

# **CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM**

2021-11

Project Proposal Report

A.D.H Jinadasa

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**

2021-11

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   |
|----------------|------------|---|
| A.D.H Jinadasa | IT18132410 |  |

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.

**Keywords** – *Cyber Physical Product Systems, Cyber Physical Systems, Industrial Internet of Things, Computer Numerical Control*

## Table of Contents

|   |    |
|---|----|
| DECLARATION .....   | 3  |
| ABSTRACT.....   | 4  |
| LIST OF TABLES .....  | 6  |
| 1. INTRODUCTION .....   | 7  |
| 1.1 Background Review.....  | 7  |
| 1.2 Literature Review.....  | 10 |
| 1.2.1 CPS & IOT.....  | 10 |
| 1.2.2 Threats and vulnerabilities in CPS .....                                | 11 |
| 1.2.3 Threats and vulnerabilities in IOT .....                                | 11 |
| 1.2.4 CPS attack incidents.....   | 12 |
| 1.2.5 Firewall & intrusion detection system (IDS) .....                       | 13 |
| 1.3 Research Gap .....  | 14 |
| 1.4 Research Problem .....  | 15 |
| 1.4.1 Collaboration between different systems .....                           | 15 |
| 1.4.2 Centralized security management .....                                   | 15 |
| 1.4.3 Secure communication.....   | 15 |
| 1.4.4 Insecure data .....   | 15 |
| 1.4.5 Initial cost.....   | 16 |
| 1.4.6 Absence of methodology to industry 4.0 .....                            | 16 |
| 2. OBJECTIVES .....   | 17 |
| 2.1 Main Objectives .....   | 17 |
| 2.2 specific Objectives .....   | 17 |
| 3. METHODOLOGY .....  | 18 |
| 3.1 System Diagram.....   | 18 |
| 3.2 Individual Component (Network Security).....                              | 18 |
| 3.2.1 Identify required CPS devices.....                                      | 19 |
| 3.2.2 Identify and evaluate security requirements of the devices .....        | 19 |
| 3.2.3Configure firewall and define rules based on security requirements ..... | 19 |
| 3.2.4 Implement IDS using hybrid approach & add rules.....                    | 19 |
| 3.2.5 Report & alert generating interface based on security logs .....        | 20 |
| 3.2.6 Test implemented security measures. ....                                | 20 |
| 3.3 Gantt Chart.....  | 21 |

|   |    |
|---|----|
| 4. DESCRIPTION OF PERSONAL AND FACILITIES ..... | 22 |
| 5. BUDGET AND BUDGET JUSTIFICATION .....        | 23 |
| REFERENCES .....                                | 24 |
| APPENDICES .....                                | 26 |
| Appendix A: Turnitin Similarity Score.....      | 26 |

## LIST OF FIGURES

|   |    |
|---|----|
| Figure 1-1: Industrial revolution .....       | 7  |
| Figure 1-2: CPS & IOT .....                   | 10 |
| Figure 1-3 CPS challenges.....                | 11 |
| Figure 1-4: IOT threats .....                 | 12 |
| Figure 3-1: Overall System Diagram .....      | 18 |
| Figure 3-2: Individual Workflow Diagram ..... | 18 |
| Figure 3-3: Network monitoring process .....  | 19 |

## LIST OF TABLES

|                                       |    |
|---------------------------------------|----|
| Table 1-1: Detection methods .....    | 13 |
| Table 1-2: Solutions comparison ..... | 14 |
| Table 4-1: Task Description .....     | 22 |
| Table 5-1: Budget .....               | 23 |

# 1. INTRODUCTION

## 1.1 Background Review

The first industrial revolution commenced with the discovery of steam power 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. Developments in microprocessors, software, fiber optic cables, and telecommunication domains made the digital revolution a success. The Fourth Industrial Revolution was first announced by the German Federal Government 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 technical integration of Cyber Physical Systems and use of IoT into industrial processes will have value creation and business models, modular structures which adopt to rapidly changing requirements. Industry 4.0 garment manufacturing systems relies on the creation of bridge between digital and physical environment through IoT and other technologies such as Cyber Physical Systems, wireless sensor networks, Machine Learning, Data analytics, augmented reality, cloud computing, 3D printing, system integration, cyber security.

