to Cyber-Physical Production Systems: An Assessment of Critical Conceptual and Technical Challenges. *IEEE Systems Journal*, *12*(4), 3816–3827. https://doi.org/10.1109/JSYST.2017.2771139

Saini, V., Duan, Q., & Paruchuri, V. (2008). Threat Modeling Using Attack Trees. *Journal of Computing Sciences in Colleges*, *23*.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Salem, M., Hershkop, S., & Stolfo, S. (2008). A Survey of Insider Attack Detection Research. In *Insider Attack and Cyber Security: Beyond the Hacker* (Vol. 39, pp. 69–90). https://doi.org/10.1007/978-0-387-77322-3_5

Sandaruwan, G. P. H., Ranaweera, P. S., & Oleshchuk, V. A. (2013). PLC security and critical infrastructure protection. *2013 IEEE 8th International Conference on Industrial and Information Systems*, 81–85. https://doi.org/10.1109/ICIInfS.2013.6731959

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526–531. https://doi.org/10.1016/S0167-4048(02)01009-X

Schultz, E., & Shumway, R. (2001). Incident Response: A Strategic Guide to Handling System and Network Security Breaches. Sams Publishing.

Seibold, C., Samek, W., Hilsmann, A., & Eisert, P. (2020). Accurate and robust neural networks for face morphing attack detection. *Journal of Information Security and Applications*, *53*, 102526. https://doi.org/10.1016/j.jisa.2020.102526

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2018). On the Origins and Variations of Blockchain Technologies. *ArXiv:1810.06130 [Cs]*. http://arxiv.org/abs/1810.06130

Shim, H., Kim, T., & Choi, G. (2019). Technology Roadmap for Eco-Friendly Building Materials Industry. *Energies*, *12*(5), 804. https://doi.org/10.3390/en12050804

Sinclair, S., & Smith, S. W. (2008). Preventative Directions For Insider Threat Mitigation Via Access Control. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, & S. Sinclair (Eds.), *Insider Attack and Cyber Security: Beyond the Hacker* (Vol. 1–39, pp. 165–194). Springer US. https://doi.org/10.1007/978-0-387-77322-3_10

Song, J., & Moon, B. Y. (2020a). *I*nsider Attack Tree for Cyber-Manufacturing System. *2020 IEEE Systems Security Symposium*.

Song, J., & Moon, Y. (2020b). Security Enhancement Against Insiders in Cyber-Manufacturing Systems. *Procedia Manufacturing*, *48*, 864–872. https://doi.org/10.1016/j.promfg.2020.05.124

Song, J., & Moon, Y. (2020c, January 21). A Secure Cyber-Manufacturing System Augmented by the Blockchain. *ASME 2019 International Mechanical Engineering Congress and Exposition*. https://doi.org/10.1115/IMECE2019-10366

Song, J., Shukla, D., Wu, M., Phoha, V. V., & Moon, Y. B. (2020, January 21). Physical Data Auditing for Attack Detection in Cyber-Manufacturing Systems: Blockchain for Machine Learning Process. *ASME 2019 International Mechanical Engineering Congress and Exposition*. https://doi.org/10.1115/IMECE2019-10442

Song, J., Wang, C., Saudrais, C., Swanson, M. K., Greaney, E. A., & Moon, Y. B. (2020). Cyber-Manufacturing System Testbed Development: Adversarial Insider Manipulation. *Procedia CIRP*, *93*, 180–185. https://doi.org/10.1016/j.procir.2020.03.007

Song, Z., & Moon, Y. (2017). Assessing sustainability benefits of cybermanufacturing systems. *International Journal of Advanced Manufacturing Technology*, *90*(5–8), 1365–1382. https://doi.org/10.1007/s00170-016-9428-0

Song, Z., & Moon, Y. (2019a). Performance analysis of CyberManufacturing Systems. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *233*(5), 1362–1376. https://doi.org/10.1177/0954405417706996

Song, Z., & Moon, Y. (2019b). Performance analysis of CyberManufacturing Systems. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *233*(5), 1362–1376. https://doi.org/10.1177/0954405417706996

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Stjepandic, J., & Biahmou, A. (2016). Towards agile enterprise rights management in engineering collaboration. *International Journal of Agile Systems and Management*, *9*, 302–325. https://doi.org/10.1504/IJASM.2016.081564

Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., & Parker, R. (2017). Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects. *Journal of Manufacturing Systems*, *44*, 154–164. https://doi.org/10.1016/j.jmsy.2017.05.007

Tao, F., Zhang, L., Venkatesh, V. C., Luo, Y., & Cheng, Y. (2011). Cloud manufacturing: A computing and service-oriented manufacturing model. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *225*(10), 1969–1976. https://doi.org/10.1177/0954405411405575

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484. https://doi.org/10.1016/j.cose.2005.05.002

Thomas, S. L., & Francillon, A. (2018). Backdoors: Definition, Deniability and Detection. In M. Bailey, T. Holz, M. Stamatogiannakis, & S. Ioannidis (Eds.), *Research in Attacks, Intrusions, and Defenses* (pp. 92–113). Springer International Publishing. https://doi.org/10.1007/978-3-030-00470-5_5

Unger, T., Mietzner, R., & Leymann, F. (2009). Customer-defined service level agreements for composite applications. *Enterprise Information Systems*, *3*(3), 369–391. https://doi.org/10.1080/17517570903033431

Wang, L., Törngren, M., & Onori, M. (2015). Current status and advancement of cyber-physical systems in manufacturing. *Journal of Manufacturing Systems*, *37*, 517–527. https://doi.org/10.1016/j.jmsy.2015.04.008

Wang, S., Wan, J., Li, D., & Zhang, C. (2016). Implementing Smart Factory of Industrie 4.0: An Outlook. *International Journal of Distributed Sensor Networks*, *12*(1), 3159805. https://doi.org/10.1155/2016/3159805

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. https://doi.org/10.1057/ejis.2009.12

Westerkamp, M., Victor, F., & Küpper, A. (2020). Tracing manufacturing processes using blockchain-based token compositions. *Digital Communications and Networks*, *6*(2), 167–176. https://doi.org/10.1016/j.dcan.2019.01.007

Westerkamp, M., Victor, F., & Kupper, A. (2018). Blockchain-based supply chain traceability: Token recipes model manufacturing processes. 1595–1602. https://doi.org/10.1109/Cybermatics_2018.2018.00267

Wu, M., & Moon, Y. (2018). DACDI (Define, Audit, Correlate, Disclose, and Improve) framework to address cyber-manufacturing attacks and intrusions. *Manufacturing Letters*, *15*, 155–159. https://doi.org/10.1016/j.mfglet.2017.12.009

Wu, M., & Moon, Y. B. (2019, January 15). Taxonomy for Secure CyberManufacturing Systems. *ASME 2018 International Mechanical Engineering Congress and Exposition*. https://doi.org/10.1115/IMECE2018-86091

Wu, M., & Moon, Y. B. (2020, January 21). Intrusion Detection of Cyber-Physical Attacks in Manufacturing Systems: A Review. *ASME 2019 International Mechanical Engineering Congress and Exposition*. https://doi.org/10.1115/IMECE2019-10135

Wu, M., Phoha, V. V., Moon, Y. B., & Belman, A. K. (2017, February 8). Detecting Malicious Defects in 3D Printing Process Using Machine Learning and Image Classification. *ASME 2016 International Mechanical Engineering Congress and Exposition*. https://doi.org/10.1115/IMECE2016-67641

Xu, L. D. (2011). Enterprise Systems: State-of-the-Art and Future Trends. *IEEE Transactions on Industrial Informatics*, *7*(4), 630–640. https://doi.org/10.1109/TII.2011.2167156

Xu, L. D., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2243. https://doi.org/10.1109/TII.2014.2300753

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. *International Journal of Production Research*, *56*(8), 2941–2962. Scopus. https://doi.org/10.1080/00207543.2018.1444806

Xu, Z., Liu, Y., Zhang, J., Song, Z., Li, J., & Zhou, J. (2019). Manufacturing Industry Supply Chain Management Based on the Ethereum Blockchain. *2019 IEEE International Conferences on Ubiquitous Computing Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS)*, 592–596. https://doi.org/10.1109/IUCC/DSCI/SmartCNS.2019.00124

Yan, Y., Kaneko, S., & Asano, H. (2020). Accumulated and aggregated shifting of intensity for defect detection on micro 3D textured surfaces. *Pattern Recognition*, *98*, 107057. https://doi.org/10.1016/j.patcog.2019.107057

