Cyber security automation for an industrial 4.0 garment manufacturing system

2021-11

Our Team

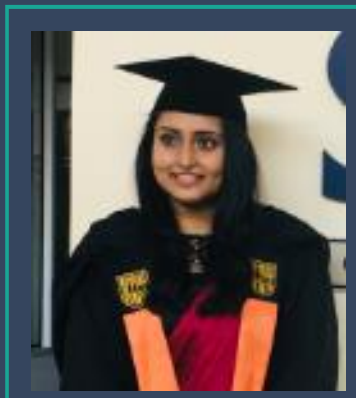
Dasunpriya Kalhara
IT18139440
Cyber Security

Anuka Jinadasa
IT18132410
Cyber Security

Udara De Alwis
IT18136098
Cyber Security

Dinuwan Randunu
IT18133578
Cyber Security

Supervisor
Prof. Pradeep Abeygunawardhana
Professor / Head | Department of Computer Systems Engineering



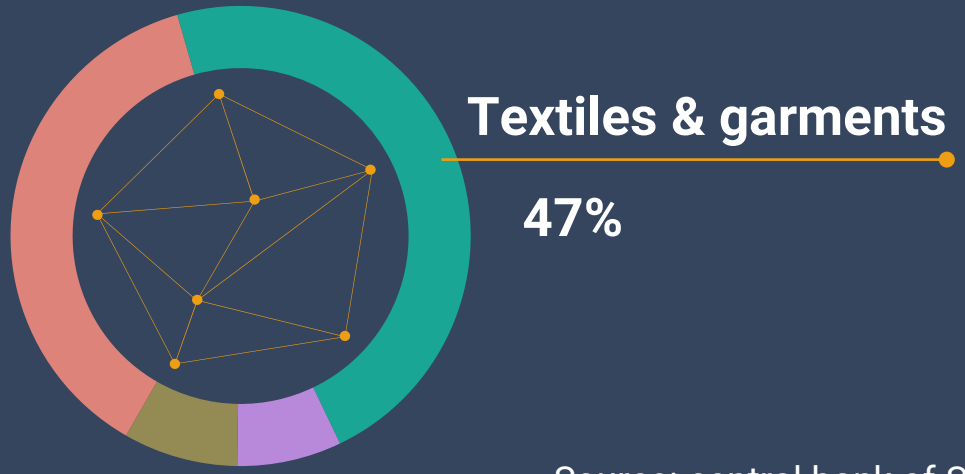
Co - Supervisor
Ms. Wellalage Sasini Nuwanthika

External – Supervisor
Mr. Gamini De Alwis

Introduction

Security is neglected when migrating into Industry 4.0 by most companies.

