

CYBERSECURITY AUTOMATION FOR AN INDUSTRY
4.0 GARMENT MANUFACTURING SYSTEM

2021-11

Final Project Thesis

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

October 2021

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

2021-11

Final Project Thesis

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

Department of Computer Systems Engineering


Sri Lanka Institute of Information Technology

Sri Lanka

October 2021

DECLARATION

We declare that this is our own work, and that this report does not contain any material previously submitted for a degree or diploma at any other university or institute of higher learning without acknowledgment, and that it does not contain any material previously published or written by another person to the best of our knowledge and belief, except where acknowledgement is made in the text. In addition, I give the Sri Lanka Institute of Information Technology the nonexclusive right to reproduce and distribute my dissertation in whole or in part in print, electronic, or other media. I reserve the right to use this information in whole or in part in future works (for example, articles or books)."

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 fourth industrial revolution, often known as Industry 4.0, is now underway across the world. It is the newest trend in automation and data transmission in industrial technology, and it encompasses cyber-physical systems (CPSs) convergence, Cyber-physical Production Systems (CPPS), Internet of Things (IoT), and robots. These revolutions have the potential to make the product lifecycle of the industrial system more efficient, decentralized, and well-connected.

Nonetheless, there are many security problems with these technologies, as well as difficulties in maintaining security criteria such as confidentiality, integrity, and availability. Because the growth of functionality rather than protection drives industrial 4.0 production systems, the integration of advanced smart manufacturing technologies greatly increases the possibility for industrial espionage and sabotage attempts. As a result of insufficient security design, the quantity and complexity of cyber-attacks on industrial automation systems is growing, and cyber security needs have yet to be established. Using the CPPS platform to create a secure environment for smart systems is a difficult task. This is now restricted due to a number of obstacles. Infringement by the CIA, increased expenses, secure communication, centralized security control, vulnerable data, difficulty complying to laws and regulations, and cooperation across multiple systems are some of them. The physical access control prevents unauthorized access and also access monitoring was done using access logs.

The objectives of this report is to offer a system that improves security while being cost-effective and efficient, as well as providing a comprehensive security standard in order to illustrate the cyber security gap security solution for current and future smart manufacturing challenges, while comparing and contrasting 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)

ACKNOWLEDGEMENT

Prof. Pradeep Abeygunawardhana and Ms. Sasini Nuwanthika, our project supervisor and co-supervisor, deserve special thanks for all of their advice and effort dedicated to our research project, as well as for their direction and guidance through challenging themes and research gaps. I'd like to express my gratitude to our external supervisor, Chartered Eng. P.A. Gamini De Alwis, for guiding us in the right direction throughout our research project by sharing his manufacturing experience, as well as Dr. Darshi De Saram, for sharing his knowledge and experience, as well as providing valuable feedback, which contributed to the project's success.

I'd like to express my gratitude to Dr. Asela Kulatunga, Head of Department of Manufacturing and Industrial Engineering, University of Peradeniya, Sri Lanka, for allowing us to visit Peradeniya University to study CNC machine and robotic applications workflow, which served as a good starting point for our research. I'd like to express my appreciation to Mr. Wijeweera, owner of Wijeweera Knit Wear (Private) Limited, for allowing us to visit the garment factory during the initiation stage of our project to assess needs.

TABLE OF CONTENTS

DECLARATION	3
ABSTRACT.....	4
ACKNOWLEDGEMENT.....	5
LIST OF FIGURES	8
LIST OF TABLES	10
1. INTRODUCTION	11
1.1 Background Review.....	11
1.2 Literature Review.....	15
1.3 Research Gap	19
2. RESEARCH PROBLEM	20
2.1 Collaboration between different systems	20
2.2 Centralized security management	20
2.3 Secure communication.....	20
2.4 Insecure data	21
2.5 Initial cost	21
2.6 Lack of strategy to industry 4.0	21
3. OBJECTIVES.....	22
3.1 Main Objective.....	22
3.2 Sub Objectives	22
3.2.1. Access log visualization.....	22
3.2.2. Report generation.....	22
3.2.3. Alert user when an anomaly occurs	23
4. METHODOLOGY.....	24
4.1 System Diagram.....	24

4.2 Individual component	25
4.2.1. Identify required devices.....	25
4.2.2. Analysis of network accessibility and physical accessibility.....	28
4.2.3. Identify security requirements	29
4.3 Commercialization.....	33
5. TESTING & IMPLEMENTATION	34
5.1 Implement login system for access and activity monitor	34
5.1.1. Requirement Analysis	34
5.1.1.1 Arduino Uno R3 board	35
5.1.1.2 Fingerprint sensor	36
5.1.1.3 Bluetooth module HC 05	37
5.1.1.4 Arduino IDE	38
5.1.1.5 Log management server	38
5.1.1.6 Elastic stack	39
5.1.2. Implementation	40
5.2 Test implemented security measures	49
6. RESULTS & DISCUSSION	50
7. CONCLUSIONS	53
8. REFERENCE LIST.....	54

LIST OF FIGURES

Figure 1.1: Revolution in Industry	12
Figure 1.2: Security requirements for the IIoT	19
Figure 4.1: Overall system diagram	24
Figure 4.2: Workflow	25
Figure 4.3: Gantt chart	26
Figure 4.4: Observe CNC devices	26
Figure 4.5: Observe CNC devices' control panel	27
Figure 4.6: Observe CNC devices' software	27
Figure 4.7: Observe CNC devices	28
Figure 4.8: CNC machine's control panel	29
Figure 4.9: Heat map	30
Figure 5.1: Flow chart of the project	34
Figure 5.2: Arduino board	36
Figure 5.3: Fingerprint Sensor	37
Figure 5.4: Physical access control system diagram	40
Figure 5.5: Connect the fingerprint sensor to Arduino	41
Figure 5.6: Fingerprint enrollment code 1	42
Figure 5.7: Fingerprint enrollment code 2	42
Figure 5.8: Fingerprint enrollment output	43
Figure 5.9: Fingerprint verification code 1	44
Figure 5.10: Fingerprint verification code 2	45
Figure 5.11: Finger test output at serial monitor	46
Figure 5.12: Connect the Bluetooth module to system	47

Figure 5.13: Implemented physical access control system	47
Figure 5.14: Kibana home page	48
Figure 5.15: Access logs	49
Figure 6.1: Degrees of Confidence	51

LIST OF TABLES

Table 1.1: Various biometric authentication techniques	18
Table 4.1: Threats	30
Table 5.1: How to connect the fingerprint sensor to the Arduino	41
Table 5.2: How to connect the Bluetooth module to the Arduino	46
Table 6.1: Key variations in performance and system structure	50

1. INTRODUCTION

1.1 Background Review

After three industrial revolutions, the world is now witnessing the fourth industrial revolution in technology and value chain organization, which brings together cyber-physical systems (CPS), the Internet of Things (IoT), the Industrial Internet of Things (IIoT), autonomous robots, simulation, system integration, cybersecurity, and cloud computing. The globe has gone through three different industrial revolutions since the 1800s. The automation of manufacturing processes towards the end of the 18th century ushered in the first industrial revolution. Electricity was then utilized to power the mass manufacturing of items based on the division of labor till the turn of the century. The 3rd industrial revolution was defined in the 1970s as the use of computers, computer networks, and information technology (IT) to achieve increased automation of industrial operations. The Federal Government of Germany initially announced Industrial 4.0 at the Hannover Fair in 2011. Flexible architectures that follow constantly evolving specifications, value development, and business models would result from the technological convergence of CPS and the use of IoT in manufacturing processes, providing efficiency, accountability, defect identification, versatility, tracking, and, above all, productivity while reducing costs. CPS communicates with each other and with humans in real time in order to make choices without the need for human involvement. Value generation and enterprise models, as well as flexible architectures that can adapt to quickly changing demands, may be found in industrial systems that have been connected with CPS and IoT. To link the digital and physical worlds, Industry 4.0 textile manufacturing systems use IoT and other technologies like as cyber physical systems, wireless sensor networks, machine learning, data analytics, augmented reality, cloud computing, robots, simulations, and cyber security. The goal of Industry 4.0 is to expand the Internet of Things (IIoT), which will combine automated technologies and network infrastructure into production to automate processes.

The textile industry has a long history and continues to expand due to the high adaptability of new developing technologies such as IIoT. The clothing business has grown in importance in the global manufacturing sector since the beginning of the first revolution. The basic flow of production processes in a clothing and apparel factory includes designing the product according to marketing demands and customer requirements, selecting appropriate clothing material, forming layers from clothing materials, cutting different shapes while minimizing material waste, various sewing operations, finishing, product quality assurance, packing, storing, and distribution.

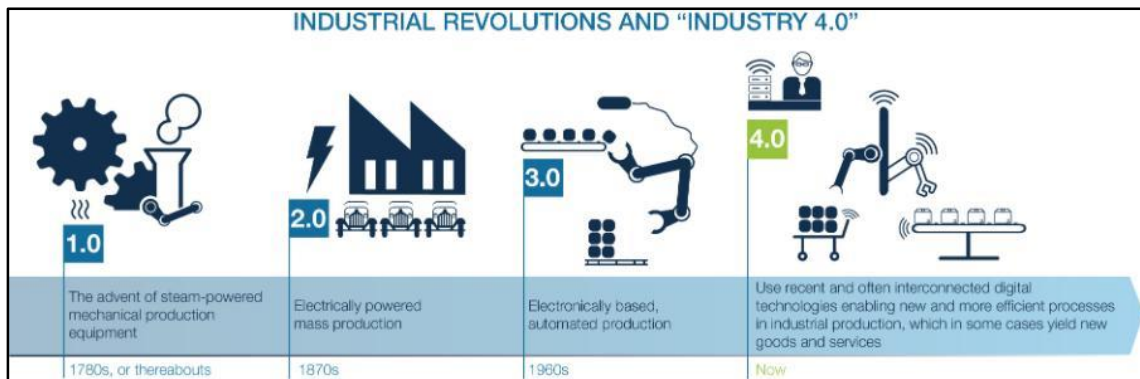


Figure 1.1: Revolution in Industry

The growth of IoT to the integration of network technology and smart computing into production for automation is Industry 4.0's direction. The Internet of Things (IoT) is a communication technology that allows computers and computer-related machines to interact with one another to increase intelligence, effectiveness, productivity, and safety. Whereas the Internet of Things (IoT) refers to a system of networked computing equipment that interact with one another and with humans in real time, it is most commonly utilized for commercial reasons, while I-IoT is used for industrial applications such as manufacturing. I-IoT encompasses a larger variety of network protocols, command and control, service needs, and smart devices than IoT.

