

CYBERSECURITY AUTOMATION FOR AN INDUSTRY
4.0 GARMENT MANUFACTURING SYSTEM

2021-11

Project Proposal Report

R.P.R.D. Randunu

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

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

February 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

February 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
R.P.R.D. Randunu	IT18133578	

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

The world is now undergoing the 4th industrial revolution, also known as Industry 4.0. It can be defined in industrial technology as the latest trend in automation and data transmission which includes cyber-physical systems (CPSs) convergence, Cyber-physical Production Systems (CPPS), Internet of Things (IoT), robotics. These revolutions can make the industrial system's product lifecycle efficient, decentralized and well-connected. The developed Supervisory Control and Data Acquisition(SCADA) system provides operators with fault isolation operation, monitoring and control functions and collection of statistics for future interpretation. An integrated Ethernet controller as known as Remote Terminal Unit (RTU) is used to transmission with digital input and output modules.

Even so, these technologies have several security concerns and difficulties to maintain security requirements such as confidentiality, integrity, and availability. Since industrial 4.0 manufacturing systems are powered by the advancement of functionality rather than defense, the integration of sophisticated smart manufacturing technologies significantly expands the potential of attacks aimed at industrial espionage and sabotage. Therefore, due to inadequate security architecture, the number and complexity of cyber-attacks in industrial automation systems is increasing and cyber security requirements have not been identified. The creation of a safe ecosystem for smart systems using the CPPS platform is very complicated. Because of many challenges that is currently constrained. They are CIA infringement, additional costs, secure communication, centralized security control, vulnerable data, difficulties of adhering to rules and regulations and coordination between different systems. The objective of this research paper is to design and automate a Computer Numerical Control(CNC) cutting machine in the direction of Industry 4.0 that adapts to security standards to illustrate the cyber security gap and discuss solutions to be applied in the apparel industry while comparing and contrasting with current security aspects in the industry's current Industrial 4.0 automated systems.

Key words - Industrial Internet of Things(IIoT), Computer Numerical Control(CNC), Cyber Physical Systems(CPS), Supervisory Control and Data Acquisition(SCADA) system, Remote Terminal Unit(RTU)

TABLE OF CONTENTS

DECLARATION	3
ABSTRACT.....	4
LIST OF FIGURES	7
LIST OF TABLES	8
1.INTRODUCTION	9
1.1 Background Review.....	9
1.2 Literature Review.....	13
1.3 Research Gap	16
1.4 Research Problem	17
1.4.1. Collaboration between different systems	17
1.4.2. Centralized security management.....	17
1.4.3. Secure communication	17
1.4.4. Insecure data	18
1.4.5. Initial cost.....	18
1.4.6. Lack of strategy to industry 4.0.....	18
2.OBJECTIVES	19
2.1 Main Objective.....	19
2.2 Sub Objectives	19
2.2.1. Access log visualization.....	19
2.2.2. Report generation.....	19
2.2.3. Alert user when an anomaly occurs	19
3.METHODOLOGY.....	21
3.1 System Diagram.....	21
3.2 Individual component	21
3.2.1. Identify required devices.....	22

3.2.2. Identify security requirements	22
3.2.3. Analysis of network accessibility and physical accessibility.....	22
3.2.4. Implement login system for access and activity monitor	22
3.2.5. Test implemented security measures.....	22
3.3 Gantt Chart.....	23
4.DESCRPTION OF PERSONAL AND FACILITIES.....	24
5.BUDGET	25
REFERENCE LIST.....	26

LIST OF FIGURES

Figure 1.1: Industry Revolution	10
Figure 1.2: IIoT Security Requirements	16
Figure 3.1: Overall System Diagram	21
Figure 3.2: Gantt Chart	23

LIST OF TABLES

Table 4.1: Description of Personal and Facilities	24
Table 5.1: Budget Justification	25