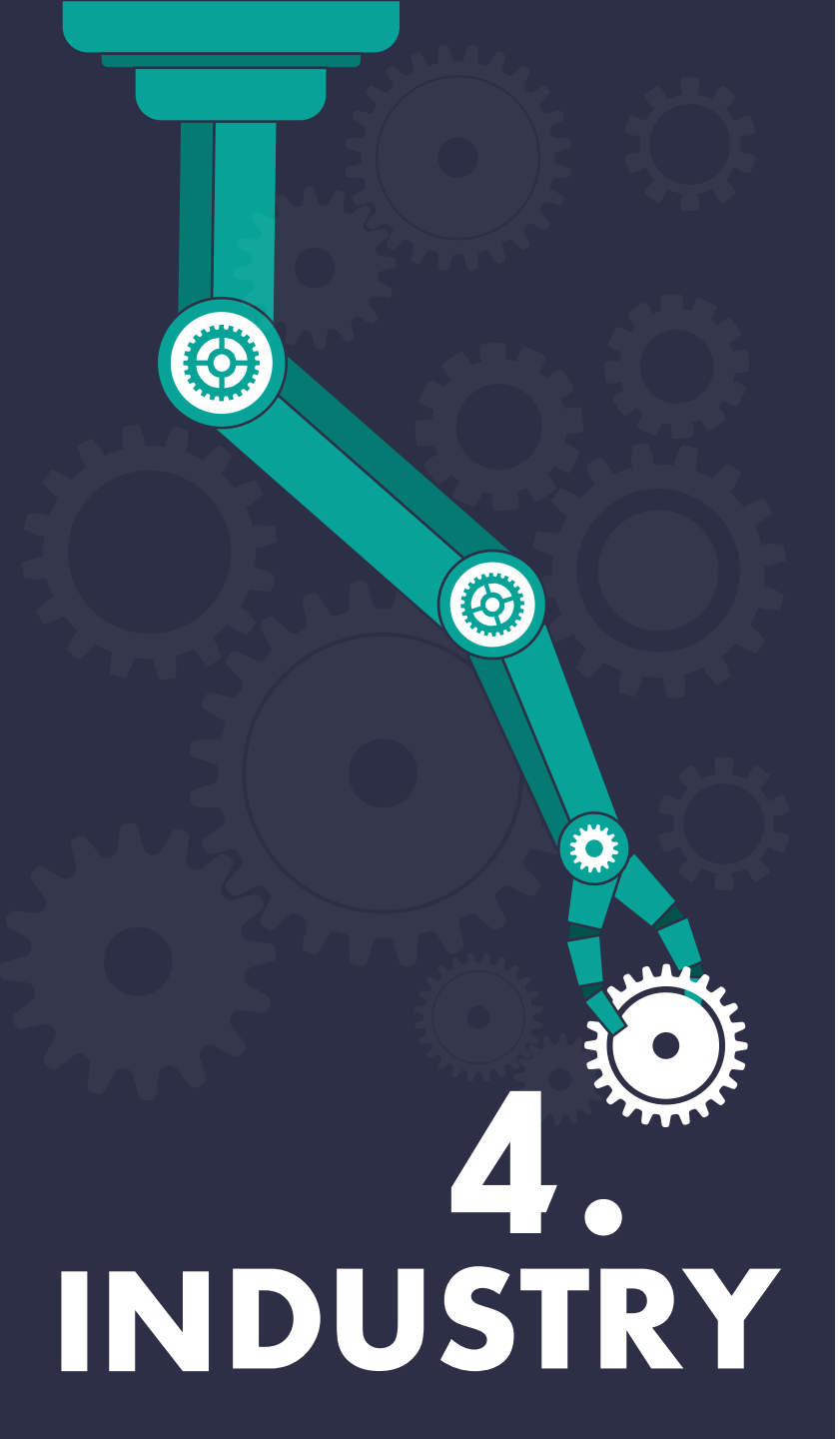
- **Why Garment Industry ?**



Textiles & garments

47%

Source: central bank of Sri Lanka



Research Question

How can we secure industrial 4.0 garment manufacturing system ?

Challenges:

- The development of the secure network environment.
- Collaboration between different systems.
- Centralized security management.
- Secure communication.
- Insecure data.
- Initial cost.
- Lack of strategy to industry 4.0.

Main and Sub Objectives

Security implementation for the potential challenges of the smart manufacturing system