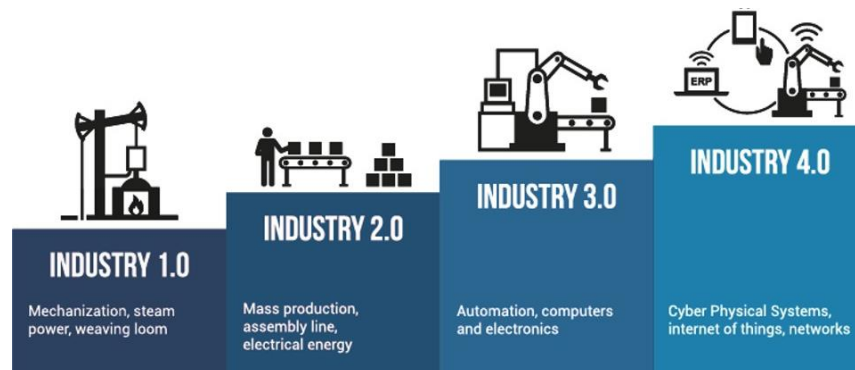


Figure 1-1: Industrial revolution

Development of I-IoT to the integration of smart computing and network technologies in manufacturing for automation is the vision of industry 4.0. IoT adopts enabling the interconnection of computers and computer related equipment to improve productivity, efficiency, intelligence as well as safety [7]. 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 unique types incorporated smart devices, network technologies, command control and service requirements.

The apparel industry has become an important sector 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 n 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 [8].

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 relies on the creation of a bridge between digital and physical environment through IoT coupled with other digital technologies, industrial espionage and sabotage is massively increasing over the past years. Weakness of existing measures, levels of awareness 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.

Cyber physical systems play a vital role in cyber security for industrial 4.0 automation 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

Industrial revolutions are significant milestone that reshape the course of mankind. After discovering steam power revelations have in a rapid pace and fourth industrial revolution now in progress. Novel changes in industry 4.0 takes keen interest from manufacturing plants. It is important for manufacturing plants around the world with productivity, customization features and operational efficiency. Industry 4.0 provide a way to deal with high volume of data, developing cyber physical systems and enhanced communication to link the digital and physical components. [1]

With industry 4.0 increasing intercommunication and data density lead to new challenges specially in cyber security. Cyber security become a major concern that should follow at the highest level of significance. With the advancement of network capabilities, cyber-attacks have become more frequent for various motivations such as financial & strategic reasons. Stakeholders that use IOT systems are affected by this problem. For the most part large organizations are exposed to cyber-attacks that cause in significant financial weight additionally to losses such as data corruption, system crashes, privacy breaches, prestige, trust and reputation. [2]

### 1.2.1 CPS & IOT

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.

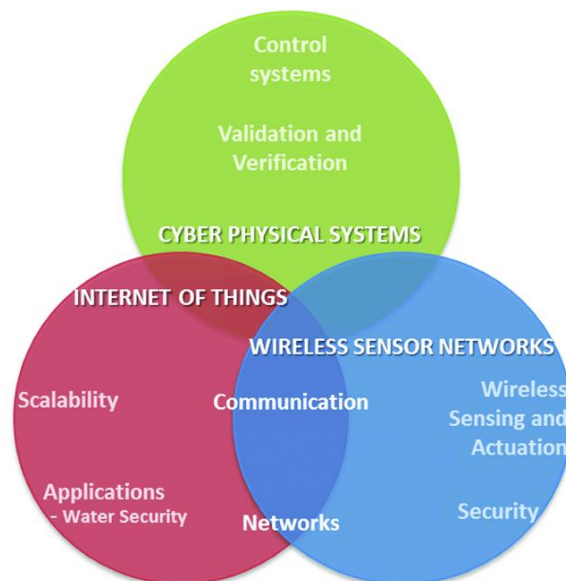


Figure 1-2: CPS & IOT

### 1.2.2 Threats and vulnerabilities in CPS

Out of the challenges listed in figure 2 below, security is the major challenge or issue. Security can be categorized as data security and control security. Data security focuses on data protection in storing and in transferring. Control security focus on operations and control systems. A unique characteristic of cyber physical threats are they mostly originate in cyberspace but impact on the physical system.