1. INTRODUCTION

1.1 Background Review

The world is now seeing the 4th industrial revolution in technology and principles of value chain organization, which brings together cyber-physical systems(CPS), the Internet of Things(IoT), the Industrial Internet of Things(IIoT) and autonomous robots, simulation, system integration, cybersecurity, cloud computing, after going ahead with three industrial revolutions. Ever since the 1800s, the world has undergone three separate industrial revolutions. The first industrial revolution occurred with the mechanization of production methods at the end of the 18th century. Electricity was then used to power into the turn of the next century, the mass manufacture of products based on the division of labour. In the 1970s, the use of computers, computer networks and information technology (IT) to accomplish greater automation of industrial processes was known as the 3rd industrial revolution. Industrial 4.0 was first declared at the Hannover Fair in 2011 by the Federal Government of Germany. The technological convergence of CPS and the use of IoT in manufacturing processes would have flexible architectures that follow constantly evolving specifications, value development and business models providing efficiency, accountability, identification of defects, versatility, tracking and, above all, productivity while reducing costs. CPS interacts with each other and with human beings in real time to eventually make decisions without human intervention. Industrial systems that have been integrated with CPS and IoT can have value creation and enterprise models, as well as modular structures that can adapt to rapidly changing needs. Industry 4.0 textile production systems focus on IoT and other technologies such as cyber physical systems, wireless sensor networks, machine learning, data analytics, augmented reality, cloud computing, robotics, simulations, cyber security, to create a connection between the digital and physical world. Industry 4.0's vision is to grow IIoT, which will incorporate automated technology and network systems into manufacturing for automation.

Due to the high adaptability of new emerging technologies such as IIoT, the textile field has a great history and continues to develop. Since the beginning of the first revolution, the apparel industry has become an important industry in the manufacturing sector of the world. In a clothing and apparel factory, the basic flow of production processes involves

designing the product according to marketing demands and customer requirements, selecting appropriate clothing material, forming layers from the materials of clothing, cutting different shapes by minimizing material waste, various sewing operations, finishing, assurance of product quality, packing, storing, distribution.

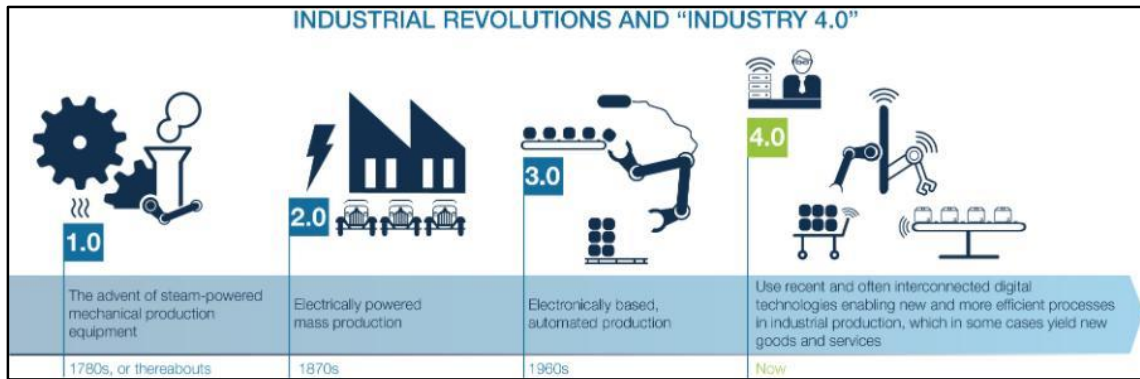


Figure 1.1: Industry Revolution

The directive of Industry 4.0 is the development of IoT to the integration of network technology and smart computing into manufacturing for automation. IoT is a technology that allows computers and computer-related machinery to communicate with one another in order to improve intelligence, effectiveness, productivity, and safety. While IoT refers to a system of interconnected computing devices that communicate with one another and with individuals in real time, it is most widely used for commercial purposes, I-IoT is used for industrial purposes such as manufacturing. In contrast to IoT, I-IoT incorporates a broader range of network protocols, command and control, service requirements, and smart devices.

Due to the waste issues, affordability and usability, labor reliance, cutting method plays a huge role in the garment automation industry and it is an expensive process. In the digital revolution, computer numerically controlled(CNC) machines were developed. This technical innovation made cutting the most advanced field in apparel sector. Different cutting devices are available. Computer-controlled knives, plasma, ultrasound, lasers, and markers are just a few examples. The existing cutting technologies have been developed with the aspects of pattern matching abilities, competitiveness, and flexibility since the first fully automated cutting system matured. Industry 4.0 is currently witnessing a revolution in cutting methods involving CNC devices, thus discussing solutions to labor-

intensive issues, pollution problems and cost savings. The concept of digitalization and integration has been pointed out in IIoT or fourth industrial revolution which CNC technology plays a vital part when automating cutting garment manufacturing systems. In industry 4.0 CNC controllers should be capable of supporting integration, sensors, cloud servers. The transition from a conventional hardware-based control architecture to a smart software architecture for automation is a challenge.

