

CYBERSECURITY AUTOMATION FOR AN INDUSTRY

4.0 GARMENT MANUFACTURING SYSTEM

H.H.D Kalhara, P.A.U.T De Alwis, A.D.H Jinadasa, R.P.R.D Randunu

(IT18139440, IT18136098, 18132410, IT18133578)

B.Sc. (Hons) Degree in Information Technology Specializing 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

H.H.D Kalhara, P.A.U.T De Alwis, A.D.H Jinadasa, R.P.R.D Randunu

(IT18139440, IT18136098, 18132410, IT18133578)

Dissertation submitted in partial fulfilment of the requirement for the
Bachelor of Information Technology Specializing in Cyber Security

Department of Computer Systems Engineering

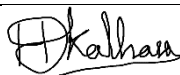



Sri Lanka Institute of Information Technology
Sri Lanka

October 2021

DECLARATION

“I 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.

Also, I hereby grant to 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 medium. I retain the right to use this content in whole or part in future works (such as articles or books).”

Name	Student ID	Signature
H.H.D Kalhara	IT18139440	
P.A.U.T. De Alwis	IT18136098	
A.D.H Jinadasa	IT18132410	
R.P.R.D Randunu	IT18133578	

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

Industry 4.0 digital transformation towards Internet of Things (IoT) focuses on productivity rather than security, therefore often face cybersecurity challenges. To overcome such, a centralized security solution focusing on four major areas 1) standardization, 2) security configurations with update management, 3) authentication and physical access control and, 4) intrusion detection was applied to a Cyber Physical System (CPS) based garment manufacturing system to overcome the security gap. Security policies based on ISO 27001:2013 and IEC 62443 security standards were applied to the security configuration management system in the design stage to achieve ‘security by design’ concept. The system is secured in terms of strategy, design, and operations rather than securing the system after deployment, especially through the compliance with standardization and policy implementation. Security and audit configurations were applied using Ansible for the automated tool that can be customized based on requirements. A Raspberry Pi 4 was utilized as IDS (Intrusion Detection System) to evaluate performance and to overcome network security challenges. Due to high number of interconnected devices having a proper network security solution is a must. However, network security solutions available in the current market are high in cost and excessive for small to medium Industry 4.0 environments. This solution based on Raspberry Pi 4 running Snort open-source IDS software with following requirements in mind, ease of use, minimum configurations towards user, portability and affordability. The physical access control prevents unauthorized access and access monitoring was done using logs. The proposed system enhances security, reaching for a cost-effective, efficient, reusable solution, and provides a comprehensive security solution for potential challenges of current and future smart manufacturing. The system is secured in terms of strategy, design, and operations rather than securing the system after deployment.

Keywords—Industry 4.0, Internet of Things (IoT), cybersecurity, Cyber Physical System (CPS), Intrusion Detection System (IDS)

ACKNOWLEDGEMENT

We wish to acknowledge the help provided by Dr. Asela Kulatunga, Head of Department of Manufacturing and industrial engineering, University of Peradeniya, Sri Lanka for giving us the opportunity to visit Peradeniya University to study CNC machine and robotic applications workflow which was a good initialization point for our research project. We wish to show our gratitude to Mr. Wijeweera, owner of Wijeweera Knit Wear (Private) Limited for letting us visit the garment factory to analyze requirements for our project in the initialization stage.

We wish to show our appreciation for our external Supervisor Chartered Eng. P.A. Gamini De Alwis for guiding us in the correct direction, throughout our research project by providing experience the manufacturing field, Dr. Darshi De Saram for sharing knowledge and experience and providing comments to make our project a success.

We wish to show our gratitude to my Supervisor Professor Pradeep Abeygunawardana and Co-supervisor Ms. Sasini Wellalage for supervising us throughout an entire year for our final year research. We would like to acknowledge the staff of Faculty of Computing, specially the Department of Computer Systems Engineering for all the support given to make this project a success. Last but not least, I would like to thank research module coordinators of Sri Lanka Institute of Information Technology for providing all the knowledge and opportunities for the research.

Table of Content

DECLARATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENT.....	v
LIST OF FIGURES	ix
LIST OF TABLES.....	x
LIST OF ABBREVIATIONS	x
1. INTRODUCTION.....	1
1.1. Background Review	2
1.2. Literature Review.....	6
1.2.1 CPS and IOT	6
1.2.2 Threats and vulnerabilities in CPS	7
1.2.3 Threats and vulnerabilities in IOT.....	7
1.2.4. IoT security frameworks	8
1.2.5. Security configurations	10
1.2.6. Firewall and Intrusion Detection System (IDS)	11
1.2.7. Authentication, and access control	14
1.3. Research Gap	16
1.3.1. Overall Research	16
1.3.2. Standardization.....	16
1.3.3. Security configurations and update management	17
1.3.4. Authentication and access control	18
1.3.5. Firewall and Intrusion Detection System (IDS)	19
1.4. Research Problem.....	20
1.4.1. Collaboration between different systems	20
1.4.2. Centralized security management.....	20
1.4.4. Secure communication.....	20
1.4.5. Insecure data.....	21
1.4.6. Initial Cost.....	21
1.4.7. Industry 4.0 plans and strategies are lacking.....	21
1.5. Research Objectives.....	22
1.5.1. Main objectives	22
1.5.2. Sub objectives	22
2. METHODOLOGY.....	26
2.1. System Diagram	26

2.2. Security standards and policy development.....	27
2.2.1 Identify the connected devices	27
2.2.2. Conduct a risk assessment.....	31
2.2.3. Identify the specific standards, procedures and guidelines for each identified components and overall system.	34
2.2.4. Choose the most suitable standards and frameworks	40
2.2.5. Verify the chosen standards and frameworks.....	43
2.2.6. Determine the types of policies that are needed.	43
2.2.7. Verify policy creation	44
2.3. Security Configurations and update management.....	45
2.3.1. Security Configurations	45
2.3.2 Update management	51
2.4. Authentication and access control.....	52
2.4.1. Analysis of network accessibility and physical accessibility	53
2.5. Firewall and Intrusion Detection System (IDS).....	53
2.5.1. Requirement Analysis for hardware requirements	53
2.5.2. Snort Installation and configuration	53
2.5.3. Barnyard2 installation and configuration.....	55
2.5.4. Pulledpork module installation and configuration.....	56
2.5.5. Configuring the Iptables firewall.....	57
2.5.6. Filebeat installation and configuration.....	58
2.5.7. Logstash install and configuration.....	59
2.5.8. Elasticsearch installation and configuration	60
2.5.9. Kibana installation and configuration.....	60
2.6. Commercialization aspect of the product	61
2.6.1 Standardization.....	61
2.6.2. Security Configurations	61
2.6.3. Firewall and Intrusion Detection System.....	62
2.6.4. Authentication and Access control	62
2.7 Testing	63
2.7.1. Standardization.....	63
2.7.2. Security configurations	63
2.7.3. Authentication and access control	66
2.7.3. Firewall and IDS.....	79
3. RESULTS, RESEARCH FINDINGS AND DISCUSSION	81

3.1. Standardization.....	81
3.1.1 Identify the specific standards and comparison of chosen security standards.....	81
3.1.2 Policy creation.....	82
3.1.3 Implementation of policies.....	83
3.2. Security Configurations	85
3.2.1. Results.....	85
3.2.2 Research Findings	88
3.4. Authentication and access control.....	89
3.3 Firewall and IDS	92
3.1.1 Results.....	92
3.1.2. Research Findings.....	96
3.5 Discussion.....	97
4. CONCLUSION.....	102
5. DESCRIPTION OF PERSONAL AND FACILITIES	104
6. REFERENCE LIST	105
7. APPENDICES	110

LIST OF FIGURES

Figure 1.1: Industrial revolution	3
Figure 1.2: CPS and IOT connection	6
Figure 1.3: CPS challenges	7
Figure 1.4: IOT threats	8
Figure 2.1: Overall System Diagram.....	26
Figure 2.2: Individual Workflow Diagram- Security standards and policy development.....	27
Figure 2.3: Visit to observe CNC devices - Robotic device	28
Figure 2.4: Observation of CNC devices 1	28
Figure 2.5: Observation of software related to CNC machines	29
Figure 2.6: Observation of CNC device 2.....	29
Figure 2.7: Screen shot of the first two pages of Business case documentation.	30
Figure 2.8: Heat map.....	32
Figure 2.9: Screen shot of the standard identification documentation.....	40
Figure 2.10: Sample device details	48
Figure 2.11: Sample audit summary	49
Figure 2.12: Sample report results table	50
Figure 2.13: Additional details about rule T_101	51
Figure 2.14: Individual Workflow Diagram- Security Updates	51
Figure 2.15: Control panel of the CNC machine	53
Figure 2.16: Custom rules.....	54
Figure 2.18: SSH attempt denied	55
Figure 2.17: Generated alerts.....	55
Figure 2.19: Barnyard2 installation.....	55
Figure 2.21: Stored signatures.....	56
Figure 2.20: Stored alerts in database	56
Figure 2.23: Pulledpork installing rules.....	57
Figure 2.24: IPtables Firewall policy rules	58
Figure 2.26: Input section Logstash configuration	59
Figure 2.27: Filter and Output section	59
Figure 2.28: The curl request and Elasticsearch response	60
Figure 2.29: Network diagram of test scenarios.....	64
Figure 2.30: Flow chart of the project.....	67
Figure 2.31: Arduino Uno R3	68
Figure 2.32: Fingerprint Sensor	69
Figure 2.33: Physical access control system diagram	71
Figure 2.34: Fingerprint enrollment code 1	72
Figure 2.35: Fingerprint enrollment code 2	73
Figure 2.37: Fingerprint verification code 1	74
Figure 2.38: Fingerprint verification code 2	75
Figure 2.39: Finger test output at serial monitor	75
Figure 2.40: Connect the Bluetooth module to system	76
Figure 3.1: Degrees of Confidence.....	91
Figure 3.3: TCPReplay replaying at 20Mbps	92

Figure 3.2: Snort idle resource consumption	92
Figure 3.4: CPU Usage of Raspberry Pi IDS.....	93
Figure 3.5: Packet loss and CPU usage.....	93
Figure 3.6: Highest recorded packet drop.....	93
Figure 3.7: RAM usage	94
Figure 3.8: Generated alert	94
Figure3.9: Port scan alerts.....	95
Figure 3.10: SSH brute force attack using Medusa	95
Figure 3.11: SSH brute force attack alerts.....	96

LIST OF TABLES

Table 1.1: Comparison of industrial standards and guidelines	9
Table 1.2: Summary of best practices for industrial Information security	9
Table 1.3: Comparison of IaC configuration management platforms.....	11
Table 1.4: Signature-based detection	12
Table 1.5: Anomaly-based detection	13
Table 1.6: Comparison of Existing Tools	17
Table 1.7: Products comparison	19
Table 2.1: Threats and related devices	33
Table 2.2: Comparison of chosen security standards for the research	42
Table 2.3: List of Information in Security Profiles	46
Table 2.4: List of Information in rules.yml	49
Table 2.5: Summary of Performed Tests.....	65
Table 2.6: How to Connect the Fingerprint Sensor to The Arduino	72
Table 2.7: How to Connect the Bluetooth Module to the Arduino	76
Table 2.8: Containing attack packets	80
Table 3.1: Security standard Vs. Security framework	81
Table 3.2: The Results from Performed Audits.....	85
Table 3.3: The Results from Performed Remediation.....	85
Table 3.4: performance and system structure between various security systems	90
Table 3.5: Simulated attack findings.....	97

LIST OF ABBREVIATIONS

Abbreviation	Description
CIA	Confidentiality, Integrity and Availability
CNC	Computer Numerical Control
CoAP	Constrained Application Protocol
CPPS	Cyber Physical Product Systems

CPS	Cyber Physical Systems
DCS	Distributed Control Sensors
DNP3	Distributed Network Protocol
DoS	Denial of Service
EN	European Standards
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
HMI	Human Machine Interface
IACS	Industrial Automation and Control Systems
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Integrated Power System
ISA	International Society of Automation
ISO	International Organization for Standardization
ISCN	Information Security Continuous Monitoring
ISMS	Information Security Management System
ISVS	IoT Security Verification Standard
JTC	Joint Technical Committee
LAN	Local Area Network
M2M	Machine to Machine
MitM	Man in the Middle
MTCS	Multi-Tier Cloud Security
NC	Numerical Controller
NIST	National Institute of Information Technology
OCTAVE Evaluation	Operationally Critical Asset and Vulnerability

OWASP	Open Web Application Security Project
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SAM	Standard Allowed Minutes
SCADA	Supervisory Control and Data Acquisition
SDLC	Secure Development Life Cycle
SHODAN	Sentient Hyper-Optimized Data Access Network
SMV	Standard Allowed Value
SN	Sensor Network
SOA	Statement of Applicability
SP	Special Publication
SU	Sub Committee
TCP	Transmission Control Protocol
TR	Technical Requirements
TS	Technical Specifications
WG	Working Group

1. INTRODUCTION

The modernization brought on by Industry 4.0 began to saturate the manufacturing sector with heterogeneous technologies and a large percentage of physical actuation components making the automation process more complex. Industrial Internet of Things (IIoT) integrate smart computing as well as network technologies in automation and data transmission according to the ongoing trend of manufacturing and industrial practices, including Cyber Physical Systems(CPS) and Internet of Things (IoT) to create more extensive, better connected and productive systems. Smart manufacturing relies on the Internet of Things (IoT) to create a link between the digital and physical worlds, as well as data analytics and machine learning. Although these technologies have been in development for some time, integrating them with industrial systems introduces new challenges as well as potential advantages such as increased efficiency.

Novel changes in Industry 4.0 lead to a passion for manufacturing plants with productivity, customization features, flexibility, operational efficiency [1] and SAM/SMV (Standard Allowed Minute/Standard Minute Value) rather than security. The integration of complex smart manufacturing technologies lead to increased intercommunication and data density, thus massively expand the scope of attacks pointing at industrial espionage and sabotage [1], because Industrial 4.0 are implemented targeting the functionality than security [2].

CPS are used to gain higher productivity in manufacturing [3], and to usher innovation due to their potential to integrate technology from different sectors for the implementation of real world processes [1][2]. Manufacturing automation is becoming a part of critical infrastructure in the present and future context. CPS is designed and implemented to be easily extendable and scalable as the structure includes heterogeneous communication technologies, which leads to technical issues, such as system verifications, frequent software updates, network and data interoperability, synchronization, privacy, and security issues [4]. The integration of IoT devices combined with various technologies is a complex task and implementing security for those systems is more complex task.

The development of the secure environment for the smart systems using The CPS platform is a large project that is currently hampered by a number of issues like, collaborating between different systems, centralized security Management, secure communication and insecure data leading to, conflicts in design model and security model, additional cost, low product quality, violation of Confidentiality, Integrity and Availability (CIA) and difficulties in adhering to laws and regulations. Therefore, cyber security has evolved into a major concern.

Objective of this project is to design and implement an automated system for garment manufacturing system focusing on four major cyber security aspects for garment manufacturing systems including:

- Frameworks and standardization
- Centralized security configurations with update management
- Authentication and Physical Access Control
- Intrusion Detection System (IDS)

A comprehensive, cost effective and efficient security solution is proposed with a centralized security approach to overcome the potential challenges of the smart system.

The reminder of the chapter is followed by a background review, analysis of the current literature on IoT, CPS and Network devices and their challenges, current literature on standardization, security configurations, intrusion detection and access control in the field, objectives and sub objectives of the overall research project.

1.1. Background Review

The first industrial revolution commenced with the discovery of steam power which was the greatest breakthrough for human productivity. Invention such as spinning machine, looms to make fabric made appearance. The first mechanical sewing machine was invented marking the beginning of the textile industry. As the first industry revolution was driven by coal, water and steam the second revolved around electricity. Gas and oil. The impact of the revolution in apparel sector is the sewing machine began to be produced in a serial manner. Third industrial revolution also known as digital revolution began with partial automation through Programmable

Management Systems. Developments in microprocessors, software, fiber optic cables, and telecommunication domains made the digital revolution a success. The German Federal Government first announced the Industrial Revolution 4.0 at the Hannover Fair in 2011. The physical world is created in the virtual environment and cyber physical systems are connected, communicated with one another and with human in real time to ultimately make decisions without human involvement, aiming to develop new internet services and business models providing efficiency, transparency, fault detection, flexibility, monitoring and most importantly productivity while reducing costs. The use of IoT in industrial applications and the technological convergence of CPS will have value creation and business models, modular structures which adopt to rapidly changing requirements and strategies.

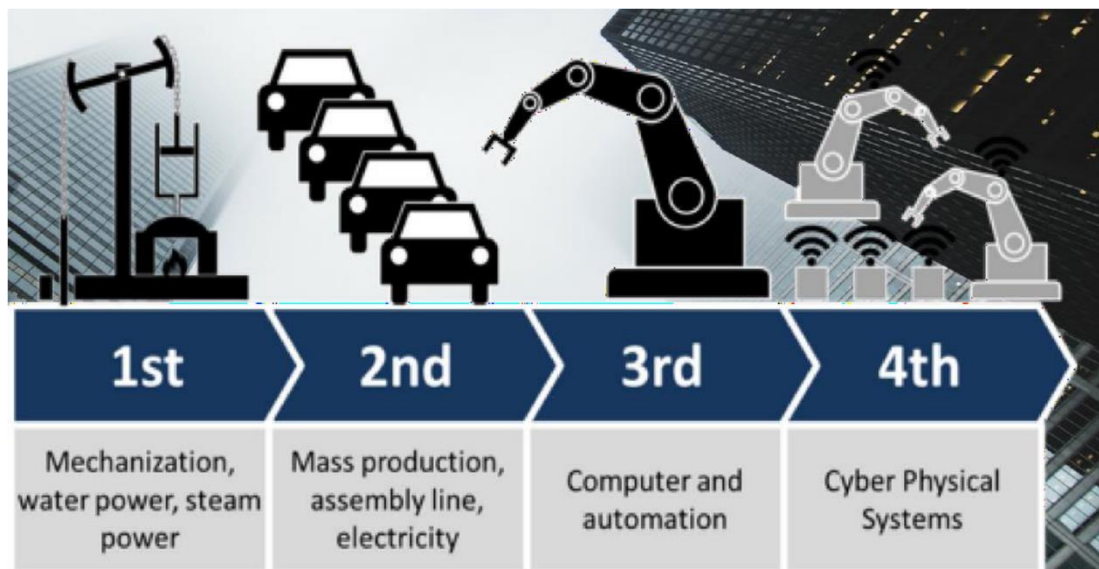


Figure 1.1: Industrial revolution

Development of IIoT to the integration of smart computing and networking in manufacturing processes for automation is the vision of industry 4.0. IoT adopts enabling the interconnection of computers and computer related equipment to improve intelligence, profitability, and effectiveness as well as safety [5]. While IoT refers to system of interrelated computing devices which communicating with each other and with people in real time it is most commonly used for consumer usage, IIoT is used for industrial purpose such as manufacturing. Unlike IOT, IIoT has more distinctive types incorporated smart devices, networking techniques, command control as well as service requirements.

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

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

Cutting process plays a huge role in garment automation industry because of the wastage problem, availability and accessibility, labor dependency and it is an expensive process. Introduced in 1900s die cutters increased cutting efficiency and quality, Numerical Controller (NC) machines appeared in 1940s and made continuous cutting possible, leading to a greater flexibility in production and more use of material [6]. Computer Numerically Controlled (CNC) machines was created in the digital revolution. This technological advancement made cutting the most advanced sector in apparel field. Various cutting devices such as computer controlled knives, laser, plasma, ultrasound and markers are available. Since the first fully automated cutting system matured with enhancement in technology the existing cutting technologies developed with the aspect of productivity, versatility and pattern matching capability [6]. Cutting processes which includes CNC machines are currently ongoing industry 4.0 revolution while addressing solutions for labor intensive problems, wastage problems and cost cutting [6].

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. The CNC is a hub which important data are flowing. In industry 4.0 CNC controllers should be capable of supporting integration, sensors, and cloud servers. A challenge is the transaction from traditional hardware based controllers architecture to a smart automation software architecture. The security related problems arise as today's industrial 4.0 automation is driven by focusing on the functionality rather than security. Lack of security might lead to increasing economic damages, loss of production and even loss of life. Existing measures' shortcoming poor levels of awareness. Readiness for upcoming confrontations is vital that is the reason for security should be important underpinning the development in industry 4.0. If the industrial 4.0 manufacturing automation developers could identify the application of cyber security requirements which are not been thoroughly captured in automation and develop systems addressing all the security aspects in automation, the developing automation systems would be potentially free of huge risks and would be safe. Cyber physical systems play a crucial role in cyber security for industrial 4.0 automation manufacturing systems.

The foundation of industrial 4.0 should enable garment cutting manufacturing automation including CNCs to deliver best possible performance based on security. It must also embrace the most accepted open security standards other than industrial best practices and standards which adhere to security laws and regulations to enhance safety as well as the security while designing the automated manufacturing systems. This also should be flexible enough to adopt to changing requirements and standards as well as strategies in the future of apparel industry.

Future trends in industrial 4.0 manufacturing systems includes, Simulators and test beds, intrusion detection and attack generation, security policy specification and enforcement and forensics.

1.2. Literature Review

Security has become a secondary concern rather than an important component in industry 4.0 automation systems, posing a significant risk in the rush for flexibility, quality, and efficiency. This problem leads to a variety of security flaws and attacks., mostly network related attacks such as Denial of Service (DoS) attacks, MitM (man in the middle) attack, eavesdropping attacks, time delay attack, data tampering attacks, false data injection attack, replay attack, spoofing attack, side channel attack, covert channel attack, zero-day attack, physical attacks, malware as well as machine learning related attacks and data analytics related attacks [7].

In early days, manufacturing security was performed by tactics like Isolation based on physical access control. Nowadays, since remote working capability which arose due to Covid–19 pandemic Ethernet, IP controls are a core part in networking. As a result, there is a significant threat level and an increased number of vulnerabilities. PLC, Remote Terminal Unit (RTU) systems, and Supervisory Control and Data Acquisition (SCADA) servers were all searched using Sentient Hyper-Optimised Data Access Network (SHODAN), a custom IoT search engine. Servers for Human Machine Interface (HMI) and DCS (Distributed Control Sensors) have been targeted [7].