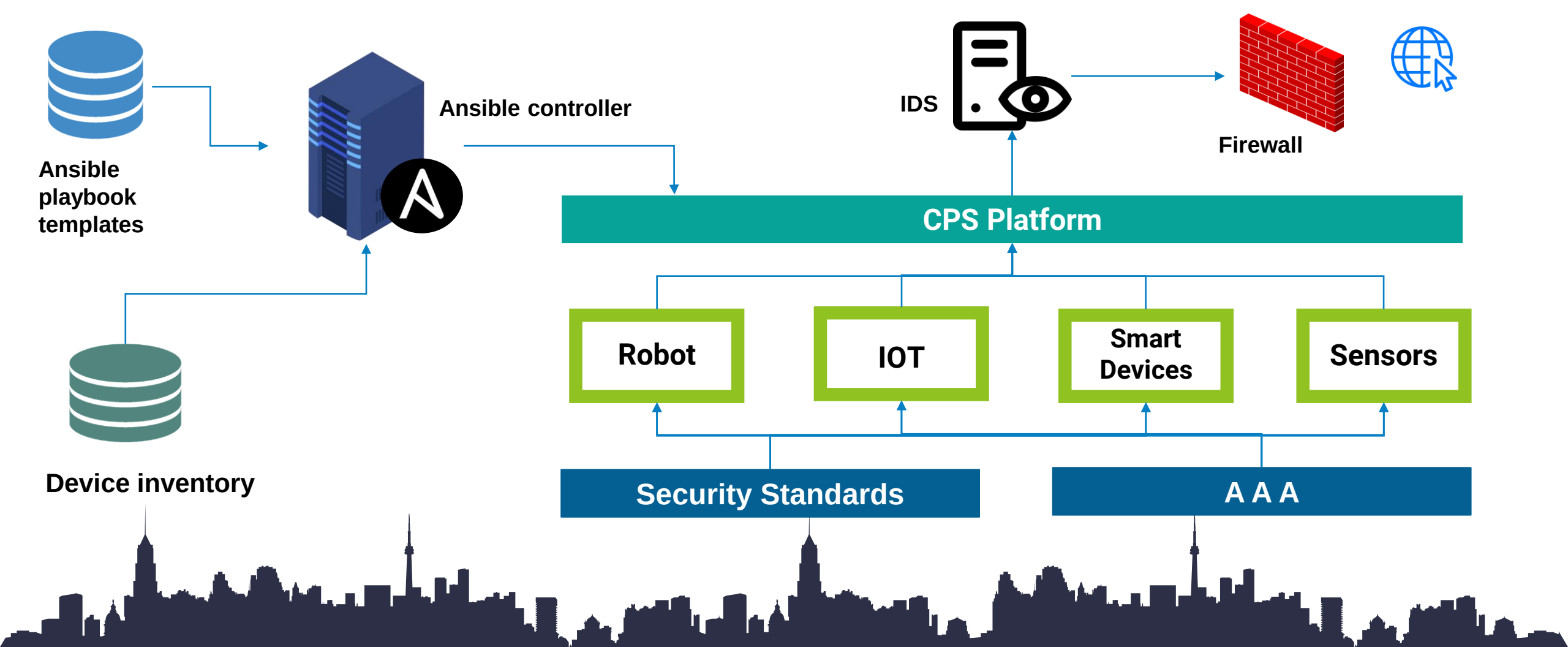
Authentication & Access Monitoring

Security Configurations

Policy Development & Update Management

Intrusion Detection

Overall System Diagram



Dasunpriya Kalhara

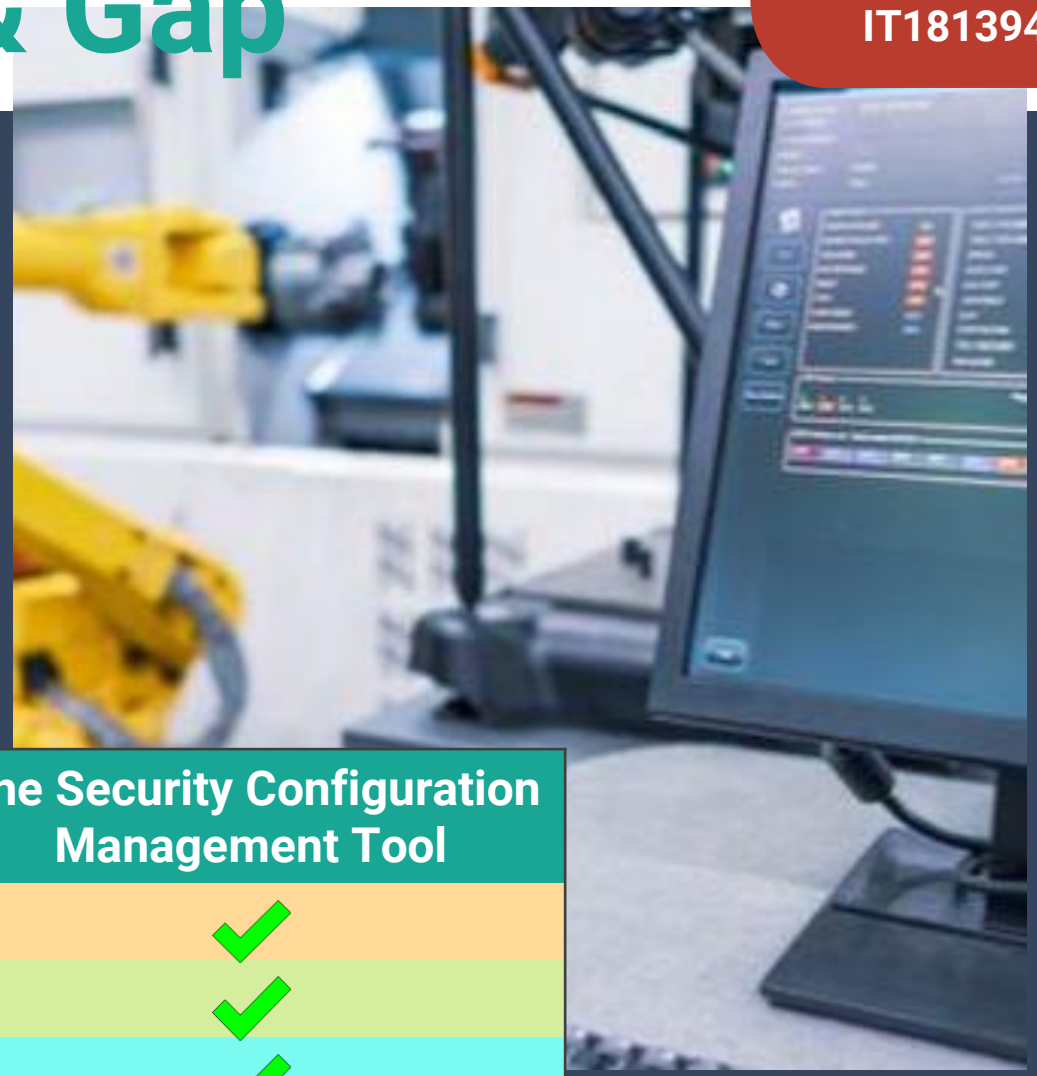
IT18139440

Cyber Security

Research Question & Gap

Dasunpriya Kalhara
IT18139440