Inefficient security may result in increased economic losses, loss of production, and even loss of life. As we all know, IoT is based on connecting the digital and physical worlds. As a result of IoT and other digital technologies, industrial espionage and sabotage has gone up significantly. Levels of awareness, the weaknesses of current measures, and preparation for future problems are critical, which is why security should be an essential underpinning of the growth of industry 4.0. If the engineers of industrial 4.0 manufacturing automation could detect the application of cyber security standards that have not been completely captured in automation and improve systems addressing all security aspects in automation, the developing automation systems would be potentially free of massive risks and safe.

The focus of the SCADA system is the management and maintenance of automatic control systems. It is an embedded program which uses commands to control the system's processing. A SCADA system consists of a number of RTUs collecting field data and sending it to a master station via a communications device. It has a connection with the software, where the given input data and receives output data with a preferred communication protocol to know if any troubleshoot to be done [1].

The security concerns emerge as today's Industrial 4.0 automation is powered instead of security by concentrating on functionality. Increasing economic risk, loss of productivity and even loss of life may result from a lack of security. The vulnerability of current controls, the level of awareness and readiness for potential threats is critical, which can be an essential reason for security to help the advancement of 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.

1.2 Literature Review

Industry 4.0 is concerned with the development of automated products and industrial processes and will allow people, machines and products to interact similarly. And they are able to process data, they can manage certain activities themselves and communicate through interfaces with humans.

The IIoT offers a communication network that connects physical things to each other or to larger networks. IIoT would make it easier for clothing manufacturers to make their goods for their consumers more interactive, insightful and customized. And the integration of suppliers to obtain the optimum quantity of raw materials at the time required. In addition, it opens a new direction for the creation of mobile electronics integrated in apparel. IoT will also allow real-time data analytics to solve problems such as product authentication, brand security, and transparency and effectiveness of the supply chain. Smart devices, network systems, command control, and service requirements are just a few of the more distinct kinds of IIoT.

The apparel industry has become a competitive marketplace now. Therefore, integrated systems are increasingly evolving within the sector, facilitating advances in industrial processes. Industry 4.0 facilitates functionality such as scalability, vast customization, customer loyalty, and control and visibility to place a value of importance in the apparel industry. Nevertheless, most automated technologies in the textile industry are evolving.

Die cutters, which were introduced in the 1900s, improved cutting performance and quality. Numerical Controller (NC) machines emerged in the 1940s and made uninterrupted cutting practical, due to higher industrial stability and increased material use. Then Computer Numerically Controlled(CNC) machines was created in the digital revolution.

SCADA ensures adequate equipment monitoring to keep operations at an optimum level by detecting and fixing issues before they become major system failures [2]. A basic SCADA system composes of RTUs, are microprocessor-based devices connected to sensors, transmitters or process equipment for the purpose of remote telemetry and control [3].

Many studies have found that CPS and IoT have the same fundamental architecture. On the IoT, cyber-physical system demonstrates a high level of combination and coordination between physical and computational components.

Rising intercommunication and data density with Industry 4.0 is contributing to new problems, especially in cyber protection. Cyber protection is a serious concern that should be tackled at the highest degree of priority. With the growth of network technologies, cyber-attacks for various purposes, such as financial and geopolitical motives, have become more common. This matter is directly or indirectly influenced by stakeholders that use IOT programs. In addition to immeasurable damages such as computer corruption, device failures, privacy violations, reputation, consumer, reliability and business losses, major companies are especially vulnerable to malicious threats that result in serious financial burdens. Mostly security has been shared with a third party, and the manufacturers should rely on the trust of the third party. There could be insider threats, loss of governance of shared data and many more threats. Most literature primarily focus only on functionality of industrial 4.0 automated systems and security is been considered as a secondary concern or a characteristic.