Cutting method plays a large part in the garment automation sector due to waste concerns, affordability and usability, labor dependency, and it is a costly operation. Computer numerically controlled (CNC) devices were created during the digital revolution. Cutting became the most sophisticated field in the garment industry as a result of this technological advancement. There are a variety of cutting instruments available. Examples include

computer-controlled blades, plasma, ultrasound, lasers, and markers, to name a few. Since the first completely automated cutting system emerged, existing cutting technologies have been developed with pattern matching abilities, competitiveness, and adaptability. Cutting methods utilizing CNC machines are undergoing a revolution as part of Industry 4.0, with solutions to labor-intensive difficulties, environmental issues, and cost reductions being discussed. In the IIoT, or fourth industrial revolution, the notion of digitalization and integration has been highlighted, and CNC technology plays a critical role in automating cutting garment production processes. CNC controllers in Industry 4.0 should be able to support integration, sensors, and cloud servers. The shift from a traditional hardware-based control architecture to a smart software-based automation architecture is difficult.

Ineffective security can lead to greater economic losses, productivity losses, and even death. The Internet of Things (IoT) is built on linking the digital and physical worlds, as we all know. Industrial espionage and sabotage have increased dramatically as a result of IoT and other digital technologies. Security should be an essential basis of the expansion of industry 4.0 because levels of knowledge, the inadequacies of existing measures, and readiness for future challenges are vital. If industrial 4.0 manufacturing automation engineers could detect the application of cyber security standards that haven't been fully captured in automation and improve systems that address all security aspects in automation, the developing automation systems would be potentially risk-free and secure.

The SCADA system is primarily used to administer and maintain automated control systems. It's a command-driven embedded software that manages the system's processing. A SCADA system is made up of many RTUs that gather data in the field and transfer it to a master station through a communications connection. It connects to software and receives input data and output data using a selected communication protocol to see if any troubleshooting is required. [1].

Security problems arise when the focus of today's Industrial 4.0 automation is on functionality rather than security. A lack of security can lead to increased economic risk, lost productivity, and even death. The vulnerability of present controls, as well as the amount of knowledge and preparation for possible attacks, is vital, and security may be an important factor in advancing Industry 4.0 development. If industrial 4.0 manufacturing

automation developers could discover cyber security needs that haven't been fully captured in automation and build systems that handle all security elements in automation, the emerging automation systems would be theoretically risk-free and secure.

1.2 Literature Review

Industry 4.0 is focused with the development of automated products and industrial processes, allowing people, machines, and products to interact in the same way. They can also analyze data, handle specific tasks, and converse with people through human-like interfaces.

The Internet of Things (IIoT) is a communication network that links physical objects to one another or to bigger networks. The IIoT would make it simpler for garment makers to make their products more interactive, informative, and personalized for their customers. Also, supplier integration to acquire the optimal quantity of raw materials at the needed time. It also opens up a new avenue for the development of mobile electronics that are incorporated into clothing. IoT will also enable real-time data analytics to address issues such as product authenticity, brand security, and supply chain transparency and efficacy. Intelligent devices, network systems, command and control, and service needs are only a few of the several types of IIoT.

The clothing business has evolved into a competitive industry. As a result, integrated systems are becoming more prevalent in the industry, allowing for faster advancements in industrial operations. Sector 4.0 allows for features like scalability, extensive customisation, client loyalty, and control and visibility to be prioritized in the garment industry. Nonetheless, in the textile sector, the majority of automation systems are in the early stages of development.

Die cutters, which were first used in the 1900s, increased cutting quality and performance. Because of improved industrial stability and increasing material consumption, numerical controller (NC) machines appeared in the 1940s and made uninterrupted cutting possible. The digital revolution led to the development of Computer Numerically Controlled (CNC) devices.

SCADA enables proper equipment monitoring in order to maintain optimal operations by recognizing and resolving problems before they become significant system breakdowns. [2]. RTUs are microprocessor-based devices linked to sensors, transmitters, or process equipment for the purpose of remote telemetry and control in a basic SCADA system. [3].

CPS and IoT share the same underlying architecture, according to several research. Cyber-physical systems on the Internet of Things show a high level of integration and coordination between technological and physical components.

Industry 4.0's increased intercommunication and data density is causing new issues, particularly in cyber security. Cyber security is a major problem that should be addressed as soon as possible. Cyber-attacks for different objectives, such as financial and geopolitical motives, have grown increasingly prevalent as network technology have advanced. Stakeholders who utilize IOT applications have a direct or indirect effect on this issue. Aside from incalculable losses such as computer corruption, device malfunctions, privacy breaches, reputation, customer, dependability, and commercial losses, big corporations are particularly vulnerable to hostile attacks that result in significant financial losses. The majority of security has been shared with a third party, and manufacturers must rely on the third party's confidence. Insider threats, a lack of governance over shared data, and a slew of other dangers might all be present. The majority of the literature focuses solely on the functioning of industrial 4.0 automated systems, with security being treated as a secondary issue or feature. Due to its varied design, reliance on private and sensitive data, and large-scale deployment, CPS is vulnerable to a number of physical and cyber security risks, including side channel attacks. [4].

Previously, industrial security was achieved via approaches such isolation based on physical access control. IP controls have been an essential element of networking with the introduction of remote working capabilities via Ethernet. As a result, the danger level has grown significantly, as has the number of vulnerabilities. PLC (Programmable Logic Controller), RTU (Remote Terminal Unit) systems, and SCADA servers were all searched using a custom IoT search engine called SHODAN. Servers for HMI (Human Machine Interface) and DCS (Distributed Control Sensors) have been targeted. [5].

The CPS has IoT systems, sensors, CNCs, and RFIDs, among other devices. Securing access to some of these devices is difficult due to poorly developed or configured authentication mechanisms. According to the Open Web Application Security Project (OWASP), CPS and IoT devices contain hardcoded passwords or passwords that are

easily guessable, and some of these credentials are publicly accessible. These gadgets, according to OWASP, lack physical security, making them vulnerable to side channel attacks. CPS devices also contain susceptible network services, which are unneeded facilities that operate on the gadgets and are accessible to the web, enabling unwanted sources to directly manipulate them. As a result, getting illegal access to computer systems is less difficult than obtaining authorized access.

On most CNC (Computer Numerical Control) units, whether the HMI (Human Machine Interface) has soft keys, key switches, or conventional keyboards, these units can be exploit because they are open to everyone. On some models, only the physical key is used to control the physical access. There are no access monitoring solutions in CPS devices [6]. As a result, intentional or accidental exposures of these systems might have disastrous consequences, forcing the implementation of comprehensive security measures. Considering these requirements, allowing these physical security systems to monitor a person's every activity must be accompanied with the presumption that this information will be used only for the purpose intended and will be secured against malicious use or unauthorized access, as well as to prevent network cyberattacks and to build strengthen security [7]. And, access control system capable of logging who accessed where and when, they can provide valuable data to help to track authorized or unauthorized accesses.

Fingerprint scanner is used to implement physical access control system in this project. A fingerprint scanner is a biometric sensor that recognizes and detects human fingerprints. Because a fingerprint scanner can recognize human fingerprints with a considerably higher degree of precision, it results in a quicker system. This project's fingerprint scanner can make a decision in less than a second. In this project, an optical fingerprint scanner is utilized since it gives more benefits than other biometric features, as stated in Table.

Table 1.1: Various biometric authentication techniques [8]

Technology	Deceivability	Uniqueness	Feasibility	Stability	Cost	Collectible	Catholicity
Signature	High	Low	Low	Low	Low	High	Low
Face shape	High	Low	Low	Mid	High	High	High
Voice	High	Low	Low	Low	Low	Mid	Mid
Fingerprint	Mid	High	High	High	Low	Mid	High
DNA	Low	High	High	High	High	Mid	High
Iris	Low	High	High	High	High	Mid	High
Retina	Low	High	High	Mid	High	Low	High
Ear shape	Mid	Mid	Mid	High	High	Mid	Mid
Hand shape	Mid	Mid	Mid	Mid	High	High	Mid
Palm	Mid	High	High	High	Low	Mid	Mid

1.3 Research Gap

Because the growth of usefulness, rather than defense, drives industrial 4.0 production systems. As a result of the lack of security design in industrial automation systems, the quantity and complexity of cyber-attacks is rising, and cyber security needs have not been recognized.

In IIoT development, wireless networks are utilized to gather data for authorized users. In a wireless network, the platform provides instructions to terminal nodes, while the terminal nodes gather and relay data to the platform. Mutual authentication is necessary during the communication process to ensure the network's security.

Then we create an automated system that focuses on cyber security issues such as authentication, authorization, and accounting in cps devices both physically and conceptually.