1.2.1 CPS and IOT

CPS and IoT shares the same core architecture. The cyber-physical system is presented a high combination and coordination between physical components and computational components on IoT.

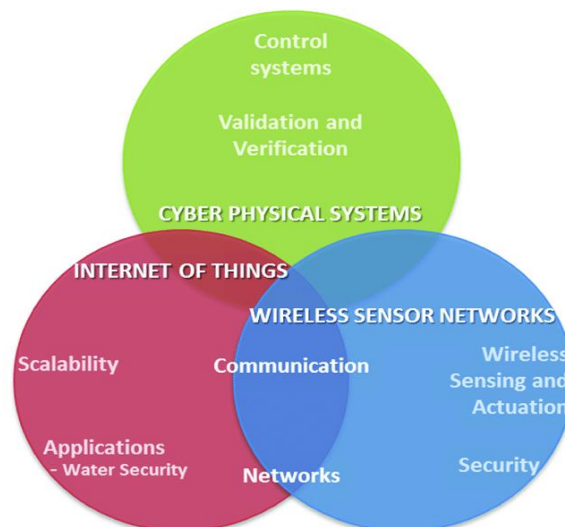


Figure 1.2: CPS and IOT connection

1.2.2 Threats and vulnerabilities in CPS

Out of the challenges mentioned below figure 3. Security can be categorized as a major challenge that often neglected or go unnoticed. Security challenges can be further divided into data security and control security. Data security focuses on protecting data at rest and data at storage. A unique characteristic of cyber physical threats are they mostly originate in cyberspace but impact on the physical system.

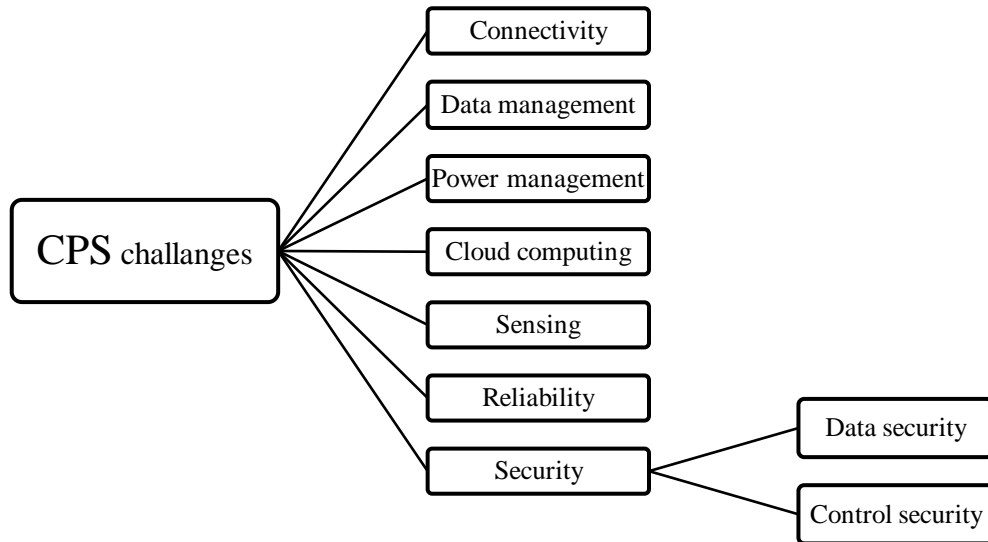


Figure 1.1: CPS challenges

Security policy violation can be defined as a vulnerability. These vulnerabilities can occur due to lack of security rules, weak system design. Vulnerabilities can be found in many different levels such as in hardware level software level design and policy level and even in user level. Hardware vulnerabilities, software vulnerabilities, network vulnerabilities, platform vulnerabilities, and management vulnerabilities are all well-known categories of cyber-physical system vulnerabilities. CPS threats are classified as denial of service (DOS), spoofing, tampering, disclosure, and repudiation.

1.2.3 Threats and vulnerabilities in IOT

IoT devices spread in an exponential rate. General IoT is a combination of four levels as shown in figure 4. The number of threats towards IoT growing every day. this created the need for a reliable protection. IoT to achieve its full potential, protection against threats and vulnerabilities is a necessary [8].

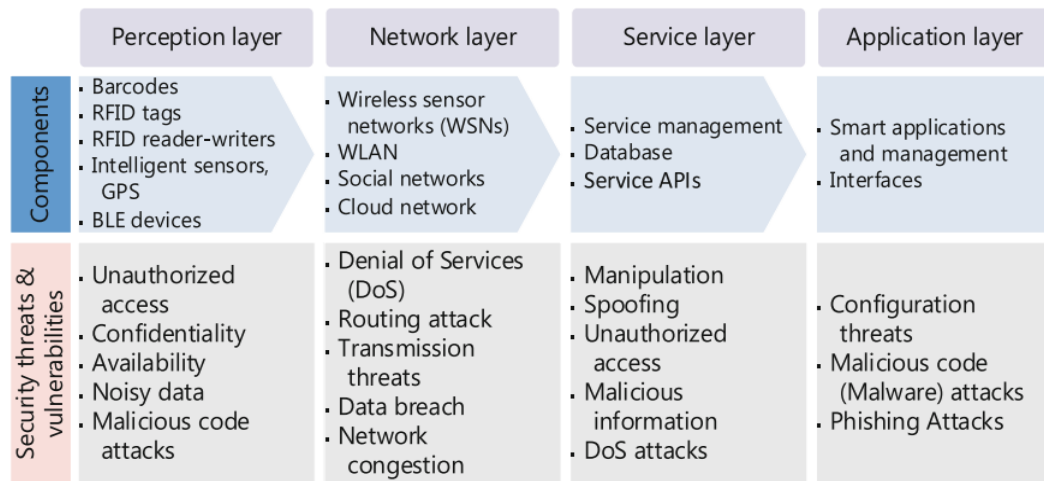


Figure 1.2: IOT threats

Further, we will discuss current security challenges and solutions for A) IoT security frameworks, B) security configurations, C) authentication, and access control as well as D) intrusion detection.

1.2.4. IoT security frameworks

Many working groups are working on factory automation, and some standards have already been published, as shown below.

International Organization for Standardization (ISO)/IEC Joint Technical Committee (JTC) 1/ Sub Committee (SC) 27 - Information security, cyber security and privacy protection standardization

- 1) Working Group WG1 Requirements, security services, and guidelines
 - WG2 Techniques and Mechanisms
 - WG3 security evaluation criteria
- 2) Standards ISA-Special Publication (SP0 99 Manufacturing and Control Systems Security Founded in 2002 ISA-TR99.00.01-2004(TR1) Published on March 12, 2004, ISA-TR99.00.02-2004(TR2) Published on April, 2004 [9].

Table 1.1: Comparison of industrial standards and guidelines

	IEC 62443	ISO/IEC 27000	ISO/IEC 15408	VDI/VDE 2182
Purpose	- Industrial communication networks - Network and system security	- Information Technology - ISMS	- Evaluation criteria for IT security	- Risk-based selection of controls and countermeasures
Structure of Documentation	- 1 Standard - 4 Categories - 12 Parts	- 1 Standard Family - 5 Categories - 16 Standards	- 1 Standard - 3 Parts	- 1 General Model - 6 Application Examples - 1 Set of Recommendations
Procedure	- Domain-tailored concepts	- 4 cyclic steps	- One-time approach	- 8 cyclic steps
Viewpoint	- Policies & procedures - (Technical) systems & components	- Management & organisation - Processes	- TOE	- Risks & threats - Countermeasures
Target Audience	- System Integrator (SI) - Product Supplier (PS) - Asset Owner (AO)	- Organizations of all types and sizes using IT	- Developers - Evaluators - Consumers	- Vendors - Machine Manufacturers - Plant Managers
Protection	- Defense in depth - Segmentation (zones & conduits) - Risk assessment (VDI/VDE 2182) - ISMS (ISO/IEC 27000)	- Security controls - Audit - Certification	- Protection profiles - Security components - Assurance components - Audit	- Asset identification - Risk assessment - Countermeasure use - Process audit
Metrics	- 4 Security Levels (SLs) - 7 Foundational Requirements (FRs) - 2-13 System Requirements (SRs) - 4 Maturity Levels (MLs) - 4 Protection Levels (PLs)	- Nothing relevant specified	- 7 Evaluation Assurance Levels (EAL)	- ≥ 3 classification levels (e.g. low, medium & high) - Probability & occurrence - Damage & impact

Table 1.2: Summary of best practices for industrial Information security

Best Practice	General Description and Purpose
NIST Cybersecurity Framework [12]	Framework for Improving Critical Infrastructure Cybersecurity
BSI ICS Security Compendium [13]	General Recommendations for Industrial Control System Security
IIC Security Framework [14]	Industrial Internet of Things Security Framework
IEEE 1686 Standard [15]	IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
IEEE Security Recommendations [16]	Practice for Privacy Considerations for IEEE 802 Technologies
NIST SP 800-30 [17]	Guide for Conducting Risk Assessments
NIST SP 800-53 [18]	Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-82 [19]	Guide to Industrial Control Systems (ICS) Security
DHS Catalog [20]	Recommendations for Standards Developers of Control System Security
IEC 61508 Standard [21]	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
NERC CIPs [22]	Securing assets within the Critical Infrastructure Protection (CIP)
NIST IR 7628 [23]	Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
ISACA COBIT [24]	Control Objectives for Information and Related Technology
CIS CSC [25]	Critical Security Controls as the basis for security audits

As illustrated in [10, Tab. 1.1] and [10, Tab. 1.2] there are several industrial standards and guidelines as well as best practices in use for industrial information security.

Various information security frameworks exist to cover IoT concepts and deployments in various verticals, classified according to the area of concern [11]. Therefore, when securing IoT systems there should be a clear strategy. Research is being done to identify current security frameworks, but there are relatively few initiatives that have been developed to be used in CPS.

Systematic reviews have been done world-wide according to the source [12], such as secure communication, embedded firewall and intrusion detection security, Authentication and Authorization controls, integration with security management systems. In an occurrence of security non-compliance, the security framework, must

address security risk assessment and controls to mitigate the risk while abiding with standards and needs [12].

Cisco's proposed security implications for IoT/Machine to Machine (M2M) constructions are extensive, necessitating the deconstruction of a workable IoT/M2M security framework that may be used to execute security in IoT contexts. ISA (International Society of Automation)/IEC 62443 cyber security standards for Industrial Automation and Control Systems (IACS) compliance can be obtained by Floodgate Security Framework. Constrained Application Protocol (CoAP) Frameworks to handle security and trust issues of IoT environments, OSCAR security framework, explores a novel approach to the problem of End to End (E2E) security in IoT [12]. It could be observed on the internet that there is much literature on aiming to minimize development and testing time in industrial environment using a framework for rapid integration. As you can see, there are various information security standards and frameworks, but it is a challenge to choose the required security standards/frameworks according to system requirements to create policies and implement in security configurations; this will be further discussed in the methodology.

1.2.5. Security configurations

As shown by OWASP [13], insecure default settings, a lack of update, and device management after deployment in production can lead to the security vulnerabilities described above.

Due to the immense number of devices, manually securing them one by one is time intensive. In order to save time, Infrastructure as Code (IaC) must be introduced. DevOps employs IaC as one of its primary strategies for automating logic for deploying, configuring, and updating devices [14]. Securing CPS devices necessitates the use of IaC's configuration and update management features. As a result, configuration management IaC platforms like Chef, Puppet, Ansible, and SaltStack [15] are ideal candidates for this purpose.

Puppet is a master-agent architecture opensource configuration management tool. Puppet master runs on a Linux/Unix server, whereas puppet agent runs on Windows,

Linux, and Unix client devices. Puppet requires signed certificates on both the master and the agents. For configuration management, Puppet uses the Puppet DSL (Domain Specific Language) [16].

Chef is master-agent architecture opensource configuration management tool. Chef resembles Puppet in many ways. Chef master runs on a Linux/Unix server, whereas Chef agents run on Windows/Linux/Unix client devices. Chef includes a workstation component that allows it to test all its configurations. To manage configurations, Chef employs Ruby as a Domain Specific Language (DSL) [17].

RedHat developed Ansible, an opensource configuration management software. Ansible is built on a client-server model, with the server being a Linux/Unix system and clients being Windows/Linux/Unix machines. Only a Secure Shell (SSH) connection between the server and the clients is required. It does not necessitate the installation of a specific agent on client devices. Ansible manages configurations with "YAML Ain't Markup Language" (YAML) [18]. YAML is a human-readable data-serialization language, not a markup language, as its name implies.

SaltStack is a master-client architecture opensource configuration management tool. Salt master is a server that runs Linux/Unix, while Salt minion (agent) is a client that runs Windows/Linux/Unix. SaltStack manages configurations with YAML. [19].

Table 1.3: Comparison of IaC configuration management platforms

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

1.2.6. Firewall and Intrusion Detection System (IDS)

CPS components and the “things” in IOT such as sensors, smart devices are commonly having less processing power and have the ability to exchange data via the internet. Even though benefits outweigh the disadvantages, Industry 4.0 security and privacy challenges cannot be ignored. Even with proper security configurations it is important

to prevent intruders from accessing the CPS components via the network. There are various methods to provide security against network intruders [20].

- Firewall.

One of these measures is utilizing a firewall. It protects devices within a network against intruders and controls the network traffic. According to predefined rule set, firewall decides whether or not the packets that arrive on the network can pass through.

- Intrusion detection system.

IDS is a software or hardware tool to detect and prevent incoming and outgoing malicious packets in a network. It works by recognizing the signs of a possible attack and sending an alert regarding the malicious packet. In some instances, it can trigger a response to combat the threat [21].

There are two different types of intrusion detection systems. First type is host-based IDS (HIDS), which installed in host machines and monitors one host at a time, HIDSs are lighter and use less processing power. The second type is network-based IDS (NIDS), which have the ability to monitors the entire network for malicious activities, NIDSs are more accurate.

There are two different detection mechanisms, they signature-based and anomaly-based detection, some occasions these two methods are combined for more reliable security [22]. Signature-based systems has predetermined set of rules and compares with the patterns in the traffic to detect attacks similar to any signature rules that has been stored in a database.

Table 1.4: Signature-based detection

<i>Signature-based detection</i>	
Pro	Con
High accuracy (lower rate of false positive)	Require database updates
Easy to configure and maintain	Unable to counter Zero-day attacks [23]

Anomaly-based detection systems first gather knowledge of normal traffic activities and then alerting user if there is any malicious activity occurs.

Table 1.5: Anomaly-based detection

<i>Anomaly-based detection</i>	
Pro	Con
Capable of detecting Zero-day attacks	High amount of false positive & false negative
Better protection against DDOS attacks	Required to define threat profiles

Whitepaper written by Michael Brennan, SANS Institute explains organizations with little to no network monitoring, opting for an expensive solution is generally not plausible. This paper focuses on the need for an IDS for companies that cannot afford one of the more quality commercial Intrusion Detection Systems available in the market. In addition, paper focuses on the IDS placement within the network “In order for Snort to be most effective, it needs to be positioned where it will see the most traffic possible.” [24]

Many research projects have been done to evaluate and compare the performance of open source intrusion detection systems.

One interesting study shows IDS’s detection techniques such as deep packet inspection are too are too much resource consuming for a Wireless Mesh Network (WMN), resulting unstable nodes. In order to address this issue authors proposed an IDS solution that was lightweight and less resource consuming. This solution however, able to provide protection only for few common attack types.

Another similar [25] study also points out the infeasibility of deploying IDS in WMNs. Both studies came to the same results and conclusion. using the full capabilities of Snort on WMNs nodes is impractical. This study proposed PRIDE (Practical Intrusion Detection in resource constrained wireless mesh network) solution which have the ability to distribute IDS functionalities to WMNs across the network, each node runs a custom version of Snort IDS with different set of rules: different nodes will be responsible for detecting different types of attack. This IDS function distribution was optimized to provide coverage to entire network.

Even though many research projects have been done to evaluate open-source Intrusion Detection Systems, but only handful of these emphasis of assessing its impact on resource constrained single board computers such as raspberry pi.

One interesting work is [26] which the authors evaluate the capability of raspberry pi 2 of running IDS and the performance of Snort and Bro (Zeek) IDS software. As for the result of these tests Raspberry pi 2 was able to run IDS and detect attacks and handled considerable number of packets, and they demonstrate that Snort has better performance than Bro IDS. However, these tests were based on older raspberry pi version 2 but still showed the potential of single board computers.

Another similar study [27] discuss the feasibility of utilizing Raspberry Pi while running Snort IDS in a distributed system. Authors specifically evaluate Raspberry Pi performance, packet drops and steady Snort configurations, and they claim Snort resource consumption did not overwhelm raspberry pi apart from high CPU usage when filtering high sets of packets.

However, these tests were done with old hardware but still showed the potential of single board computers. This thesis is focus on integrating raspberry pi 4b as a IDPS sensor to a medium size network that contains IOT devises, and evaluate resource usage and effectiveness by performing various type of network attacks.

1.2.7. Authentication, and access control

CPS, despite its numerous advantages, is exposed to a variety of physical security and cyber security threats in terms of authentication and access control. For an example, due to its diverse nature, reliance on private and sensitive data, and large-scale implementation is open to side channel attacks [28]. On most CNC (Computer Numerical Control) units used in manufacturing, whether the HMI (Human Machine Interface) has soft keys, key switches, or conventional keyboards, these units can be exploited 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 [29]. As a result, intentional or accidental exposures of these systems might have disastrous consequences, requiring the implementation of comprehensive security measures. Considering such requirements, allowing 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 [30]. The authentication and access control system proposed in the methodology gives a more secure approach.

1.3. Research Gap

1.3.1. Overall Research

Industrial 4.0 transaction from traditional hardware-based controllers' architecture to a secure smart automation software architecture is a challenge. When, implementing security, there are decentralized and layered approaches as solutions for the implementation and maintenance of smart manufacturing systems. It was observed that the layered and decentralized security approaches were common among the literature, but those approaches affected for the decreased efficiency of the overall smart system. Therefore to increase the efficiency a comprehensive centralized security solution was implemented and tested for industrial automated systems. Clearly the found security gap which affected to the system's efficiency of the industrial automated garment manufacturing system was closed by choosing the effective solutions.

The research focus on designing an automated system focusing centralized cyber security approach to the manufacturing system for security configurations and update management, intrusion detection and access control aligned with standardization as a solution to close the gap.

1.3.2. Standardization

The standardization for the centralized smart system will be focusing on the major cyber security aspects mentioned above. Based on the major aspects a step by step standardization approach for policy management is implemented and integrated for each aspect for the centralized system.

There are several IoT security frameworks in various stages of development. Comparison of the security standards and best practices for the different industrial automation domains are available [31]. The challenge was to compare, contrast and choose the effective IoT security standards and frameworks suitable to the system.

The security threats and drawbacks of the manufacturing system are evaluated according to risk assessments. A solution to eliminate risks and threats after evaluating the problems encountered while implementing security to the system was encouraged.

Through past literature, analyzing what approaches were taken to overcome those security problems are encountered. Security standards and creating policies for implementation and integration of major cyber security aspects to overcome the current security challenges. Standard verification and policy creation verification for the manufacturing system were evaluated by an industry expert to ensure that the standardization solution was effective enough to close the gap.

1.3.3. Security configurations and update management

1.3.3.1. Security configurations

OpenSCAP and CIS-CAT Pro are two popular industrial tools for security configurations and system hardening. However, these tools are designed for server hardening, and none of them are capable of hardening CPS device-based operating systems such as Raspbian OS and Robot OS (ROS). To automate security configuration and minimize system downtime, the proposed tool is primarily focused on CPS or IoT devices operating system hardening, which includes the above-mentioned operating systems as well as Ubuntu Linux. A comparison of operating system configuration capability between existing tools and the proposed tool is shown in the table below.

Table 1.6: Comparison of Existing Tools

Operating System	OpenSCAP	CIS-CAT Pro	Proposed tool
Ubuntu Linux	✗	✓	✓
Robot OS	✗	✗	✓
Raspbian OS	✗	✗	✓

1.3.3.2 Update management

Security patching process and updates are not easy to manage. Lack of security awareness is one of the main reasons for neglecting security update management. Updates could break systems that works fine, applying updates disturbs the business process and there could be fear for functionality changes. Therefore, the update

management system is aligned with the security configuration management system through Ansible while giving a centralized update management approach.

Rather than downloading and installing apps from a server repository on all client systems every time, it is effective to save all applications on a Local Area Network (LAN) server and distribute them to client systems as needed. Using a local repository is a very quick and efficient method because all essential apps are transferred from the local server via a fast LAN connection. As a result, it saves Internet bandwidth and, as a result, lowers the annual Internet cost.

1.3.4. Authentication and access control

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.

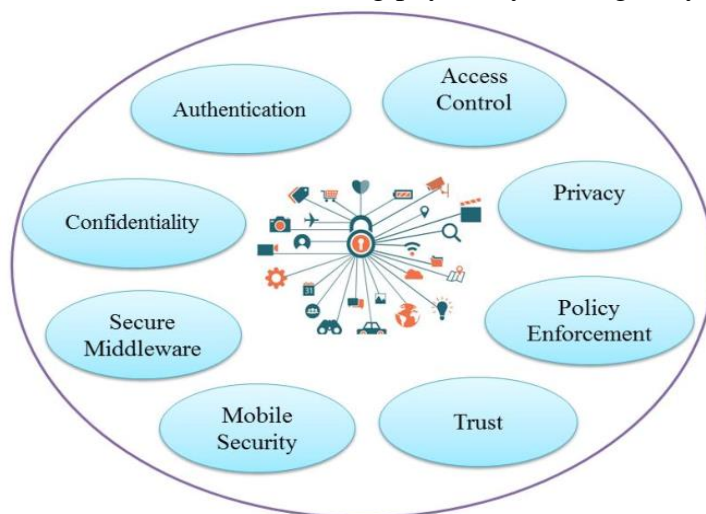


Figure 1.5: IIoT security requirements

1.3.5. Firewall and Intrusion Detection System (IDS)

Industry 4.0 creates a massive hunting ground for malware, botnets and other malicious activity, as the threats towards CPS and IoT continue to rise. In order to combat these network threats security systems such as IDS, Firewalls must also evolve. Even though highly capable network security solutions are available for cooperate networks shown in table 3, these solutions are expensive and unattainable and excessive for small to medium industries who are migrating into industry 4.0. This thesis is focus on designing a cost effective, lightweight yet reliable IDS/IPS system with a dashboard visualize alert logs. This IDS solution is small, portable, pre-packaged with Snort IDS and have the ability to deploy anywhere seamlessly [32].