Previously, security in manufacturing was accomplished through techniques such as isolation based on physical access control. Since the advent of remote working capabilities Ethernet, IP controls have become an integral part of networking. As a result, there is a significant threat level and an increased number of vulnerabilities. Custom designed search engine for IoT like SHODAN, was used to search PLC (Programmable Logic Controller), RTU (Remote Terminal Unit) systems, SCADA servers. HMI (Human machine Interface) servers, DCS (Distributed control sensors) were been under attack [4].

IoT systems, sensors, CNCs, and RFIDs are among the devices found in the CPS. Because some of these devices have poorly implemented or configured authentication systems, securing access to them is challenging. CPS and IoT devices, according to the Open Web Application Security Project (OWASP), have hardcoded passwords or poor guessable passwords that can be brute forced quickly, and some of these passwords are publicly accessible. According to OWASP, these devices lack physical security, which makes for side channel attacks. And also CPS devices have vulnerable network services, which are unnecessary services that run on the devices and are

exposed to the internet, allowing unauthorized sources to control them remotely. As a result, gaining unauthorized access to computer systems is easier than gaining approved access.

1.3 Research Gap

Since industrial 4.0 manufacturing systems are powered by the advancement of functionality rather than defense. Therefore, due to poor security architecture, the number and complexity of cyber-attacks in industrial automation systems is increasing and cyber security requirements have not been identified.

Wireless networks are used to collect data for authorized users in IoT development. The platform sends instructions to terminal nodes in a wireless network, and the terminal nodes collect and transmit information to the platform. To ensure the network's security, mutual authentication is required during the communication process.

Then we design an automated system focusing cyber security aspects like authentication, authorization and accounting physically and logically in cps devices.

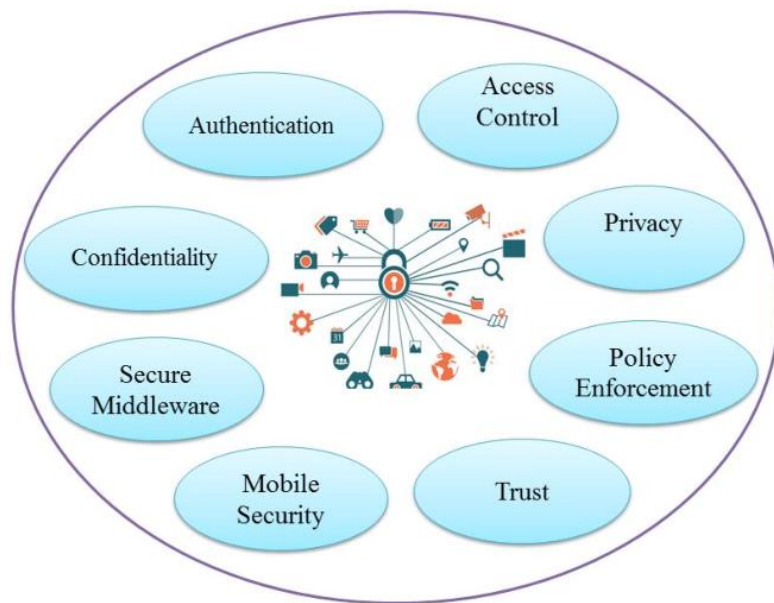


Figure 1.2: IIoT security requirements

1.4 Research Problem

When automating a manual system or semi-automated system in the direction of the fourth industrial revolution (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 establishment of a secured network workplace.

The system environment of Industry 4.0 is evolving with the help of a CPPS platform based on CPS technology. Building the CPPS platform is a complicated project that is currently hampered by a number of factors, including the CPS challenges listed below.

1.4.1. Collaboration between different systems

A Collaborative model between physical devices and computer systems is essential for exchanging information, [5] 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 [6]. Physical devices environment, software, and hardware platforms, and other functional and non-functional must consider in a typical CPS model in addition to CPS modeling language [5].

1.4.3. Secure communication

CPS that use the SCADA systems is connected to the internet over TCP/IP protocols without additional protection [7], which have known vulnerabilities.

1.4.4. Insecure Data

During the implementation of Industry 4.0, there was a lack of system integrations to ensure data security for manufacturing companies. The IoT-based CPSs that are connected to many of embedded sensors and communication devices pose a significant risk linked with the growth of data usage and the much higher risks of system breaches [8].