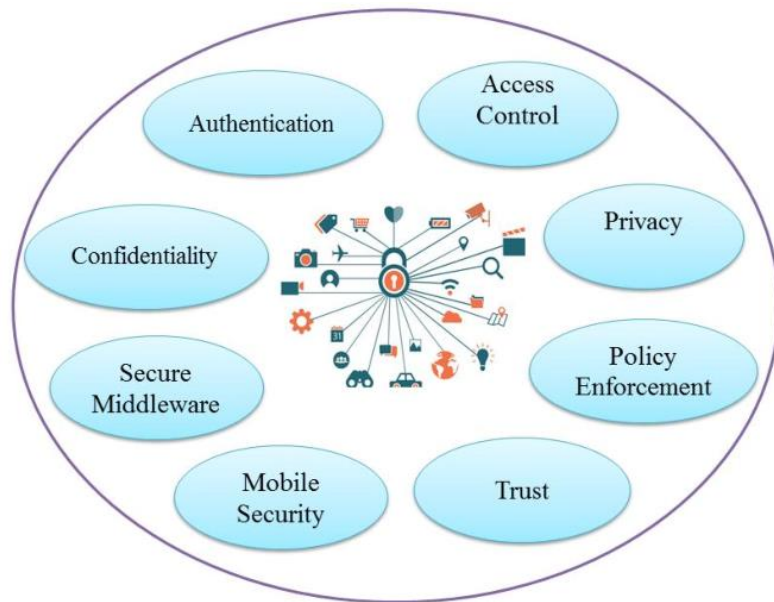


Figure 1.2: Security requirements for the IIoT

2. Research Problem

Smart computing is combined with technologies such as IoT, cognitive computing, machine learning, and data analytics when automating a manual or semi-automated system in the direction of the fourth industrial revolution (Industry 4.0). When building an industrial 4.0 automated system, most system developers are unaware of the cyber security problems. The goal of the study is to find applications of cyber security needs that haven't been fully covered by automation.

Challenges:

The creation of an effective security working environment.

With the aid of a CPPS platform based on CPS technology, the Industry 4.0 system environment is growing. The CPPS platform is a difficult project that is currently hindered by several issues, including the CPS difficulties described below.

2.1. Collaboration between different systems

Exchanging information, storing information, documenting, decision-making, and corrective and preventative action all require a collaborative paradigm between physical systems and computer networks [9].

2.2. Centralized security management

Using a centralized control system such as Supervisory control and data acquisition (SCADA) to apply security configurations/updates to physical devices and monitor physical devices to enhance efficiency [10]. In addition to the CPS modeling language, physical devices, software, and hardware platforms, as well as other functional and non-functional factors, must be included in a typical CPS model [9].

2.3. Secure communication

CPS that use the SCADA systems is connected to the internet over TCP/IP protocols without additional protection [11], which have known vulnerabilities.

2.4. Insecure Data

There was a lack of system interfaces to assure data security for industrial businesses throughout the deployment of Industry 4.0. IoT-based CPSs, which are connected to a large number of embedded sensors and communication devices, offer a major risk due to the increase in data use and the increased possibility of system breaches [12].

2.5. Initial Cost

Industry 4.0 migration In a manufacturing firm, will result in end-to-end integration to develop and execute the architecture according to the business demands a significant initial investment in terms of money and time is necessary [13].

2.6. Lack of strategy to Industry 4.0

In the manufacturing industry, there is a lack of a dynamic strategy plan to assist the transition to Industry 4.0 [14].

3. OBJECTIVES

3.1 Main Objective

The major goal is to include Authentication, authorization, and accounting (AAA). Authenticate users when communicating with IIoT devices to enable secure access to services, monitor and filter user behavior on the system to prevent illegal entry and network attacks, and develop strong security to protect the system for small to medium industry 4.0 companies are my security components. This primary goal is broken down into three sub goals: access log viewing, report creation, and alerting the user when an abnormality occurs.

3.2 Sub Objectives

3.2.1 Access log visualization

The ability to log, monitor, and evaluate all identification events in this proposed system is critical for recognizing security threats and maintaining customer data for compliance reasons. We want to make sure that the system creates sufficient authentication records and that they will be stored in a standardized, easy and effective way that enables for complex log analysis.

3.2.2 Report generation

This suggested tool has a feature that allows you to generate reports depending on audit results. Weekly or monthly reports can be set for automated creation. As a consequence, these audit reports may be utilized to show the security settings of the system.

3.2.3 Alert user when an anomaly occurs

Something that is out of the usual in compared to the norm is referred to as an anomaly. The most practical way is to utilize an analytics platform with anomaly detection algorithms capable of swiftly analyzing huge amounts of data and detecting anomalies. Essentially, everything that differs from previous data should be regarded as an abnormality.

4. METHODOLOGY

4.1 System Diagram

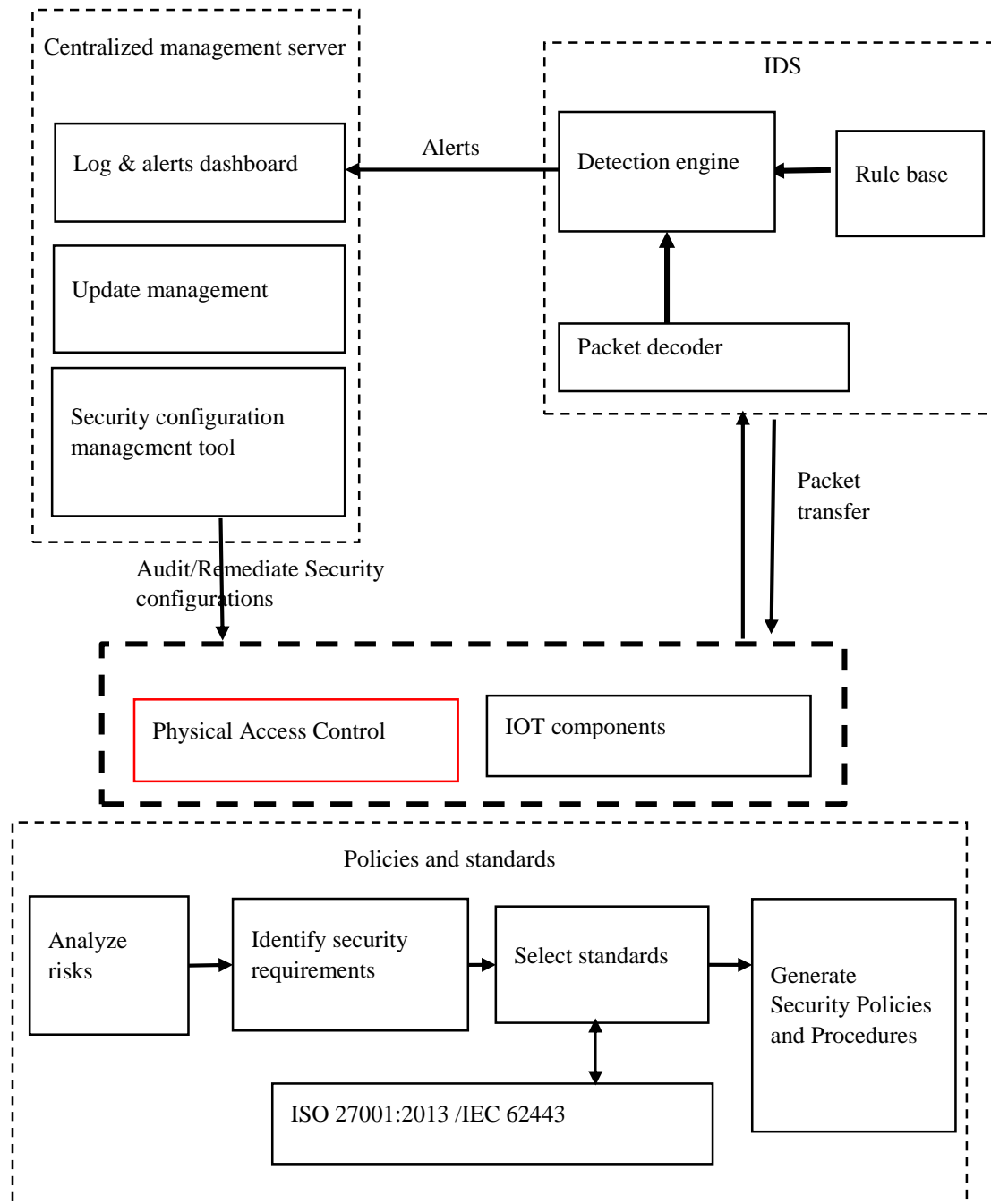


Figure 4.1: Overall system diagram

My component of physical access control system is highlighted in the above entire system diagram. It shows how fulfill our main security solution of industry 4.0 garment manufacturing system. Authenticate users connecting to IIoT devices and provide safe accessibility, as well as track and analyze user activities on the system to avoid illegal entry and harmful assaults.

4.2 Individual Component

My workload is broken down into the following sections.

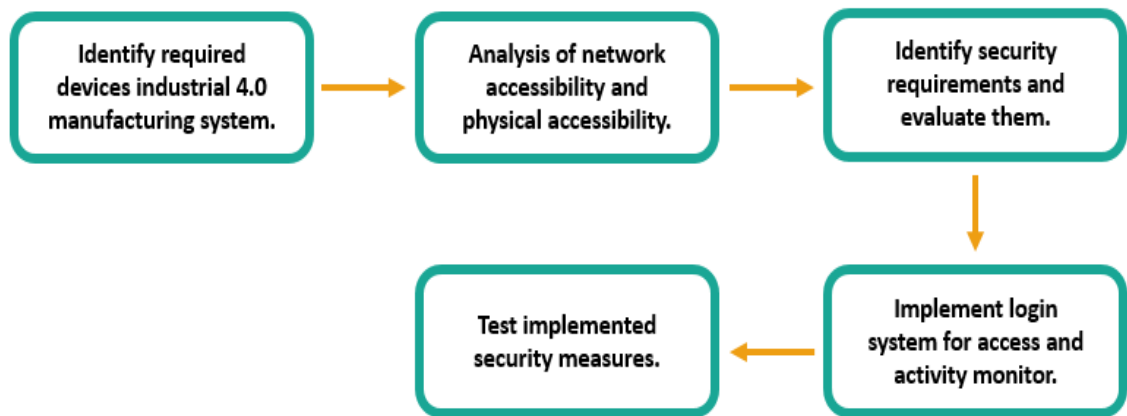


Figure 4.2: Workflow

4.2.1 Identify required devices

The cutting process in the garment sector production is the subject of this study. Following that, we discovered a CNC cutting machine, as well as several IoT gadgets, smart objects, and sensors. To make future security solutions easier, these detected devices needed to be classified according to their device type. To achieve our main goal, a first background research was done to acquire information concerning authentication and access monitoring.

The main project idea was discussed with the supervisor and co-supervisor as the first stage. The panel received the topic evaluation document, which included individual sub-components. Then constructing a Gantt chart and establishing a work breakdown structure after the project was authorized.

