CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM

Project Id: 2021-011

Project Proposal Report

H.H.D Kalhara

B.Sc. (Hons) Degree in Information Technology Specialization in Cyber Security

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

March 2021

CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM

Project Id: 2021-011

Project Proposal Report

B.Sc. (Hons) Degree in Information Technology Specialization in Cyber Security

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

March 2021

DECLARATION

We declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
H.H.D Kalhara	IT18139440	DKalhara

The supervisor/s should certify the proposal report with the following declaration.

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the supervisor: Prof. Pradeep Abeygunawardhana Date:

Signature of the co-supervisor: Ms. Wellalage Sasini Nuwanthika Date:

ABSTRACT

Smart manufacturing or Industrial Internet of Things (IIoT) are also known as industry 4.0, integrate smart computing and network technologies in automation and data transmission according to the ongoing trend of manufacturing and industrial practices, including Cyber Physical Systems (CPS), Cyber Physical Product Systems (CPPS), Internet of Things (IoT), robotics to create more extensive, better connected and productive systems. Smart manufacturing depends on the connection between digital and physical environment through IoT, combined with improvements such as machine learning and data analytics. Although these individual advancements have been being developed for a while, their incorporation with industrial systems raised new difficulties and advantages such as productivity.

These complex smart manufacturing technologies have become a frequent target of industrial sabotage and industrial espionage attacks because industrial 4.0 manufacturing systems are driven by focusing on the development of functionality rather than security. Therefore, the volume and sophistication of cyber threats in industrial automation systems are growing due to poor security design and cyber security requirements are not been captured. The development of the secure environment for the smart systems using CPPS platform has become complex project due to following limitations, collaborating between different systems, centralized security Management, secure communication and insecure data leading to, conflicts in design model and security model, additional cost, low product quality, violation of Confidentiality, Integrity and Availability (CIA) and difficulties in adhering to laws and regulations. Therefore, designing and automating a Computer Numerical Control cutting machine into the direction of industry 4.0 which adapts with security standards to illustrate the cyber security gap and discuss solutions to apply in the apparel industry while comparing and contrasting with current security aspects in the current industrial 4.0 automated systems in the industry is the objective of the research.

Key words – Cyber Physical Product Systems, Cyber Physical Systems, Industrial Internet of Things, Computer Numerical Control

Table of Contents

DECLARATION 3

ABSTRACT 4

LIST OF FIGURES 6

LIST OF TABLES 6

LIST OF APPENDICES 6

1. INTRODUCTION 7

1.1 Background Review 7

1.2 Literature Review 10

1.3 Research Gap 15

1.4 Research Problem 16

1.4.1 Collaboration between different systems 16

1.4.2 Centralized security management 16

1.4.3 Secure communication 16

1.4.4 Insecure data 17

1.4.5 Initial cost 17

1.4.6 Absence of methodology to industry 4.0 17

2. OBJECTIVES 18

2.1 Main Objectives 18

2.2 Specific Objectives 18

2.2.1 Audit security configurations 18

2.2.2 Centralized device configuration management 18

2.2.3 Generate audit reports 18

3. METHODOLOGY 19

3.1 System Diagram 19

3.2 Individual Component (Security Configuration) 19

3.2.1 Identify required CPS devices 20

3.2.2 Identify and evaluate security requirements of the devices 20

3.2.3 Implement a tool for security hardening 20

3.2.4 Implement report generating tool 21

3.2.5 Test security configurations ... 21
3.2.6 Integrate hardening tool to the entire solution ... 21
3.3 Gantt Chart ... 22
4. DESCRIPTION OF PERSONAL AND FACILITIES ... 23
5. BUDGET AND BUDGET JUSTIFICATION ... 24
REFERENCE LIST ... 25
APPENDICES ... 28
Appendix A: Turnitin Similarity Score ... 28

LIST OF FIGURES

Figure 1.1: Industrial revolution 8
Figure 1.2: Composition of Exports - 2019 11
Figure 3.1: Overall System Diagram 19
Figure 3.2: Individual Workflow Diagram 19
Figure 3.3: Sample Structure of the hardening tool 20
Figure 3.4: Gantt Chart 22

LIST OF TABLES

Table 1.1: Comparison of IaC configuration management platforms 15
Table 1.2: Comparison of Existing Tools 15
Table 4.1: Description of Personal and Facilities 23
Table 5.1: Budget and Budget Justification 24

LIST OF APPENDICES

Appendix A: Turnitin Similarity Score 28

1. INTRODUCTION

1.1 Background Review

With the discovery of steam power led to the first industrial revolution which was the greatest breakthrough for human productivity. Invention such as spinning machine, looms to make fabric made appearance. The first mechanical sewing machine was invented marking the beginning of the textile industry. As the first industry revolution was driven by coal, water and steam the second revolved around electricity. Gas and oil. The impact of the revolution in apparel sector is the sewing machine began to be produced in a serial manner. Third industrial revolution also known as digital revolution began with partial automation through Programmable Management Systems. Advancements in microchips, programming, fiber optic links, and telecom spaces made the digital revolution a success. the German Federal Government was first to declare the fourth industrial revolution at the Hannover Fair in 2011. The physical world is created in the virtual environment and cyber physical systems are connected, communicated with one another and with human in real time to ultimately make decisions without human involvement, aiming to develop new internet services and business models providing efficiency, transparency, fault detection, flexibility, monitoring and most importantly productivity while reducing costs. The industrial processes that have integrated with CPS and IoT will have value creation and business models, modular structures which adopt to rapidly changing requirements. Industry 4.0 garment manufacturing systems depends on the connection between digital and physical environment through IoT and other technologies such as Cyber Physical Systems, wireless sensor networks, Machine Learning, Data analytics, cyber security, cloud computing, system integration, augmented reality, 3D printing.