Table 1.7: Products comparison

Product	HIDS/NIDS	Signature based	Anomaly based	Base Price
McAfee NSP	NIDS	✓	✓	\$ 10,995
Cisco Firepower	HIDS	✓	✓	\$ 100,000
CrowdStrike	HIDS	✓	✓	\$ 4,000
Tipping Point	HIDS	✓	X	\$ 6,000
Proposed Solution	NIDS	✓	✓	Less than \$ 200

Source: www.esecurityplanet.com

1.4. Research Problem

Smart manufacturing integrate many technologies. Most system developers do not entirely recognize the cyber security challenges when designing, implementing or maintaining an industrial 4.0 automated system as there are many inter connected devices and technologies. Also vendors and manufactures are focused on productivity rather than security. The research was to identify the application of cyber security requirements which are not been thoroughly captured in automation of garment manufacturing and give a comprehensive security solution to overcome security challenges through a centralized management system.

Challenges:

For the creation of a safe network environment a Cyber Physical Production System (CPPS) platform based on CPS technology is being used to improve the network environment in Industry 4.0. Building the CPPS platform is a difficult task that is currently hampered by a number of factors, including the need to adhere to CPS challenges.

1.4.1. Collaboration between different systems

Physical devices and computer systems working together for a collaborative model is essential for exchanging information, [33] store information, documentation, decision making, corrective and preventive action. How can we develop and implement an intrusion detection system in the industry 4.0 environment that is accurate and efficient as well as easy to operate by an average user, while overcoming collaboration challenges.

1.4.2. Centralized security management

Creating CPS models to apply security configurations and updates to physical devices and monitor physical devices using a centralized control system such as SCADA to maximize efficiency is a challenge [34]. 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 [33].

1.4.4. Secure communication

CPS that use the SCADA systems is connected to the internet over TCP/IP protocols without additional protection [35], which have known vulnerabilities.

1.4.5. Insecure data

During the implementation of Industry 4.0, there would be a lack of system integrations to ensure data security for manufacturing firms. IoT-based CPSs, which are connected to a large number of embedded sensors and communication devices, pose a major risk due to the increase in data usage and the increased risk of system breaches. [36].

1.4.6. 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 incorporate architecture in accordance with business requirements In terms of cost and time, a significant initial investment is required. [37]

1.4.7. Industry 4.0 plans and strategies are lacking.

In the manufacturing industry, there is a lack of a dynamic strategic plan to support the transition to Industry 4.0 [38].

Main focus for the standardization aspect arise the questions such as how to identify and create security policies, how to integrate security strategies suitable for IoT and CPS devices, are there IoT security standards which can be implemented to the implementation, integration and maintenance of the smart system, which standards are suitable for the policy creation, how to choose effective security standards according to the project requirements and how to implement proper security update mechanisms. Developing industrial security policies, considering industrial guidelines, procedures and standards which adhere to laws and regulations is essential when automating the system towards industrial 4.0 automated garment manufacturing system. In order to implement the automated system securely, chosen security standards should be verified and the security policies should be according to the best practices aligned with the effective standards.

1.5. Research Objectives

1.5.1. Main objectives

Main objective of the overall research project is security implementation for the potential challenges of the smart garment manufacturing system. An automated garment manufacturing system which has been securely implemented to overcome the potential security challenges in the garment manufacturing industry according to the security standards, which is also verified for authentication and access control for the utilized IoT devices, automated centralized security configurations using Ansible, security updates and intrusion detection system.

1.5.2. Sub objectives

1.5.2.1. Risk assessment

Identifying the components and devices and conducting risk assessment to identify current and future threats and security policy creation for different components using security and industrial standards to secure the industry 4.0 garment manufacturing system is the main objective of standardization component.

1.5.2.2 Standardization and policy implementation

Create and develop security policies for the major cyber security aspects in the project including, centralized security configuration management, intrusion detection and access control such as privacy policy, password policy, network policy, audit policy, authorization and access control, backup policy according to industrial guidelines and standards which are verified by an industrial expert to design, implement and maintain the secured automated system safely. Come up with procedures and methods to implement the identified security policies if needed. Verify the security policies before implementing for the accountability of the research. Evaluate and give solutions for the problems encountered when implementing security policies.

1.5.2.3. Security configurations

The main goal of this research component is to develop a solution for automating security configurations for CPS devices. By default, these CPS devices have

vulnerable configurations, and their life cycles are shorter than that of computer systems. As a result, system administrators must often analyze current security configurations and apply security configurations. Manual security configuration is inefficient and result in more system downtime. To reduce system downtime, the idea is to create a program that can automate and manage security configurations.

1.5.2.3.1 Audit security configurations

A mechanism to audit security configurations is included in this suggested tool to ensure that security configurations are appropriately configured in CPS devices. The audit function will be written in bash and python, with ansible delivering the scripts to the CPS devices as ansible tasks. The audit function saves the results as a comma-separated values (csv).

1.5.2.3.2. Centralized device configuration management

The suggested tool will be installed on a Linux-based ansible controller. Using SSH keypairs or password-based authentication, SSH connections are established between ansible controller and CPS devices. The ansible controller's goal is to centralize the configuration management of CPS devices.

1.5.2.3.3 Generate audit reports

There is a function in this suggested tool to generate reports depending on audit results. The following information is included in the report: security configuration name, severity, description, and rationale. As a result, these audit reports can demonstrate applied security measures on a system to the users and management.

1.5.2.3.4. Update Management

Update Management will be used for the update management configurations giving a solution for increased use of internet bandwidth while downloading and updating software for each devices. Objective is to come up with a solution to lower the use of internet bandwidth while updating deices reducing the cost.

1.5.2.4. Authentication and access control

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 for small to medium industry 4.0 environments 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.

1.5.2.4.1. 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.

1.5.2.4.2. 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.

1.5.2.4.3. 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.

1.5.2.4. Firewall and IDS

This research component targeted towards implementing a lightweight, reliable accurate, and easy to implement and operate IDS/IPS system targeted towards small to medium industry 4.0 environments. In order to monitor the network for anomalies, malicious activities, policy violations and alert the user. This IDS will be implemented with following requirements in mind:

- Portability: the device should be portable enough to carry with users, must be able to relocate to another location without an effort.
- Minimum configuration: the device should be pre-configured. However, user have full power to add or remove configuration to suit their needs.
- Ease of use: user will have the ability to deploy the IDS seamlessly without any complications
- Versatility: the device could be used anywhere from home to medium size industrial environments.
- Affordable: the device initial and operational cost should not exceed 1000 USD per year.

2.METHODOLOGY

2.1. System Diagram

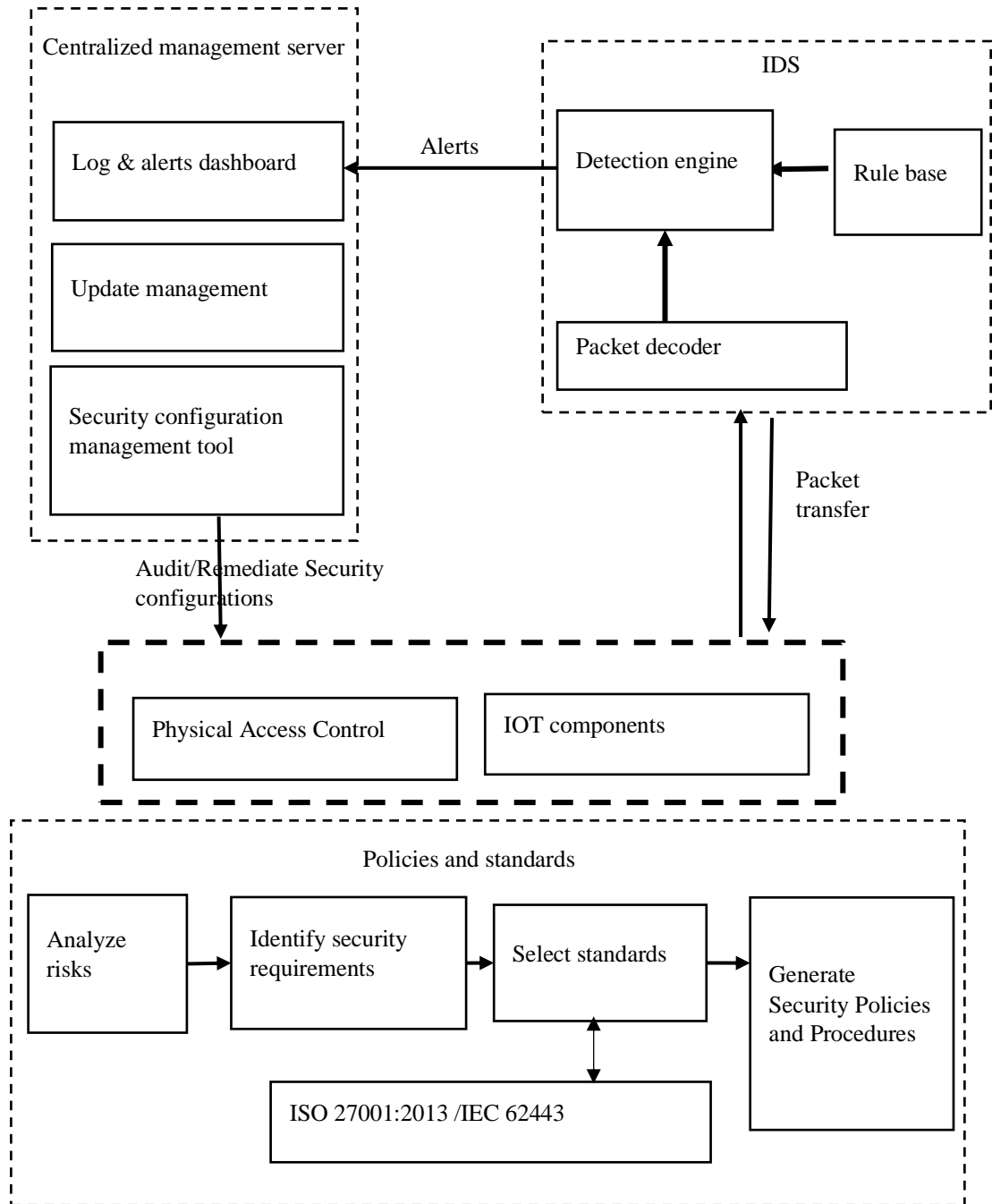


Figure 2.1: Overall System Diagram

2.2. Security standards and policy development

Below shows the work break down structure for security standards and policy development.

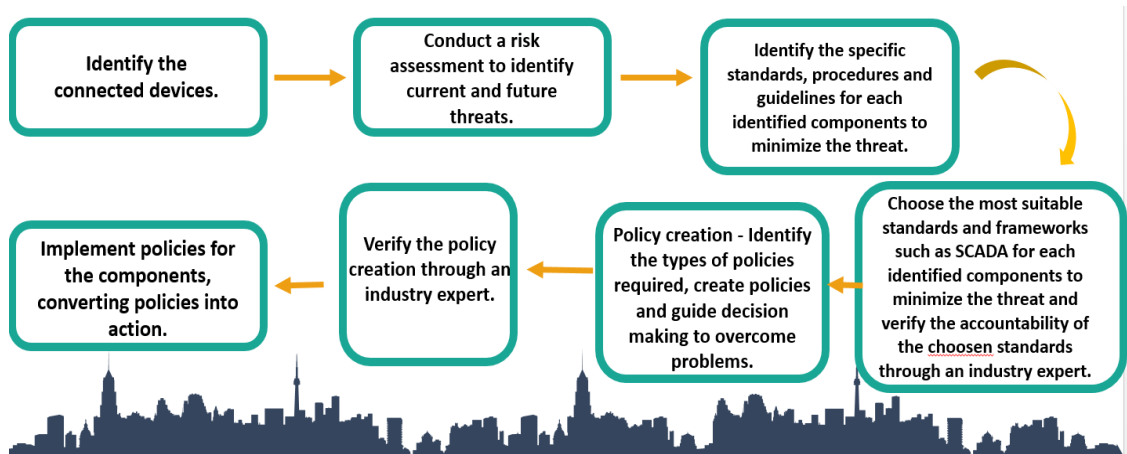


Figure 2.2: Individual Workflow Diagram- Security standards and policy development

2.2.1 Identify the connected devices

After going through the current literature regarding the topic, it was essential to have a better understanding about the current local apparel industry and CNC machines.

Therefore, a field visit to a local knit wear garment manufacturing factory was arranged to get a better idea about the apparel industry and local garment manufacturing machines. The processes were manual but, the workflow of the garment factory was observed. Each machinery for production processes was observed. A better idea about the cutting process and its machinery was taken by the factory visit. The requirements and customer-partner relationships were noted down to document the requirements, limitations, costs and benefits of the research.



Figure 2.3: Visit to observe CNC devices - Robotic device



Figure 2.4: Observation of CNC devices 1



Figure 2.5: Observation of software related to CNC machines



Figure 2.6: Observation of CNC device 2

As shown in the above figures, a field visit to the Peradeniya Engineering Faculty, Sri Lanka was arranged to get a better idea about how the CNC machines work and how to collaborate IoT and cyber security for the available local CNC systems. The industrial visit gave us a thorough observation of the following:

- CNC machine workflow
- The current security aspect of the CNC machines
- What components we should specially focus
- How to secure access terminals
- What are the related software and hosted operating systems
- Engineering point of view for the security of CNC machines
- Gaps between IT and engineering applications of CNC machines
- How the machines are operated

Most importantly we got a good initialization point for our research project to have an accurate direction to the research as a detailed idea about the fundamental concept of the topic for the research was taken by the visit. The more we progress in-depth of the research, the more we understand the importance of the visit to Peradeniya Engineering faculty thanks to the support as well as the detailed explanation given by your academic staff members.

A business case was documented by analyzing business requirements, understanding future customer-partner requirements, defining the scope and the purpose of the project while analyzing ISMS benefits and costs.

This chapter sets out the benefits and provides a business case for the information security management system (ISMS) that conforms to the ISO 27001:2013 standard and IEC 62443 standard.

Purpose

Main objective of the overall project is security implementation for the potential challenges of the smart manufacturing system. A secure automated garment manufacturing system which has been securely implemented to overcome the potential security challenges in the garment manufacturing industry according to the security and industrial standards which are verified for authentication and access monitoring for the utilized IoT devices, automated security configurations using Ansible, security updates using Ansible and intrusion detection system. Identifying the components and devices and conducting risk assessment to identify current and future threats. Security policy creation for different components using security and industrial standards. Update Management using Ansible, Python, Django, Bash technologies will be used for the update management configurations.

Scope

Create and develop security policies such as privacy policy, password policy, network policy, audit policy, authorization and access control, backup policy according to industrial guidelines and standards to design the secured automated system safety. Come up with procedures and methods to implement the identified security policies for the components including centralized security Management, intrusion detection, authentication and access control and update management.

Introduction

Novel changes in Industry 4.0 lead to a passion for manufacturing plants with productivity, customization features, flexibility, operational efficiency and SAM SMV (Standard Allowed Minute-Standard Minute Value) rather than security. The integration of complex smart manufacturing technologies lead to increased intercommunication and data density, thus massively expand the scope of attacks pointing at industrial espionage and sabotage, because Industrial 4.0 are implemented targeting the functionality than security. CPS are used to gain higher productivity in manufacturing, and to usher innovation due to their potential to integrate technology from different sectors for the implementation of real world processes. Manufacturing automation is becoming a part of critical infrastructure in the present and future context. CPS is designed and implemented to be easily extendable and scalable as the structure includes heterogeneous communication technologies, which leads to technical issues, such as system verifications, frequent software updates, network and data interoperability,

synchronization, privacy, and security issues. The integration of IoT devices combined with various technologies is a complex task and implementing security for those systems is more complex task. Therefore, cyber security has evolved into a major concern. Objective of this project is to design and implement an automated system for garment manufacturing system focusing on four major cyber security aspects for garment manufacturing systems including:

- Frameworks and standardization
- Centralized security configurations with update management
- Authentication and Physical Access Control
- Intrusion Detection Systems (IDS)

A comprehensive, cost effective and efficient security solution is proposed with a centralized security approach to overcome the potential challenges of the smart system.

ISMS benefits

Information security risk reduction

1. Educate employees with the concepts of cyber security, threats and cyber-attacks by security awareness programs and training the employees to operate systems security according to policies.
2. Enhance established control environments for information security by (re)emphasizing the security control criteria of business information, updating existing security controls for information, monitoring etc. and offering incentives to evaluate information protection and enhancing regularly access controls when required.
3. A systematic, excellently-structured strategy improves a chance of recognizing, assessing and rationally managing all applicable security information risks, vulnerabilities and impacts.
4. It improves our ability to pass selectively those threats to insurers or other third parties and can make it easier to negotiate reduced rates when key controls are introduced and handled.
5. Trained, systematic and rational risk management strategy ensures consistency across various ICT and business processes throughout the time and handles information security threats regarding the relative objectives.
6. Prevents from fines, legal charges, financial losses and loss of reputation.

Benefits of standardization

1. Improves protection in system and information reliability.
2. Enhanced trust for consumers and business partners about the manufacturing smart system and the process.
3. Allows to focus on unique additional safety standards to protect those information assets.
4. Stop the same fundamental controls in every circumstance repeatedly.

Figure 2.7: Screen shot of the first two pages of Business case documentation.

The business case was documented according to ISO 27001:2013 standard. The overall business case states the purpose, scope, Information Security Management Systems (ISMS) benefits, how to reduce information security risks, benefits of standardization for ISO 27001:2013 and IEC 62443, benefits of structured approach, benefits of getting certifications, benefits of being compliant to the standards, ISMS implementation costs, operation and maintenance costs, training costs. Analyzing the business requirements for the system were done and documented.

Discussing aspects of security CIA and how they might apply to the standardization requirements of cyber security in the system and identifying each security aspect were done. Categorization of the aspects according to ISO 27001:2013 were done and controls/reasons for the controls are justified with the overview of implementing each security aspect in Statement of Applicability (SOA) documentation. For each aspect the controls/control objective, whether the current controls are fully applied or applied to some extent is analyzed and highlighted. If the controls are not in place remarks with justification were stated. The selected controls and reasons for selection is marked according to the aspects of legal requirements, contractual obligations, business

requirements/adopted best practices or results of risk assessments. The overview of implementation for each aspect is documented through the Statement of Applicability.

2.2.2. Conduct a risk assessment

Determined issues which has to be addressed, also to which instance or degree should the issues be addressed in the overall system. Risk management is a set of coordinated activities for directing and controlling risks.

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) risk assessment framework is a methodology for identifying and assessing asset information security risks. OCTAVE is highly personalized, self-directed, and adaptable. Octave could be customized according to the requirements. Therefore, the risk assessment was conducted using OCTAVE Allegro. The following aspects are highlighted in Octave:

- Determine the importance of vital assets.
- Concentrate risk analysis on the most critical assets.
- Think about the connections between critical assets, threats to assets, and vulnerabilities that expose assets to threats. Assess risks in a real-world setting.
- To reduce risk, develop a practice-based protection strategy and risk mitigation plans.

Risk assessment was conducted for identified assets and each critical asset was evaluated through OCTAVE Allegro worksheet 8 and OCTAVE Allegro worksheet 10.

1. Allegro worksheet 8: Critical information asset profile – For each critical asset rationale for selection, stating why the information asset is important to the organization, agreed description for the critical asset, who owns the asset, CIA security requirements and other requirements are stated along with the most important security requirement.

2. Allegro worksheet 10: Information asset risks are identified for each critical asset. The threats were identified with the area of concern and the actor, means, motive, outcome, security requirements and probability of occurrence and consequences for the threat were identified. The severity was scored in a 1-10 scale according to the impact area to finally, get the relative risk score for each threat.
3. According to the information gathered from OCTAVE risk assessment, a heat map was generated for the critical assets to determine which threats are most likely to occur in the system.