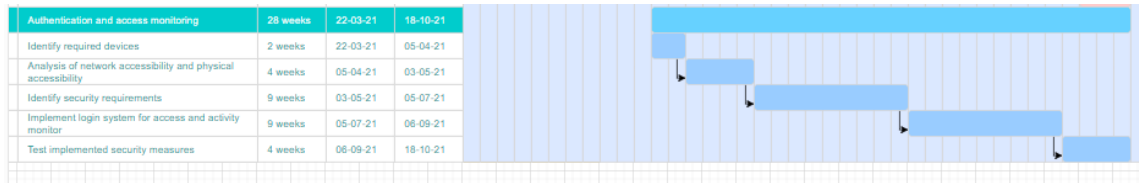


Figure 4.3: Gantt chart

Then, to have a deeper understanding of the clothing business and local garment manufacturing equipment, we went to a local knit wear garment manufacturing plant. The industrial tour provided a deeper understanding of the cutting process and associated machinery.

After that, we went to the Peradeniya Engineering Faculty in Sri Lanka to acquire a better understanding of how CNC machines function and how to collaborate on IoT and cyber security for the available local CNC systems, as shown below.

After reading the existing literature on the subject, it was necessary to have a better understanding of the present state of the local apparel industry and CNC machines.



Figure 4.4: Observe CNC devices



Figure 4.5: Observe CNC devices' control panel



Figure 4.6: Observe CNC devices' software



Figure 4.7: Observe CNC devices

The industrial visit gave us a thorough observation of the following:

- What kind of CNC machines are used
- The present security aspect of CNC machines
- What components we should pay special attention
- What relevant software and hosted operating systems are available
- Workflow of a CNC machine
- CNC machine operations
- Security knowledge of the operators
- General overview of the working environment of a process
- Recognize the industrial control system.
- Aware of the roles in industries

4.2.2 Analysis of network accessibility and physical accessibility

We want to make sure that legitimate, trustworthy access to systems, services, and IoT devices is available. Determine who wants access and who doesn't, as well as the identification and access monitoring techniques utilized.

On most CNC units, whether the HMI has soft keys, key switches, or conventional keyboards, these units can be exploit because they are open to everyone. On some models,

only the physical key is used to control the physical access. As a result, intentional or accidental exposures of these systems might have disastrous consequences, forcing the implementation of comprehensive security measures.



Figure 4.8: CNC machine's control panel

4.2.3 Identify security requirements

The most essential activity in enhancing awareness between the business and innovation teams is analysis. For each device, we want to do a risk evaluation and examine the CPS-based risks and vulnerabilities. The threats to systems and information are then prioritized and rated.

A heat map was created for the key assets based on the information obtained from the Octave risk assessment to indicate which risks are most likely to arise in the system.

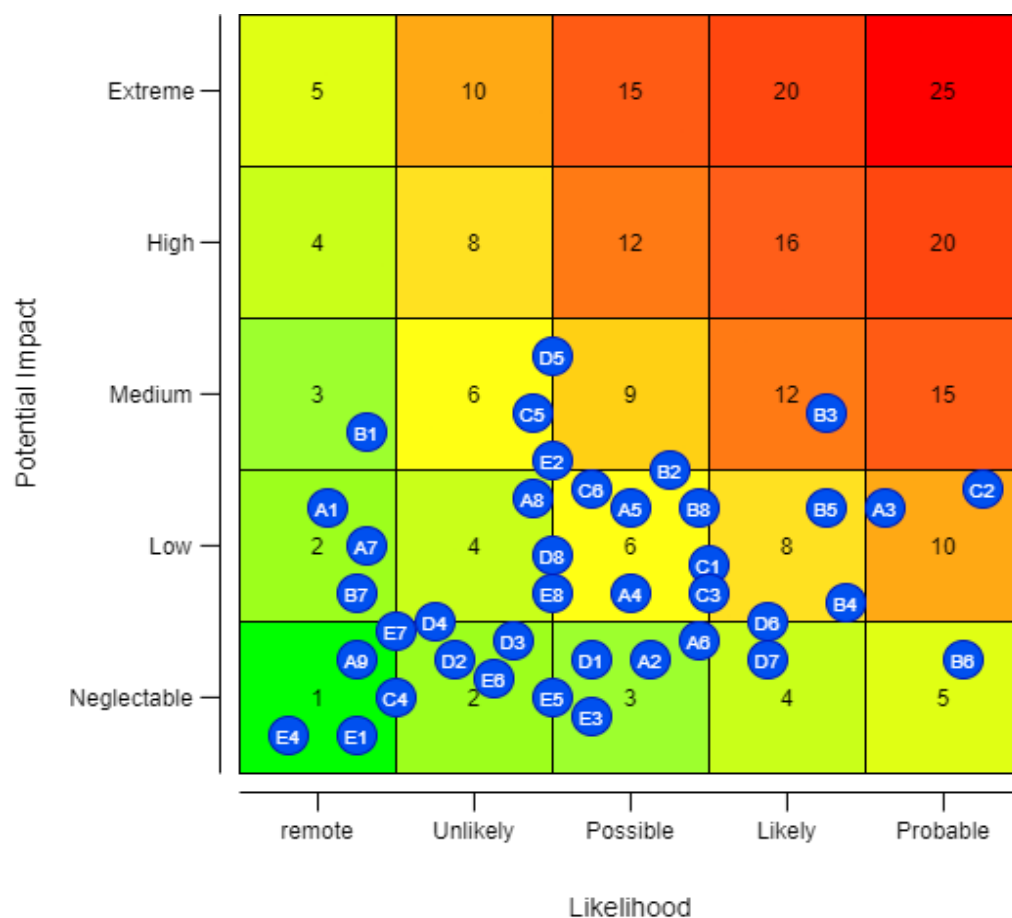


Figure 4.9: Heat map

Table 4.1: Threats

ID	Name
A1	Unauthorized access to ansible controller via network - Ansible controller
A2	Disclosure of access credentials - Ansible controller
A3	Denial of service attacks - Ansible controller
A4	Unauthorized access to ansible controller via console - Ansible controller
A5	Ransomware - Ansible controller

A6	Spyware - Ansible controller
A7	Power outage - Ansible controller
A8	Trojan - Ansible controller
A9	Overloading system storage - Ansible controller
B1	Overheat - IOT
B2	Ransomware - IOT
B3	Unauthorized access to ansible controller via network - IOT
B4	Disclosure of access credentials - IOT
B5	Denial of service attacks - IOT
B6	Spyware - IOT
B7	Power outage - IOT
B8	Overloading system storage - IOT
C1	Unauthorized network scans and reconnaissance attacks - Internal network
C2	DOS attack - Internal network
C3	Unauthorized connected devices - Internal network
C4	Backdoors - internal network
C5	Malware - internal network
C6	Brute force attacks - internal network
D1	Automated CNC machines can be left unattended - CNC
D2	power failure - CNC

D3	Natural disaster - CNC
D4	Overheat - CNC
D5	Hardware failure - CNC
D6	Unauthorized access through network - CNC
D7	Unauthorized connected devices - CNC
D8	Malware - CNC
E1	Power outage - Sensors
E2	Hardware failure - Sensors
E3	Unauthorized access through an unsecured network - Sensors
E4	Unauthorized access through outdated and insecure devices - Sensors
E5	Tamper a network physically - Sensors
E6	Natural disaster - Sensors
E7	Overheat - Sensors
E8	Unauthorized connected devices - Sensors

4.3 Commercialization

Most manufacturers use Industry 4.0 to increase productivity, and security isn't a top priority for them. Only bigger firms have the financial resources to engage cyber security experts to protect their production systems. Despite this, most manufacturers ignore security or delegate security management to other parties. Due to economic restrictions, small and medium enterprises may have to entirely disregard security. To safeguard their systems, large, medium, and small industry 4.0 manufacturers can use this physical access control system. This system is low budget access control system using arduino platform. As a result, manufacturers may save money on security. Instead of executing the same security processes manually, industry 4.0 manufacturers may decrease production loss due to security procedures by employing the physical access control system. We will gauge our target audience through social media like Facebook, Twitter, and Instagram campaigns and website.

5. TESTING & IMPLEMENTATION

5.1 Implement login system for access and activity monitor

The Access Control System is used to identify, authenticate, and authorize a person that access into the premises or devices, ensure the system's security and offering comprehensive protection. Authentication is provided secure access to services, and monitor and filter user behavior on the system to avoid unauthorized access and venomous network assaults. To achieve our main goal, a first background research was done to acquire information concerning authentication and access monitoring. It provides security by allowing for flexible control about who is allowed to access.

5.1.1 Requirement Analysis

The project operations are carried out in accordance with the process flow shown in Figure 5.1. The method depicts the activities from start of the project to its conclusion.

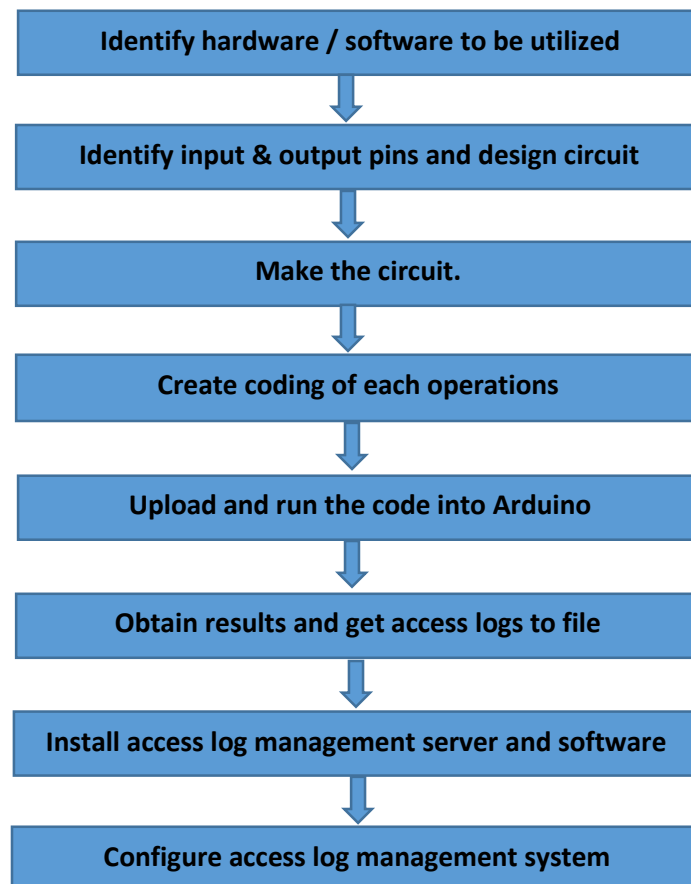


Figure 5.1: Flow chart of the project

Hardware requirements:

- Arduino board
- Fingerprint sensor
- Solenoid door lock
- Bluetooth module
- Breadboard
- 9V batteries
- Jumper wires
- Transistor
- USB cable

5.1.1.1 Arduino Uno R3 board

The Arduino Uno is a microcontroller board designed by Arduino that uses the ATmega328P microprocessor. This is the third version of an Arduino board, which was introduced in 2011. On this board, we can find 14 digital input/output pins, 6 analog inputs, a 16 MHz ceramic resonator, an USB connector, a power jack, an ICSP header, and a reset button. It comes with everything that need to get started with the microcontroller; simply plug it into a computer with a USB connection or power it with an AC-to-DC converter or battery [15].