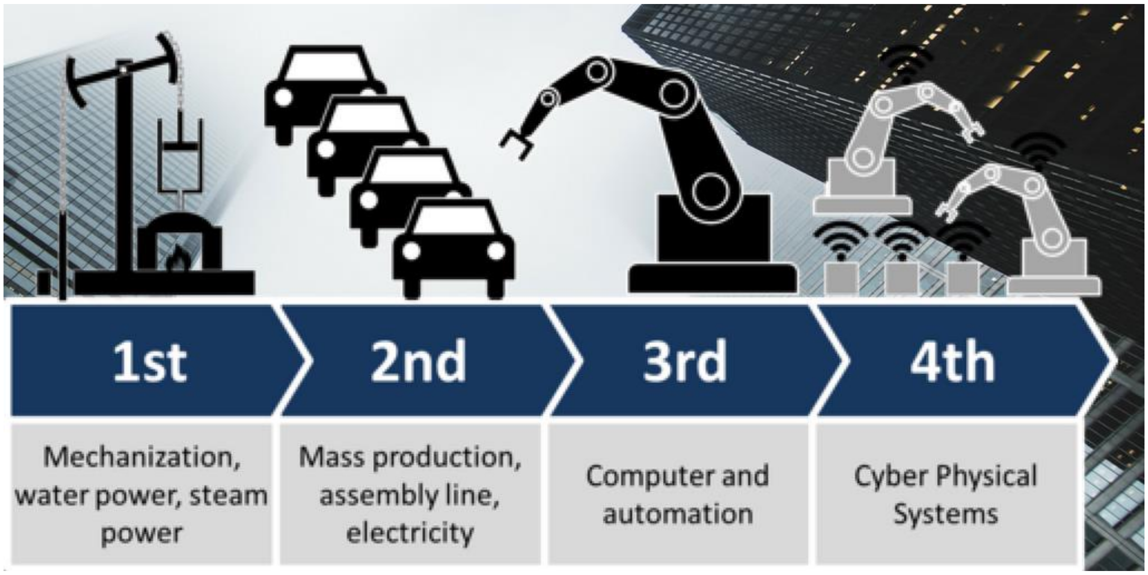

1st
Mechanization, water power, steam power
2nd
Mass production, assembly line, electricity
3rd
Computer and automation
4th
Cyber Physical Systems

Figure 1.1: Industrial revolution

Development of I-IoT to the integration of network technologies and smart computing into manufacturing for automation is the directive of industry 4.0. IoT adopts enabling the intercommunication between computers and computer related equipment to increase intelligence, efficiency, productivity as well as safety. While IoT refers to system of interrelated computing devices which communicating with each other and with people in real time it is most commonly used for consumer usage, I-IoT is used for industrial purpose such as manufacturing. Unlike IOT, I-IoT has more remarkable sorts of incorporated network technologies, command control, service requirements, and smart devices.

The apparel industry has become a significant area in the world's manufacturing field since the beginning of the first revolution. Textile field has a great history and it keep on developing due to the high adaptability for new arising technologies such as IIoT. Apparel fashion industry has become a highly competitive industry. Therefore, integrated technologies within the industry are rapidly advancing allowing innovations in the manufacturing processes. Industry 4.0 allows characteristics such as scalability, customization in massive scale, customer satisfaction and control and visibility which place a significance value in apparel industry. Nevertheless, most automation systems are evolving around garment industry.

The basic flow of the production processes in a clothing and apparel factory includes design the product according to the marketing demands and customer requirements, selecting suitable clothing material, Forming layers from the clothing materials, Cutting various shapes by minimizing the wastage of materials, different sewing operations, finishing, product quality assurance, packing, storing and distribution.

Cutting process plays a huge role in garment automation industry because of the wastage problem, availability and accessibility, labor dependency and it is an expensive process. Introduced in 1900s die cutters increased cutting efficiency and quality, Numerical Controller (NC) machines appeared in 1940s and made continuous cutting possible, leading to a greater flexibility in production and more use of material. Computer Numerically Controlled (CNC) machines was created in the digital revolution. This technological advancement made cutting the most advanced sector in apparel field. Various cutting devices such as computer-controlled knives, laser, plasma, ultrasound and markers are available. Since the first fully automated cutting system matured with enhancement in technology the existing cutting technologies developed with the aspect of productivity, versatility and pattern matching capability. Cutting processes which includes CNC machines are currently ongoing industry 4.0 revolution while addressing solutions for labor intensive problems, wastage problems and cost cutting.