Yin, S., Bao, J., Zhang, Y., & Huang, X. (2017). M2M Security Technology of CPS Based on Blockchains. *Symmetry*, *9*(9), 193. https://doi.org/10.3390/sym9090193

Yu, C., Jiang, X., Yu, S., & Yang, C. (2020). Blockchain-based shared manufacturing in support of cyber physical systems: Concept, framework, and operation. *Robotics and Computer-Integrated Manufacturing*, *64*, 101931. https://doi.org/10.1016/j.rcim.2019.101931

Yu, Z., Ouyang, J., Li, S., & Peng, X. (2017). Formal modeling and control of cyber-physical manufacturing systems. *Advances in Mechanical Engineering*, *9*(10). Scopus. https://doi.org/10.1177/1687814017725472

Yue, H., Wang, H., Chen, H., Cai, K., & Jin, Y. (2020). Automatic detection of feather defects using Lie group and fuzzy Fisher criterion for shuttlecock production. *Mechanical Systems and Signal Processing*, *141*, 106690. https://doi.org/10.1016/j.ymssp.2020.106690

Zhang, F., Liu, M., & Shen, W. (2017). Operation modes of smart factory for high-end equipment manufacturing in the Internet and Big Data era. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 152–157. https://doi.org/10.1109/SMC.2017.8122594

Zhang, J., Peng, C., Masroor, S., Sun, H., & Chai, L. (2016). Stability analysis of networked control systems with denial-of-service attacks. *2016 UKACC 11th International Conference on Control (CONTROL)*, 1–6. https://doi.org/10.1109/CONTROL.2016.7737622

Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., & Tao, F. (2019). Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System. *IEEE Transactions on Computational Social Systems*, *6*(6), 1386–1394. https://doi.org/10.1109/TCSS.2019.2918467

Zhang, Z., Bai, S., Xu, G., Liu, X., Wang, F., Jia, J., & Feng, Z. (2020). Research on the knitting needle detection system of a hosiery machine based on machine vision. *Textile Research Journal*, *90*(15–16), 1730–1740. https://doi.org/10.1177/0040517519899173

Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent Manufacturing in the Context of Industry 4.0: A Review. *Engineering*, *3*(5), 616–630. Scopus. https://doi.org/10.1016/J.ENG.2017.05.015

Zhu, X., Shi, J., Huang, S., & Zhang, B. (2020). Consensus-oriented cloud manufacturing based on blockchain technology: An exploratory study. *Pervasive and Mobile Computing*, *62*, 101113. https://doi.org/10.1016/j.pmcj.2020.101113

VITA

JINWOO SONG

Phone: 1-315-800-3573 | Email: jsong09@syr.edu

EDUCATION

Syracuse University, Syracuse, NY

- Doctor of Philosophy in Mechanical & Aerospace Engineering **Aug 2021**
  Dissertation: Mitigating Insider Threat Risks in Cyber-Physical Manufacturing Systems
  Advisor: Dr. Young Bai Moon
- Master of Science in Engineering Management **May 2018**

Dongguk University, Seoul, South Korea

- Bachelor of Science in Physics **Jun 2015**

RESEARCH INTERESTS

- Blockchain applications for manufacturing systems to enhance security against outside or inside attackers
- Insider Threats in manufacturing systems: detection, prevention, and evaluation
- Real-time attack detection system development by using machine learning algorithms
- Design and simulation of Cyber-Physical Attacks on physical testbeds that represent a small-scaled Cyber-Physical Manufacturing Systems (CPMS)

AWARDS & HONORS

2021 Syracuse University Outstanding Teaching Assistants Award	**Spring 2021**
2021 Mechanical & Aerospace Engineering Outstanding Teaching Assistants Award	**Spring 2021**
2021 NAMRC 49 / MSEC 2021 NSF Student Support Award	**Spring 2021**
2020 ECS Research Day Poster Competition 1st place Award	**Fall 2020**
2020 Summer Research Assistantship Award	**Summer 2020**
MAE Travel Award for the International Mechanical Engineering Congress & Exposition	**Fall 2019**
2019 ECS Research Day Poster Competition 1st place Award	**Spring 2019**
Graduate Teaching Assistantship	**2018-2021**
L.C. Smith College of Engineering and Computer Science Graduate Student Grant	**2016-2018**