Figure 5.2: Arduino board

The following are the specifications for the Arduino Uno R3 board:

- Microcontroller based on the ATmega328P
- The Arduino's operating voltage is 5V.
- 7V to 12V is the recommended input voltage range.
- EEPROM is 1 KB
- The boot loader uses 0.5 KB of flash memory and 32 KB of flash memory.
- Each I/O Pin has a DC current of 20 mA.
- Pins for digital input and output (PWM)-6
- Pins for digital input and output-14
- The CLK operates at a frequency of 16 MHz.
- 50 mA is the DC current utilized for the 3.3V pin.
- There are 6 analog i/p pins.

5.1.1.2 Fingerprint sensor

Fingerprint sensor modules, such as the one shown below, make fingerprint recognition more accessible and simple to include into projects. In control access systems, fingerprint

scanners are frequently used. The reason for this is that each individual has a unique fingerprint minutia that helps in properly recognizing a person's real data. This implies that collecting, registering, comparing, and searching fingerprints is a breeze.

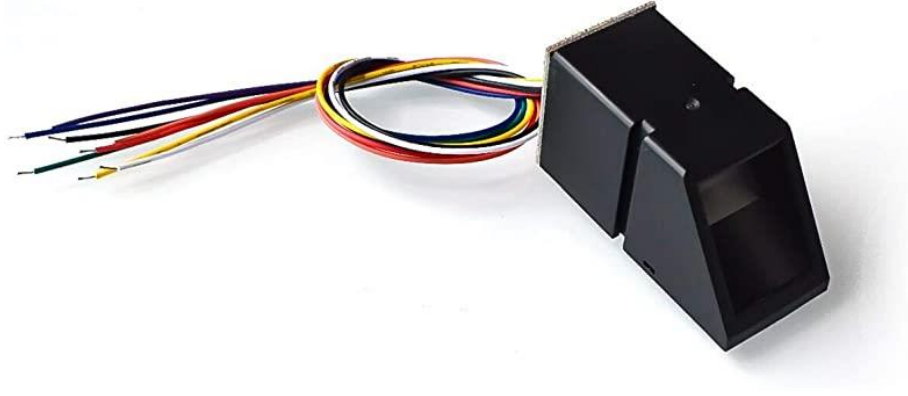


Figure 5.3: Fingerprint Sensor

Optical and capacitive fingerprint scanners are the two types of fingerprint sensors. The distinction among these two types of fingerprint scanners is that the optical fingerprint sensor catches fingerprints using light, while the capacitive fingerprint scanner captures minutiae using electricity. The optical scanner is utilized in this project since it is less susceptible to electrostatic discharge (ESD) than a capacitive fingerprint sensor.

These modules include flash memory to store fingerprints and operate with any TTL serial microcontroller or system [16]. Attendance tracking systems, security systems, and door locks, and other systems can all benefit from these modules. This sensor can store 127 unique fingerprints.

5.1.1.3 Bluetooth module HC 05

Bluetooth is a great example of a wireless connection. It may be used in a variety of ways. Bluetooth consumes very little electricity. The HC-05 is a Bluetooth module that can send and receive data. Hence it is full duplex. It is compatible with the majority of microcontrollers. Because it employs the Serial Port Protocol(SSP), it is able to do so. This Bluetooth module communicates using a 9600 baud rate USART (Universal

Synchronous/Asynchronous Receiver/Transmitter) [17]. It can simply be connected to a laptop or a mobile phone through Bluetooth.

Software requirements:

- Arduino IDE
- Ubuntu server
- Elastic stack

5.1.1.4 Arduino IDE

The Arduino Uno R3 can be programmed with the Arduino IDE software. Writing code, compiling the code to see if there are any issues and uploading code to the arduino board is very easy with the Arduino Software (IDE). This program can be used with any Arduino board in the market. To support the languages C and C++, the Arduino IDE includes its own set of code structure rules. The software library that comes with the Arduino IDE and allows you to do a variety of basic input and output functions. It is a cross-platform application that works with all operating systems, including Windows, Linux, and macOS. When a user creates and compiles code, the IDE produces a Hex file, which is then delivered to the board via USB connection.

5.1.1.5 Log management server

Logs of access are gathered and sent to a log management server, where administrators can search, visualize, and analyze logs in any time. This can be accomplished with either a local or cloud-based server. We utilized a local server running the Ubuntu server operating system for testing this project.

5.1.1.6 Elastic stack

Elastic Stack is a collection of free software Elastic products that enable user to discover, analyze, and visualize data in real time in any format and from any sort of source. Elastic Search, Logstash, and Kibana are the three key components that make up an Elastic stack.

Elastic Search – Engine for search and analytics.

Logstash – Pipeline for data processing

Kibana – Data visualization dashboard

5.1.2 Implementation

In below figure represent the process of the physical access control system.

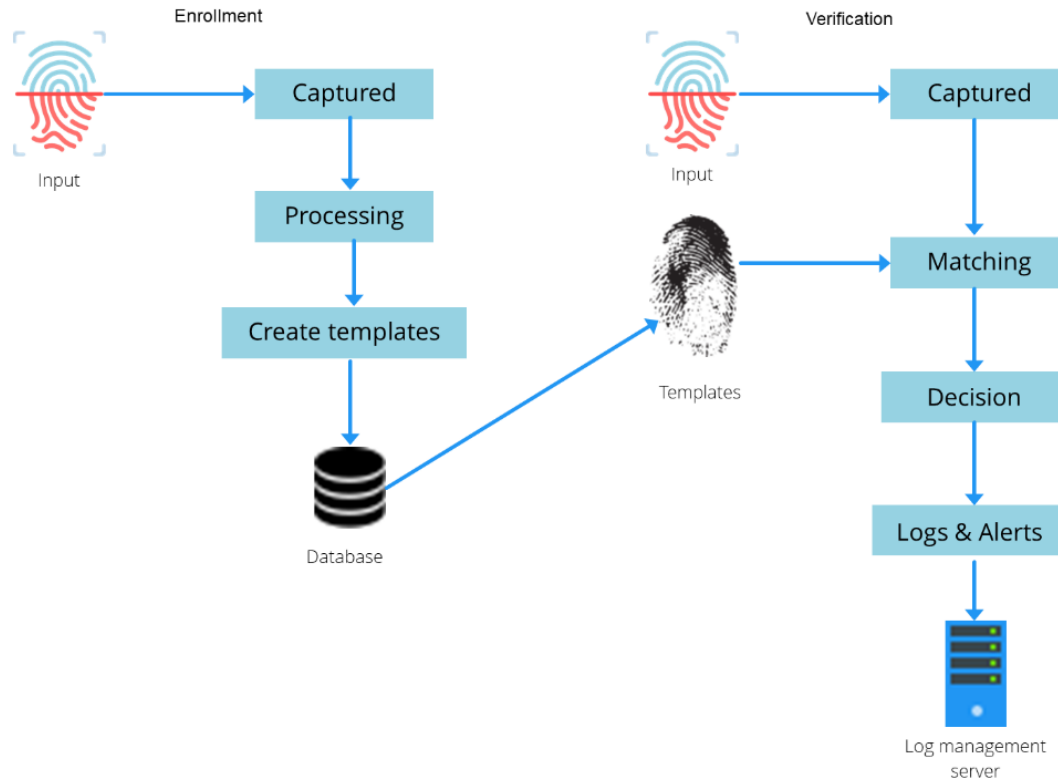


Figure 5.4: Physical access control system diagram

All of the research knowledge and components acquired will be put to use in this implementation phase. To achieve our main goal, we conducted preliminary study to gather information on authentication and access monitoring.

We must first discover how to utilize the fingerprint sensor on its own. The connections are quite easy; this fingerprint sensor has six wires, of which only four are needed for Arduino interface, with two cables used for power and two for data.

The table below demonstrates how to connect the fingerprint sensor to the Arduino.