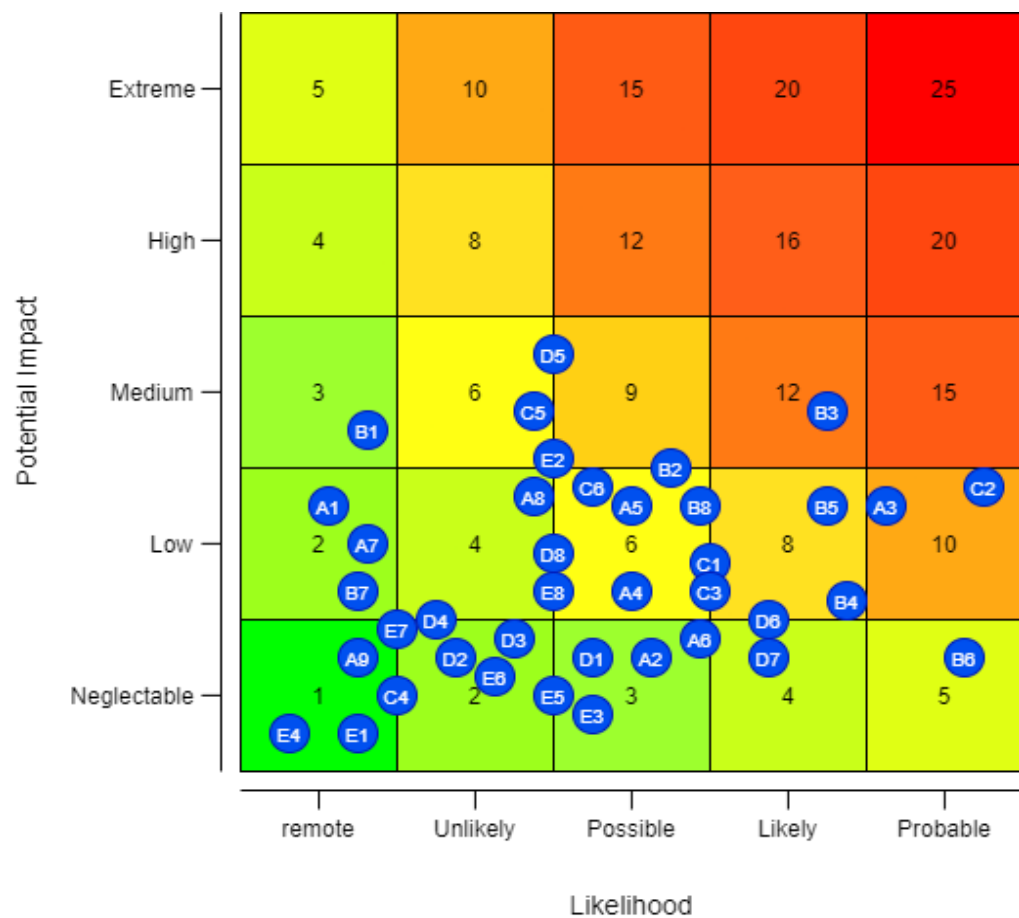


Figure 2.8: Heat map

Table 2.1: Threats and related devices

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

2.2.3. Identify the specific standards, procedures and guidelines for each identified components and overall system.

An overview of overall cyber security and IoT security standards and frameworks were identified and evaluated after searching via the internet blogs, articles, research papers, journals and digital libraries. Suitable frameworks and standards for the project was thoroughly researched, identified and evaluated for policy creation. The information about suitable standards and frameworks were gathered through internet and literature found in research libraries such as Google scholar and Institute of Electrical and Electronics Engineers (IEEE). They provided information about frameworks and standards in development as well as the standards and frameworks widely popular around the world articles and blogs from the internet provided significantly important and necessary information about suitable IoT security standards.

Frameworks such as NIST, ISO, IEC, SCADA can be used according to the different aspects of IoT, therefore a thorough research was done to identify what standards and

frameworks are most important to each critical asset for the smart system. There are many Information security management standards and IoT security standards which are implemented in different organizations and systems globally.

2.2.3.1. Standards identified for critical aspects in the research.

2.2.3.1.1 Firewall and network security

Using NIST Special Publication 800-4, Guidelines on Firewalls and Firewall Policy, create a firewall policy that specifies how firewalls can handle inbound and outbound network traffic. Creates firewall rules, as well as picking, configuring, inspecting, installing, and managing firewalls, with step-by-step instructions. The National Institute of Standards and Technology - United States has released a free special publication for firewall security aspect.

2.2.3.1.2. CPS

CPS are at the heart of the next generation of industrial control systems. Framework for Cyber-Physical Systems, NIST Special Publication 1500-201. The IEC 61499 standard adds a higher level of design, allowing for the versatile combination of software components while maintaining hardware independence. On top of Raspberry Pi boards, this work addresses the design of applications using the IEC 61499 standard.

2.2.3.1.3. Authentication and access monitoring

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST Special Publication 800-137, is a NIST special publication for authentication and access monitoring, and NIST SP 800-92 is a guide to Computer Security Log Management. Electronic authentication rules are outlined in NIST SP-800-63-1.

Cyber security standards are techniques that are commonly set out in published materials that are intended to protect a user's or organization's cyber environment. Users, networks, computers, software, processes, information in storage or transit, applications, facilities, and systems that can be linked directly or indirectly are all part

of this area to be protected. ISO 27001 for information security management systems, IEC 62443 which defines processes, techniques and requirements for Industrial Automation and Control Systems, NIST framework and ISO/IEC 30163:2021 standard which specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset are some of the standards that could be used for the research. The Software Development Life Cycle (SDLC) is a well-defined approach for producing high-quality, low-cost software in the shortest possible amount of time framework.

A document which provides a brief overview of standards and frameworks that could be used in the research project about cyber security automation of industrial 4.0 garment manufacturing system was created.

Written norms are expected to render cyber security initiatives clear therefore the standard identification document was prepared according to all suitable security standards and frameworks after a discussion with the group members and a security policy developer's instruction were taken. Cyber security standards, are generic collections of prescriptions for the best implementation of specific steps, created by industry experts. Therefore, Methods, protocols, reference structures, and other items may be included in the specifications. It ensures security reliability, promotes integration and interoperability, and allows for practical measure comparison. A written specification that defines a common language, includes a technical specification or other precise requirements, and is intended to be used consistently, as a law, a guideline, or a description. The aim of security standards is to make information technology (IT) systems, networks, and essential infrastructures more secure.

2.2.3.2. Evaluation for the identification of most suitable standards and frameworks

2.2.3.2.1 ISO 27000 Series

It is the family of information security standards which is developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to provide a globally recognized framework for

best information security management practices. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organizations face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology. ISMS is a systemic approach to risk management, including measures to address people, processors and technology.

2.2.3.2.1.1 ISO 27001

This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS. The only standard in the series that can be audited and certified against is ISO IEC 27001: 2013.

ISO 27001 based ISMS can demonstrate many efficiencies and other benefits such as;

- **Improved system dependability and security:** Security is frequently characterized as safeguarding an asset's Confidentiality, Integrity, and Availability. The stated objectives will be satisfied if a standards-based strategy is used in a system or an organization, which ensures that proper controls, processes, and procedures are in place. By default, achieving the CIA's security goals will increase the dependability, availability, and accessibility of the system. Having stable, secure and reliable systems ensures that interruptions to those systems are minimized, thereby increasing their availability and productivity. In addition to the above, a standards-based approach to information security demonstrates to customers that the company can be trusted with their business. This can increase profitability by retaining existing, and attracting new, customers.
- **Reduced Costs:** Standards based approach to information security ensures that all controls are measured and managed in a structured manner. As a result, processes and procedures become more simplified and effective, minimizing expenses. Companies have realized they can better manage the tools they have in place by consolidating

redundant systems or re-assigning other systems from assets with low risk to those with higher risk.

- **Legislation compliance:** Having a well-structured Information Security Management System in place makes compliance considerably easier.
- **Better Management:** Knowing what's in place and how it should be managed and safeguarded makes it easier to manage information resources inside a company.
- **Improved Customer and Partner Relationships:** Customers and trading partners can interact with the company with confidence knowing that the company has taken an independently verifiable approach to information security risk management.

ISO 27001 can be adopted as a framework for an organization to work against, or the organization can seek certification against the standard. An organization's certification to ISO/IEC 27001 shows that it has designed and implemented best-practice information security processes. Certification will be benefited when gaining new clients and improve competitiveness, enhancing reputation, improve structure and focus.

2.2.3.2.2. IEC 62443

The IEC 62443 cyber security standard defines processes, techniques and requirements for Industrial Automation and Control Systems (IACS). Its documents are the result of the IEC standards creation process where all national committees involved agree upon a common standard. Targets at three main roles:

- **Product suppliers** that develop, distribute and maintain components or systems used in automated solutions.
- **System integrators** that design, deploy and commission the automated solution.
- **Asset owners** that operate, maintain and decommission the automated solution.

Planned and published IEC 62443 work products for IACS Security. All IEC 62443 standards and technical reports are organized into four general categories called General, Policies and Procedures, System and Component.

1. The first category includes foundational information such as concepts, models and terminology.
2. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.
3. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model.
4. The fourth category includes work products that describe the specific product development and technical requirements of control system products.

2.2.3.2.3. ISO/IEC 30163:2021

This standard specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services.

2.2.3.2.4. NIST Cyber Security Framework

To assist firms in managing their cyber security risks, the Framework incorporates industry standards and best practices. It establishes a common vocabulary that enables employees at all levels of a company and at all points in the supply chain to acquire a shared awareness of their cyber security threats. The Framework not only helps organizations understand their cyber security risks. Improve the security of the essential infrastructure, shielding it from both internal and external threats. NIST Cyber Security Framework describes five functions that manage the risks to data and information security which are identify, protect, detect, respond, and recover. The primary components consist of the Core, Profiles, and Implementation Tiers. The Core offers guidance to organizations wanting to get better protection for their information systems.

**IDENTIFICATION OF POTENTIAL CYBER SECURITY
STANDARDS, PROCEDURES, GUIDELINES AND
FRAMEWORKS FOR THE CYBER SECURITY AUTOMATION
OF INDUSTRIAL 4.0 GARMENT MANUFACTURING SYSTEM**

Abstract

Cyber security standards are techniques that are commonly set out in published materials that are intended to protect a user's or organization's cyber environment. Users, networks, computers, software, processes, information in storage or transit, applications, facilities, and systems that can be linked directly or indirectly are all part of this area to be protected. ISO 27001 for information security management systems, IEC 62443 which defines processes, techniques and requirements for Industrial Automation and Control Systems, NIST framework and ISO/IEC 30163:2021 standard which specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset are some of the standards that could be used for the research. The Software Development Life Cycle (SDLC) is a well-defined approach for producing high-quality, low-cost software in the shortest possible amount of time framework. This document provides a brief overview of standards and frameworks that could be used in the research project about cyber security automation of industrial 4.0 garment manufacturing system

1. Introduction

Written norms are expected to render cyber security initiatives clear. These requirements are referred to as cyber security standards, and they are generic collections of prescriptions for the best implementation of specific steps, created by industry experts. Methods, protocols, reference structures, and other items may be included in the specifications. It ensures security reliability, promotes integration and interoperability, and allows for practical measure comparison. A written specification that defines a common language, includes a technical specification or other precise requirements, and is intended to be used consistently, as a law, a guideline, or a description. The aim of security standards is to make information technology (IT) systems, networks, and essential infrastructures more secure.

Figure 2.9: Screen shot of the standard identification documentation

2.2.4. Choose the most suitable standards and frameworks

The most suitable standards and frameworks were chosen after evaluating the details for each component and their requirements. Two security standards were chosen after discussing and evaluating the details of most suitable standards with group members and policy developers in the industry. The most practical standards to implement in the research project was chosen according to the system requirements. Therefore, the research needed a standard for information security management and IoT security. The chosen standards were compared and documented.

2.2.4.1. ISO 27001:2013

This International Standard provides requirements for establishing, implementing, maintaining and continually improving an information security management system to support strategic decisions for needs and objectives, security requirements, system processes used, size of the audience and structure in ISMS. Also a comparison of chosen cyber security standards for the cyber security automation of industrial 4.0 garment manufacturing system were conducted.

2.2.4.2. IEC 62443

Developed to secure industrial automation and control systems (IACS) throughout their lifecycle. It currently includes nine standards, technical reports (TR) and technical specifications (TS). IEC 62443 was initially developed for the industrial process sector but IACS are found in an ever-expanding range of domains and industries.

IACS technologies are central to critical infrastructure. Implementing IEC 62443 can help to lessen the effects of cyber-attacks and even avoid them. It can improve security and lower expenses throughout the lifecycle.

IEC 62443 covers not just the technology that makes up a control system, but also the processes, countermeasures, and people working in it.

Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.

2.2.4.3. Importance of using both standards

There are significant variations between Operational Technology (OT) and Information Technology (IT) systems. One of the most notable differences is that industrial process failures frequently have an impact on the physical world, they might impair human health and welfare, risk the environment by spilling hazardous materials, or have an economic impact, such as in the case of severe power outages. In addition, the emphasis on basic security objectives. IT emphasizes data confidentiality, whereas OT prioritizes system availability; the security goals of both domains are thus diametrically opposed.

IEC 62443 lays forth the specific requirements of IACS while also building on existing best practices. This means that sections of IEC 62443 were written with ISO 27001 under reference, but they also take into account the distinctions between IACS and IT systems. In addition, the standard not only outlines how to design a management system, but it also specifies precise functional and process requirements for both individual IACS components as well as complete control systems. As a result, IEC

62443 has a far broader scope than ISO 27001 and is more customized to the needs of IACS.

Both can be used together in a sense that ISO 27001 practices can help protect the information used to implement IACS and ensure the development process is effective in implementing the security practices defined by IEC 62443. Addressing the cyber security of these systems using a customer service management system that meets the requirements laid out in IEC 62443.

Table 2.2: Comparison of chosen security standards for the research

	ISO 27001	IEC 62443
Organizations involved on creating the standard	ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)	The International Electrotechnical Commission (IEC)
Directives	Drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.	This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.
Scope	Information Security Management Systems	Cyber Security Management System (CSMS) for industrial automation and control systems (IACS)
Certifications	Yes	Yes. Number of organizations offering the certifications are smaller, some of the most prominent players are TÜV, exida, CertX, UL, DEKRA and ISASecure.

Controls	114 controls in 14 categories	Thirteen documents which are organized into four groups: General, Policies and Procedures, System, and Component.
-----------------	-------------------------------	---

2.2.4.4. Relationship between IEC 62443 standard and ISO/IEC 27001

Much of the content in the ISO standard is applicable to IACS as well. The IEC 62443 standard emphasizes the need for consistency between the practices to manage IACS cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. IEC 62443 standard builds on the guidance in the ISO/IEC standards. It addresses some of the important differences between IACS and general business/information technology systems. It introduces the important concept that cyber security risks with IACS.

2.2.5. Verify the chosen standards and frameworks

Verified the accountability of the chosen standards and frameworks whether they could be accountable to the automated manufacturing system through the advice from industrial experts. Industrial security standards verification was done through external supervisor. Security standards were verified through a security industry expert.

2.2.6. Determine the types of policies that are needed.

Identify the types of policies needed to the automation system such as password policies, network and authentication and access control policies, security update policies, acceptable use policies, encryption policies, vulnerability management policies according to standards and legislations. This information about policy creation was also gathered through various blog sites about standardization which determined how to implement ISO 27001:2013 and IEC 62443. The two standards were thoroughly analyzed and according to the system requirements the policies were identified. Each policy was created combining the two standards giving a customized policy creation according to the two standards. The policy documentation were done

according to the steps to implement ISO 27001. The ISO 27001 toolkit documentation lead to a better understanding how to implement the policies.

2.2.7. Verify policy creation

Created information security policies can be verified by the security expert from the industry before implementing the policies. So that we could be sure that our implemented security policies are secure.

2.2.8. Implement policies for the components

Properly installed and set up all of the key technologies and tools in the system, prepare the actual policies and procedure documents, import the initial set of policies, customize rule sets ensuring that the policies are adhered to in the tools to enforce policies accordingly.

2.3. Security Configurations and update management

2.3.1. Security Configurations

The Security configuration management tool is mainly written in Python3, YAML, and Ansible. The tool only provides command line interaction to the user and it only supports Linux because Ansible does not support Windows as the host. The tool provides following main functionalities to the users,

- Audit selected group of IoT devices
- Remediate selected group of IoT devices,
- Generate audit reports

In addition to mentioned main functionalities the tool has several sub functionalities to provide details to the users about available security profiles and rules. The Components in Figure 2.4 are used to implement the functionalities. Implementation of main functionalities are described in later part of this document.

2.3.1.1 Audit function

The audit function in the security configuration management tool is used for scanning compliance of selected IoT devices based on security rules stated in the security profile. The audit function takes security profile id and host group as inputs. The tool requires active SSH connections and administrative access to the selected IoT devices otherwise the audit will fail. As mentioned before Ansible requires SSH connections to communicate between host and clients. Ansible requires administrative access to IoT devices to perform certain actions for example. Accessing bootloader configurations for auditing requires administrative access because these configurations are saved in grub file which can only be accessed by the root user.

The main objective of using security profile is to define which rules to be audited or remediated using the tool. These profiles can be custom tailored based on level of security required by the organization. The security profiles are written in YAML and contains following information shown on the Table 2.2,

Table 2.3: List of Information in Security Profiles

Label	Description
ID	Security profile ID
Name	Security profile name
Category	Security profile category
Applicable hosts	Security profile is applicable to which type of IoT devices
Target system	Name of the Operating system used in IoT devices
Target system version	Version of the Operating system used in IoT devices
Description	Description about the security profile
Version	Version of the security profile
Rules	Contains the rule ids of the selected rule set

The host group defines group IoT devices to be audited. Ansible uses host group to deliver audit commands to client IoT devices. Host group is saved in a file called inventory located in the tool's root directory. The users can define IoT device host name, IoT device IP and group them based on requirements. The users must provide access credential to client IoT devices in the inventory otherwise Ansible cannot establish SSH connection with IoT devices.

Once valid inputs are provided audit function calls profile processor to process the selected security profile and load its rules to create a YAML file called 'extra_vars.yml'. While loading rules, Profile processor will call Rule processor to cross validate mentioned rules are stated in 'rules.yml'. Then the audit function will create an Ansible playbook using audit playbook template that contains audit role combined with given host group. Then the audit function runs the playbook with previously created 'extra_vars.yml'. Finally, the audit function calls report function to generate reports based on audit findings.

Audit role is an Ansible role, created to deliver audit commands to client IoT devices via SSH. The commands to audit selected rules are converted into tasks inside the audit role. These tasks contain following ansible modules,

- File – create and delete .csv audit reports
- Lineinfile – insert audit findings to the .csv audit reports
- Shell – audit current system configurations

Once audit role is executed, it will access 'main.yml' stored in tasks directory and executes tasks mentioned in 'main.yml' sequentially. The first task is to create an audit report on home directory of the user which ansible use to access the system. Report is a .csv file named after device host name and device IP address as shown below. Ansible uses 'ansible_facts' to gather information about system such as host name and IP address.

'Device hostname'_'Device IP address'_Audit_report.csv

For an example, if a device has its host name as 'IOTA' and device IP address is 10.0.0.2 the name of the created audit report is shown below.

IOTA_10.0.0.2_Audit_reprot.csv

Then tasks in sections executes in sequential order to audit security rules and write findings to the audit report. Once the tasks in sections are complete, the report is fetched to ansible controller and the report in client is deleted.

2.3.1.2 Remediate function

The remediate function in the security configuration management tool is used for reconfiguring non complaint systems to secure them. Similar to audit function, remediation takes security profile id and host group as inputs. The tool requires active SSH connections and administrative access to the selected IoT devices otherwise the remediate function will fail because remediating most of the security rules requires administrative privileges.

Once valid inputs are provided remediate function calls audit function by passing received inputs and an extra input called 'state'. By default, the value of 'state' variable in the audit function is set to 'Audit' however in this scenario remediate function overrides 'state' value as 'Before'. As mentioned before audit function will call profile processor to create a YAML file called 'extra_vars.yml'. The value of 'state' is also added to 'extra_vars.yml'. Then the audit function will create an Ansible playbook and

run the playbook with previously created 'extra_vars.yml'. Once the audit is finished, the remediate function will create an Ansible playbook using remediate playbook template that contains remediate role combined with given host group. Then the remediate function runs the playbook with previously created 'extra_vars.yml'. Once the remediation is finished, the remediation function calls audit function by passing received inputs and value of 'state' as 'After'. The value of 'state' is also added to 'extra_vars.yml'. Finally, two audit reports of each device are combined using 'dataframes' in 'pandas' Python library and report function is called to generate reports based on the combined audit reports.

2.3.1.3. Report function

Report function is used to generate comprehensive reports that can be viewed by users and organization management. Each report contains device details such as device host name, device IP, device host group, report created date, and time. Reports also contain graphs to illustrate summary about total rules scanned during audit. The graphs are used to illustrate total rules scanned their pass/fail ratio, high severity rules pass/fail ratio, medium severity rules pass/fail ratio, and low severity rules pass/fail ratio. Sample device details are shown in Figure 2.10 and sample summary about total rules scanned during audit shown in Figure 2.11.

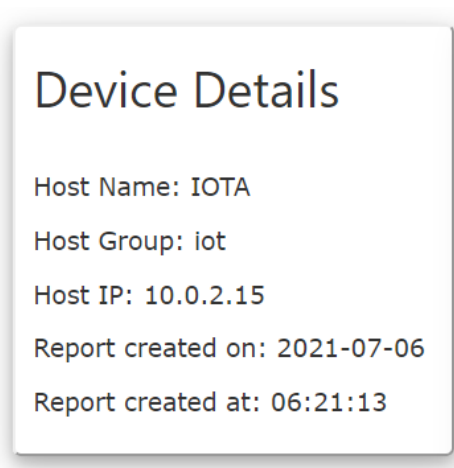


Figure 2.10: Sample device details

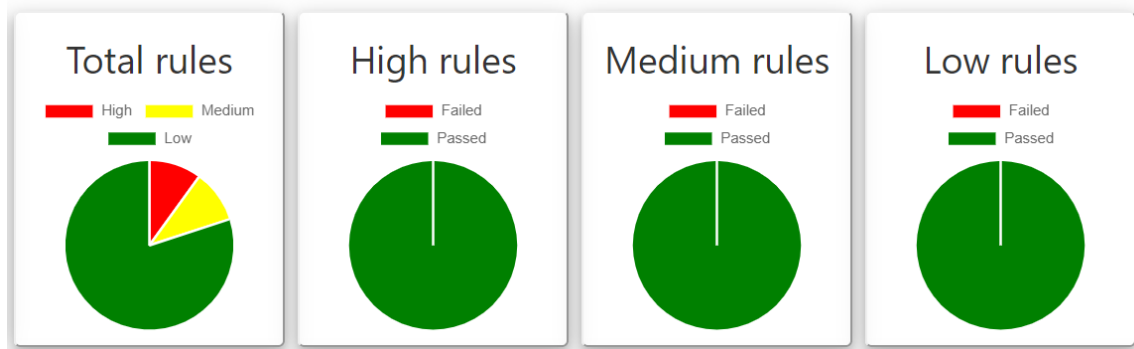


Figure 2.11: Sample audit summary

Once report function is called report function will read received audit reports from audit or remediate. Then report function extracts rule ids from audit reports and calls rule processor to get more information about a rule. Rule processor loads rules.yml file and search rules by rule_id and obtain the information about rules stored in rules.yml file. The rules.yml file contains following information shown in table 2.4.