RESEARCH EXPERIENCES

Industrial simulation research and development project

Arena simulation model development for Marquardt Switches (Arena Simulation) **Summer 2017**

- Developed an Arena simulation model for a new switch manufacturing line to improve its productivity
- Visited a local manufacturing line shop floor and interviewed workers and managers in production lines
- Participated in executive meetings and demonstrated the simulation model with a Q&A session

Blockchain research and development for manufacturing systems security

Security enhancement against insiders by using blockchain (OpenPLC, Python, C) **Fall 2019**

- Developed two testbeds in different network environments: PLC and Blockchain networks
- Demonstrated an effectiveness of the blockchain in manufacturing systems security

Convolutional neural networking imagery classification via blockchain (Node JS) **Spring 2019**

- Developed a simple CNN to detect failures in 3D-printing layer images via the blockchain

• Simplified and optimized CNN for a real-time attack detection system in additive manufacturing

Physical Data Auditing System via blockchain (MATLAB, R, Python, Node JS) **Spring 2019**

• Established Cyber-Manufacturing System augmented by blockchain technology

• Developed three physical data (Movement, Image, Acoustic) auditing systems via blockchain

Machine learning research and development for manufacturing systems security

Semi-supervised learning model development for additive manufacturing (Python) **Spring 2020**

• Developed Infill Defective Detection System (IDDS) augmented by semi-supervised learning

• Achieved 94.58% accuracy of classification without pre-training

Layered image collection method development (MATLAB) **Spring 2020**

• Led a research team consisting of two graduate students

• Developed Layered Image Collection Method (LICM) to reduce redundant delays and resources

• Validated LICM with various machine learning classification tests

Supervised machine learning development for layer imagery for 3D printing (R) **Fall 2017**

• Designed KNN, RandomForest models to classify layer imagery to detect Cyber-Physical Attacks

Physical testbed development for manufacturing systems security research

Supply chain Cyber-Manufacturing System testbed (APM, OpenPLC, Python, C) **Summer 2019**

• Designed and developed a fully integrated manufacturing model via UDP/IP and PLC protocols

• Developed a testbed consists of a CNC machine, conveyor slider, Auto Guided Vehicle, robotic arms, and 3D-printers

Cyber-Manufacturing System testbed prototype (APM, OpenPLC, Python) **Spring 2018**

• Developed a testbed consists of conveyor belt, ultrasonic sensors, robotic arms, and 3D-printers

• Collected three physical-data to corelate with cyber-data to detect Cyber-Physical Attack on the testbed

TEACHING EXPERIENCES

Data Analysis for Engineers **Fall 2020**

• Supported 39 undergraduate students in overall use of computational tools for data analysis, including: collecting & pre-processing engineering data, probability distributions & inferences, estimation, engineering experimental design, and statistical process control & reliability

• Presented one full-time class lecture about three machine learning examples

• The lecture was remotely presented via online platform due to the covid-19 safety policy. (Video Link for the lecture: https://youtu.be/7NoZHZ8ktZs)

• Advised 14 groups' projects regarding real-life data analysis by using machine learning

Simulation and Data Analytics **Spring 2020**

• Helped 41 graduate students in learning various simulation models via Arena Simulation Software, including: discrete-event simulation, system dynamics, agent-based simulation, hybrid simulation modeling, input and output data analysis, and uses of simulation for predictive and prescriptive analytics

• Presented two full-time class lectures about introducing input and process analyzers with designing experiments

• Advised 14 groups' projects regarding real-life data analysis by using machine learning

Statistics for Engineers **Fall 2019**

• Assisted 48 graduate students in learning various fundamental statistics for engineers, including: confidence intervals, simple hypothesis testing, nonparametric tests, curve fitting and regression, analysis of variance, factorial experiments, and engineering applications

• Developed the course materials including 11 Assignments, 7 quizzes, 3 exams, and 1 lecture slide
• Presented one full-time class lecture about introducing R application case study and 6 statistic distributions with 8 in-class exercises