How can we Automate Security configuration for Cyber Physical System devices?



Research Gap

	SCAP Workbench [3]	CIS-CAT Pro [4]	The Security Configuration Management Tool
Ubuntu Linux	✗	✓	✓
Robot OS	✗	✗	✓
Raspberry OS	✗	✗	✓

Specific & Sub Objectives

Dasunpriya Kalhara
IT18139440

Specific Objective :

A tool for Automating security configurations

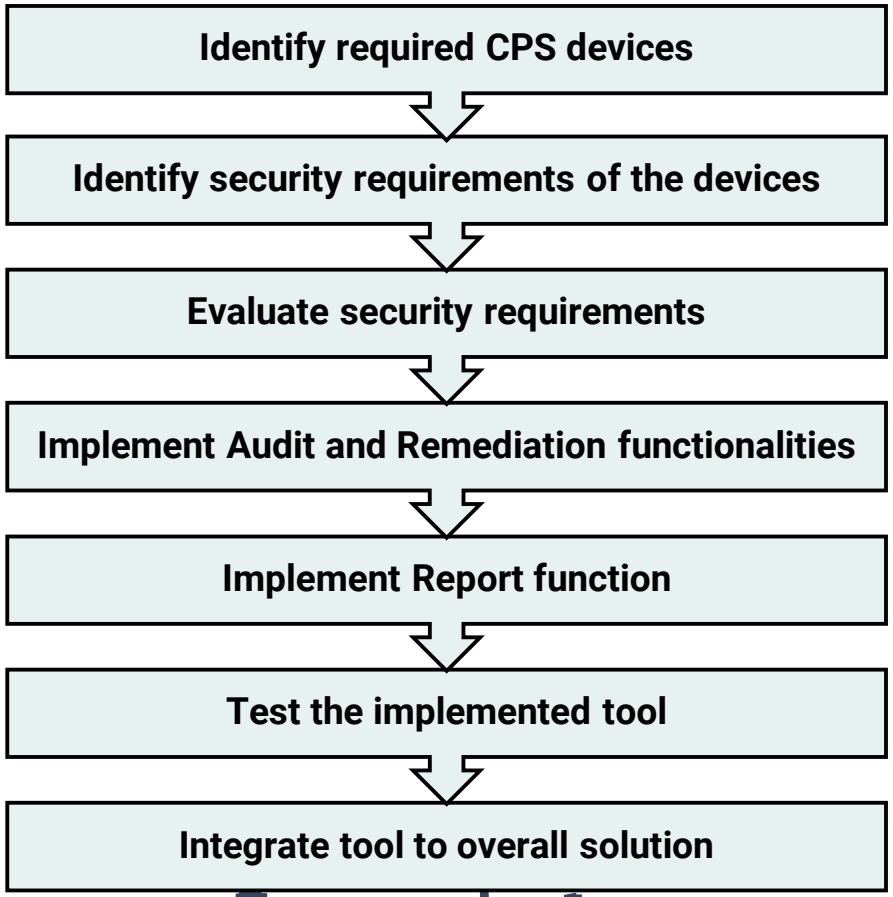
Sub Objectives :