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 design and implement the architecture as per the business needs considerable initial investment in the matter of cost and time is required [9]

1.4.6. Lack of strategy to Industry 4.0

Lack of dynamic strategic plan to support the migration to Industry 4.0 in the manufacturing Industry [10].

2. OBJECTIVES

2.1 Main Objective

The main objective is to incorporate Authentication, authorization, and accounting (AAA) and ensure security in order to define general access control principles and user access control management rules by establishing baselines for user registration, identification, and authentication, as well as access rights management. Authenticate users when connecting between IIoT devices and ansible controllers to enable secure access to the services, monitor and filter the user behavior on the system to prevent unauthorized access and to prevent attacks on the networks and build the strong security and encryption method to safeguard the system are my security parts in this research. I break this main objective to the three sub objectives as Access log visualization, Report generation, Alert user when an anomaly occurs.

2.2 Sub Objectives

2.2.1 Access log visualization

In this proposed system, we able to log, monitor, and analyze all authentication events is key for identifying security threats and managing customer records for compliance purposes. We want to make sure that our system generates authentication logs with enough information and that they are written in a standard, easily accessible format that allows for complicated analysis of all logs.

2.2.2 Report generation

There is a function in this suggested tool to produce reports based on audit results. Reports can be scheduled for automatic generation on a weekly or monthly basis. As a result, these audit reports can be used to demonstrate the system's security configurations.

2.2.3 Alert user when an anomaly occurs

An anomaly is something that is out of the ordinary in comparison to the norm. The most realistic approach is to use an analytics platform with anomaly detection algorithms that

can quickly analyze large quantities of data and identify anomalies. Basically, anything that deviates from past data should be considered an anomaly.

3. METHODOLOGY

3.1 System Diagram

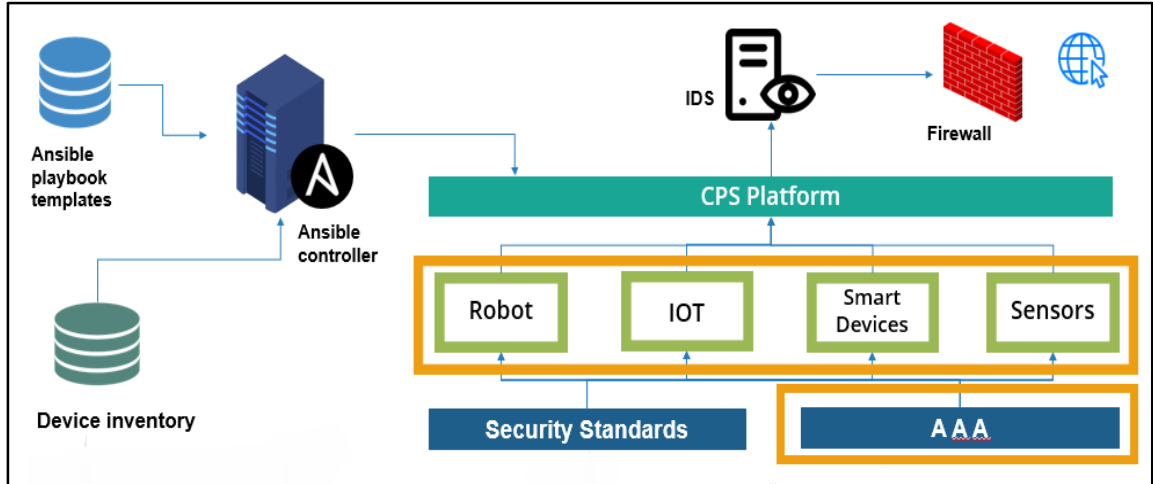


Figure 3.1: Overall system diagram

Initial background study has been conducted to gather the knowledge about authentication and access monitoring to fulfil our main objective. Authenticate users when connecting between IoT devices and ansible controllers to enable secure access to the services, monitor and filter the user behavior on the system to prevent unauthorized access and to prevent malicious attacks on the networks and build the strong security and encryption method to safeguard the system are my security parts in this research.

3.2 Individual Component

My workload is divided into following components.