Table 5.1: How to connect the fingerprint sensor to the Arduino

Arduino	Fingerprint Sensor
GND	GND
5V or 3.3V	VCC
Digital pin 3	RX
Digital pin 2	TX

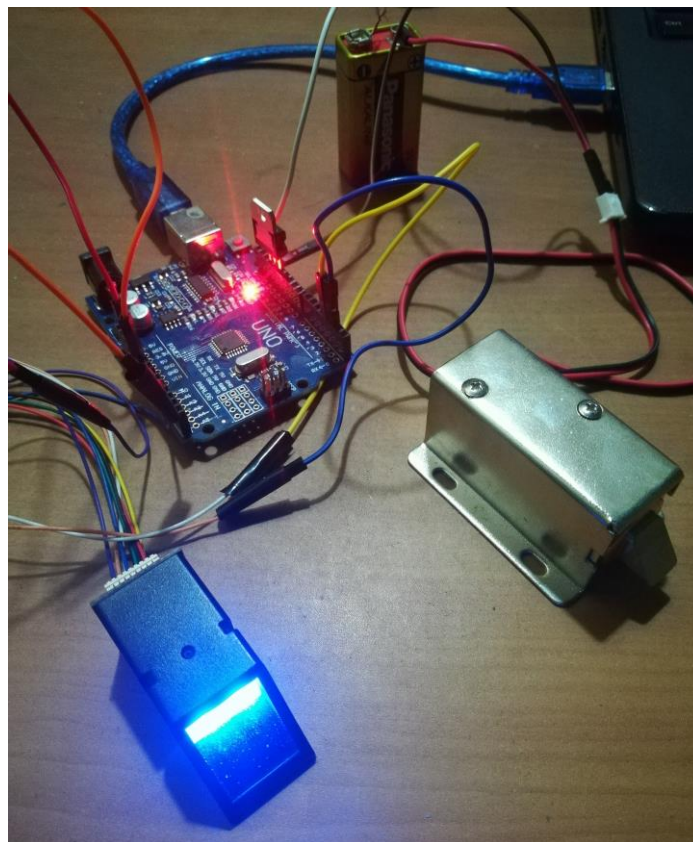
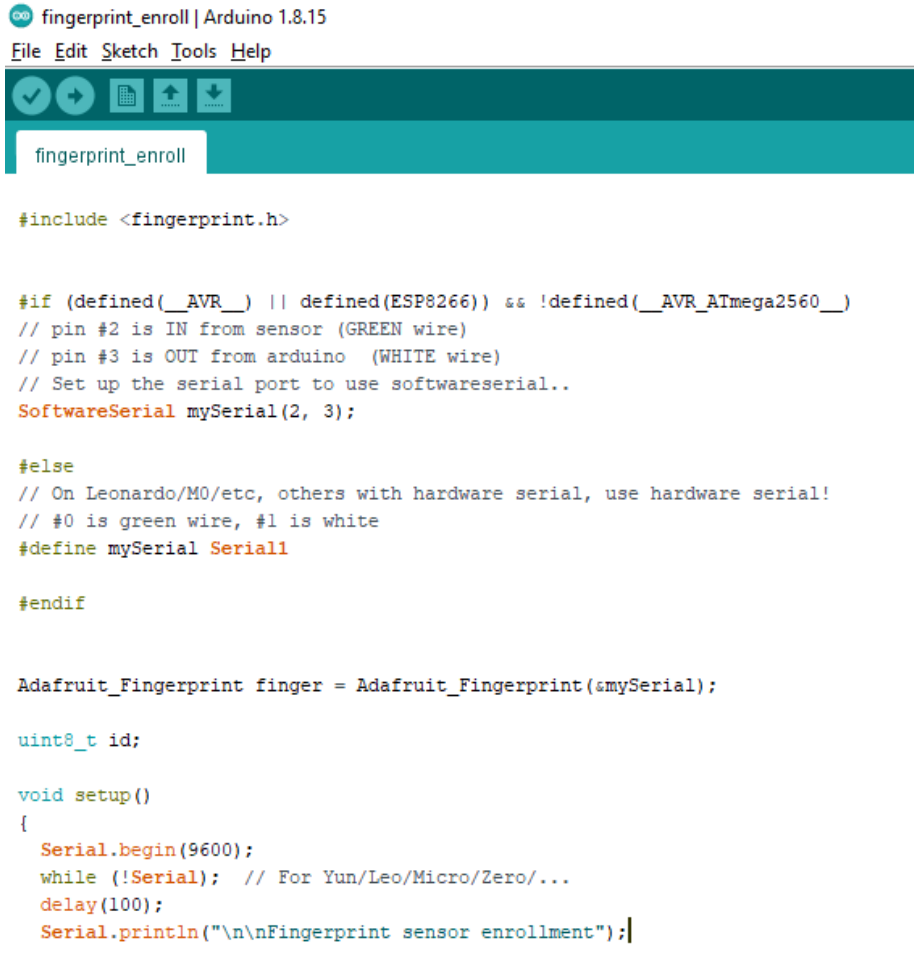


Figure 5.5: Connect the fingerprint sensor to Arduino

When you acquire the fingerprint module, it does not have any fingerprints recorded in its memory, therefore we must first enter our information.



```
#include <fingerprint.h>

#if (defined(__AVR__) || defined(ESP8266)) && !defined(__AVR_ATmega2560__)
// pin #2 is IN from sensor (GREEN wire)
// pin #3 is OUT from arduino (WHITE wire)
// Set up the serial port to use softwareserial..
SoftwareSerial mySerial(2, 3);

#else
// On Leonardo/M0/etc, others with hardware serial, use hardware serial!
// #0 is green wire, #1 is white
#define mySerial Serial1
#endif

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

uint8_t id;

void setup()
{
  Serial.begin(9600);
  while (!Serial); // For Yun/Leo/Micro/Zero/...
  delay(100);
  Serial.println("\n\nFingerprint sensor enrollment");
}
```

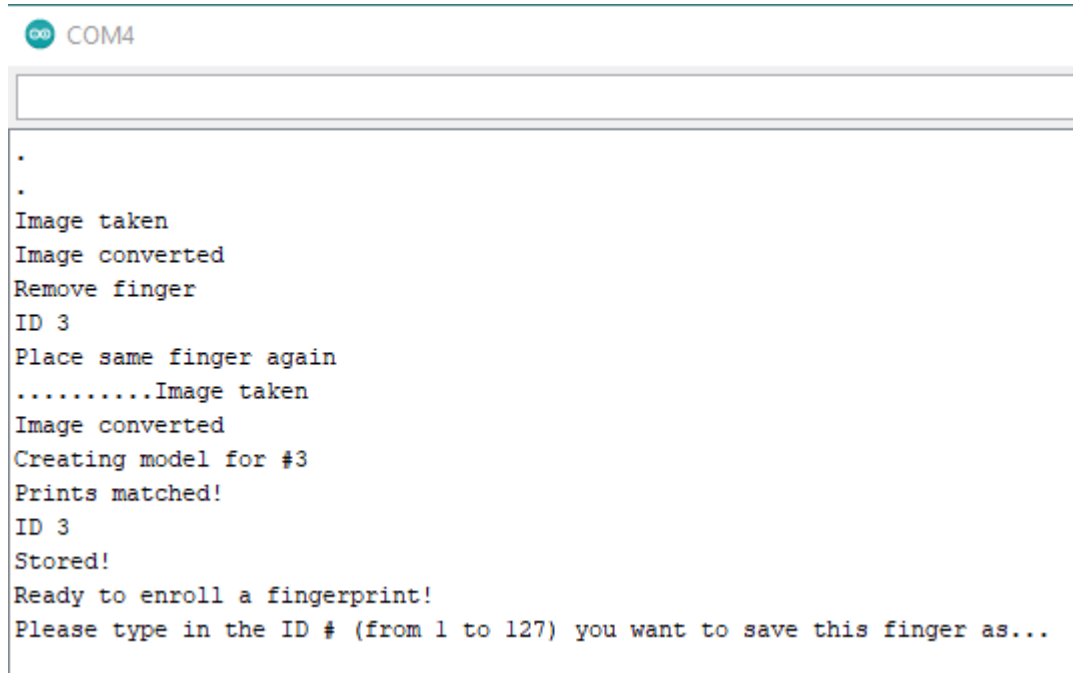
Figure 5.6: Fingerprint enrollment code 1

```
uint8_t getFingerprintEnroll() {

  int p = -1;
  Serial.print("Waiting for valid finger to enroll as #"); Serial.println(id);
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
      case FINGERPRINT_OK:
        Serial.println("Image taken");
        break;
      case FINGERPRINT_NOFINGER:
        Serial.println(".");
        break;
      case FINGERPRINT_PACKETRECEIVEERR:
        Serial.println("Communication error");
        break;
      case FINGERPRINT_IMAGEFAIL:
        Serial.println("Imaging error");
        break;
      default:
        Serial.println("Unknown error");
        break;
    }
  }
}
```

Figure 5.7: Fingerprint enrollment code 2

Open serial monitor and choose the 9600 baud rate after uploading the code to the Arduino. When Arduino detects a fingerprint scanner, the user must be send the number for the ID between 1 and 127 to the place where you wish to save the new fingerprint. Enter ID and follow the on-screen instructions. Scan the finger once, then remove it and scan it again to save the updated information. Fingerprint is stored now on the database. Figure 5.8 shows the outcome of a fingerprint registration. The user's fingerprint minutiae is enrolled with the ID 3 as shown in the image below. It is then saved in the onboard flash memory of the fingerprint scanner.