- Audit security configurations
- Centralized device configuration management
- Generate Audit reports

Methodology

Dasunpriya Kalhara
IT18139440

- **IDE** – PyCharm
- **Program Languages** - Python, YAML, Ansible, java script
- **Virtualization technology** - type 2 hypervisor
- **Virtualization tool** – VirtualBox
- **Risk assessment** – OCTAVE
- **Python Libraries** – pyyaml, benedict, pandas, jinja2, os, sys, re, calendar, datetime

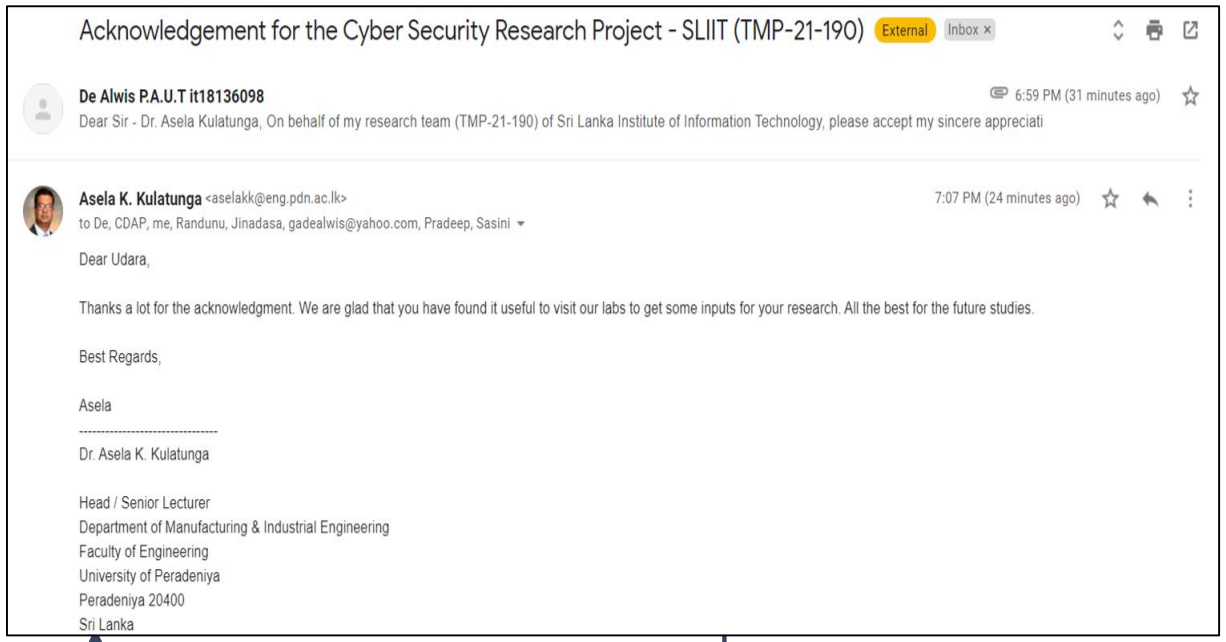


Completion of the project

Dasunpriya Kalhara
IT18139440

Identify required CPS devices for cutting process and categorize.