- Identify required devices industrial 4.0 manufacturing system
- Analysis of network accessibility and physical accessibility
- Identify security requirements and evaluate them
- Implement login system for access and activity monitor
- Test implemented security measures

3.2.1. Identify required devices

In this research, we are looking at the cutting process of the apparel industry manufacturing. Then we identified CNC cutting machine, some IoT devices, smart devices and sensors. These identified devices required to be categorized based on their device type to simplify future security implementations.

3.2.2. Identify security requirements

The analysis is the most important activity to gain the understanding between the business team and the development team. We want to do risk assessment and analyze the CPS based threats and vulnerabilities for each device. Then prioritization and rating of the risks to systems and data.

3.2.3. Analysis of network accessibility and physical accessibility

We want to ensuring legitimate reliable access to systems, applications, IoT devices. Identify who want to access, who is not, what methods are used for authentication and access monitoring.

3.2.4. Implement login system for access and activity monitor

The Access Control System identifies, authenticates, and authorizes a person's entry into the premise, providing full protection and guaranteeing the system's security. It offers security by allowing you to have flexible control over who is permitted to enter your premises. Then want to implement store access logs and error logs of the login system.

3.2.5. Test implemented security measures

The most critical testing for an application is security testing, which checks whether confidential data remains confidential. In this kind of testing, the tester pretends to be an intruder and manipulates the system. The security control testing occurs to ensure that all security controls are implemented in properly.