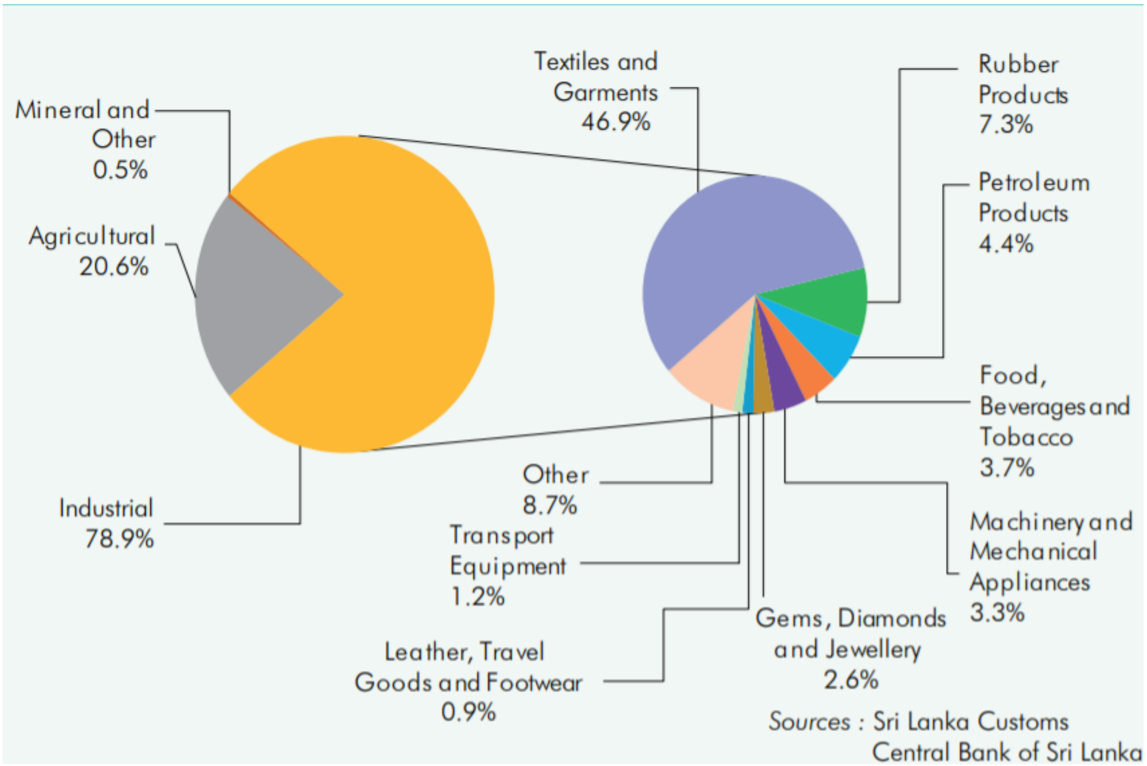
The concept of digitalization and integration has been pointed out in I-IoT or fourth industrial revolution which CNC technology plays a vital part when automating cutting garment manufacturing systems. The CNC is a hub which important data are flowing. In industry 4.0 CNC controllers should be capable of supporting integration, sensors, cloud servers. A challenge is the transaction from traditional hardware-based controllers' architecture to a smart automation software architecture. The security related problems arise as today's industrial 4.0 automation is driven by focusing on the functionality rather than security. Lack of security might lead to increasing economic damages, loss of production and even loss of life. As we know, IoT depends on the connection between digital and physical environment through IoT along with other digital technologies, industrial espionage and sabotage is massively increasing over the past years. Levels of awareness, weakness of existing measures, and preparation for future challenges is vital that is the reason for security should be important underpinning the development of the development in industry 4.0. If the industrial 4.0 manufacturing automation developers could identify the application of cyber security requirements which are not been thoroughly captured in automation and develop systems addressing all the security aspects in automation, the developing automation systems would be potentially free of huge risks and would be safe.

CPS play an essential part in cyber security for industrial 4.0 automated manufacturing systems.

The foundation of an industry 4.0 should enable garment cutting manufacturing automation including CNCs to deliver best possible performance based on security.

1.2 Literature Review

2019 Annual Report of Central bank Sri Lanka shows, 46.9% of Industrial exports are textiles and garments and 14.6% of imported intermediate goods are textiles and textile articles [1]. Adapting Industry 4.0 concepts and creating textile 4.0 manufacturing facilities will increase production rate which impacts export rates.



Sources : Sri Lanka Customs
Central Bank of Sri Lanka

Figure 1.2: Composition of Exports - 2019

Garment manufacturing systems have many processes such as knitting, cutting, sewing, finishing, product quality assurance, packing, storing and distribution. Textile industry produces 60 billion square meters of scarp fabrics per year [2]. Most of the scarp fabrics are generated by cutting process. Abu Sadat Muhammad Sayem and Shreshta Ramkalaon [2] introduced Zero-Waste Pattern Cutting (ZWPC) to overcome this problem. Modern textile industry uses CNC based cutting machines to automate cutting process with the assistance of Computer Aided Designing (CAD) and Computer Aided Manufacturing (CAM) programs. In Industry 4.0 cutting process can be automated using a CPS with smart CNC and IoT devices.

CPS

As shown by many researches CPS and IoT sharing same basic architecture. The cyber-physical system is presented a high combination and coordination between physical components and computational components on IoT. There are two main layers CPS architecture. The physical layer does these tasks, captures sensed data, performs actions according to commands received from cyber layer and send captured data back to cyber layer. The cyber layer does these tasks, processes data received from physical layer and issue required commands to physical layer [4].

When considering cyber-attacks against CPS, Stuxnet worm is a malware to target CPS. This conventional cyber warfare weapon’s goal is to physically destroy its target rather than steal, manipulate, or erase information [5]. In 2010, Stuxnet worm was successful on infecting itself to Iranian nuclear facility at Natanz and gain access to the operating systems at the facility through four zero-day vulnerabilities. Stuxnet achieved it goal by disrupting power to centrifuges which resulted to stop Iranian nuclear program [6].

Stuxnet attack proved that consideration of CIA triad is not sufficient for CPS security. According to CPS security analysis done by Yosef Ashibani and Qusay H. Mahmoud [7] suggests following characteristics to be considered when securing CPS.

Securing access to devices

As mentioned before CPS contains different kinds of devices such as IoT devices, sensors, CNCs, and RFIDs securing access to these devices is challenging because some of these devices have poorly implemented or configured authentication systems [8]. As a result, unauthorized access to the systems are easier compared to gaining authorized access to computer systems. The Open Web Application Security Project (OWASP) states that CPS and IoT devices have hardcoded passwords or weak guessable passwords which can be brute forced easily and some of these passwords are publicly available [9]. OWASP also states that these devices have lack of physical security that allows side channel attacks. Attackers can guess or recreate actions performed by these devices by launching side channel attack that analyzes sounds or electrical signals made by the devices [10].

Securing data transmissions

Like other network devices CPS are also vulnerable to Denial of Service (DoS) attacks which disrupt the network activities and make CPS unavailable [11]. OWASP states that CPS devices have insecure network service that are unnecessary services running on the devices and exposed to the internet [9], allowing these devices to remote controlled by unauthorized sources. Due to their low data processing abilities and storage capacities some CPS devices can not considered as complete computer systems [12]. Moreover, most CPS device manufactures focus on functionality over security or reliability. This makes CPS devices more vulnerable to following attacks malware, unauthorized access, eavesdropping, and Distributed Denial of Service (DDoS) attacks [7].