Engineering Computational Tools **Spring 2019**

• Mentored 64 undergraduate students in learning MATLAB and EXCEL to solve various engineering problems
• Helped the professor to develop the course materials including 10 Lab sessions, 10 Assignments, 8 quizzes, 3 projects, 6 exams, 1 lecture slide
• Gave one full-time class lecture about probability, normal distribution, and their relationship with 8 in-class exercises. (Video Link for part of the lecture: https://youtu.be/34mYBKeskuQ)
• Graded and gave individual feedback for a total of 2,048 materials

Engineering Economics and Technology Valuation **Fall 2018**

• Helped 47 graduate students in learning Value-based assessment and management of engineering, technology projects, depreciation, risk-adjusted, Monte Carlo simulations, decision trees, real options, and project portfolio management
• Created the instruction and answers for the course materials. (9 Assignments, 2 exams)

ADVISING EXPERIENCES

Graduate Student Research **Spring 2020**

• Mentored two graduate students to develop a new layered image collection method
• Taught how to use 3D printer and collect layered images from the printing process

Graduate Student Research **Fall 2019**

• Led a graduate student to develop a blockchain testbed environment in the lab
• Advised how to use Ethereum platform to construct blockchain applications via Python

Summer Research Internship for Exchanging Student **Summer 2019**

• Managed a graduate student from INSA University in France for a summer research internship
• Advised a testbed development for insider threat security in Cyber-Manufacturing System

Research Experience for Undergraduate (REU) **Summer 2019**

• Mentored a student in developing a research subject and designing an experiment
• Advised the final poster, and the student won 1st place in 2019 REU poster competition

PUBLICATIONS

(2021) **J. Song**, X. He, and Y. B. Moon, "Insider Attack Scenario Assessment Framework," ASME 2021 International Mechanical Engineering Congress and Exposition, submitted.
(2021) **J. Song**, J. Wang, and Y. B. Moon, "Blockchain Applications of Manufacturing Systems: A Survey," ASME 2021 International Mechanical Engineering Congress and Exposition, submitted
(2021) **J. Song** and Y. B. Moon, "A Layer Image Auditing System Secured by Blockchain," 49th SME North American Manufacturing Research Conference, NAMRC 49, Ohio, USA.
(2020) **J. Song** and Y. B. Moon, "Infill defective detection system augmented by semi-supervised learning," ASME 2020 International Mechanical Engineering Congress and Exposition, Portland.
(2020) **J. Song**, H. Bandaru, X. He, Z. Qiu and Y. B. Moon, "Layered image collection for real-time defective inspection in additive manufacturing," ASME 2020 International Mechanical Engineering Congress and Exposition, Portland.

(2020) M. Wu, **J. Song**, S. Sharma, J. Di, B. He, Z. Wang, J. Zhang, L.W.L. Lin, E.A. Greaney, and Y. Moon, "Development of testbed for cyber-manufacturing security issues," International Journal of Computer Integrated manufacturing, vol. 33, pp. 302-320.

(2020) **J. Song** and Y. B. Moon, "Security Enhancement Against Insiders for Cyber-Manufacturing Systems," 48th SME North American Manufacturing Research Conference, Ohio.

(2020) **J. Song**, C. Wang, C. Saudrais, M. K. Swanson, E. A. Greaney, Y. B. Moon "Cyber-Manufacturing System Testbed Development: Adversarial Insider Manipulation," 53rd CIRP Conference on Manufacturing Systems, Illinois.

(2020) **J. Song** and Y. B. Moon, "Insider Attack Tree for Cyber-Manufacturing System," 2020 IEEE Systems Security Symposium, Virginia.

(2019) **J. Song**, D. Shukla, M. Wu, V. V. Phoha, and Y. B. Moon, "Physical Data Auditing for Attack Detection in Cyber-Manufacturing Systems: Blockchain for Machine Learning Process," ASME 2019 International Mechanical Engineering Congress and Exposition, Utah.

(2019) **J. Song** and Y. B. Moon, "A secure Cyber-Manufacturing System augmented by the Blockchain," ASME 2019 International Mechanical Engineering Congress and Exposition, Utah.

(2018) M. Wu, **J. Song**, L. Lin, N. Aurelle, Y. Liu, B. Ding, Z. Song, and Y.B. Moon, "Establishment of intrusion detection testbed for CyberManufacturing systems" Procedia Manufacturing, vol. 26, pp. 1053-1064.