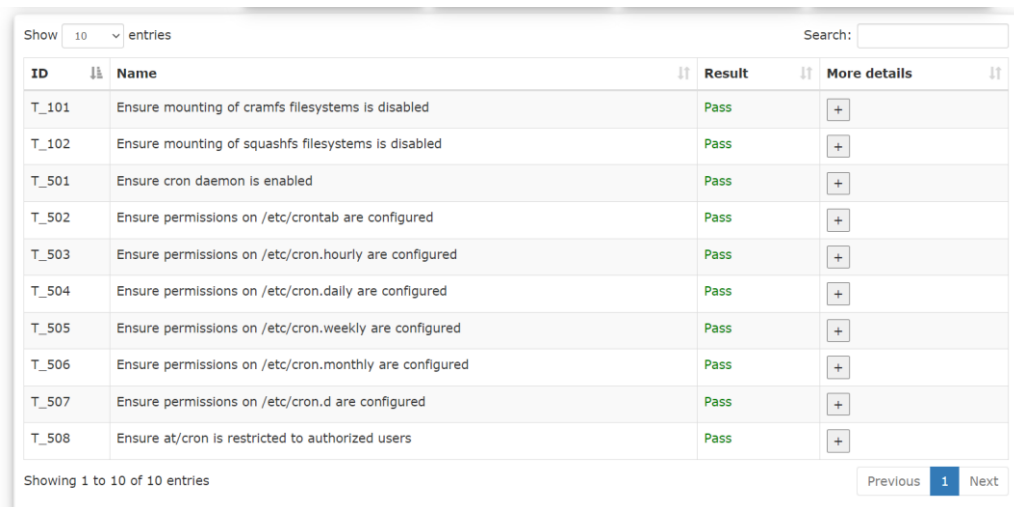
Table 2.4: List of Information in rules.yml

Label	Description
rule_id	Contains the security rule ID.
name	Contains the security rule name.
scored	States whether security rule has an impact or not.
severity	Criticality of the security rule, if the vulnerabilities were exploited.
version	Version of the security rule.
description	Brief description about the security rule explaining what vulnerabilities are mitigated by the security rule.
rationale	Brief description about the outcome, if vulnerabilities mentioned in description are exploited.
applicable_to	States which types of devices are affected by the security rule.

Once information about rules are returned to report function, the function will determine rule severity and calculate audit summary based on audit result and rule

severity of each rule. Once all rules in audit report are processed, report function write rule results and information to html template files using ‘jinja2’ python library. There are two different templates for audit and remediate because systems are audited twice during remediation.

The templates contain placeholders for device details summary, results table, results summary, and additional details about rules. Templates are used because reports are dynamic based on devices and their system configurations. These templates contain html code with bootstrap scripts to generate dynamic tables, graphs, and modals. The bootstrap ‘datatables’ library allows generation of dynamic tables with sorting, searching, and pagination functionalities. A sample results table is shown in Figure 2.12. According to Table 2.4, rules contain variety of information that cannot be entered to results tables because it causes table to be unreadable. Therefore, modals are used to display that additional information to the user. A sample modal is shown in Figure 2.13.



The screenshot shows a web-based table with 10 entries. The table has columns for ID, Name, Result, and More details. The results are all 'Pass'. The 'More details' column contains a '+' button for each entry. The table is part of a larger interface with a search bar and pagination controls.

ID	Name	Result	More details
T_101	Ensure mounting of cramfs filesystems is disabled	Pass	+
T_102	Ensure mounting of squashfs filesystems is disabled	Pass	+
T_501	Ensure cron daemon is enabled	Pass	+
T_502	Ensure permissions on /etc/crontab are configured	Pass	+
T_503	Ensure permissions on /etc/cron.hourly are configured	Pass	+
T_504	Ensure permissions on /etc/cron.daily are configured	Pass	+
T_505	Ensure permissions on /etc/cron.weekly are configured	Pass	+
T_506	Ensure permissions on /etc/cron.monthly are configured	Pass	+
T_507	Ensure permissions on /etc/cron.d are configured	Pass	+
T_508	Ensure at/cron is restricted to authorized users	Pass	+

Figure 2.12: Sample report results table

Ensure mounting of cramfs filesystems is disabled	
Attributes	Details
ID	T_101
Name	Ensure mounting of cramfs filesystems is disabled
Scored	1
Version	1.0.0
Severity	high
Description	The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image.
Rationale	Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.
Applicable To	IOT,ROS
Audit Result	Pass

Figure 2.13: Additional details about rule T_101

2.3.2 Update management

Create a centralized security update management system using local repositories.

Below shows the work break down structure for the update management component.

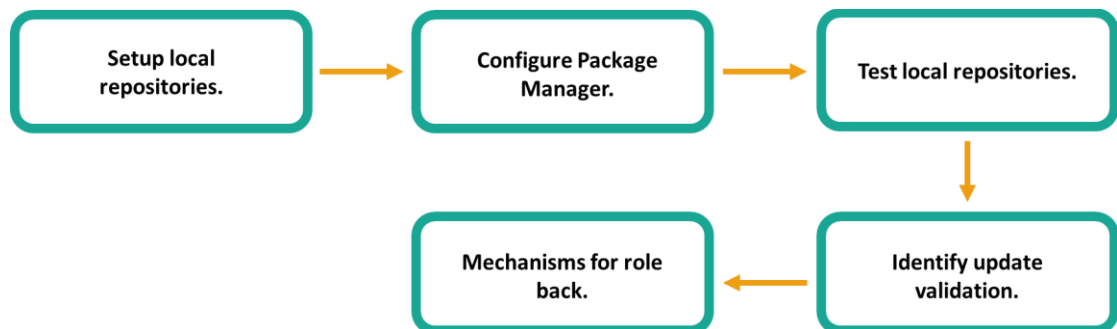


Figure 2.14: Individual Workflow Diagram- Security Updates

2.3.2.1 Setup local repositories

System administrators should always install software, security updates for all the devices. It is consuming a lot of internet bandwidth. As a solution to this above mentioned issue, instead of downloading software each time to all systems, all applications are saved in a local server in the LAN and distributed among clients when required in the same time. This solution is fast and efficient because the LAN connections are faster. This saves the internet bandwidth reducing the cost for internet.

Creating a local repository is advantages when the devices are connected and have to install more software. Setup a central local repository in the server, so that the clients can install, update and upgrade the packages from the central repository without using internet.

Host the created repo using apache server.

Add required packages to the local repository frequently. Pull the packages from public repositories from the package server and save locally. Install apt-mirror.

2.3.2.2 Configure package manager

Create a directory in the hard disk to save all packages. Go to the latest mirror package repository and run apt-mirror to get all the packages in the repository.

2.3.2.3 Configure IoT devices to access previously setup local repository

Web server is needed to be able to access the repo from other devices. Configure the Apache server. Create a link. Add repository source in other devices to fetch the repository and packages.

2.3.2.4 Test local repositories

Install packages using added local repository

2.3.2.5 Verify update

Verify updates using GPG keys to identify rogue updates.

2.3.2.6 Mechanisms for roll back

Keep previous version of packages to roll back or downgrade updates.

2.4. Authentication and access control

The component shows how to fulfill main security solution of industry 4.0 garment manufacturing system with Authenticating users when connecting to IIoT devices and enable secure access to the services, monitor and filter the user behavior on the system to prevent unauthorized access and to prevent malicious attacks.

2.4.1. 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.

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 2.15: Control panel of the CNC machine

2.5. Firewall and Intrusion Detection System (IDS)

2.5.1. Requirement Analysis for hardware requirements

Extensive studies were carried out in order to identify requirements. Initially, outlined the hardware requirements of the base device; second, selected the IDS software and assessed the compatibility with the base device. At this stage required key components for the IDS had been identified. Required components can be divided into two categories, which is software and hardware components.

2.5.2. Snort Installation and configuration

Initially there are three plugins needs to install as prerequisite plugins for Snort IDS to operate properly. Those plugins are pcap (Packet Capture), pcre (Perl Compatible

Regular Expressions) and libdnet (a low-level portable interface for networking routines)

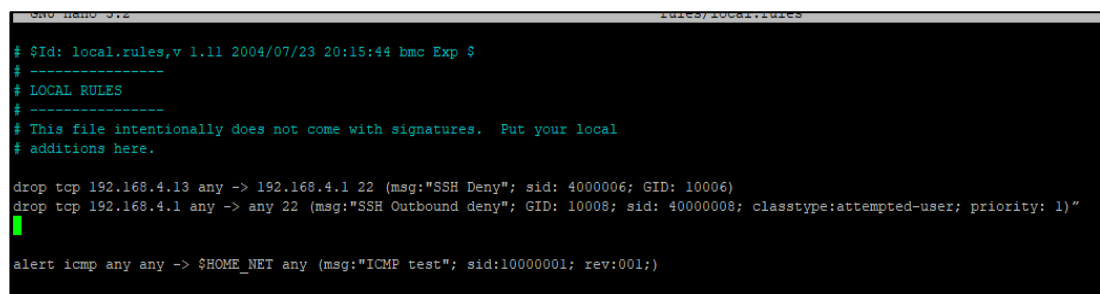
After installing these plugins Snort DAQ ((Data Acquisition Library) was source code was downloaded, compiled and installed, which was a necessary tool for packet monitoring.

Finally, all the pre requirements are installed, then Snort source code can be downloaded. The latest source codes are available in Snort official website. In order to compile and install use below command

```
./configure && make && sudo make install
```

Snort registered rule set were used in this project. However, in addition to those rules user can write their own rules in Snort. By default, these rules were stored in “/etc/snort/rules/local.rules” file. The rules are specified based on protocol layer, packet type, priority, source and destination. User can refer to “/etc/snort/classification.config” file to get a better understanding of priority types.

As for demonstration purposes we created two custom rules figure 14, first rule is to drop SSH connections from the host 192.168.4.13. Second rule is to prevent attacks from the inside, by dropping outbound SSH traffic. Third rule is just there for testing, it alerts to ICMP ping requests.



```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

drop tcp 192.168.4.13 any -> 192.168.4.1 22 (msg:"SSH Deny"; sid: 4000006; GID: 10006)
drop tcp 192.168.4.1 any -> any 22 (msg:"SSH Outbound deny"; GID: 10008; sid: 40000008; classtype:attempted-user; priority: 1)

alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

Figure 2.16: Custom rules

```

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_MODEBUS Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Commencing packet processing (pid=5262)
Decoding Ethernet

10/03-07:23:52.620413  [*] [1:10000001:1] ICMP test [*] [Priority: 0] {IPV6-ICMP} fe80::16
91:82ff:febe:5e4e -> ff02::1
10/03-07:23:56.045143  [Drop] [*] [10008:40000008:0] SSH Outbound deny [*] [Classification
: Attempted User Privilege Gain] [Priority: 1] {TCP} 192.168.4.1:46932 -> 192.168.4.9:22
10/03-07:24:07.514620  [Drop] [*] [10006:40000006:0] SSH Deny [*] [Priority: 0] {TCP} 192.1
68.4.13:64773 -> 192.168.4.1:22

```

Figure 2.17: Generated alerts

```

C:\Users\Admin>ssh pi@192.168.4.1
pi@192.168.4.1's password:
Connection reset by 192.168.4.1 port 22

C:\Users\Admin>

```

Figure 2.18: SSH attempt denied

2.5.3. Barnyard2 installation and configuration

After verifying Snort configurations, we proceed to install Barnyard2 module. This module is use to convert Snort unified2 binary files into human readable format. Same as before this module is also installed from the source code compilation. As for the configurations Barnyard2 was configured to read unified2 log files and write them into a MySQL database. Figure 2.19 shows Barnyard2 version, Figure 2.20 and 2.21 shows stored data in database.

```

pi@raspberrypi:~ $ /usr/local/bin/barnyard2 -v

  _ _ _ _ _      -*> Barnyard2 <*-
 /  ' '  \      Version 2.1.14 (Build 337)
|o"  )~|      By Ian Firms (SecurixLive): http://www.securixlive.com/
+ ' ' ' +      (C) Copyright 2008-2013 Ian Firms <firnsy@securixlive.com>

```

Figure 2.19: Barnyard2 installation

```
MariaDB [snort]> use snort
Database changed
MariaDB [snort]> select * from signature limit 30;
```

sig_id	sig_name	sig_class_id	sig_priority	sig_rev	sig_sid	sig
1	dnp3: DNP3 Application-Layer Fragment uses a reserved function code.	0	0	0	6	
2	dnp3: DNP3 Link-Layer Frame uses a reserved address.	0	0	0	5	
3	dnp3: DNP3 Reassembly Buffer was cleared without reassembling a complete message.	0	0	0	4	
4	dnp3: DNP3 Transport-Layer Segment was dropped during reassembly.	0	0	0	3	
5	dnp3: DNP3 Link-Layer Frame was dropped.	0	0	0	2	
6	dnp3: DNP3 Link-Layer Frame contains bad CRC.	0	0	0	1	
7	modbus: Reserved Modbus function code in use.	0	0	0	3	

Figure 2.20: Stored alerts in database

```
MariaDB [snort]> select * from event;
```

sid	cid	signature	timestamp
1	1	507	2021-06-11 06:57:55
1	2	508	2021-06-11 06:57:55
1	3	509	2021-06-11 06:57:55
1	4	507	2021-06-11 06:57:56
1	5	508	2021-06-11 06:57:56
1	6	509	2021-06-11 06:57:56
1	7	507	2021-06-11 06:57:57
1	8	508	2021-06-11 06:57:57
1	9	509	2021-06-11 06:57:57
1	10	507	2021-06-11 06:57:58
1	11	508	2021-06-11 06:57:58

Figure 2.21: Stored signatures

2.5.4. Pulledpork module installation and configuration

In order to automate ruleset update process, we utilized Pulledpork module. It is written in Perl language. As done in previous installations this also can be downloaded as the source code.

Before configuration, user needs to register in Snort official website the obtain a register key known as “oinkcode”. Afterwards place the key inside Pulledpork configuration file located inside /etc/snort/pulledpork.conf. Below figure 2.22 shows the Pulledpork configuration file.

```
# note that the url, rule file, and oinkcode itself are separated by a pipe |
# i.e. url|tarball|123456789,
rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot-29170.tar.gz|cb2e54fa8adea49239e3eb362c3c7886af1b846f
# NEW Community ruleset:
rule_url=https://snort.org/downloads/community/|community-rules.tar.gz|Community
# NEW For IP Block lists! Note the format is urltofile|IPBLOCKLIST|<oinkcode>
# This format MUST be followed to let pulledpork know that this is a blocklist
rule_url=https://snort.org/downloads/ip-block-list|IPBLOCKLIST|open
# THE FOLLOWING URL is for emergingthreats downloads, note the tarball name change!
```

Figure 2.22: Pulledpork configuration

For the first-time run Pulledpork script manually. Then after this script can be added to a crontab. For optimum security ruleset must update at least once a week.

```
Writing /var/log/sid_changes.log....
Done
Rule Stats...
  New:-----300
  Deleted:---0
  Enabled Rules:----10168
  Dropped Rules:----2
  Disabled Rules:---32516
  Total Rules:-----42686
IP Blocklist Stats...
  Total IPs:-----1414

Done
Please review /var/log/sid_changes.log for additional details
Fly Piggy Fly!
```

Figure 2.23: Pulledpork installing rules

Rule validation can be done by using below command

```
sudo snort -T -c /etc/snort/snort.conf -i wlan0:eth0
```

2.5.5. Configuring the Iptables firewall

Since this device operating in the middle of the network set of firewall policy rules were created as an extra layer of protection for the IDS These rules were created in a manner, normal operations will not be interrupt. Additionally, these rules will ease the load from Snort IDS process.

These rules are able to provide protection against attacks such as DDoS attacks, SSH attacks, brute force attacks and more.

```

pi@raspberrypi:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination              ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere               anywhere                  ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere               anywhere                  ctstate RELATED,ESTABLISHED
DROP       all  --  anywhere               anywhere                  state INVALID
DROP       icmp --  anywhere               anywhere                  icmp address-mask-request
DROP       icmp --  anywhere               anywhere                  icmp timestamp-request
ACCEPT     tcp  --  anywhere               anywhere                  tcp flags:RST/RST limit: avg 2/sec burst 2
ACCEPT     tcp  --  anywhere               anywhere                  tcp dpt:ssh ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere                  tcp spt:ssh ctstate ESTABLISHED
ACCEPT     tcp  --  192.168.4.0/24          anywhere                  tcp dpt:rsync ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere                  multiport dports http,https ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  192.168.4.0/24          anywhere                  tcp dpt:mysql ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere                  tcp dpt:smtp ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere                  tcp dpt:imap2 ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere                  tcp dpt:imaps ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere                  tcp dpt:pop3 ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere               anywhere                  tcp dpt:pop3s ctstate NEW,ESTABLISHED
LOG         all  --  10.0.0.0/8             anywhere                  limit: avg 5/min burst 7 LOG level warning p
DROP       all  --  10.0.0.0/8             anywhere
DROP       all  --  anywhere               anywhere                  MAC 00:0F:EA:91:04:08
ACCEPT     tcp  --  anywhere               anywhere                  tcp dpt:ssh MAC 00:0F:EA:91:04:07
REJECT     all  --  1.2.3.4                anywhere                  TTL match TTL < 40 reject-with icmp-port-unr
           tcp  --  anywhere               anywhere                  tcp dpt:ssh ctstate NEW recent: SET name: DE
syn_flood  tcp  --  anywhere               anywhere                  tcp flags:FIN,SYN,RST,ACK/SYN
ACCEPT     icmp --  anywhere               anywhere                  limit: avg 1/sec burst 1
LOG         icmp --  anywhere               anywhere                  limit: avg 1/sec burst 1 LOG level warning p
DROP       icmp --  anywhere               anywhere
DROP       all  -f  anywhere               anywhere
DROP       tcp  --  anywhere               anywhere                  tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RS
DROP       tcp  --  anywhere               anywhere                  tcp flags:FIN,SYN,RST,PSH,ACK,URG/NONE

```

Figure 34: IPtables Firewall policy rules

2.5.6. Filebeat installation and configuration

In order to securely ship alert log files from IDS to log management server, Beats data shipper was installed in IDS. Once Filebeat is downloaded and installed the logs which needs to shipped to Logstash has to be specified in “/etc/filebeat/filebeat.yml” file, along with the log server IP and port number. However, this communication is not secured, to remedy this problem we encrypted this communication using as SSL certificate as shown in figure 2.25.

```
# ----- Logstash Output -----

filebeat.inputs:
- type: log
  paths:
    - /var/log/snort/snort.csv
  tags: ["snort"]

output.logstash:
  hosts: ["192.168.4.6:5044"]
  ssl.certificate_authorities: ["/etc/pki/filebeat/logstash.crt"]
  ssl.certificate: "/etc/client.crt"
  ssl.key: "/etc/client.key"
```

Figure 2.25: Filebeat configuration

2.5.7. Logstash install and configuration

Logstash collect data for Filebeat agents and filter them according to configurations, those filtered data will be forwarded to Elasticsearch. As shown in the figure 23 the host and port are defined. This IP and port number is the same host and port as mentioned in the filebeat output section additionally user needs to mention the SSL certificates that been used. User has to define the filters according to the data that been sent to Logstash. Output section contains the Elasticsearch address.

```
input {
  beats {
    port => "5044"
    type => "Snort"
    ssl => true
    ssl_certificate_authorities => ["/etc/ca.crt"]
    ssl_certificate => "/etc/server.crt"
    ssl_key => "/etc/server.key"
    ssl_verify_mode => "force_peer"
  }
}
```

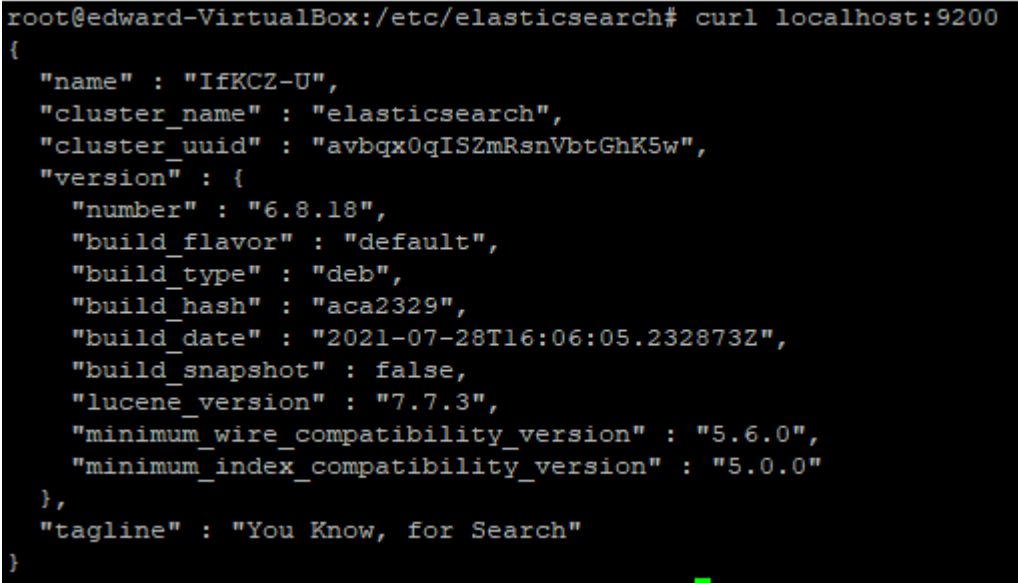
Figure 2.26: Input section Logstash configuration

```
filter {
  csv {
    separator => ","
    skip_header => "true"
    columns => ["msg", "timestamp", "proto", "src", "dst"]
  }
}
```

Figure 2.27: Filter and Output section

2.5.8. Elasticsearch installation and configuration

Elasticsearch has the ability to store, search and analyze huge volumes of data rapidly. This can be used with Logstash to collect, aggregate and parse the data to then file the data to the GUI Kibana. In order to install, Elasticsearch can be downloaded from elastic official website. There are no any configurations to be done initially to use Elasticsearch alongside with elastic stack.



```
root@edward-VirtualBox:/etc/elasticsearch# curl localhost:9200
{
  "name" : "IfKCZ-U",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "avbqx0qISZmRsnVbtGhK5w",
  "version" : {
    "number" : "6.8.18",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "aca2329",
    "build_date" : "2021-07-28T16:06:05.232873Z",
    "build_snapshot" : false,
    "lucene_version" : "7.7.3",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Figure 2.28: The curl request and Elasticsearch response

2.5.9. Kibana installation and configuration

Kibana module is working in harmony with Elasticsearch to display alert logs. Kibana can be used to search, view and interact with the data stored by the Elasticsearch. User have the full ability to create and customize data charts and graphs to display in a presentable manner. Having a web-based interface makes it easy to access understand large volumes of data. Same as before Kibana can be downloaded via the Elastic official website. Afterwards, entering “<IP address>:5061” (5061 being Kibana’s default port) in the browser URL field Kibana should load up.