Securing applications

The main security challenge associated with application layer is privacy. Other security challenges have rare chance of occurrence in the application layer. In the context of garment manufacturing, data such as fashion design templates and employee data can be considered as private data. Loss of privacy leads to legal fines and penalties. Therefore, applications used CPS need to be protected [13]. OWASP confirms that these applications have lack of privacy protection [9].

Securing data storage

Most CPS devices are resource-constrained nodes that does not protect data at rest [11]. Memory and processing power limited in CPS devices such as sensors. Because of this requires lightweight ciphers to encrypt data at rest [14]. Most software-based solutions do not use lightweight cipher. That makes these software-based solutions incompatible with CPS devices.

Securing actuation

Since CPSs can perform physical actions any command to provided to a device in CPS should issue from trusted and authorized sources. Securing actuation prevents CPS from preforming based on rogue feedbacks and commands issued by adversaries [12]. If the CPSs are controlled over an internet connection it involves internet related following attack types replay attacks, eavesdropping, spoofing, Man in the middle attacks, and compromised keys. Therefore, security must implement for the whole system [11].

OWASP mentions [9] that insecure default settings these devices shipped with, lack of update and device management after deploying in production may lead to above mentioned security issues.

Due to large number of devices, managing these devices manually one by one is time consuming. Therefore, adapting Infrastructure as Code (IaC) is required to reduce time consumption. IaC is one of the main tactics used by DevOps to automate logic for deploying, configuring, and updating devices [15]. Configuration management and update management facilities in IaC is required for securing CPS devices. Therefore, Configuration management IaC platforms such as Chef, Puppet, Ansible and SaltStack [16] are suitable candidate automation platform for the task.

Puppet is an opensource configuration management tool that has master-agent architecture. Puppet master runs on a Linux/Unix server and puppet agent can be installed on Windows/Linux/Unix clients. Puppet requires certificate signing between master and agents. Puppet uses Puppet DSL (Domain Specific Language) for configuration management [17].

Chef is an opensource configuration management tool that has similar characteristics to Puppet. It has master-agent architecture, where Chef master runs on a Linux/Unix server and Chet agent runs on Windows/Linux/Unix clients. Chef has an extra component called workstation, where Chef tests its all configurations. Chef uses Domain Specific Language (DSL) Ruby to manage configurations [18].

Ansible is an opensource configuration management platform developed by RedHat. Ansible has client-server architecture where server must be a Linux/Unix machine and clients can be Windows/Linux/Unix machine. It only requires Secure Shell (SSH) connection between server and clients. It does not require a special agent to installed on clients. Ansible uses “YAML Ain’t Markup Language” (YAML) to manage configurations [19]. As its' name states YAML is a human readable data-serialization language and it is not markup language.

SaltStack is an opensource configuration management tool that has master-client architecture. Salt master runs on a Linux/Unix server and Salt minion (agent) runs on Windows/Linux/Unix clients. SaltStack uses YAML to manage configurations [20].

Table 1.1: Comparison of IaC configuration management platforms

	Puppet	Chef	Ansible	SaltStack
Code	Opensource	Opensource	Opensource	Opensource
Language	Puppet DSL	Ruby	YAML	YAML
Ease of Setup	Difficult	Difficult	Easy	Difficult

1.3 Research Gap

There are several industrial tools for security configurations or system hardening such as OpenSCAP and CIS-CAT Pro. But these tools are used for server hardening and none of these tools are capable of hardening following CPS device based operating systems Raspberry Operating System and Robot Operating System (ROS). Proposed tool is mainly focused on CPS device operating system hardening which include above mentioned operating systems and Ubuntu Linux to automate security configuration and minimize the system downtime. The following table illustrates a comparison of operating system configuration capability existing tools and proposed tool.

Table 1.2: Comparison of Existing Tools

	OpenSCAP	CIS-CAT Pro	Proposed tool
Ubuntu Linux	✗	✓	✓
Robot OS	✗	✗	✓
Raspberry OS	✗	✗	✓

1.4 Research Problem

When automating a manual system or semi – automated system towards Industry 4.0 smart computing is integrated with technologies including IoT, cognitive computing, machine learning and data analytics. Most system developers do not entirely recognize the cyber security challenges when designing an industrial 4.0 automated system. The research is to identify the application of cyber security requirements which are not been thoroughly captured in automation.

Challenges:

The development of the secure network environment

Industry 4.0's network environment is developed using a CPPS platform. developing the CPPS platform has become a difficult project due to following limitations,

1.4.1 Collaboration between different systems

A Collaborative model between computer systems and physical devices is essential for exchanging information, [21] store information, documentation, decision making, corrective and preventive action.

1.4.2 Centralized security management

Creating CPS models to apply security configurations/updates to physical devices and monitor physical devices using a centralized control system such as Supervisory control and data acquisition (SCADA) to maximize efficiency [22]. Software, physical devices environment, hardware platforms, and other functional and non-functional must consider in a typical CPS model in addition to CPS modeling language [21].

1.4.3 Secure communication

CPS that use the SCADA systems is connected to the internet over TCP/IP protocols without additional protection [23], which have known vulnerabilities.

1.4.4 Insecure data

Manufacturing companies neglect data security when moving towards Industry 4.0. The IoT-based CPSs that are connected to many of embedded sensors and communication devices present a significant risk linked with the growth of data usage and the much higher risks of system breaches [24].

1.4.5 Initial cost

Migration to industry 4.0 is not an instantaneous process, in a manufacturing company will result in end-to-end integration to plan and execute the engineering according to the business needs impressive introductory interest in the matter of cost and time is required [25].

1.4.6 Absence of methodology to industry 4.0

Absence of dynamic vital arrangement to help the movement to Industry 4.0 [26].