A screenshot of a serial monitor window titled 'COM4'. The window shows a series of text messages from an Arduino. The messages are: a blank line, a period, another blank line, 'Image taken', 'Image converted', 'Remove finger', 'ID 3', 'Place same finger again', '.....Image taken', 'Image converted', 'Creating model for #3', 'Prints matched!', 'ID 3', 'Stored!', 'Ready to enroll a fingerprint!', and 'Please type in the ID # (from 1 to 127) you want to save this finger as...'.

```
.  
.  
Image taken  
Image converted  
Remove finger  
ID 3  
Place same finger again  
.....Image taken  
Image converted  
Creating model for #3  
Prints matched!  
ID 3  
Stored!  
Ready to enroll a fingerprint!  
Please type in the ID # (from 1 to 127) you want to save this finger as...
```

Figure 5.8: Fingerprint enrollment output

Another code that detects the scanned fingerprint is now given. Upload the scan fingerprint code shown below using the same schematic as previously.



```
fingerpint_verify | Arduino 1.8.15
File Edit Sketch Tools Help

fingerprint_verify

void loop()
{
  getFingerprintID();
  delay(50);
}

uint8_t getFingerprintID() {
  uint8_t p = finger.getImage();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println(" ");
      Serial.println("Image taken");
      break;
    case FINGERPRINT_NOFINGER:
      //Serial.println(".");
      return p;
    case FINGERPRINT_PACKETRECEIVEERR:
      Serial.println("Communication error");
      return p;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      return p;
    default:
      Serial.println("Unknown error");
      return p;
  }

  // OK success!
```

Figure 5.9: Fingerprint verification code 1

```

// found a match!
Serial.print("Found ID #"); Serial.print(finger.fingerID);
Serial.print(" with confidence of "); Serial.println(finger.confidence);

if (Serial.available()) {
    processSyncMessage();
}
if (timeStatus() != timeNotSet) {
    digitalClockDisplay();
}
if (timeStatus() == timeSet) {
    digitalWrite(13, HIGH); // LED on if synced
} else {
    digitalWrite(13, LOW); // LED off if needs refresh
}

return finger.fingerID;
}

```

Figure 5.10: Fingerprint verification code 2

The saved minutiae must be verified once the fingerprint has been enrolled to ensure that the fingerprint scanner is accurate. Place your finger on the sensor and open the serial monitor as shows in Figure 5.11. That is all there is to it. ID was found, which is the ID for the finger that was previously scanned. The fingerprint sensor has an amount of confidence that ranges from zero to 255, indicating how precise it is. It expresses the level of confidence in the correctness of the present scanned fingerprint and those kept in flash memory.

```

Waiting for valid finger...
Sensor contains 3 templates

Image taken
Image converted
Found a print match!
Found ID #3 with confidence of 68
20:20:43 4 7 2021

Image taken
Image converted
Did not find a match
20:20:47 4 7 2021

Image taken
Image converted
Found a print match!
Found ID #1 with confidence of 192
20:20:54 4 7 2021

```

Figure 5.11: Finger test output at serial monitor

The table below shows how to connect the Bluetooth module to the Arduino board.

Table 5.2: How to connect the Bluetooth module to the Arduino

Pins in Arduino	Pins in Bluetooth module
GND	GND
5V	VCC
TX (Pin 1)	RX
RX (Pin 0)	TX

The data is received by the Bluetooth module and sent to Arduino through the TX pin of the Bluetooth module (RX pin of Arduino).

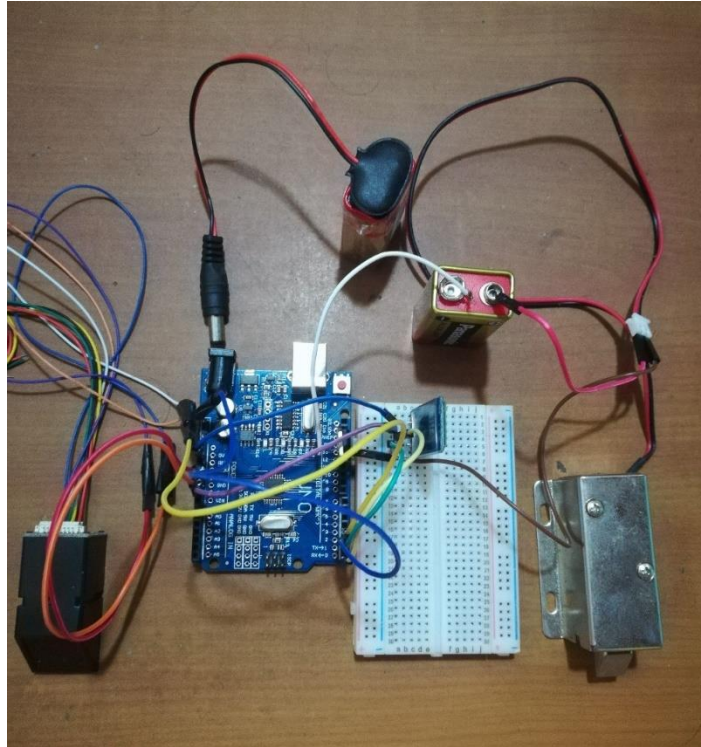


Figure 5.12: Connect the Bluetooth module to system

Two 9V power supplies are used in the circuit shown in Figure 5.12. The solenoid electric lock requires 9V, but an Arduino Uno board requires just 5V.

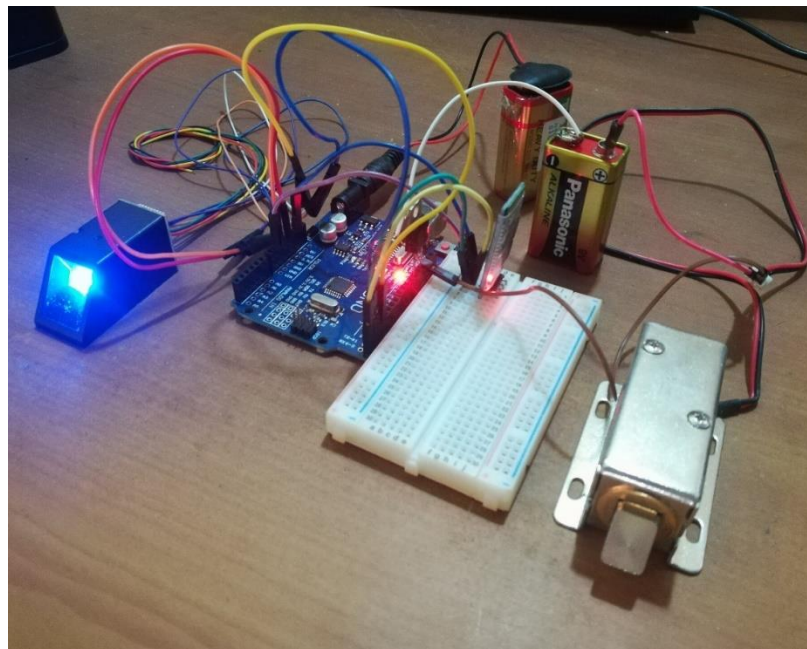


Figure 5.13: Implemented physical access control system

Now, Elastic stack must be installed to the Ubuntu server to gather and visualize the access logs. First, Elasticsearch can be install using elastic website. Elasticsearch can quickly store, search, and analyze large amounts of data. After that install Kibana dashboard to the server. A web-based interface makes it simple to retrieve and comprehend enormous amounts of data. The user has complete control over the creation and customization of data charts and graphs for presentation. Kibana is a tool for searching, analyzing, and visualizing with Elasticsearch data. To show access logs, the Kibana dashboard works in combination with Elasticsearch. Then, installing and configuring Logstash to the system. Although Beats can send data straight to Elasticsearch, it is more usual to process the data via Logstash. This gives you more options for gathering data from many sources, transforming it into a common format, and exporting it to another database. The Elastic Stack collects data from multiple sources and transports it to Logstash or Elasticsearch using Filebeat data shippers. Finally, it must be install to the log management server. After that, set up Filebeat to connect to Logstash. Go to <http://localhost:5601> in the browser to access Kibana. The Kibana home page will be displayed.

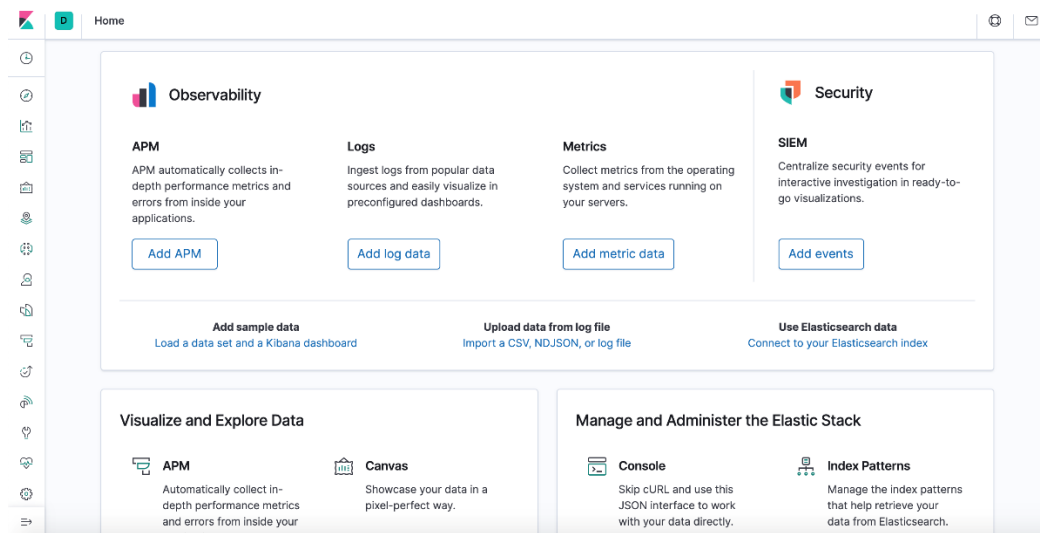


Figure 5.14: Kibana home page

Now, we can search and read access logs, as well as modify the dashboard.

5.2 Test implemented security measures

The testing step begins once the installation and configurations have been verified. Security testing is the most important type of application testing since it ensures that personal data remains private. The tester acts as an intruder and manipulates the system in this type of testing. The purpose of security control testing is to guarantee that all security measures are correctly applied.

For the testing purpose, matching and unmatching fingers are scanned using the fingerprint sensor and got the following results as access logs.

1	Time	Date	Capture status	Image status	Template status	Fingerprint ID	Confidence Level
2	1:55:02 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 241
3	1:55:03 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 220
4	1:55:06 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #3	with confidence of 201
5	1:55:07 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #3	with confidence of 415
6	1:55:08 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #3	with confidence of 201
7	1:55:10 AM	10/1/2021	Image taken	Image_converted	Did not find a match	.	
8	1:55:11 AM	10/1/2021	Image taken	Image_converted	Did not find a match	.	
9	1:55:14 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 308
10	1:55:15 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 216
11	1:55:18 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #3	with confidence of 317
12	1:55:20 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 124
13	1:55:23 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #3	with confidence of 206
14	1:55:25 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 164
15	1:55:27 AM	10/1/2021	Image taken	Image_converted	Did not find a match	.	
16	1:55:29 AM	10/1/2021	Image taken	Image_converted	Did not find a match	.	
17	1:55:32 AM	10/1/2021	Image taken	Image_converted	Did not find a match	.	
18	1:55:33 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 194
19	1:55:35 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 177
20	1:55:36 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 228
21	1:55:38 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #3	with confidence of 129
22	1:55:40 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #2	with confidence of 57
23	1:55:42 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #1	with confidence of 125
24	1:55:45 AM	10/1/2021	Image taken	Image_converted	Did not find a match	.	
25	1:55:48 AM	10/1/2021	Image taken	Image_converted	Found a print match!	Found ID #3	with confidence of 265

Figure 5.15: Access logs

6. RESULTS & DISCUSSION

Authentication and access control is required to provide comprehensive management of data and permissions across organizations that coordinate throughout the industrial life cycle because of the multiplicity of attack points. A fingerprint smart door lock lowers the risk of break-ins by replacing traditional locks with keys that can be stolen or misplaced. A physical smart lock that fuses fingerprint technologies for better identification accuracy and security. It is a reliable solution for all CPS and IoT devices. And also the level of confidence indicates how well your current fingerprint matches that of the sensor database. So in this sensor database we can store 127 fingerprints and it has a false acceptance rate of less than 0.001%, making it quite safe. This physical smart lock system has an alert function that will notify you if there is a failed access attempt and will monitor access and error records.