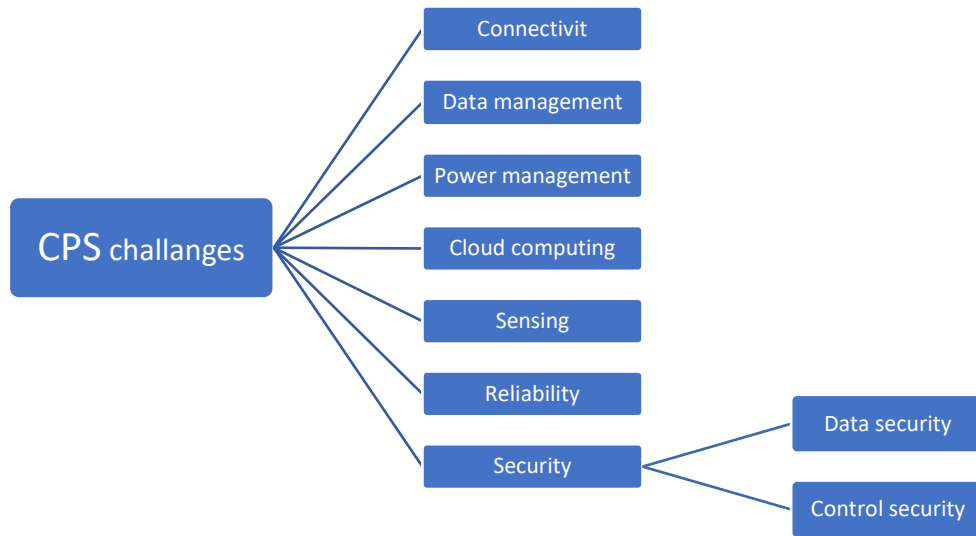


Figure 1-3 CPS challenges

Vulnerabilities can define as violation of security policy of the CPS. These vulnerabilities can occur due to lack of security rules, weak system design. The Vulnerabilities have been found in hardware, software, design policies, procedures, users themselves and misconfiguration of the cyber-physical systems. Well, known categories of vulnerabilities of a cyber-physical system are hardware vulnerabilities, software vulnerabilities, network vulnerabilities, platform vulnerabilities, management vulnerabilities. The classification of CPS threats consists with denial of service (DOS), Spoofing, Tampering, disclosure and repudiation.

### 1.2.3 Threats and vulnerabilities in IOT

In generally IOT is a combination of four levels as shown in figure 4. The spread of IOT devices is exponential. This has created a need for reliable security. The number of sophisticated cyber-attacks are increasing every day. For IoT to achieve its full capabilities, protection against threats and vulnerabilities is a must. [2]