2. OBJECTIVES

2.1 Main Objectives

A tool for automating security configurations for CPS devices is the main objective of this research component. These CPS devices have insecure configurations by default and these devices have shorter life cycle compared to computer systems. Therefore, system operators/administrators must apply security configurations frequently. Doing the configurations manually is inefficient and have increased downtime. The solution is to develop a tool that is capable of automating security configurations to reduce system downtime.

2.2 Specific Objectives

2.2.1 Audit security configurations

In this proposed tool, there is a function to audit security configuration to verify that security configurations are properly applied to the CPS devices. Audit function is mainly to be written using bash and python and ansible is used to transport the scripts to the CPS devices. Audit function stores results as comma separated values.

2.2.2 Centralized device configuration management

The proposed tool is to be installed on an ansible controller that runs CentOS. Secure Shell (SSH) connections are establish between ansible controller and CPS devices using SSH keypairs or password-based authentication. The purpose of the ansible controller is to centralize CPS devices' configuration management.

2.2.3 Generate audit reports

In this proposed tool, there is a function to generate reports based on audit result. The report contains following details, configuration name, rationale, severalty, and description. Therefore, these audit reports can be used to illustrate the security configurations that have made to the system.

3. METHODOLOGY

3.1 System Diagram

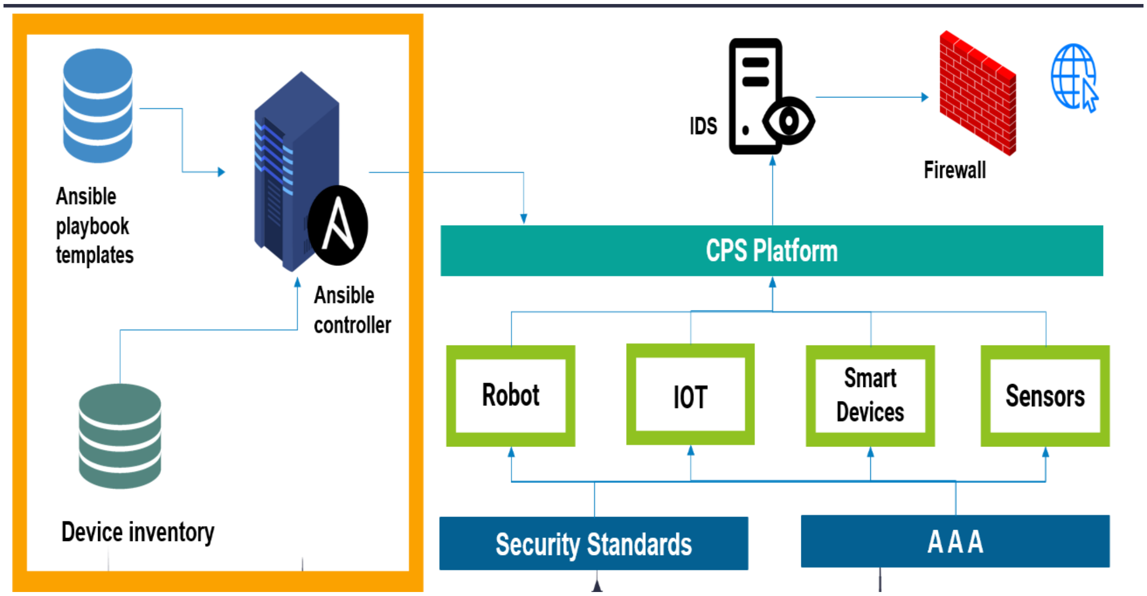


Figure 3.1: Overall System Diagram

3.2 Individual Component (Security Configuration)

Below Individual workflow will be followed by myself during this research.

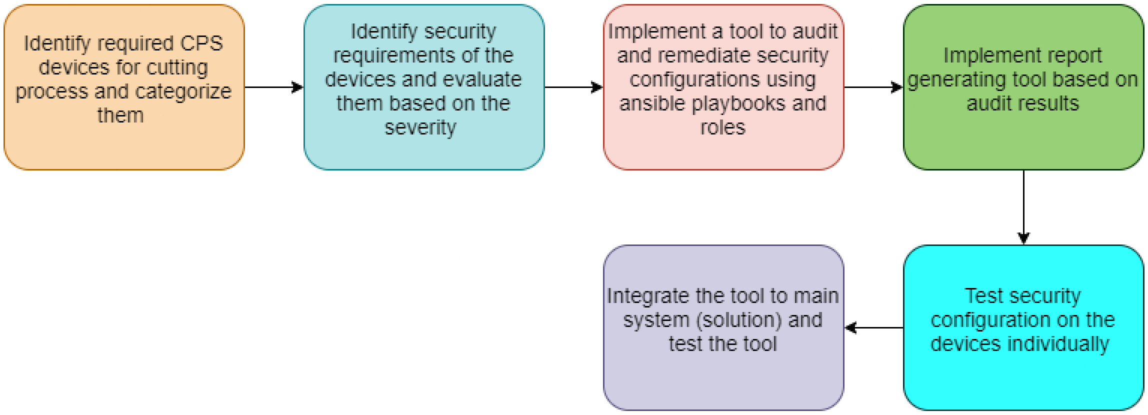

Identify required CPS devices for cutting process and categorize them
Identify security requirements of the devices and evaluate them based on the severity
Implement a tool to audit and remediate security configurations using ansible playbooks and roles
Implement report generating tool based on audit results
Test security configuration on the devices individually
Integrate the tool to main system (solution) and test the tool

Figure 3.2: Individual Workflow Diagram

3.2.1 Identify required CPS devices

A CNC cutter is the main component of the CPS based cutting system. Additionally, several IoT devices and sensors are required to take measurements to ensure quality of the product.

These identified devices required to be categorized based on their device type to simplify future security implementations.