- Visiting the knit wear garment factory in Arangala to get an idea about the apparel industry
- Visit University of Peradeniya to get knowledge about CNC machines



Acknowledgement for the Cyber Security Research Project - SLIIT (TMP-21-190) External Inbox ×

De Alwis P.A.U.T it18136098 6:59 PM (31 minutes ago)

Dear Sir - Dr. Asela Kulatunga, On behalf of my research team (TMP-21-190) of Sri Lanka Institute of Information Technology, please accept my sincere appreciati

Asela K. Kulatunga <aselakk@eng.pdn.ac.lk> 7:07 PM (24 minutes ago)

to De, CDAP, me, Randunu, Jinadasa, gadealwis@yahoo.com, Pradeep, Sasini

Dear Udara,

Thanks a lot for the acknowledgment. We are glad that you have found it useful to visit our labs to get some inputs for your research. All the best for the future studies.

Best Regards,

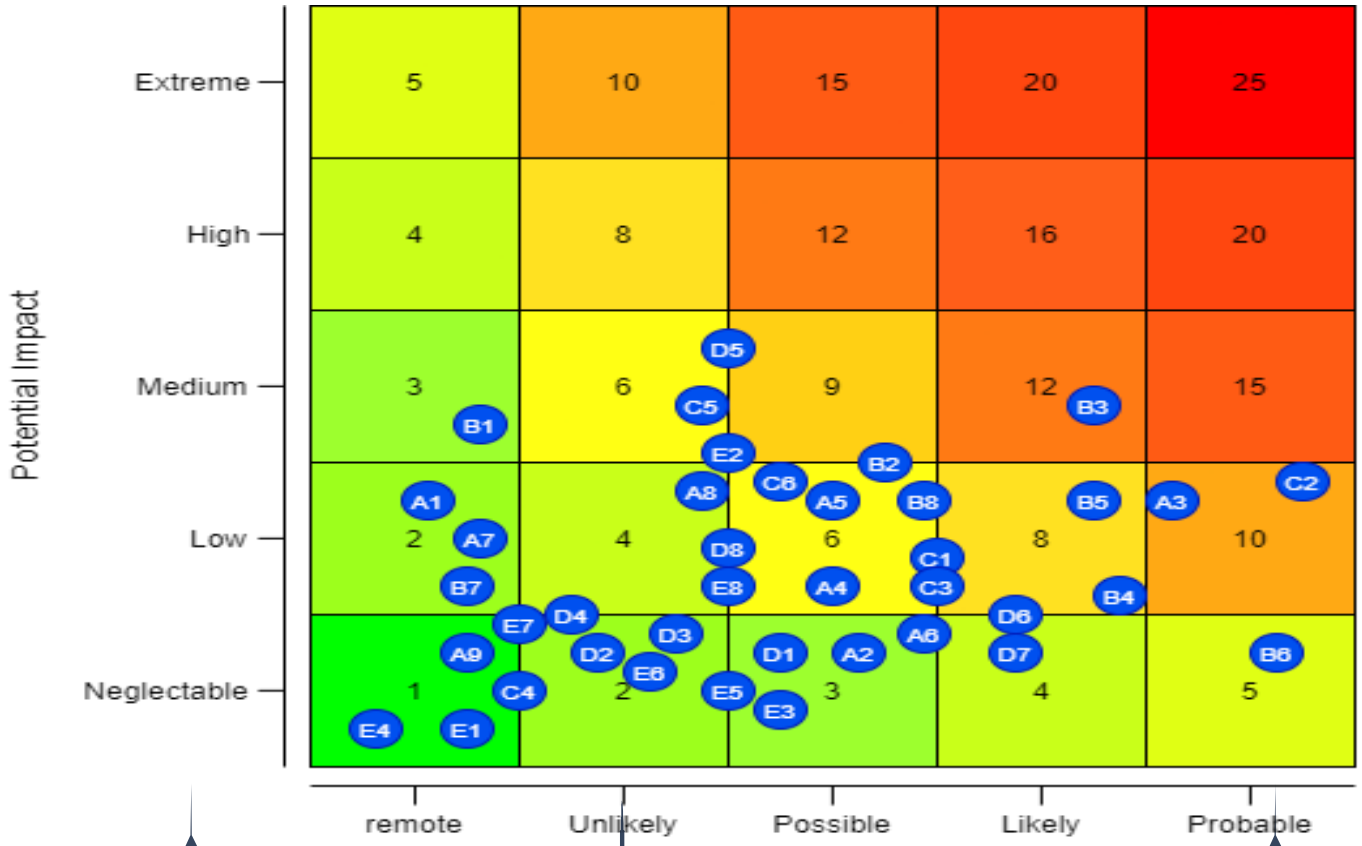
Asela

Dr. Asela K. Kulatunga

Head / Senior Lecturer
Department of Manufacturing & Industrial Engineering
Faculty of Engineering
University of Peradeniya
Peradeniya 20400
Sri Lanka

Completion of the project

Dasunpriya Kalhara
IT18139440



Identify security requirements and evaluate based on severity.

- Conduct octave risk analysis on IoT devices and ansible controller

Completion of the project

Dasunpriya Kalhara
IT18139440

- Implemented security rules based on risk assessment
- Security rules are divided into 6 sections,
  1. Initial Setup
  2. Service
  3. Network configuration
  4. Logging and Auditing
  5. Access, Authentication and Authorization
  6. System maintenance

```
class RuleProcessor:
    def __init__(self):
        self.rules = benedict({})
        self.rule_spec_file = os.path.join(config.get('default', 'rule_directory'), 'rules.yaml')
        with open(self.rule_spec_file, 'r') as file:
            rule_spec = yaml.load(file, Loader=yaml.FullLoader)
            self.rules.merge(rule_spec)

    def find_rule_by_id(self, rule_id):
        rule = self.rules.search(rule_id, in_keys=False, in_values=True, exact=True, case_sensitive=True)
        if rule:
            return rule[0][0]
        else:
            error = {
                'error_status': 'E002',
                'error_message': 'Invalid rule id'
            }
            return error