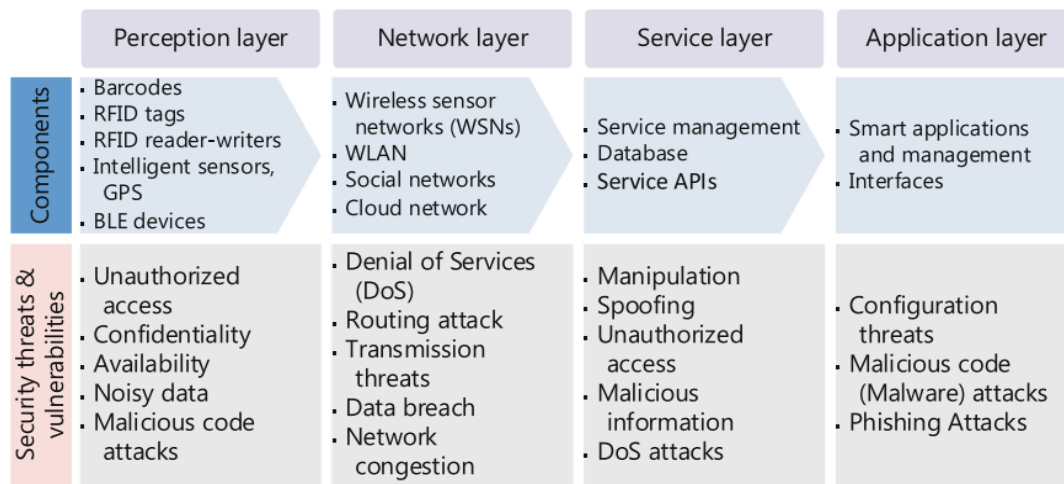


Figure 1-4: IOT threats

### 1.2.4 CPS attack incidents

These are some extreme cases of CPS incidents from various sources.

- Stuxnet

In the year 2010, a worm known as Stuxnet attacked at nuclear facilities in Iran. Stuxnet is a combination of 4 zero-day vulnerabilities. The worms used default passwords to access the operating systems of Windows that run PCS7 and WinCC programs. [4]

- Saudi Aramco attacks

An externally originated virus attacked Saudi Aramco Oil corporation by infecting 30,000 workstations. The company suspected this attack is a counter attack from Iranian government. However, Aramco Oil corporation forced to isolate their electronic systems from outside. [5]

- Mirai Botnet

Mirai botnet infects IOT devices and controlling them as a Zombie network for malicious activities. Mirai targets the devices with default username and password which are set by the manufacturers [11]

### 1.2.5 Firewall & intrusion detection system (IDS)

CPS components and the “things” in IOT such as sensors, smart devices are commonly having less processing power and have the ability to exchange data via the internet. Even though benefits outweigh the disadvantages. Industry 4.0 security and privacy challenges cannot be ignored. Securing smart devices is not a priority for manufacturers. Firewall and IDS have the ability to monitor the network for anomalies, malicious activities and policy violations. There are two main types of detection mechanisms, namely signature-based and anomaly-based detection, the combination of these two mechanisms known as hybrid method [13]. Signature-based detection uses already collected attack signatures that stored in a database, when comes to anomaly based it has the ability to identify the behavior patterns. [9],[10]

| <i>Anomaly-based detection</i>         |  |
|--|--|
| Pro                                    | Con  |
| Detect unknown attacks                 | High amount of false positive & false negative |
| Better protection against DDOS attacks | Need to define rules and profiles              |
| <i>Signature-based detection</i>       |  |
| Pro                                    | Con  |
| High accuracy, less false positive     | Needs frequent database updates                |
| Easy to configure and maintain         | Cannot detect Zero-day attacks [14]            |

Table 1-1: Detection methods

### 1.3 Research Gap

Industrial 4.0 transaction from traditional hardware-based controllers' architecture to a secure smart automation software architecture is a challenge. The security related problems arise as today's industrial 4.0 automation is driven by focusing on the functionality rather than security.

The research focusses on designing an automated system focusing cyber security aspects to the identified garment manufacturing system, according to the external supervisor's advice from the manufacturing field, while considering security threats and drawbacks of current automated garment manufacturing systems in the local industry. After designing the automated system, will consider the problems encountered while implementing the system and analyze whether those security problems are encountered in the current local industrial automated systems, in order to find the security gap between the current industrial automated garment manufacturing systems currently available locally and the proposed system for the research.

Designing and implement a private network with a firewall and an intrusion detection & prevention system to improve security and provide network monitoring and alerts, even though the industrial IDS/IPS solutions are capable of providing reliable security, these solutions are expensive and technical details are not readily available. Our goal is to design a cost effective, lightweight yet reliable IDS/IPS system with a dashboard for easy configurations. [11]

| Product           | HIDS/NIDS | Signature based | Anomaly based | Base Price       |
|-------------------|-----------|-----------------|---------------|------------------|
| McAfee NSP        | NIDS      | ✓               | ✓             | \$ 10,995        |
| Cisco Firepower   | HIDS      | ✓               | ✓             | \$ 100,000       |
| CrowdStrike       | HIDS      | ✓               | ✓             | \$ 4,000         |
| Tipping Point     | HIDS      | ✓               | X             | \$ 6,000         |
| Proposed Solution | NIDS      | ✓               | ✓             | Less than \$ 500 |

Table 1-2: Solutions comparison

## **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, [2] 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 [3]. 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 [2].