2.6. Commercialization aspect of the product

Targeted audience are small and medium 4.0 industries or industries that migrating into industry 4.0 to secure their systems. Most manufacturers switch to industry 4.0 to increase their productions and security is not their primary concern. Only larger manufacturers have enough budget to hire employees to handle cyber security of their manufacturing systems. Even though, most manufacturers neglect security or transfer responsibilities of handling security to third vendors. Small and medium manufacturers may have to completely neglect security due to budget constraints. Proposed centralized security management system will be a better solution for above concerns. Also, the advantage of our project is we can promote individual aspects independently according to the four cyber security aspects mentioned below. We will gauge our target audience through Facebook, Twitter, Instagram campaigns, and official webpage.

2.6.1 Standardization

The standardization aspect could be commercialized after developed as a customized security framework for industrial 4.0 manufacturing systems at a reasonable price.

The overall security system could be successfully tested and promote as a cost-effective solution for small to medium businesses, targeting towards businesses who are migrating towards Industry 4.0.

2.6.2. Security Configurations

The security configuration management tool is ideal for large, medium, and small manufacturers to secure their IoT systems. The tool automates security hardening and it does not require security professionals to use the tool. System administrators can effortlessly audit and remediate IoT systems using the tool. This allows manufacturers to reduce budget spent on security. Manufacturers can reduce production loss due to security procedures by using the tool rather than performing same security procedures manually.

2.6.3. Firewall and Intrusion Detection System

Advanced and efficient anti-virus solutions with built-in host-based intrusion detection systems are available in current market for a reasonable price. An argument can be made anti-virus solutions can protect for cyber threats. These solutions are targeted to protect only one host machine such as a computer and unable protect the vast amount of interconnected IOT devices from cyber threats. Only network-based IDS solutions are capable of protecting the entire network such solutions can be unaffordable for smaller organizations.

After successful testing phase we planned to promote this solution as a cost-effective network security and monitoring solution for small to medium businesses as well as home owners. Specially targeted towards businesses who are migrating towards Industry 4.0.

2.6.4. Authentication and Access control

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.

2.7 Testing

2.7.1. Standardization

The policy creation was verified by an industry expert. Furthermore, after implementing the policies members who are responsible for each component conducted testing, auditing to ensure and verify that the applied policies are secured. The results were successful without error.

2.7.2. Security configurations

A virtual environment is used for testing the security configuration management tool. VirtualBox is used to create virtual machines and virtual network for testing simulations. 6 virtual machines are created for testing, one virtual machine acts as ansible controller while other 5 virtual machines act as client devices. Ansible controller runs on Ubuntu Linux. 3 client devices run on Raspberry Pi OS and 2 client devices run ROS. The security configuration management tool is installed in ansible controller with all its dependencies. SSH connection is configured on client devices and ansible controller. Administrative accounts are created on client devices and the credentials are given to the security configuration management tool. The devices are connected to each other through a Host-Only network shown in Figure 2.28.

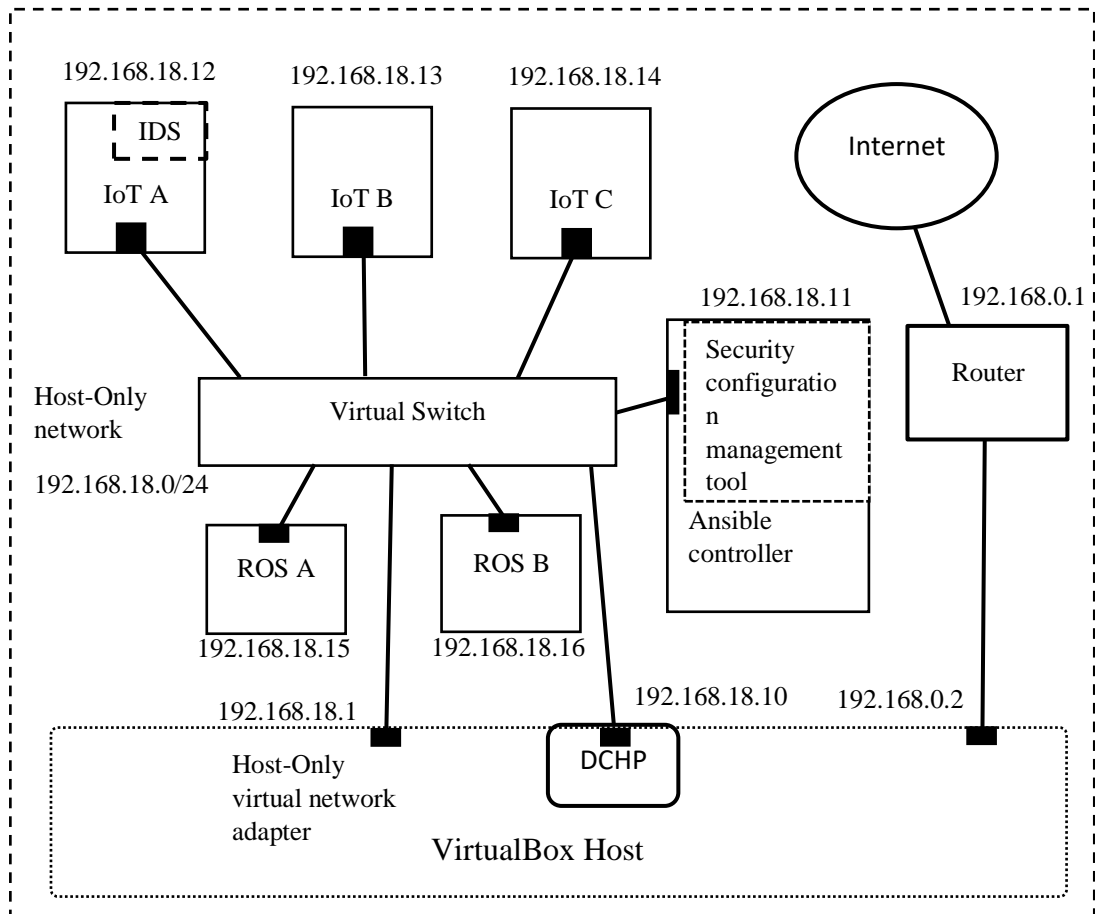


Figure 2.29: Network diagram of test scenarios

Two test scenarios are created to test the security configuration management tool using previously mentioned virtual machines. The propose of using these scenarios is to identify the tools effectiveness and efficiency of using centralized system against decentralized system where manual command line configurations or shell scripts are used to secure devices.

In first scenario, 3 IoT systems and 2 ROS systems start with default configurations. In addition to default configurations active SSH service and administrative accounts are created on all these systems. To test whether security mitigations affects existing services IDS is installed on IoT A. The security configuration management tool is used to remediate devices and the time it takes to remediate IoT, ROS systems are recorded separately. The virtual machines are reverted. The same security mitigations applied manually using commands or shell scripts and the time it takes to remediate systems

are recorded separately. The security rules or mitigations used during test is shown in Table 2.5.

In second scenario, 3 IoT systems and 2 ROS systems start with default configurations. In addition to default configurations active SSH service and administrative accounts are created on all these systems. To test whether that the tool can identify pre-remediated systems, IoT A and ROS A are remediated before the tests. To test whether security mitigations affects existing services IDS is installed on IoT A. IoT B is partially remediated to test whether the tool can identify already remediated security rules and remediate only necessary security rules that are not remediated before. The security configuration management tool is used to remediate devices and the time it takes to remediate IoT, ROS systems are recorded separately. The virtual machines are reverted to the test starting phase. The same security mitigations applied manually using commands or shell scripts and the time it takes to remediate systems are recorded separately. The summary of performed tests on two test scenarios are shown in Table 2.5.

Table 2.5: Summary of Performed Tests

Test ID	Test 1	Test 2	Test 3	Test 4
Used method	The security configuration management tool	Manual commands and shell scripts	The security configuration management tool	Manual commands and shell scripts
IoT A starting configuration	Default configuration	Default configuration	Secured	Secured
IoT B starting configuration	Default configuration	Default configuration	Partially secured	Partially secured
IoT C starting configuration	Default configuration	Default configuration	Default configuration	Default configuration
ROS A starting configuration	Default configuration	Default configuration	Secured	Secured

ROS B starting configuration	Default configuration	Default configuration	Default configuration	Default configuration
---	--------------------------	--------------------------	--------------------------	--------------------------

2.7.3. Authentication and access control

2.7.3.1. 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, 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.

The project operations are carried out in accordance with the flow chart shown in below figure. The method depicts the activities from the start of the project to its conclusion.

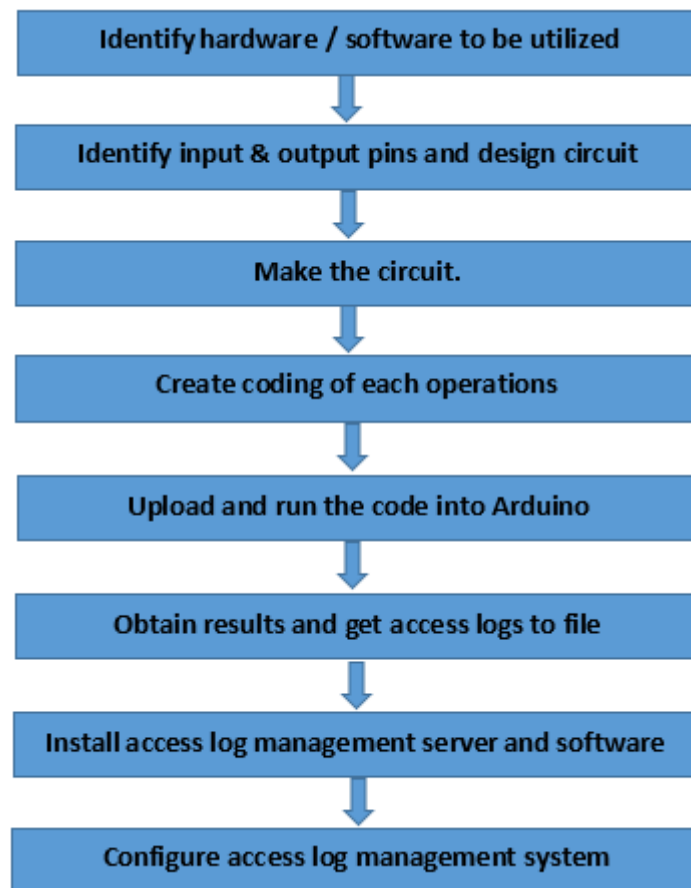


Figure 2.30: Flow chart of the project

Hardware requirements:

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

- 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 2.31: Arduino Uno R3

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
- Fingerprint sensor

Fingerprint sensor modules, such as the one shown below, make fingerprint recognition more accessible and simpler 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.

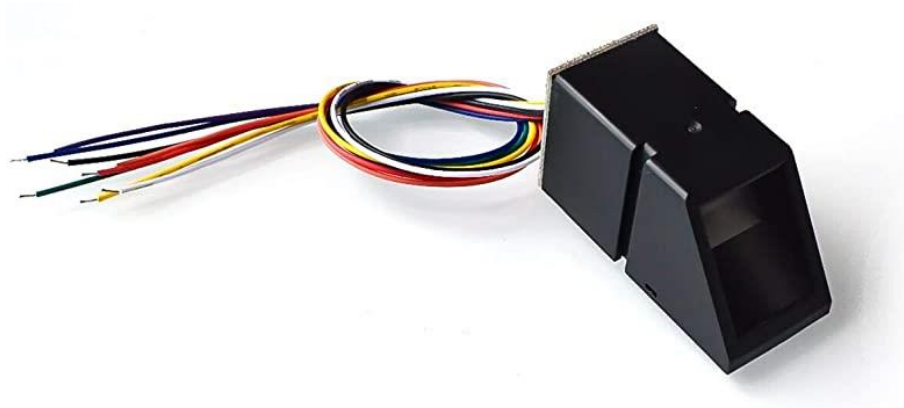


Figure 2.32: Fingerprint Sensor

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.

- Bluetooth module

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

- 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.

- 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.

- 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

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

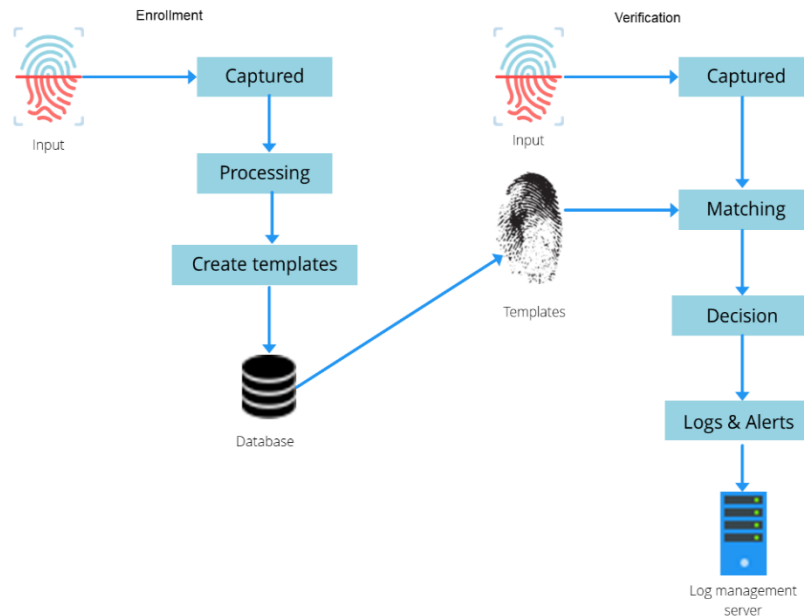


Figure 2.33: Physical access control system diagram

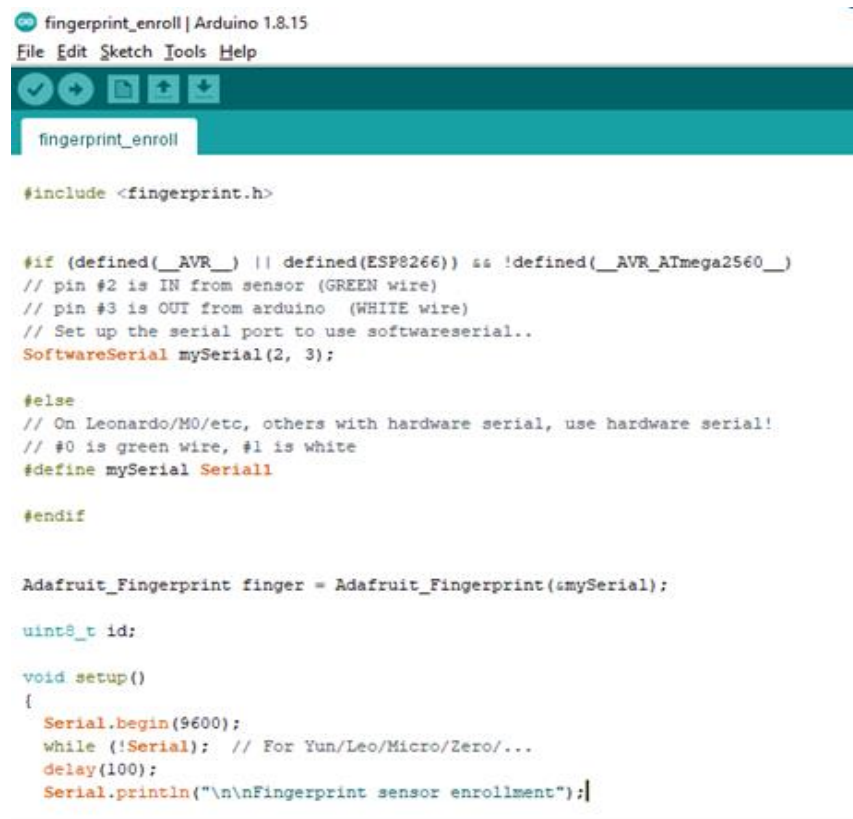
All of the research knowledge and components acquired will be put to use in this implementation phase. To achieve our main goal, we conducted preliminary study to gather information on authentication and access monitoring.

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 2.6: 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



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

#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 2.34: Fingerprint enrollment code 1

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

```

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 2.35: 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 -- 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.

```
COM4

.
.
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 2.36: 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.

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

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 2.37: 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(l3, HIGH); // LED on if synced
} else {
  digitalWrite(l3, LOW); // LED off if needs refresh
}