3.3 GANTT CHART

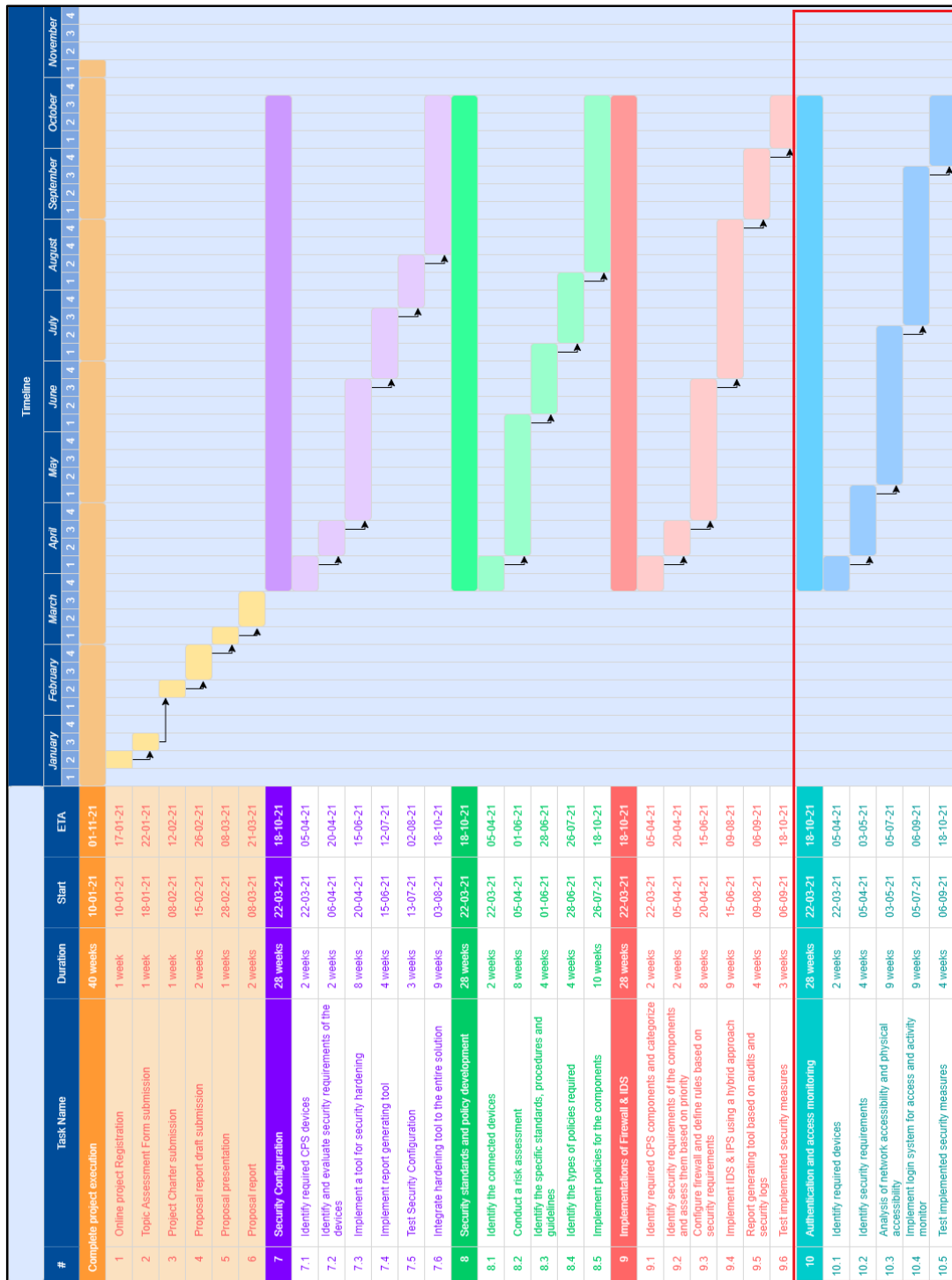


Figure 3.2: Gantt chart

4. DESCRIPTION OF PERSONAL AND FACILITIES

Table 4.1: Description of Personal and Facilities

Registration No	Name	Task Description
IT18133578	R.P.R.D. Randunu	<ul style="list-style-type: none">• Create database to store access logs and error logs.• Implement a Physical Security System.• Data visualization from access logs.• Alert user when an anomaly occurs.• Report generation from access logs.• Testing

5. BUDGET

Table 5.1: Budget Justification

Items	Cost(LKR)
Web server hosting	5,000.00
Firewall + IDS/IPS hardware	18,000.00
Physical security system hardware	5,000.00
Raspberry Pi 3	12,000.00
Total	40,000.00

REFERENCE LIST

- [1] Yogeshwar, B. & Sethumadhavan, M. & Srinivasan, Seshadhri & Amritha, P.. (2021). A Light-Weight Cyber Security Implementation for Industrial SCADA Systems in the Industries 4.0. 10.1007/978-981-15-7062-9_46.
- [2] M. M. Ahmed and W. L. Soo, "Supervisory Control and Data Acquisition System (SCADA) based customized Remote Terminal Unit (RTU) for distribution automation system," 2008 IEEE 2nd International Power and Energy Conference, Johor Bahru, Malaysia, 2008, pp. 1655-1660, doi: 10.1109/PECON.2008.4762744.
- [3] Francis Enejo Idachaba and Ayobami Ogunrinde, "Review of Remote Terminal Unit (RTU) and Gateways for Digital Oilfield deployments" International Journal of Advanced Computer Science and Applications(IJACSA), 3(8), 2012. <http://dx.doi.org/10.14569/IJACSA.2012.030826>
- [4] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," Journal of Manufacturing Systems, vol. 47, pp. 93–106, Apr. 2018, doi: 10.1016/j.jmsy.2018.04.007.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] Kamble, S., Gunasekaran, A. and Gawankar, S., 2020. Sustainable Industry 4.0 Framework: A Systematic Literature Review Identifying The Current Trends And Future Perspectives.
- [9]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.
- [10]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

The screenshot displays a Turnitin Match Overview report. The main document preview on the left shows the title "CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM", the year "2021-11", the type "Project Proposal Report", the author "R.P.R.D. Randana", the degree "B.Sc. (Hons) Degree in Information Technology Specialization in Cyber Security", the department "Department of Computer Systems Engineering", the institution "Sri Lanka Institute of Information Technology", and the location "Sri Lanka". The date "February 2021" is also visible. The right panel shows a "Match Overview" with a total similarity score of 20%. Below the score is a list of 7 matches, each with a rank, source, and similarity percentage.

Rank	Source	Similarity
1	Submitted to Sri Lanka ... Student Paper	5%
2	Submitted to Middlese... Student Paper	1%
3	Submitted to University... Student Paper	1%
4	erevistas.uacj.mx Internet Source	1%
5	"Information and Com... Publication	1%
6	Yury N. Kofanov, Svetla... Publication	1%
7	thesai.org Internet Source	1%