### **1.4.3 Secure communication**

CPS that uses the SCADA systems is connected to the internet over TCP/IP protocols without additional protection [4], which have known vulnerabilities. 17

### **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 [5].

#### **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 [6].

#### **1.4.6 Absence of methodology to industry 4.0**

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



## **2. OBJECTIVES**

### **2.1 Main Objectives**

The main objective of this research component is to implement a firewall and lightweight yet reliable IDS/IPS system. In order to monitor the network for anomalies, malicious activities, policy violations and alert the user.

### **2.2 specific Objectives**

- Provide easy access dashboard to the user.
- Visualize network behavior to user.
- Enable add/ remove firewall rules through the dashboard.
- Alert user when an anomaly occurs.

### 3. METHODOLOGY

#### 3.1 System Diagram

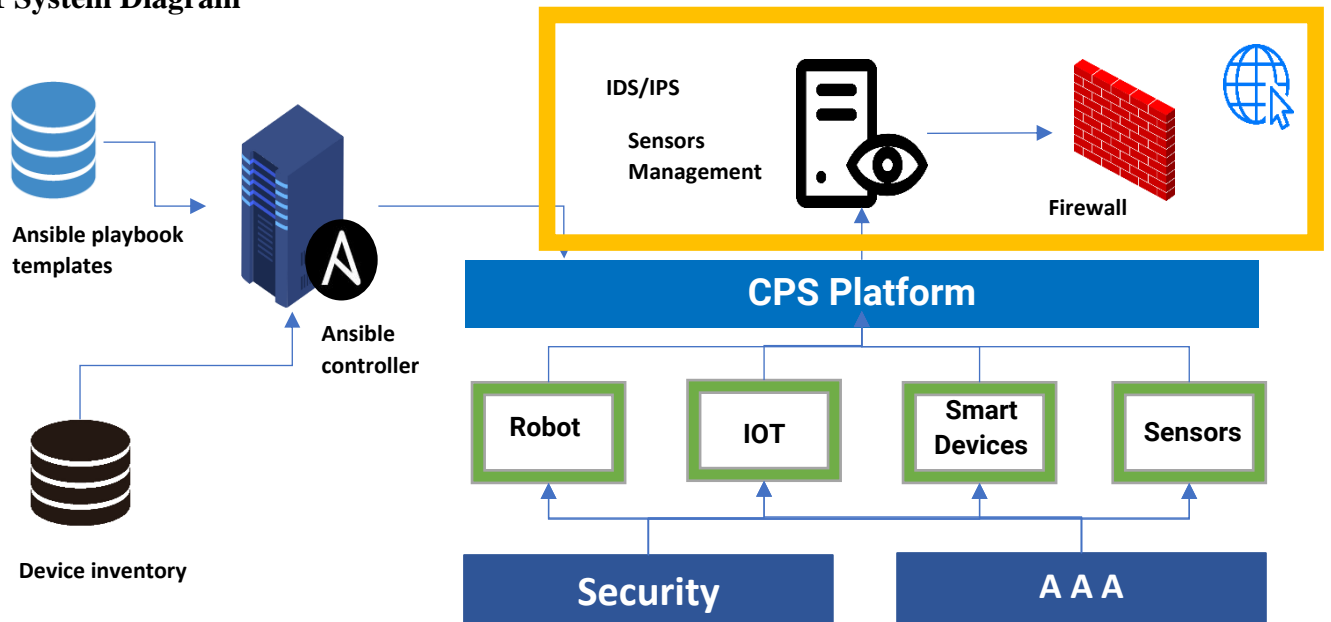


Figure 3-1: Overall System Diagram

Figure 3.1:

#### 3.2 Individual Component (Network Security)

Below Individual workflow will be followed by myself during this research

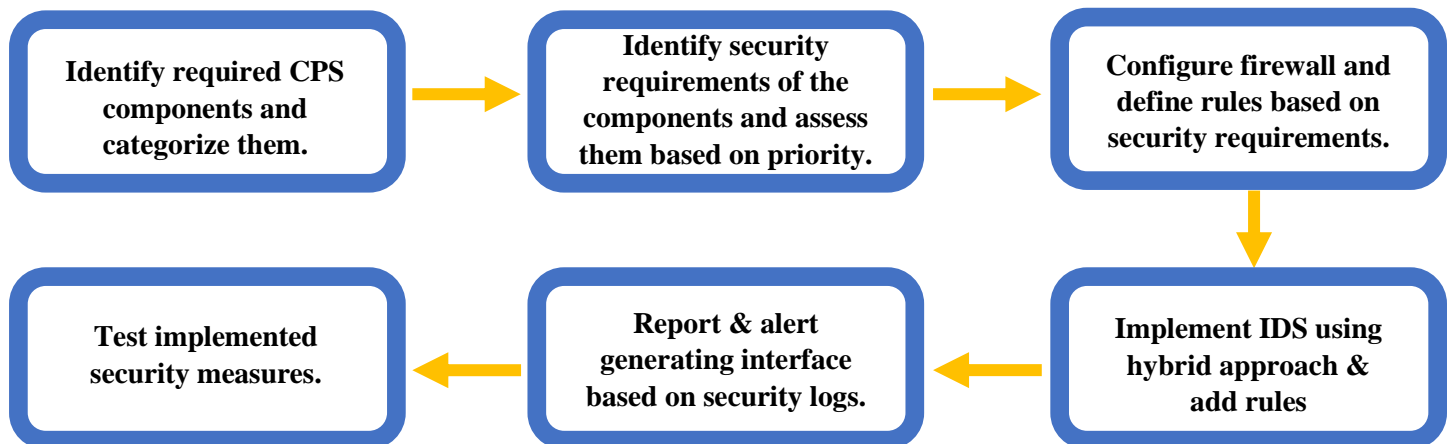


Figure 3-2: Individual Workflow Diagram

### 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 Configure firewall and define rules based on security requirements

This step needs to conduct with the collaboration of the policy makers. The firewall rules need to be defined according to the security policies and standards. These rules will apply to the all the cps components inside the network [15].

### 3.2.4 Implement IDS using hybrid approach & add rules

3This step needs some pre-requirements such as network configurations and install some security tools such as Detection Engine, Basic Analysis and Security Engine (BASE) and TCP replay. Define rules in the next part of this step setting up a signature database and pattern profiles these rules need to specific to CPS. These detection methods need to be optimized to reduce the amount of false positive and false negative alerts [12].

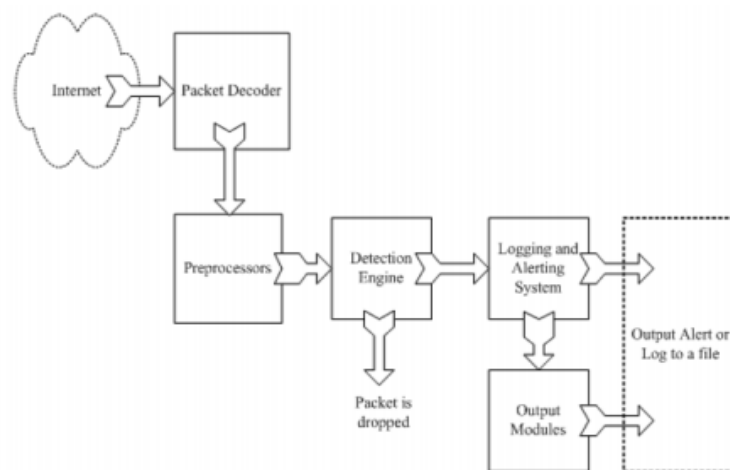


Figure 3-3: Network monitoring process

### **3.2.5 Report & alert generating interface based on security logs**

A dashboard that has the ability to configure rules, visualize the network behavior and usage, generate alerts and reports. To implement this dashboard planned to use django framework, react JS, PostgreSQL and ELK stack [16].