return finger.fingerID;
}

```

Figure 2.38: 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 --. 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 2.39: Finger test output at serial monitor

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

Table 2.7: 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).

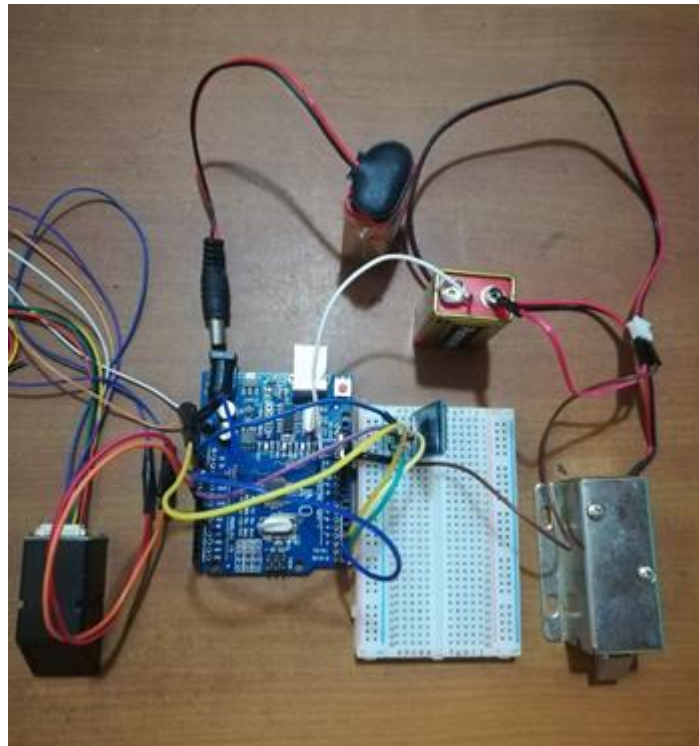


Figure 2.40: Connect the Bluetooth module to system

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

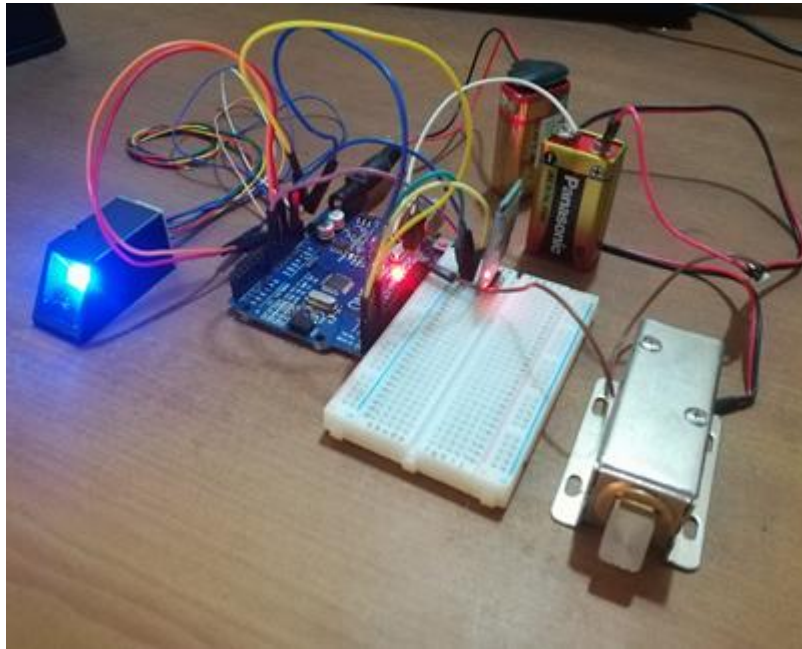


Figure 2.41: Implemented physical access control system

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.

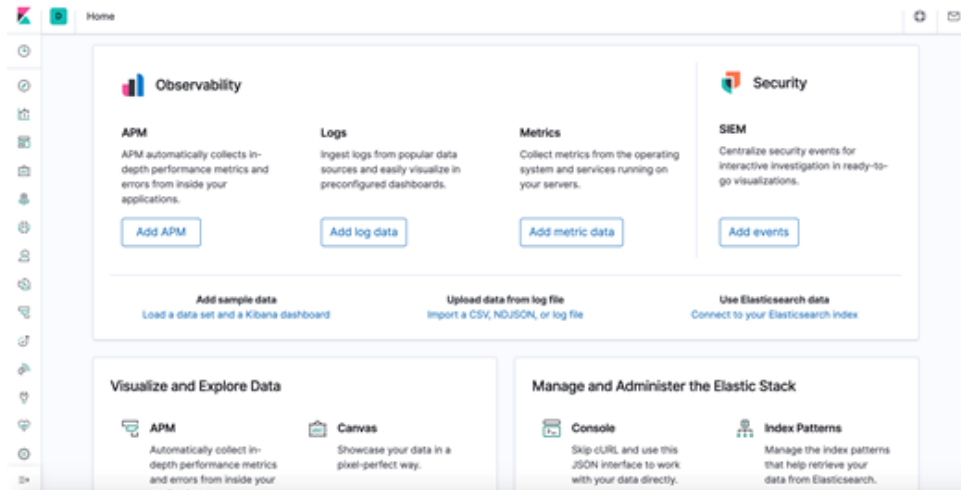


Figure 2.42: Kibana home page

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

2.7.3.2.1. 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 2.43: Access logs

2.7.3. Firewall and IDS

The main goal of testing phase is to assess the Raspberry Pi4's performance while running Snort IDS. After validating installation and configurations, testing phase begins. There are two methods of testing will be used. The first method is to test using intrusion detection evaluation dataset. The second method is simulating real world attack scenarios. For all testing purposes we used Kali Linux virtual machine and some of its pre-install tools to simulate attacks. All these test scenarios were conducted using 1200 (Community ruleset), 3000, 6000 and 10 000 lines of rules, because previous research shows lines of rules have a direct correlation with RAM usage. Iptables Firewall rules were flushed and disabled.

2.7.3.1. Intrusion detection evaluation dataset

This method evaluates IDS's resource consumption as well as attack detection capabilities by using packet trace file dataset, using a Kali Linux virtual machine with TCPReplay 4.3.3 to replay network traffic at different speeds. While executing these attacks, IDS is running in-line mode between the interfaces eth0 and wlan0 with Barnyard2 and Filebeat processors running in background.

An intrusion detection dataset is a dataset that created to evaluate the performance of an IDS. These datasets are formulated by researchers under a specific set of requirements and conditions containing various types of normal internet traffic patterns as well as attack patterns such as DoS, DDoS, port scanning, brute force attacks and ransomware attacks.

Choosing a correct dataset for specific need is a challenge. There are two ways to choose a dataset. One method is to Creating a dataset from scratch satisfies the purpose of the experiment. This however is not an easy task. The researcher should have the time and capabilities to run, capture, and label different types of attacks. The other method is to use an existing dataset from internet sources. There are many types of datasets can be found in the internet varying from simple trace files contains 1000 lines to massive datasets such as Canadian Institute of Cybersecurity Intrusion Detection Dataset (CICIDS2017) containing 30 000 000 lines [39].

Since the CICIDS2017 dataset is a huge dataset with 2,830,744 rows, it is unrealistic to our requirements. We customized and created our own dataset by using many trace files from internet sources. We created this dataset in such manner it has the diversity of CICIDS2017 dataset. Our dataset contains 200 000 rows and illustrate below types of attacks table 4.

Table 2.8: Containing attack packets

Attack Type	Count
Brute Force attacks	1200
DDOS attacks	5000
Bot attacks	8000
Port Scans	700
Ransomware attacks	740

2.7.3.2. Simulation of attacks

This method is mainly focusing on evaluating attack detection capabilities by performing set of real-world attack simulations against host machine connected to the Raspberry Pi access point. using a Kali Linux virtual machine with its pre-installed tools and various other attack scripts. While executing these attacks, IDS is running in-line mode between the interfaces eth0 and wlan0.

3. RESULTS, RESEARCH FINDINGS AND DISCUSSION

3.1. Standardization

3.1.1 Identify the specific standards and comparison of chosen security standards

Before identifying the standards and the research indicated it was important to learn the difference between security standards and frameworks. As a result, it was important to have an idea about the difference between standards and frameworks. Then as per the discussion with the group members and professionals two standards were chosen ISO 27001:2013 and IEC 62443, but when followed and the policies were made according to the security standards NIST cyber security framework special publications were needed to create policies.

Table 3.1: Security standard Vs. Security framework

Security Standard	Security Framework
<p>A cyber security standard defines both functional and assurance requirements within a product, system, process, or technology environment. Well-developed cyber security standards enable consistency among product developers and serve as a reliable metric for purchasing security products.</p> <ul style="list-style-type: none">• Best-known practice.• Defines the steps and procedures involved.• Internationally recognized standards mean that the same procedure is followed throughout the globe to perform a certain task if that particular standard has been adopted.	<p>A security framework is a compilation of state-mandated and international cyber security policies and processes to protect critical infrastructure. It includes precise instructions for companies to handle the personal information stored in systems to ensure their decreased vulnerability to security-related risks.</p> <ul style="list-style-type: none">• Structure underneath or beyond a system.• Not defined to the point.• Gives an outline.

<ul style="list-style-type: none"> Ensures that all companies follow the bare-minimum requirements to keep their client's data safe. 	
<p>IOT Security Standards examples:</p> <p>European Telecommunications Standards Institute (ETSI) EN 303 645 - ETSI TS 303 645 V2.1, provisions for the security of consumer devices that are connected to a network, ENISA Baseline security recommendations for IoT in the context of Critical Information Infrastructures, The National Institute of Standards and Technology's (NIST's) set of basic IoT security practices for manufacturers, OWASP Internet of Things Security Verification Standard (ISVS) provides security requirements for IoT applications.</p>	<p>IoT security Frameworks examples:</p> <p>IoT security Compliance framework, from the IoT security foundation, IEC 62443</p>

After identifying and comparing, the most suitable security standards were chosen and those standards were followed for policy creation.

3.1.2 Policy creation

The ISO 27001:2013 toolkit was followed as a guide for policy creation, but as it is mostly used for organizational processes, only the parts required for the smart system was considered. The asset registry and the business case documentation were created and they were useful for the risk assessment to identify requirements and assets.

3.1.3 Implementation of policies

3.1.3.1 Password policy

According to the ISO 27001 standard, the password policy should include an interactive password management system that ensures quality passwords.

According to IEC 62443 there are three main password requirements highlighted:

1. Password-based authentication's strength
2. Password generation and lifetime constraints
 - Human users
 - Software processes and devices
3. All users' passwords have a lifetime limit (humans, software processes, devices)

Human users should be identified for all access to components. The authentication passwords are used when authenticating to the Linux centralized security management system and the firewall is password protected when authenticating via interface.

The standard requires multi factor authentication for authentication of all access components. Limitations are that the multi factor authentication is costly. A key management server is required if using tokens for authentication. There also could be security overhead, if multi factor authentication in each IoT device. Instead, the access through the smart lock is authenticated through biometrics using finger prints. The smart lock is connected to the security management system through console, but the security management system is also password protected. The password less accounts are automatically locked through root. The biometric smart lock is the first layer of defense of the physical security for the smart system. An Identifier such as an ID for the user or a physical key can be used for physical security as multi factor authentication for smart lock. In our proposed system, only the critical assets are password protected based on the cost, but for future endeavors tokens can be used for multi factor authentication. The security management system has group based authentication. The permissions granted to the identified human user must be followed. The authentication enforcement is further discussed under Authentication and

authorization policies. Passwords are always stored with hash function, not in plain text.

According to IEC 62443 NIST SP 800-63-1 password guidelines were used to enforce password security policies.

Guidelines for password entropy and throttling have been simplified.

3.1.3.2 Audit policy

According to ISO 27001 standard audits at predetermined intervals should determine whether the information security management system complies with information security management system requirements, the requirements of this International Standard while being implemented and maintained effectively.

The audit policy should plan, establish, administer, and maintain audit programs, including frequency, methodology, responsibilities, planning requirements, and reporting. The audit programs must take into account the importance of the processes in question as well as prior audit results determining the audit criteria and scope for each audit. Choose auditors is also an important task according to the standard. There should be feedback of the ISMS including trends in audit results.

According to IEC 62443 standard, system usage such as monitoring, recording and subject to audit should be notified via a system usage notification, but in our system when auditing, the system is in a down state as auditing of the systems are been audited at a chosen time for all devices reducing the interruption for each device. Scheduled audits take place four times a year. When there are more devices through the network, when the audits are done in a centralized manner in the same time the cost and the redundancy is reduced. It is the system administrators' responsibility to maintain and control the audits.

Components shall support a supervisor manual override for a configurable time or sequence of events. In our system the administrator can log for specific events and they are logged and monitored, whether those logins were failed/successful, what commands were used.

According to IEC 62443, audit records on write-once media is a requirement, but in our system this mechanism is not used. Instead, only the root user can read audit records. The audit records are written in system level and nobody can access or modify the records. Programming access to audit logs is only given by the logs of a centralized system. All notifications of tampering shall be logged. Active monitoring would not be done as it would be unnecessary for the system. The performance will be decreased when actively monitoring the environment.

3.2. Security Configurations

3.2.1. Results

The results from performed test scenarios are recorded in Table 3.2 and Table 3.3. Time in Test 2 and Test 4 includes time it took due to human error and filling check lists due extensive security rule list used for the tests.

Table 3.2: The Results from Performed Audits

Device	Test 1	Test 2	Test 3	Test 4
IoT A audit time	12 minutes	100 minutes	12 minutes	95 minutes
IoT B audit time	12 minutes	95 minutes	12 minutes	105 minutes
IoT C audit time	12 minutes	90 minutes	12 minutes	105 minutes
ROS A audit time	13 minutes	95 minutes	13 minutes	90 minutes
ROS B audit time	13 minutes	105 minutes	13 minutes	100 minutes
Total time	25 minutes	485 minutes	25 times	495 minutes

Table 3.3: The Results from Performed Remediation

Device	Test 1	Test 2	Test 3	Test 4
IoT A remediation time	23 minutes	190 minutes	23 minutes	0 minutes
IoT B remediation time	23 minutes	200 minutes	23 minutes	150 minutes
IoT C remediation time	23 minutes	185 minutes	23 minutes	195 minutes
ROS A remediation time	25 minutes	195 minutes	25 minutes	0 minutes

ROS B remediation time	25 minutes	205 minutes	25 minutes	200 minutes
Total time	48 minutes	885 minutes	48 minutes	495 minutes

Test 1 and Test 3 have shown that the security configuration management tool simultaneously audit/remediate all the devices in IoT host group and ROS host group. Moreover, Test 3 have shown that the security configuration management tool simultaneously audit/remediate one security rule at a time before moving on to the next security rule. IoT A remediation time in Test 4 is 0 because IoT A is already secured. However, in Test 3 IoT A remediation time depends on IoT C because ansible performs tasks sequentially. Therefore, a task in IoT A must wait until the same task is completed in IoT B and IoT C.

Test 3 revealed that the security configuration management tool can identify insecure systems, partially secure systems, and secure systems to apply necessary required remediations on the systems. Although IoT A must wait until the same task is completed in IoT B and IoT C, the task did not make any changes to existing IoT A configurations. In Test 4 accidental misconfiguration or adding same configurations twice to some sensitive configurations files on IoT A resulted system and service failures. These configurations files include grub configuration files, PAM configuration files, SSH configuration file and other system configuration files.

Before configuring of mentioned sensitive configuration files all the selected CPS systems for remediation must halt their current activities to prevent any data loss that may happen during remediation. For an example, if SSH used to communicate between CPS devices misconfigurations in SSH configurations may cause SSH service failures which interrupts communication between CPS devices.

During manual remediations (Test 2 and Test 4), noticeable time were spent on correcting misconfigurations and human error due to extensive list of security rules used on several devices. Automated remediations using the security configuration management tool (Test 1 and Test 3) had shown that time was not wasted due to human

error or misconfigurations, if ansible tasks were properly tested prior to the remediations.

Since the security configuration management tool can analyze audit results and produce audit reports, users do not have pay much attention to outputs displayed by the tool during audits and remediations. However, during Test 2 and Test 4 outputs of audit commands must be manually analyzed and recorded to create reports. During Test 2 and Test 4 devices were audited individually to reduce human error when analyzing audit commands outputs and creating reports. This addition time to create report is considered when calculating execution time.

3.2.2 Research Findings

There are several security hardenings guides for Raspbian OS (Raspberry Pi OS) and ROS. However, there are lack of automated tools for security hardening on IoT devices. The security configuration management tool automates security auditing and remediation of IoT devices that runs on ROS and Raspbian OS. There are popular tools such as OpenSCAP and CIS-CAT Pro provides similar functionality as the security configuration management tool but none of these tools supports IoT based OS.

The centralized architecture of the overall system allows ansible controller to connect all devices at once if required. This allows the security configuration management tool to automate security auditing and remediation of the IoT devices from a single centralized server.

The security configuration management tool does not require special agent programs to be installed on client IoT devices. OpenSCAP and CIS-CAT Pro require special agent programs to be installed on client devices.

The security configuration management tool can audit or remediate multiple IoT devices at once. OpenSCAP and CIS-CAT Pro can audit or remediate a single device at a time. The simultaneous auditing and remediating of the security configuration management tool greatly reduces total system down time due to security hardening compared to manual security hardening. The automated tool greatly reduces human error during security hardening and auditing compared to manual security hardening and auditing.

Ansible normally used for configuring multiple systems remotely. However, in the security configuration management tool ansible is used for both auditing system configurations and configuring multiple systems remotely. Even though shell scripts and commands are more suitable for auditing configurations, ansible tasks provide reliable platform to audit multiple devices at once. Where shell scripts and commands can only audit single device at a time.

3.4. Authentication and access control

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 3.4: 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. Below figure 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 thumb with the most accurate result is the left thumbprint, which has a percentage of 79.9%, followed by the right thumbprint, right index finger, and left index finger, which have 60.6 percent, 70.2 percent, and 78.0% accuracy, respectively.

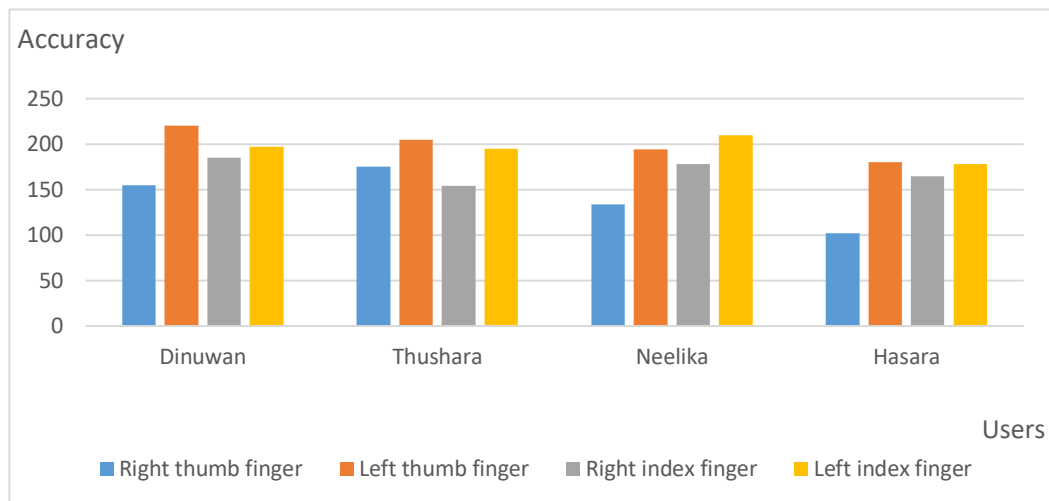


Figure 3.1: Degrees of Confidence

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).

3.3 Fireall and IDS

3.1.1 Results

These test results can be used for validate the feasibility of the proposed IDS solution. Below figure 30 shows the Snort IDS idling at 3.3 % of CPU usage and 709MB of Memory used with 10 000 lines of rules loaded.

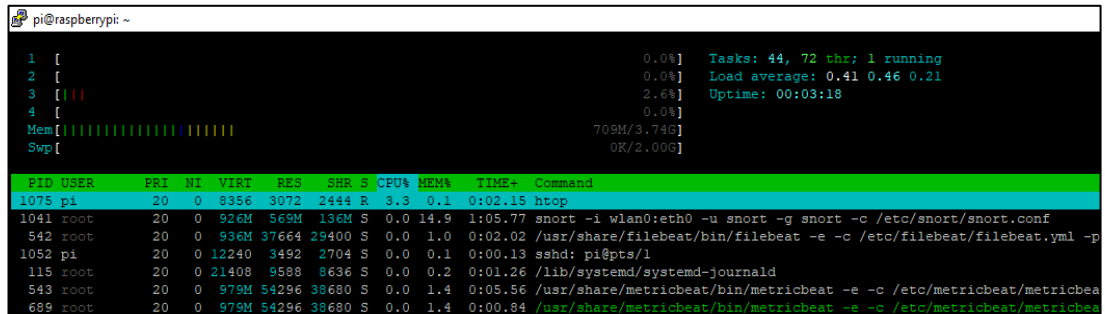


Figure 3.2: Snort idle resource consumption

Next the customized PCAP dataset were replayed using TCP replay at 5 different speeds starting from 5Mbps to 30 Mbps. This data speed was selected after benchmarking the Raspberry Pi 4's inbuilt wireless adaptor.

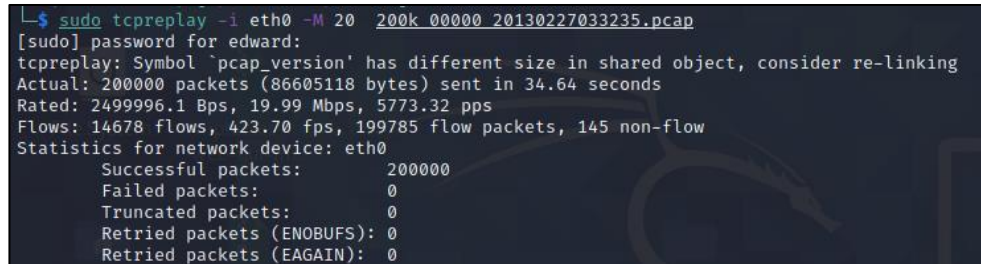


Figure 3.3: TCPReplay replaying at 20Mbps

3.1.1.1 CPU usage

Figure32 shows the relationship between the data rate which packets were transmitted from and the Raspberry Pi 4 CPU consumption. The main cause for this behavior is CPU interrupts, when a new packet arrives at IDS it triggers an CPU interrupt to inform about net packet arrival, these interrupts can overwhelm the CPU and could lead to packet drops. Moreover, tests reveal the number of rules have no considerable impact on CPU usage.

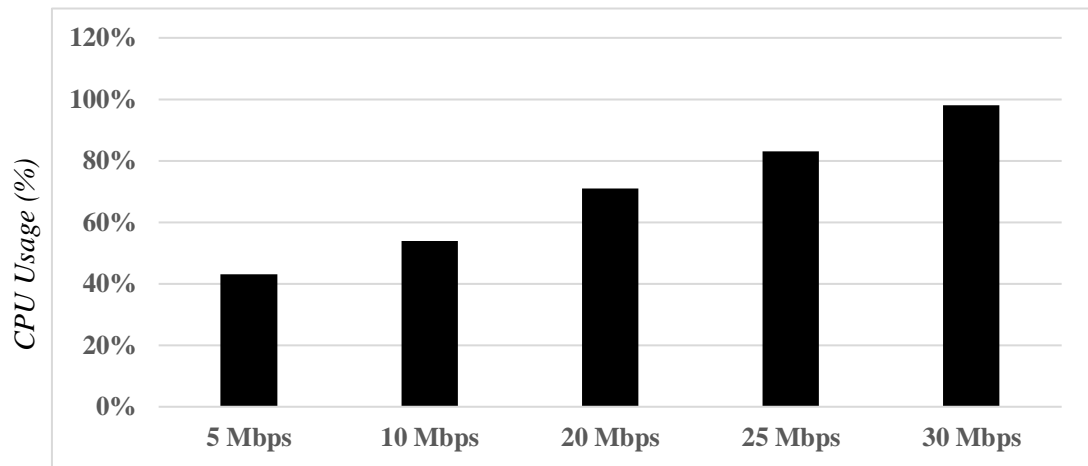


Figure 3.4: CPU Usage of Raspberry Pi IDS

Highest recorded CPU usage stated at 98%, this results a considerable amount of packet drops. below line graphs Figure 33 shows CPU usage and packet loss rate have a direct relationship.

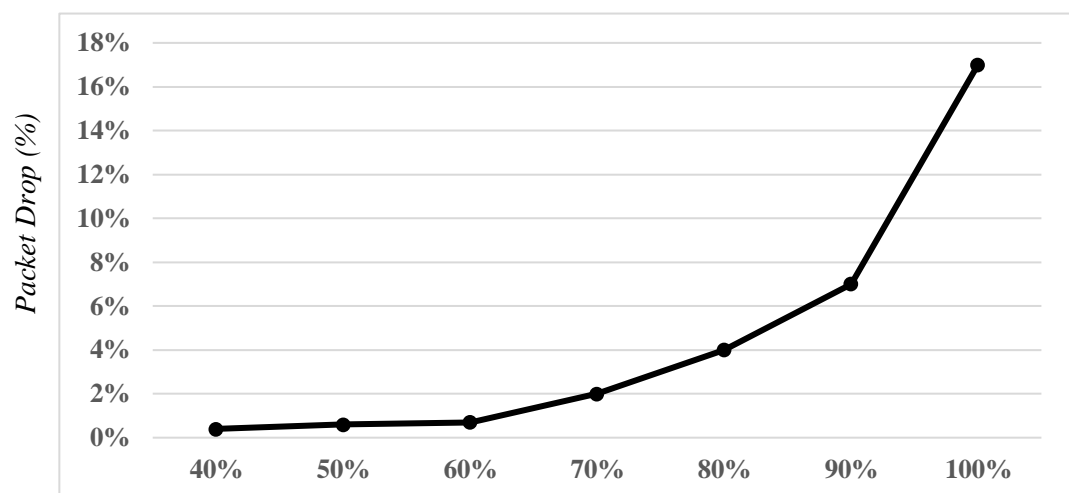


Figure 3.5: Packet loss and CPU usage