3.2.2 Identify and evaluate security requirements of the devices

This can be done by analyzing CPS related attacks and security surveys identify security requirements of each device and category identified in step 1 and performing risk analysis to identify security threats related to CPS devices. After identifying security requirements prioritize them according to severity of threats and importance of security requirements.

3.2.3 Implement a tool for security hardening

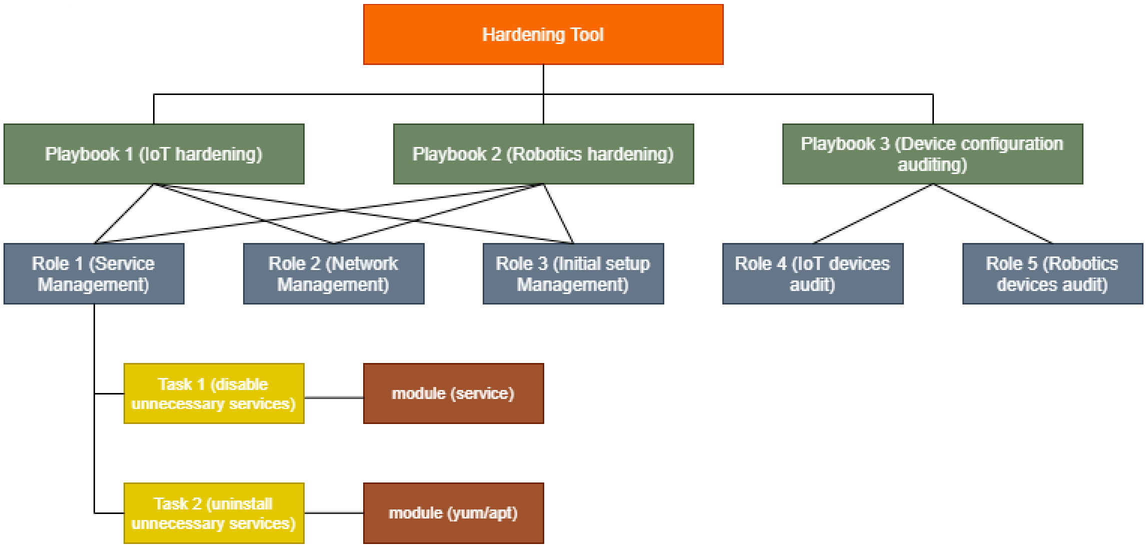

Hardening Tool
Playbook 1 (IoT hardening)
Playbook 2 (Robotics hardening)
Playbook 3 (Device configuration auditing)
Role 1 (Service Management)
Role 2 (Network Management)
Role 3 (Initial setup Management)
Role 4 (IoT devices audit)
Role 5 (Robotics devices audit)
Task 1 (disable unnecessary services)
module (service)
Task 2 (uninstall unnecessary services)
module (yum/apt)

Figure 3.3: Sample Structure of the hardening tool

Implement Ansible tasks to configure security and achieve required security requirements in 2nd step. These tasks can be included in ansible roles. Based on categorized device types in 1st step ansible playbooks can be created to access ansible roles to create a tool for security hardening as above. Additionally, above structure allows another members' security implementation to be included to the tool.

3.2.4 Implement report generating tool

This tool is used generate html report that can be represent to the customer. This tool uses python pandas library to read audit results (ex: result.csv) then it uses bootstrap 4 data tables to generate html reports.