### **3.2.6 Test implemented security measures.**

In order to test the effectiveness of the Firewall & IDS planned to simulate network attacks such as DOS attacks, brute force attacks and information gathering traffic packets.

3.3 Gantt Chart

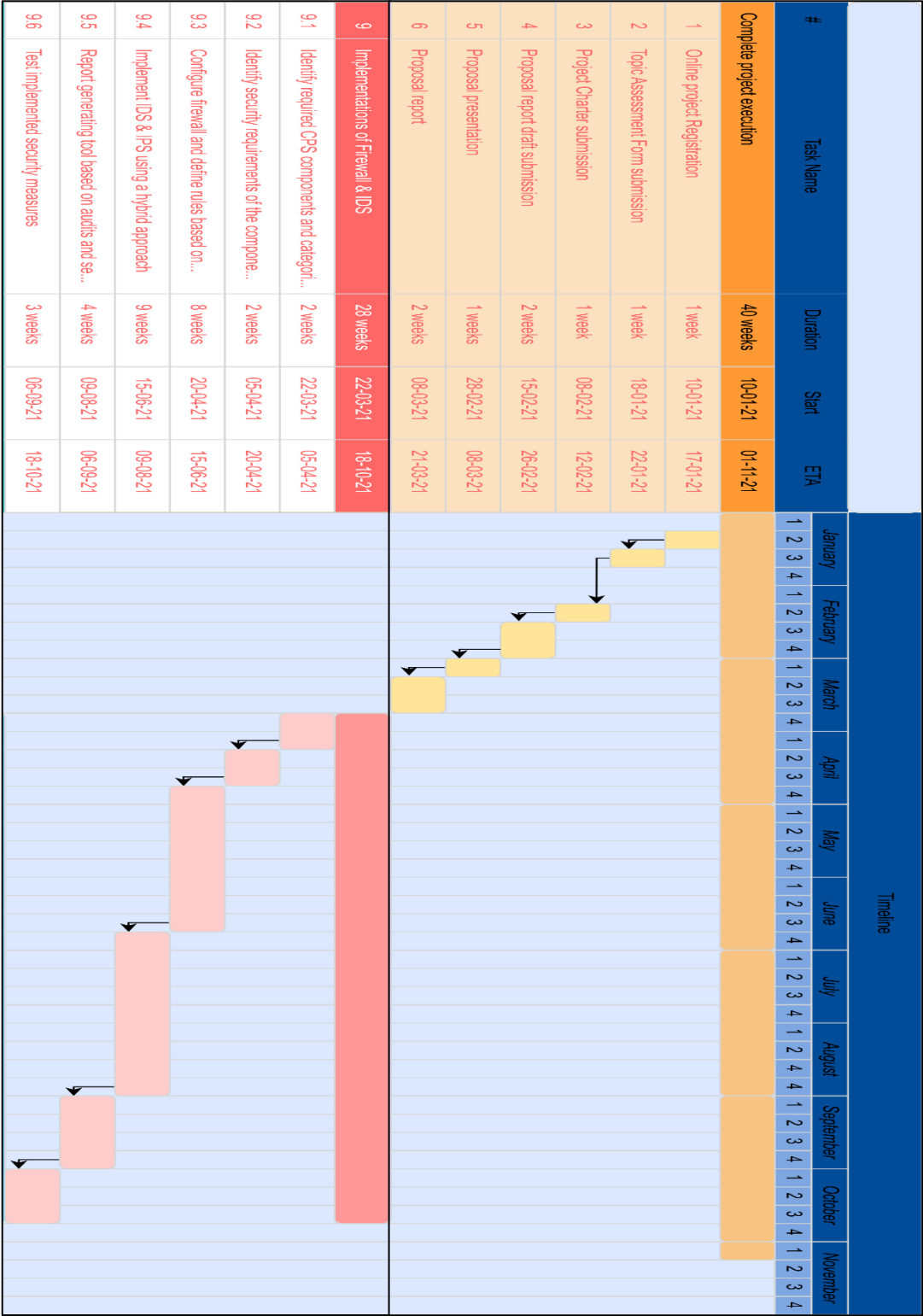


Figure 3-4: Gantt Chart

#### 4. DESCRIPTION OF PERSONAL AND FACILITIES

| Registration no | Name           | Task Description  |
|-----------------|----------------|---|
| IT18132410      | A.D.H Jinadasa | <ul style="list-style-type: none"><li>• Configure firewall and define rules</li><li>• Implement an IDS</li><li>• Create IDS detection database and profiles</li><li>• Design a dashboard for the IDS</li><li>• Testing implemented security measures.</li></ul> |

Table 4-1: Task Description

## 5. 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   |

Table 5-1: Budget

## REFERENCES

- [1] 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.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] Lins, Theo & Rabelo, Ricardo & Correia, Luiz & Sá Silva, Jorge. (2018). Industry 4.0 Retrofitting. 8 -15. 10.1109/SBESC.2018.00011. [6] 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.
- [6] 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.
- [7] 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.
- [8] M. Suh, "Automated Cutting and Sewing for Industry 4.0 at ITMA 2019," p. 13, 2019.
- [9] Ioulidou, Philokypros & Vassilakis, Vassilios & Moscholios, Ioannis. (2018). A Signature-based Intrusion Detection System for the Internet of Things (accessed Mar. 07, 2021).
- [10] Robert Mitchell and Ing-Ray Chen. 2014. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. 46, 4, Article 55 (April 2014), 29 pages (accessed Mar. 07, 2021).
- [11] N. Gupta, V. Naik and S. Sengupta, "A firewall for Internet of Things," 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bengaluru, India, 2017, pp. 411-412, doi: 10.1109/COMSNETS.2017.7945418.
- [12] D. E. Denning. "An Intrusion-Detection Model". IEEE transactions on software engineering, Volume : 13 Issue: 2, February 1987.