```

Packet I/O Totals:
  Received:      182792
  Analyzed:      182791 ( 99.999%)
  Dropped:       37727 ( 17.108%)
  Filtered:       0 ( 0.000%)
  Outstanding:   1 ( 0.001%)
  Injected:       0
  
```

Figure 3.6: Highest recorded packet drop

3.1.1.2 RAM usage

Figure 35 shows the correlation between the RAM usage and Snort rulesets. Even though rules have a negligible impact on CPU usage, it can directly impact RAM usage. The main cause is that Snort Detection engine loaded all the defined rules to its memory to carry out IDS functionalities, owing to this fact a higher number of rules demands a higher consumption of memory. A clear difference can be seen between the four rulesets.

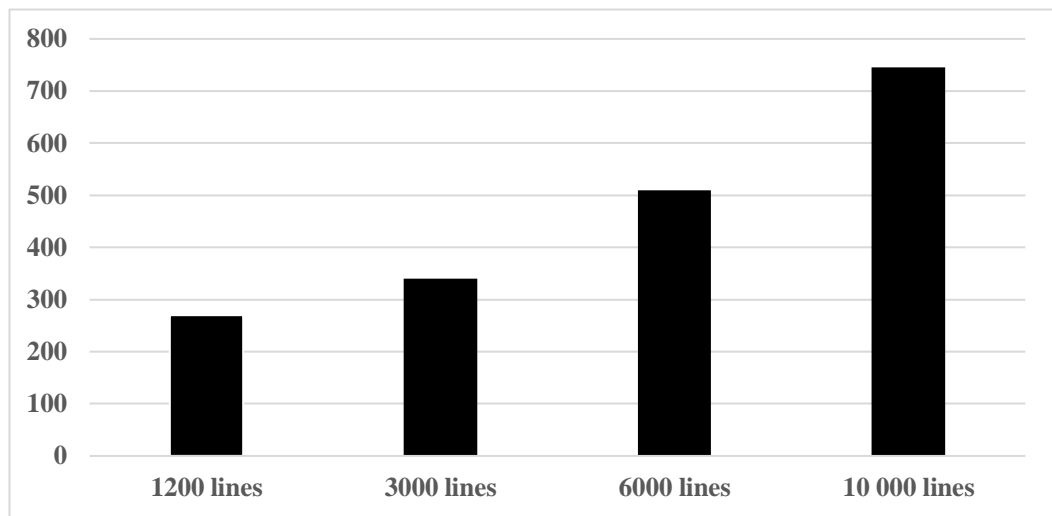


Figure 3.7: RAM usage

3.1.1.3 Generated alerts

Figure 3.8 shows the generated alerts while using the three different rulesets.

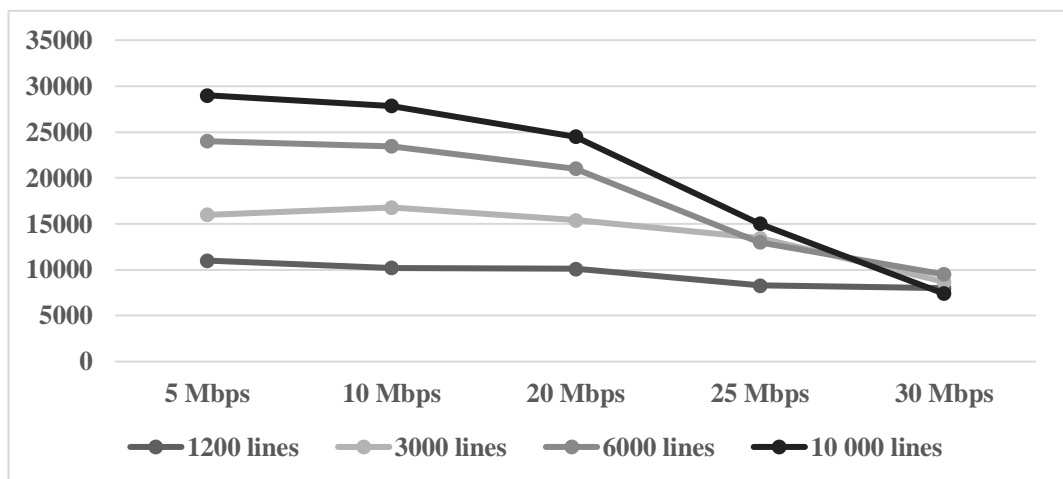


Figure 3.8: Generated alert

While running this test we observed the number of generated alerts were dropped when the data rate increases. The main reason for this is high CPU usage as shown in figure 32. As discussed previously when the CPU is overwhelmed with interrupts it loses the ability to process every packet, this will lead to packet drops and less rules will get triggered.

3.1.1.4 Real-world attack simulation

- Port scan

Initially a Nmap port scan was conducted using Kali Linux just to trigger a response from the IDS. As expected, Snort identified the attack and generated alerts. Below command was used and figure shows the generated alerts.

```
nmap -p- -sV -sT -A 192.168.4.1
```

Figure3.9: Port scan alerts

Low Orbit Ion Cannon (LOIC) was utilized to simulate the DDOS attacks against Apache web server running on Ubuntu OS that were inside the same network.

Snort was able to recognize this attack, LOIC was created more than 500 000 requests towards the web server. Snort was able to detect average of 95% of packets.

- Slowloris attack

Another DOS attack was launched using a python script from internet sources [23]. This is a Slowloris type DOS attack. Slowloris is an application layer attack that transmits partial packets to a web server. In this case Snort community ruleset failed to detect this attack. However, with registered rule set the attack was detected without any issue.

- Simulating Brute Force attack

In order to simulate brute force attack, Kali Linux pre-installed tool named Medusa was used.

Figure 40: SSH brute force attack using Medusa

In this case Snort did not successfully detect all the SSH brute force attacks. Snort was only able to detect 104 out of 221 attempts. The detection average was 48%.

```

xcs10/07-12:48:28.832555  [**] [1:4:1] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] (TCP) 192.168.4.9:58054 -> 168.4.1:22
xcs10/07-12:48:28.832555  [**] [1:4:1] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] (TCP) 192.168.4.9:58054 -> 168.4.1:22
10/07-12:48:58.402667  [**] [1:4:1] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] (TCP) 192.168.4.9:58060 -> 192.4.1:22
10/07-12:49:17.410910  [**] [1:10000001:1] ICMP test [**] [Priority: 0] (IPv6-ICMP) fe80::1691:82ff:febe:5e4e -> ff02::1
10/07-12:49:30.593694  [**] [1:4:1] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] (TCP) 192.168.4.9:58066 -> 192.4.1:22
10/07-12:49:39.044552  [**] [1:10000001:1] ICMP test [**] [Priority: 0] (IPv6-ICMP) fe80::1691:82ff:febe:5e4e -> ff02::1
^[[10/07-12:49:55.061438  [**] [1:10000001:1] ICMP test [**] [Priority: 0] (IPv6-ICMP) fe80::1691:82ff:febe:5e4e -> ff02::1
10/07-12:50:01.971562  [**] [1:4:1] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] (TCP) 192.168.4.9:58072 -> 192.4.1:22
10/07-12:50:06.404346  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] (TCP) 138.201.57.222:443 -> 10.235.126.119:80

```

Figure 3.11: SSH brute force attack alerts

- Man in the middle attack

To simulate MITM attack, Ettercap tool was utilized. Ettercap was successfully poisoned the ARP cache and all the packets were routed through the attacker host machine. However, Snort was failed to detect this attack so the below custom rule was added to the snort ruleset.

```

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg : "ICMP redirect host"; icode : 1; itype : 5; sid : 472; )

```

When an MITM attack occurs all the traffic were routed through the attacker machine and thus a longer route is used to packets to reach the gateway router. By using this theory above rule was able to detect MITM attack.

3.1.2. Research Findings

These test results revealing intrusion detection system based on Raspberry Pi 4 can handle 7 to 10 number of hosts with low to moderate traffic without any compromises. Well suited for home or small Industry 4.0 environments

While testing, we observed data rate and the CPU usage have a direct relationship as shown in figure 32, when packets transmitted with higher bandwidth the CPU usage reaches maximum, which also lead to packet drops and impact alert generate task. When it comes to RAM usage even with 10 000 lines of rules, IDS uses less than 1GB of RAM leaves plenty of headspace for other processors.

When simulating attacks community rule set performed poorly. It failed to detect any of network attacks other than the port scan. After adding 3000 lines of rules, it was able to detect LOIC DDOS simulation attack. 6000 lines of rules were able to detect

Slowloris attack as well as brute force attack. However, even with 10 000 lines of rules IDS failed to detect MITM attack. This finding shows the important of custom rules. The results are presented in Table.

Table 3.5: Simulated attack findings

	Community	Registered		
Attack Type	1200 lines	3000 lines	6000 lines	10 000 lines
Port SCAN	✓	✓	✓	✓
LOIC DDOS simulation		✓	✓	✓
Slowloris attack			✓	✓
Brute force attack			✓	✓
MITM attack	A custom rule was created			

One of the main drawbacks of Raspberry Pi4 is its weak Wi-Fi bandwidth and strength, while benchmarking it only reaches 29.7 Mbps. This can be remedy by adding a capable external wireless adaptor or and external antenna. When it comes to heat generation with a 7mm cooling fan and heatsink maximum operating temperature recorded was 45 degrees Celsius.

3.5 Discussion

The tool and manual security hardening are used on two separate systems that have N number of insecure IoT devices. Based on obtained tests results audit time, remediate time per device, and total system down time can be calculated using following equations.

If time loss due to human error and analysis time in manual auditing and remediating is neglected, down time of a device using both methods will be same. For a given security profile audit time per device is t_1 and remediate time per device is t_2 . Down time of a device is calculated below

$$\text{Down time of a device}(r) = t_1 + t_2$$

Depending on security profile,

$$5 \text{ min} \leq t_1 \leq 20 \text{ min}$$

$$15 \text{ min} \leq t_2 \leq 30 \text{ min}$$

Total system down time calculation is shown below, here r is down time of a device.

$$\text{Total system down time} = \sum_{r=1}^N r$$

Manual method total system down time is shown below.

$$\text{Total system down time} = \sum_{r=1}^N r = Nr = N(t_1 + t_2)$$

Since the security configuration management tool is capable of audit and remediating devices simultaneously total system down time is same as down time of a device (r) if all the devices are based on same OS.

$$\text{Total system down time} = r = t_1 + t_2$$

Due to extensive security rules in security profile and large number of devices (N), time spent on correcting human error, results analysis and results evaluation cannot be neglected. This has significant impact on total system down time when using manual security hardening methods. If total time spent on correcting human error, results analysis and results evaluation is μ , total system down time when manual security hardening methods are used is calculated as shown below

$$\text{Total system down time} = \left(\sum_{r=1}^N r \right) + \mu = Nr + \mu = N(t_1 + t_2) + \mu$$

Results analysis and evaluation is automated in the security configuration management tool because of this time spent on correcting human error, results analysis and results evaluation do not have any significant impact on total system down time when using the security configuration management tool.

Since the security configuration management tool is automated, its tasks must be properly tested prior to security hardening. Otherwise, the tool will generate false

results and cause misconfigurations on the systems. However, this test is only required once. Compared to time spent on correcting human error, results analysis and results evaluation during manual security hardening this test is much less time consuming.

The performed tests and analysis of tests results proves that the security configuration management tool much more effective than manual security hardening. Total system down time due to security hardening is also greatly reduced when using the security configuration management tool and number of devices does not affect total system down time. On the other hand, total system down time increase with number of devices when manual security hardening is used.

Manual security hardening does not generate detailed reports. The system administrators or security personal in charge of handling security in IoT devices must put extra effort to analyze and evaluate audit results to create reports. However, the security configuration management tool generates comprehensive human readable reports without using any extra labor from employees.

Centralized architecture of ansible controller allows the security configuration management tool to connect all the IoT devices in the network. This becomes a disadvantage, if ansible controller is compromised to attackers all the IoT devices in the network will be compromised because the tool has administrative access to IoT devices. Therefore, ansible controller becomes single point of failure and it must be secured. The security configuration management tool is also not effective in a system that has de centralized architecture because the tool cannot access all the IoT devices in the network at once. This will increase the total down time of the system because security hardening must be performed on devices separately.

With use of Ansible tasks combined with security rules, the security configuration management tool is scalable enough to accommodate further sections that involves services or application-level security to audit or remediate services or applications that runs on IoT devices.

Existing security rules can be used on more than one security profile. Most security rules are applicable for both Raspbian OS and ROS. The tool reuses security rules several security profiles. Some of These rules are also applicable to other OS types as

well. Therefore, these security rules can be reused when expanding the tool supportability to other OS types. Security profiles can be customized based on requirements allowing tool to be more flexible.

Since opensource technologies such as ansible and python are used to implement security configuration management tool, initial cost of implementing the tool is reduced.

The security configuration management tool is ideal for large, medium, and small manufacturers to secure their IoT systems. The tool automates security hardening and it does not require security professionals to use the tool. System administrators can effortlessly audit and remediate IoT systems using the tool. This allows manufacturers to reduce budget spent on security.

The tool can be further developed by increasing its supportability to other OS types and addition sections to ansible tasks to audit and remediate services and application such as web server applications and database server services.

According to Statista, there are around 21.5 billion interconnected devices in the world in 2021. IoT security standards should be selected carefully according to the requirements, as there are many IoT security standards addressing different areas. Various information security frameworks exist to cover IoT concepts and deployments in various verticals, classified according to the area of concern. The chosen standards and security frameworks should be aligned with organization's strategies, vision and mission or security requirements of the system. Therefore, the best solution is to customize a framework according to the requirements of the system to gain hardware root of trust and privacy by design.

The security configuration management tool narrows down the knowledge gap between system administrators and security experts. As shown in results centralized architecture of the tool reduces total down time of the system for remediation and reduces workload of the system administrators compared to decentralized management system. The tool reduces system down time due to human error while remediation. The ansible controller must be secured to avoid single point of failure. Because it has administrative access to all the IoT devices.

Rule management is a major part of Snort IDS, loading a high number of rules is not recommended since it could influence high resource usage and packet drops. Our test results show Raspberry Pi 4 can handle 6000 to 9000 lines of rules without any significant performance compromises, however, weak Wi-Fi range in Raspberry Pi 4b could cause bottlenecks in the network. This can be easily remedied by using an external Wi-Fi adaptor or range extender.

Hereafter, further development of this solution towards a standard security framework is planned, along with a cloud-based management server deployment.

4. CONCLUSION

Objective of the research is to design and implement an automated system for garment manufacturing system focusing on four major cyber security aspects including, frameworks and standardization, centralized security configurations with update management, authentication and Physical Access Control and Intrusion Detection System (IDS). A comprehensive, cost effective and efficient security solution is proposed with a centralized security approach to overcome the potential challenges of the smart system based on standardization. Standardization.

The research highlighted the fact that, IoT security standards should be chosen carefully according to the requirements, as there are many IoT security standards addressing different areas. The best solution is to customize a framework based on proper standardization according to the requirements of the system. The research showed that if proper standardization is used according to effective standards or frameworks the smart system will be more secure reducing the scope for attacks. Standardization is a proactive measure for reducing threats for an IoT smart system. The threats can be reduced through proper standardization while increasing efficiency and the quality of the smart system.

Security configuration management tool is created and installed it on a centralized server to accomplish the main objective. Security auditing and report generation based on audit result functionalities added in the tool to provide further understanding for the users or organization management. The report contains details about applied security measure on the devices and their purpose.

The security configuration management tool uses Ansible to deliver security configuration instructions to the IoT devices because of this the tool support IoT based OS such as Raspbian OS and ROS. Ansible allows the tool to simultaneously audit and remediate IoT systems. This increase the tools efficiency while reducing system down time due system hardening. With use of ansible task and security profiles the tool provides scalability for future development and reusability of existing security

rules. The security profiles are also customizable based on organizational requirements making the tool more flexible.

Test results validate our claims, that the Raspberry Pi 4 is capable of running Snort IDS and act as a Wi-Fi access point without any major compromises. Even though security should be prioritized, organizations neglect security due to budget constraints. The proposed IDS solution is an ideal cost-effective solution for small to medium Industry 4.0 environments.

Our recommendation is to utilize 8000 to 12 000 lines of rules for optimal performance and security since the management is an important task in Snort IDS. Adding more rules blindly does not translate to more security; adding correct rules is more important than adding lots of rules. Adding a higher number of rules is not recommended as it could lead to high CPU and RAM usage eventually causing packet drops.

To improve wireless connectivity speed, our recommendation is to invest in an external wireless adaptor that supports 150 Mbps, or else the option is available to connect to a switch and enable port mirroring. Having a proper cooling system is equally important; if the device gets hot, it results in thermal throttling.

The issue of door security is addressed by incorporating the notion of biometrics into the door lock system. As a result, this project is using fingerprints as a one-of-a-kind key to construct a device that locks or unlocks a door. 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.

5. DESCRIPTION OF PERSONAL AND FACILITIES

Table 5.1: Description of Personal and Facilities

Registration no	Name	Task Description
IT18136098	P.A.U.T. De Alwis	<ul style="list-style-type: none"> Security standards and policy development <p>Conduct a risk assessment</p> <p>Choose suitable framework and standards</p> <p>Policy creation</p> <p>Policy verification</p> <ul style="list-style-type: none"> Update management <p>Create a tool to provide security updates to IoT devices.</p>
IT18132410	A.D. H Jinadasa	<ul style="list-style-type: none"> Implementing IDS based on Raspberry pi 4 Customizing rules Implementing log management server Evaluating IDS performance
IT18139440	H.H.D Kalhara	<ul style="list-style-type: none"> A Python tool to automate security configurations. Add new audit and remediations to the python tool. Select and deselect remediations to create optimize compliance profile based on resource usage of the devices. A report generating function to generate audit reports. Testing
IT18133578	R.P.R.D. Randunu	<ul style="list-style-type: none"> Implement a Physical Security System using Arduino Store access logs and error logs. Data visualization from access logs. Alert user when an anomaly occurs. Report generation from access logs. Testing

6. REFERENCE LIST

- [1] K. Zhou, Taigang Liu, and Lifeng Zhou, “Industry 4.0: Towards future industrial opportunities and challenges,” in 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, Aug. 2015, pp. 2147–2152, doi: 10.1109/FSKD.2015.7382284.
- [2] H. Xu, W. Yu, D. Griffith, and N. Golmie, “A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective,” *IEEE Access*, vol. 6, pp. 78238–78259, 2018, doi: 10.1109/ACCESS.2018.2884906.
- [3] A. Bhattacharjee, S. Badsha, and S. Sengupta, “Blockchain-based Secure and Reliable Manufacturing System,” *IEEE Green Computing and Communications (GreenCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, Rhodes, Greece, Nov. 2020, pp. 228–233. doi: 10.1109/iThings-GreenCom-CPSCoM-SmartData-Cybermatics50389.2020.00052.
- [4] N. Zainuddin, M. Daud, S. Ahmad, M. Maslizan, and S. A. L. Abdullah, “A Study on Privacy Issues in Internet of Things (IoT),” in 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), Zhuhai, China, Jan. 2021, pp. 96–100. doi: 10.1109/CSP51677.2021.9357592.
- [5] 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.
- [6] M. Suh, “Automated Cutting and Sewing for Industry 4.0 at ITMA 2019,” p. 13, 2019.
- [7] 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.
- [8] 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.

- [9]] Mitsuo Harada, “Security management of factory automation,” in *SICE Annual Conference 2007*, Takamatsu, Japan, Sep. 2007, pp. 2914–2917, doi: 10.1109/SICE.2007.4421488.
- [10] M. Ehrlich, H. Trsek, L. Wisniewski, and J. Jasperneite, “Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing,” in *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, Portugal, Oct. 2019, pp. 2849–2854, doi: 10.1109/IECON.2019.8927559.
- [11] 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.
- [12] M. Irshad, “A Systematic Review of Information Security Frameworks in the Internet of Things (IoT),” in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Sydney, Australia, Dec. 2016, pp. 1270–1275. doi: 10.1109/HPCC-SmartCity-DSS.2016.0180.
- [13] M. A. A. Faruque, S. R. Chhetri, A. Canedo, and J. Wan, “Acoustic Side-Channel Attacks on Additive Manufacturing Systems,” in *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, Apr. 2016, pp. 1–10, doi: 10.1109/ICCPS.2016.7479068.
- [14] P. Masek, M. Stusek, J. Krejci, K. Zeman, J. Pokorny, and M. Kudlacek, “Unleashing Full Potential of Ansible Framework: University Labs Administration,” in *2018 22nd Conference of Open Innovations Association (FRUCT)*, Jyvaskyla, May 2018, pp. 144–150, doi: 10.23919/FRUCT.2018.8468270.
- [15] P. Webteam, “Welcome to Puppet 7.4.1.” https://puppet.com/docs/puppet/7.4/puppet_index.html (accessed Mar. 03, 2021).
- [16] “Chef Documentation.” <https://docs.chef.io/> (accessed Mar. 03, 2021).
- [17] “Ansible Documentation — Ansible Documentation.”
- [18] “SaltStack Documentation.” <https://docs.saltproject.io/en/latest/> (accessed Mar. 03, 2021).

- [19] 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.
- [20] Robert Mitchell and Ing-Ray Chen. 2014. A survey of intrusion detection techniques for cyber-physical systems. *ACM Comput. Surv.* 46, 4, Article 55 (April 2014), 29 pages (accessed Mar. 07, 2021).
- [21] Bace, R. and Mell, P. (2001), *Intrusion Detection Systems*, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD
- [22] Hwang,K., Cai,M., Chen,Y and Qin,M. , "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", *IEEE Transactions on Dependable Computing*, Volume: 4 Issue: 1, pp. 41- 55, 2007.
- [23] 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.
- [24] Michael P. Brennan "Using Snort For a Distributed Intrusion Detection System", version 1.3 in SANS Institute 2020, January 29, 2002
- [25]] F. Hugelshofer, P. Smith, D. Hutchison, and N. J. Race, "OpenLIDS:a lightweight intrusion detection system for wireless mesh networks,"in *Proceedings of the 15th annual international conference on Mobile computing and networking*. ACM, 2009, pp. 309–320.
- [26] A. K. Kyaw, Yuzhu Chen and J. Joseph, "Pi-IDS: evaluation of open-source intrusion detection systems on Raspberry Pi 2," 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), 2015, pp. 165-170.
- [27] A. Sforzin, F. G. Mármol, M. Conti and J. Bohli, "RPiDS: Raspberry Pi IDS — A Fruitful Intrusion Detection System for IoT," 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress.
- [28] 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.

- [29] 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.
- [30]“IT Automation with Ansible.” <https://www.ansible.com/overview/it-automation>.
- [31] M. Ehrlich, H. Trsek, L. Wisniewski, and J. Jasperneite, “Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing,” in *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, Portugal, Oct. 2019, pp. 2849–2854, doi: 10.1109/IECON.2019.8927559.
- [32] eSecurityPlanet. 2021. Best Intrusion Detection & Prevention Systems [2021]: Compare 5+ Solutions | eSP. [online] Available at: <<https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/>> .
- [33] 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.
- [34]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.
- [35] 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.
- [36]Kamble, S., Gunasekaran, A. and Gawankar, S., 2020. Sustainable Industry 4.0 Framework: A Systematic Literature Review Identifying The Current Trends And Future Perspectives.
- [37] 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.

[38] 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

[39] Unb.ca. 2021. IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. [online] Available at: <<https://www.unb.ca/cic/datasets/ids-2017.html>>.

7. APPENDICES