```

```
----------------------------------------
Rule ID : T_116
Name : Install Advanced Intrusion Detection Environment (AIDE)
Scored : 1
Severity : medium
Version : 1.0.0
Description : AIDE takes a snapshot of filesystem state including mod
ification times, permissions, and file hashes which can then be used
to compare against the current state of the filesystem to detect modi
fications to the system.

Rationale : By monitoring the filesystem state compromised files can
be detected to prevent or limit the exposure of accidental or malicio
us misconfigurations or modified binaries.

Applicable Device Types : ['IOT', 'ROS']
----------------------------------------
```

Completion of the project

Dasunpriya Kalhara
IT18139440

Implement security profiles for systems

- Security rules for Raspbian OS.
- Security rules for ROS.

```
class ProfileProcessor:
    def __init__(self):
        self.profile_spec_location = os.path.join(config.get('default', 'profile_directory'))
        self.profile_list = []
        self.no_of_profiles = 0
        profile_spec_files = get_spec_list(self.profile_spec_location)
        for profile_spec_file in profile_spec_files:
            with open(profile_spec_file, 'r') as file:
                profile_spec = yaml.load(file, Loader=yaml.FullLoader)
                profile_dict_obj = benedict(profile_spec)
                kl = profile_dict_obj.keypaths()
                profile_key = kl[0]
                profile = profile_dict_obj[profile_key]
                self.profile_list.append(profile)
        self.set_no_of_profiles()
```

```
(venv) root@auditor-VirtualBox:/opt/Configuration-management-tool#
python3 ./src/config_manager_cli.py profiles_list
0 : iot_raspbian_os
1 : robot_os
(venv) root@auditor-VirtualBox:/opt/Configuration-management-tool#
python3 ./src/config_manager_cli.py profile_details 0
Profile Details
---------------------------------------
ID : iot_raspbian_os
Name : IOT::Raspberry
Category : IOT
Applicable hosts : IOT
Target System : Debian
Target System Version : 10
Profile description : Secure Configuration of raspbian OS
Profile version : 1.0.0
---------------------------------------
(venv) root@auditor-VirtualBox:/opt/Configuration-management-tool#
```