- [13] Hwang,K., Cai,M., Chen,Y and Qin,M. , “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes”, IEEE Transactions on Dependable Computing, Volume: 4 Issue: 1, pp. 41- 55, 2007.
- [14] Sclabs.blogspot.com. 2021. CCNA Security Chapter 5 - Implementing Intrusion Prevention ( IPS/IDS ). [online] Available at: <<http://sclabs.blogspot.com/2012/09/chapter-5-implementing-intrusion.html>> [Accessed 22 March 2021].
- [15] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, “End-to-end transport security in the ip-based internet of things,” in 2012 21st International Conference on Computer Communications and Networks (ICCCN). IEEE, 2012, pp. 1–5.
- [16] Elastic.co. 2021. *Elastic Stack and Product Documentation / Elastic*. [online] Available at: <<https://www.elastic.co/guide/index.html>> [Accessed 22 March 2021].

# APPENDICES

## Appendix A: Turnitin Similarity Score

The screenshot displays a Turnitin Match Overview report. The document title is "CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM", dated "2021-11", and is a "Project Proposal Report" by "A.D.H Jinadasa". The overall similarity score is 20%. A list of matches is shown on the right, with the first match highlighted in red.

| Match Number | Source                                      | Similarity Percentage |
|--------------|---|-----------------------|
| 1            | Submitted to Sri Lanka ...<br>Student Paper | 5%                    |
| 2            | Yury N. Kofanov, Svetla...<br>Publication   | 2%                    |
| 3            | Submitted to Middlese...<br>Student Paper   | 1%                    |
| 4            | erevistas.uacj.mx<br>Internet Source        | 1%                    |
| 5            | thinkspace.csu.edu.au<br>Internet Source    | 1%                    |
| 6            | Alp Ustundag, Emre Ce...<br>Publication     | 1%                    |
| 7            | Submitted to Manchest...<br>Student Paper   | 1%                    |

**Match 1 (Highlighted):** B.Sc. (Hons) Degree in Information Technology Specialization in Cyber Security