This fingerprint door lock system is more sophisticated, efficient, and secure than a standard protected method. A typical security system consists of locks that are unlocked when they come into contact with the right keys. The only key to opening the protected lock mechanism in our system is an authorized and matching fingerprint. A fingerprint door lock system is a biometric lock that uses a fingerprint interface as the unlocking key. Fingerprints are unique and cannot be reproduced, making them safer and more secure. There are several fundamental differences between various locking methods. Traditional lock and key systems, fingerprint lock systems, password/pin code systems, and biometric lock systems are just a few examples of security systems that can be easily implemented. Each system's advantages and disadvantages make it efficient, secure, recognizable, and difficult to breach.

The following are some key variations in performance and system structure between various security systems:

Table 6.1: Key variations in performance and system structure between various security systems

Types of differences	Traditional lock and key	Fingerprint access control
Interfaces	Key	Fingerprint
Composition	It is made up of only two parts: a lock and a key.	Fingerprint sensor and wireless connectivity are included.
Function	Unlocks by key only	Unlocks by fingerprint
Performance	Low	High

Strength	Moderate	High
Vulnerability and efficiency	Less effective and vulnerable to attack	Highly efficient as well as less vulnerable

The accuracy test is used to determine the fingerprint scanner's security level. Figure 6.1 depicts the validity test result is dependent on the level of confidence. The assessment was carried out on four people, with their two left hand fingers and two right hand fingers. Left and right thumbprints, as well as left and right index fingers, were scanned. The left thumb finger, which has a percentage of 79.9%, is the fingerprint with the highest accurate result. The accuracy of the right thumb finger, right index finger, and left index finger, respectively, is 60.6%, 70.2%, and 78.0%.

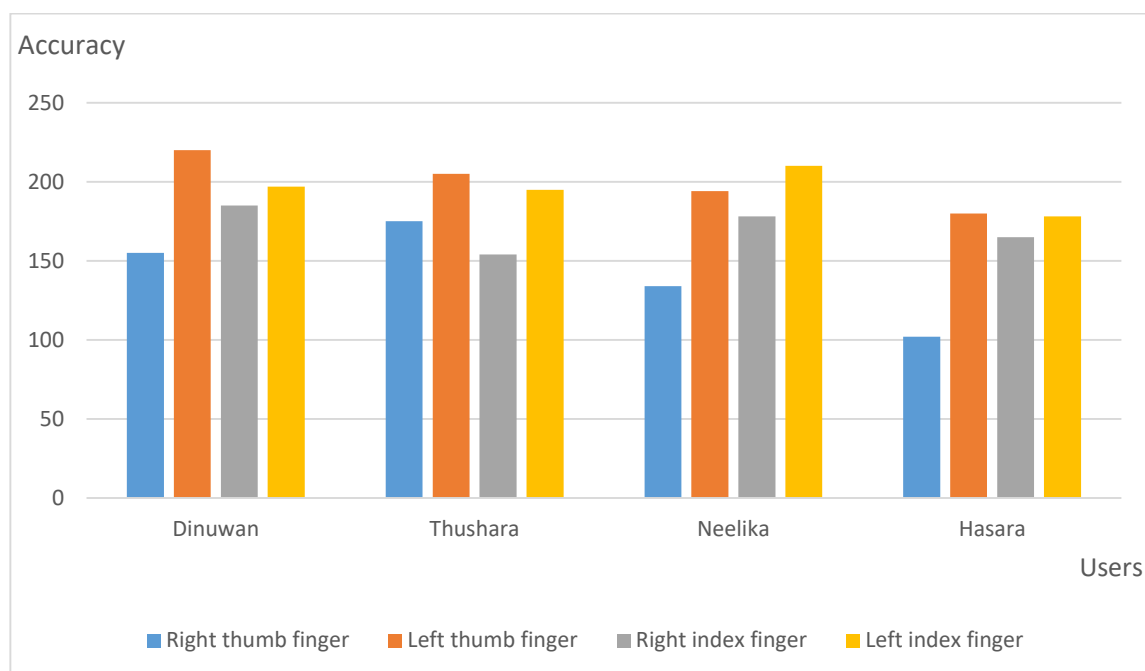


Figure 6.1: Degrees of Confidence

In comparison to other security systems, the fingerprint lock system with access logging features is extremely helpful and secure. It not only prevents unauthorized access, but it also notifies the owner of any incursion and logs access.

More intense development can improve this concept, and more features such as more locks can be added to the system. As a result, we don't need to spend as much money on a single lock if it can manage several doors. It is possible to store prints without using a computer, although this would require more parts than the ones we used. The entire mechanism should be placed within the door panel or on the other side of the door to maintain proper protection. A battery system or even a solar-powered system may be built. The adaptability of this system is one of its primary features. This system may be used to implement a variety of different systems.

The system is quite safe. Fingerprints are one-of-a-kind, and the sensor can recognize all of them during testing. It gives you more control over who has access to restricted areas. There are certain disadvantages to this system, such as It also requires a lot of power to run, thus supplying continuous power via batteries might be difficult at times. It will become unusable if there is a power outage. In such scenario, we may add rechargeable batteries to the system or link it to an Integrated Power System (IPS).

7. CONCLUSIONS

The manufacturing system will face several changes as a result of the fourth industrial revolution. However, it will introduce a number of security issues into the manufacturing system's product lifecycle. Access control mechanisms are a set of hardware, software, or firmware characteristics, as well as operational and management processes, that work together to detect and prohibit unauthorized access to information systems while maintaining its confidentiality, integrity, and availability.

This report attempted to address the issue of door security by incorporating the notion of biometrics into the door lock. As a result, this project is using finger prints as a one-of-a-kind key to construct a device that locks or unlocks a door. This report covered the many components that we would require to construct this project using Arduino, i.e. presented the project's hardware and software requirements.

The fingerprint-based door lock system may be customized and used in a variety of ways. This door locking mechanism is less expensive than the lock systems now available on the market. Our fingerprint-based lock technology is extremely accurate and quick to identify fingerprints, allowing for seamless interaction with users and increased security. This system should be affordable to both large and small industries. According to Figure 6.1, the accuracy of a fingerprint scanner is quite good, with an accuracy rate of around 80% for the tested fingerprints. The Arduino method also solves the problem of updating since it includes a microcontroller that can be modified and reprogrammed several times. The fingerprint scanner utilized in this research is also efficient because it takes less than a second to acquire results while recognizing minutiae.

Finally, the development of an Arduino-based physical access control system. Because Arduino platform is an open source technology, programming it takes less time. In comparison to the present physical access control system, it is a high-quality system. This system's characteristics assist in overcoming security concerns. Because Arduino board has a microcontroller that can be updated to use it with any evolving system, the suggested method eliminates the concerns of future device maintenance. Creating a physical access system with bluetooth and fingerprint scanner technologies results in a access control system with a simple technique.

8. 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]] Yaacoub, Jean-Paul & Salman, Ola & Noura, Hassan & Kaaniche, Nesrine & Chehab, Ali & Malli, Mohammad. (2020). Cyber-Physical Systems Security: Limitations, Issues and Future Trends. Microprocessors and Microsystems. 10.1016/j.micpro.2020.103201.
- [5] 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.
- [6] Lopez, Javier & Rubio, Juan. (2018). Access control for cyber-physical systems interconnected to the cloud. Computer Networks. 134. 46-54. 10.1016/j.comnet.2018.01.037.
- [7] Fink, Glenn & Edgar, Thomas & Rice, Theora & MacDonald, Douglas & Crawford, Cary. (2017). Overview of Security and Privacy in Cyber Physical Systems: Foundations, Principles and Applications. 10.1002/9781119226079.ch1.
- [8] Zhu, Z., & Chen, F., Fingerprint recognition-based access controlling system for automobiles, Image and Signal Processing (CISP), 4th International Congress, Vol. 4, p. 1899-1902, (2011)
- [9] 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.
- [10] 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.
- [11] 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.

- [12] Kamble, S., Gunasekaran, A. and Gawankar, S., 2020. Sustainable Industry 4.0 Framework: A Systematic Literature Review Identifying The Current Trends And Future Perspectives.
- [13]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.
- [14]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.
- [15] ElProCus - Electronic Projects for Engineering Students. 2021. Arduino UNO R3 Microcontroller, Specifications, and Pin Diagram. [online] Available at: <<https://www.elprocus.com/what-is-arduino-uno-r3-pin-diagram-specification-and-applications/>> [Accessed 11 October 2021]
- [16] Randomnerdtutorials.com. 2021. Fingerprint Sensor Module with Arduino | Random Nerd Tutorials. [online] Available at: <<https://randomnerdtutorials.com/fingerprint-sensor-module-with-arduino/>> [Accessed 11 October 2021]
- [17] Arduino Project Hub. 2021. Interfacing Bluetooth Module (HC-05) with Arduino Uno. [online] Available at: <<https://create.arduino.cc/projecthub/akshayjoseph666/interfacing-bluetooth-module-hc-05-with-arduino-uno-f5209b>> [Accessed 11 October 2021]

9. APPENDICES

Appendix A :

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