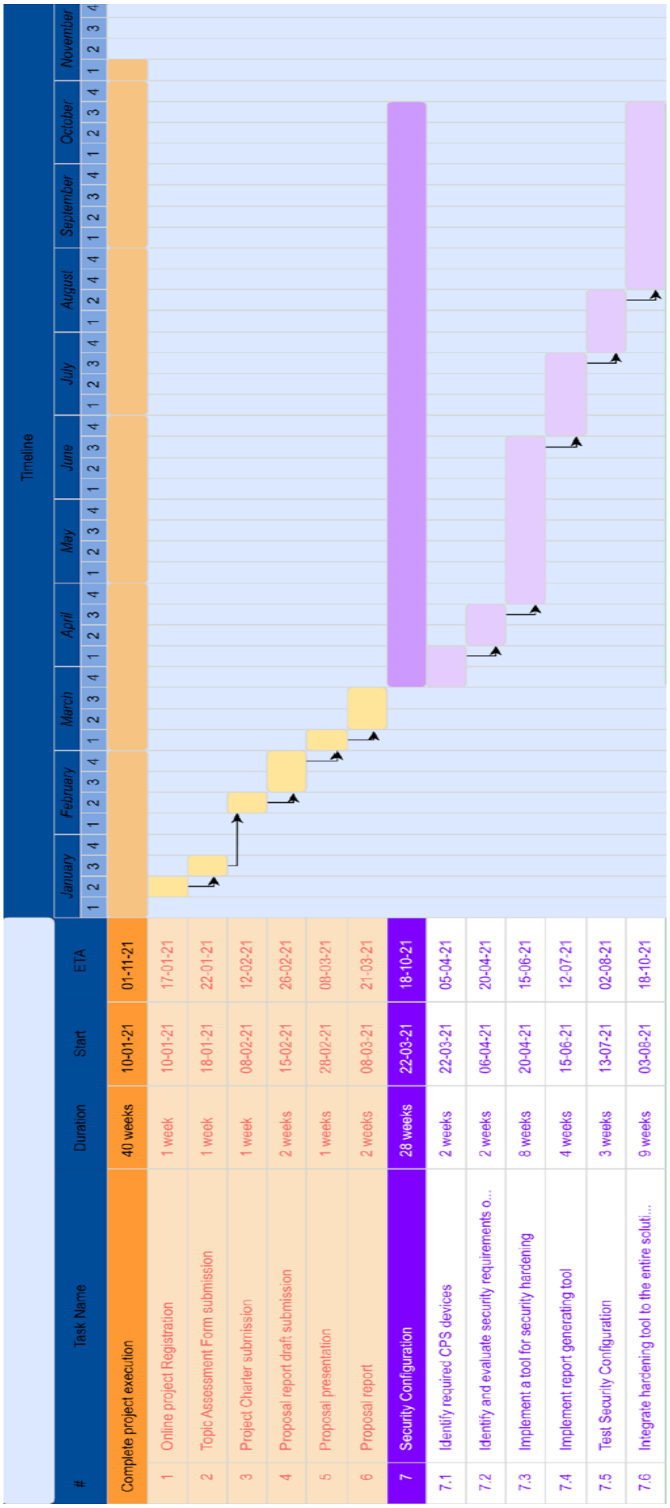
3.2.5 Test security configurations

Since most CPS devices have low memory and processing powers before testing security configurations first, implement required functionality of the devices and analyze the resource usage of the devices. Then assign security configurations based on severity identified in 2nd step and monitor device usage to avoid putting heavy constraint due to security configurations. Create optimal security profiles for each device types based on the analysis.

3.2.6 Integrate hardening tool to the entire solution

Integrate hardening tool with a Django application and host the application in Apache HTTP server which can be accessed over the internet.

3.3 Gantt Chart



#	Task Name	Duration	Start	ETA
	Complete project execution	40 weeks	10-01-21	01-11-21
1	Online project Registration	1 week	10-01-21	17-01-21
2	Topic Assessment Form submission	1 week	18-01-21	22-01-21
3	Project Charter submission	1 week	08-02-21	12-02-21
4	Proposal report draft submission	2 weeks	15-02-21	26-02-21
5	Proposal presentation	1 weeks	28-02-21	08-03-21
6	Proposal report	2 weeks	08-03-21	21-03-21
7	Security Configuration	28 weeks	22-03-21	18-10-21
7.1	Identify required CPS devices	2 weeks	22-03-21	05-04-21
7.2	Identify and evaluate security requirements o...	2 weeks	06-04-21	20-04-21
7.3	Implement a tool for security hardening	8 weeks	20-04-21	15-06-21
7.4	Implement report generating tool	4 weeks	15-06-21	12-07-21
7.5	Test Security Configuration	3 weeks	13-07-21	02-08-21
7.6	Integrate hardening tool to the entire soluti...	9 weeks	03-08-21	18-10-21

Figure 3.4: Gantt Chart

4. DESCRIPTION OF PERSONAL AND FACILITIES

Table 4.1: Description of Personal and Facilities

Registration no	Name	Task Description
IT18139440	H.H.D Kalhara	• A Python tool to automate security configurations. • Add new audit and remediations to the python tool. • Select and deselect remediations to create optimize compliance profile based on resource usage of the devices. • A report generating function to generate audit reports. • Testing

5. BUDGET AND BUDGET JUSTIFICATION

Table 5.1: Budget and Budget Justification

Item(s)	Cost (LKR)
Web server hosting	5000.00
Firewall + IDS/IPS hardware	18000.00
Physical security system hardware	5000.00
Raspberry Pi 3	12000.00
Total	**40000.00**

REFERENCE LIST

[1] “Annual Report 2019 | Central Bank of Sri Lanka.” https://www.cbsl.gov.lk/en/publications/economic-and-financial-reports/annual-reports/annual-report-2019 (accessed Feb. 26, 2021).

[2] S. Ramkalaon and A. S. M. Sayem, “Zero-Waste Pattern Cutting (ZWPC) to tackle over sixty billion square metres of fabric wastage during mass production of apparel,” The Journal of The Textile Institute, vol. 0, no. 0, pp. 1–11, Jun. 2020, doi: 10.1080/00405000.2020.1779636.

[3] T. Lu, J. Lin, L. Zhao, Y. Li, and Y. Peng, “A Security Architecture in Cyber-Physical Systems: Security Theories, Analysis, Simulation and Application Fields,” IJSIA, vol. 9, no. 7, pp. 1–16, Jul. 2015, doi: 10.14257/ijsia.2015.9.7.01.

[4] R. Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” IEEE Security Privacy, vol. 9, no. 3, pp. 49–51, May 2011, doi: 10.1109/MSP.2011.67.

[5] “What Is Stuxnet? | McAfee.” https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html (accessed Feb. 27, 2021).

[6] Y. Ashibani and Q. H. Mahmoud, “Cyber physical systems security: Analysis, challenges and solutions,” Computers & Security, vol. 68, pp. 81–97, Jul. 2017, doi: 10.1016/j.cose.2017.04.005.

[7] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, and Y. Jin, “Cyber-physical systems: A security perspective,” in 2015 20th IEEE European Test Symposium (ETS), May 2015, pp. 1–8, doi: 10.1109/ETS.2015.7138763.

[8] “OWASP Internet of Things Project - OWASP.” https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 (accessed Feb. 28, 2021).

[9]M. A. A. Faruque, S. R. Chhetri, A. Canedo, and J. Wan, “Acoustic Side-Channel Attacks on Additive Manufacturing Systems,” in 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Apr. 2016, pp. 1–10, doi: 10.1109/ICCPS.2016.7479068.

[10] S. Raza, ‘Lightweight Security Solutions for the Internet of Things’, PhD dissertation, Mälardalen University, Västerås, Sweden, Västerås, Sweden, 2013.

[11] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, “Security Issues and Challenges for Cyber Physical System,” in 2010 IEEE/ACM Int’l Conference on Green Computing and Communications Int’l Conference on Cyber, Physical and Social Computing, Dec. 2010, pp. 733–738, doi: 10.1109/GreenCom-CPSCom.2010.36.

[12] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” Wireless Netw, vol. 20, no. 8, pp. 2481–2501, Nov. 2014, doi: 10.1007/s11276-014-0761-7.

[13] T. Lu, B. Xu, X. Guo, L. Zhao, and F. Xie, “A New Multilevel Framework for Cyber-Physical System Security,” p. 2.

[14] W. Hummer, F. Rosenberg, F. Oliveira, and T. Eilam, “Testing Idempotence for Infrastructure as Code,” in Middleware 2013, vol. 8275, D. Eyers and K. Schwan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 368–388.

[15]P. Masek, M. Stusek, J. Krejci, K. Zeman, J. Pokorny, and M. Kudlacek, “Unleashing Full Potential of Ansible Framework: University Labs Administration,” in 2018 22nd Conference of Open Innovations Association (FRUCT), Jyvaskyla, May 2018, pp. 144–150, doi: 10.23919/FRUCT.2018.8468270.

[16] P. Webteam, “Welcome to Puppet 7.4.1.” https://puppet.com/docs/puppet/7.4/puppet_index.html (accessed Mar. 03, 2021).

[17] “Chef Documentation.” https://docs.chef.io/ (accessed Mar. 03, 2021).

[18] “Ansible Documentation — Ansible Documentation.” https://docs.ansible.com/ansible/latest/index.html (accessed Mar. 03, 2021).

[19] “SaltStack Documentation.” https://docs.saltproject.io/en/latest/ (accessed Mar. 03, 2021).

[20] K. Zhou, Taigang Liu, and Lifeng Zhou, “Industry 4.0: Towards future industrial opportunities and challenges,” in 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, Aug. 2015, pp. 2147–2152, doi: 10.1109/FSKD.2015.7382284.

[21] H. Xu, W. Yu, D. Griffith, and N. Golmie, “A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective,” IEEE Access, vol. 6, pp. 78238–78259, 2018, doi: 10.1109/ACCESS.2018.2884906.

[22] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. Al Faruque, “Security trends and advances in manufacturing systems in the era of industry 4.0,” in 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, Nov. 2017, pp. 1039–1046, doi: 10.1109/ICCAD.2017.8203896.

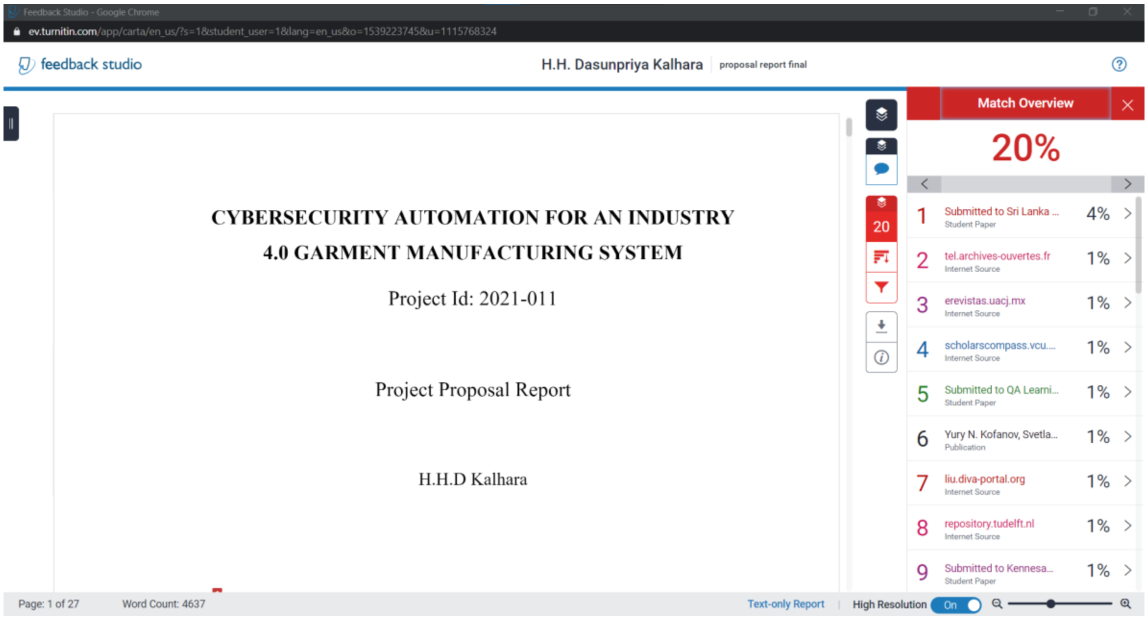
[23] Kamble, S., Gunasekaran, A. and Gawankar, S., 2020. Sustainable Industry 4.0 Framework: A Systematic Literature Review Identifying The Current Trends And Future Perspectives.

[24] Lins, Theo & Rabelo, Ricardo & Correia, Luiz & Sá Silva, Jorge. (2018). Industry 4.0 Retrofitting. 8-15. 10.1109/SBESC.2018.00011.

[25] Moktadir, M., Ali, S., Kusi-Sarpong, S. and Shaikh, M., 2019. Assessing Challenges For Implementing Industry 4.0: Implications For Process Safety And Environmental Protection.

APPENDICES

Appendix A: Turnitin Similarity Score



Feedback Studio - Google Chrome

ev.turnitin.com/app/carta/en_us/?s=1&student_user=1&lang=en_us&o=1539223745&u=1115768324

feedback studio

H.H. Dasunpriya Kalhara | proposal report final

CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM

Project Id: 2021-011

Project Proposal Report

H.H.D Kalhara

Match Overview

20%

1	Submitted to Sri Lanka ... Student Paper	4%
2	tel.archives-ouvertes.fr Internet Source	1%
3	erevistas.uacj.mx Internet Source	1%
4	scholarscompass.vcu.... Internet Source	1%
5	Submitted to QA Learni... Student Paper	1%
6	Yury N. Kofanov, Svetla... Publication	1%
7	liu.diva-portal.org Internet Source	1%
8	repository.tudelft.nl Internet Source	1%
9	Submitted to Kennesa... Student Paper	1%

Page: 1 of 27 Word Count: 4637

Text-only Report | High Resolution On