Completion of the project

Dasunpriya Kalhara
IT18139440

Implement audit and remediate roles

- Include security rule audits and remediates as tasks

```yaml
---
- name: set log_martians to 1
  sysctl:
    name: "{{ item }}"
    value: '1'
    state: present
    sysctl_file: /etc/sysctl.d/network_security.conf
    sysctl_set: yes
    reload: yes
  loop:
    - net.ipv4.conf.all.log_martians
    - net.ipv4.conf.default.log_martians

- name: Flush route
  sysctl:
    name: net.ipv4.route.flush
    value: '1'
    state: present
    sysctl_set: yes
```

```
resources/audit/
├── defaults
│   └── main.yml
├── files
│   └── banners.sh
├── handlers
│   └── main.yml
├── meta
│   └── main.yml
├── README.md
├── tasks
│   ├── main.yml
│   ├── section_1
│   ├── section_1.yml
│   ├── section_2
│   ├── section_2.yml
│   ├── section_3
│   ├── section_3.yml
│   ├── section_4
│   ├── section_4.yml
│   ├── section_5
│   ├── section_5.yml
│   ├── section_6
│   └── section_6.yml
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml
```

Completion of the project

Dasunpriya Kalhara
IT18139440

Implement Audit functionality

Execute audit comannd → Process security profile → Create extra_vars .yml → Create audit_role_playbook using template → Run Audit role → Pass csv reports to report function → Detailed reports

```
def create_audit_role(self, profile_id, host_group, state):
    work_dir = os.path.join(self.work_location, self.session_id)
    if not os.path.exists(work_dir):
        os.makedirs(work_dir, 0o744)
    report_dir = os.path.join(self.report_location, self.session_id)
    if not os.path.exists(report_dir):
        os.makedirs(report_dir, 0o744)

    self.profile_obj.create_extra_vars_for_ansible_roles(profile_id, work_dir)
    self.prepare_playbook(work_dir, host_group, 'audit_playbook.yml')
    self.edit_extra_vars_file(work_dir, report_dir, state)
    self.run_playbook(work_dir, 'audit_playbook.yml')
    if state == 'audit':
        self.report_obj.process_csv_reports(self.session_id, state, host_group)
        self.make_reports_available(report_dir)
```

Completion of the project

Dasunpriya Kalhara
IT18139440

Implement Remediate functionality

Execute remediate comannd → Audit function → Create remediate_role_playbook using template → Edit extra_vars.yml → Run Remediate role → Merge csv reports → Pass csv reports to report function → Detailed reports

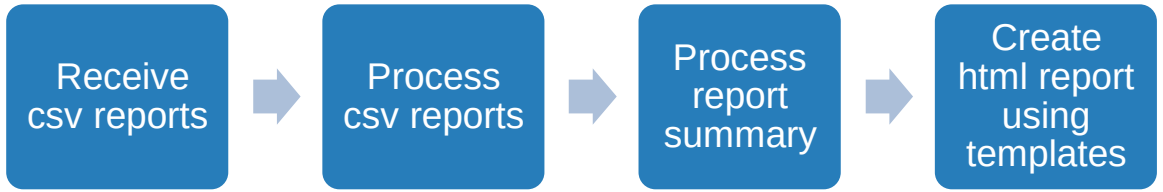
```
def create_remediate_role(self, profile_id, host_group):
    work_dir = os.path.join(self.work_location, self.session_id)
    report_dir = os.path.join(self.report_location, self.session_id)
    self.create_audit_role(profile_id, host_group, 'before')

    self.prepare_playbook(work_dir, host_group, 'remediate_playbook.yml')
    self.edit_state(work_dir, 'after')
    self.run_playbook(work_dir, 'remediate_playbook.yml')
    self.find_reports_to_merge()
    self.report_obj.process_csv_reports(self.session_id, 'remediate', host_group)
    self.make_reports_available(report_dir)
```

Completion of the project

Dasunpriya Kalhara
IT18139440

Implement Report functionality

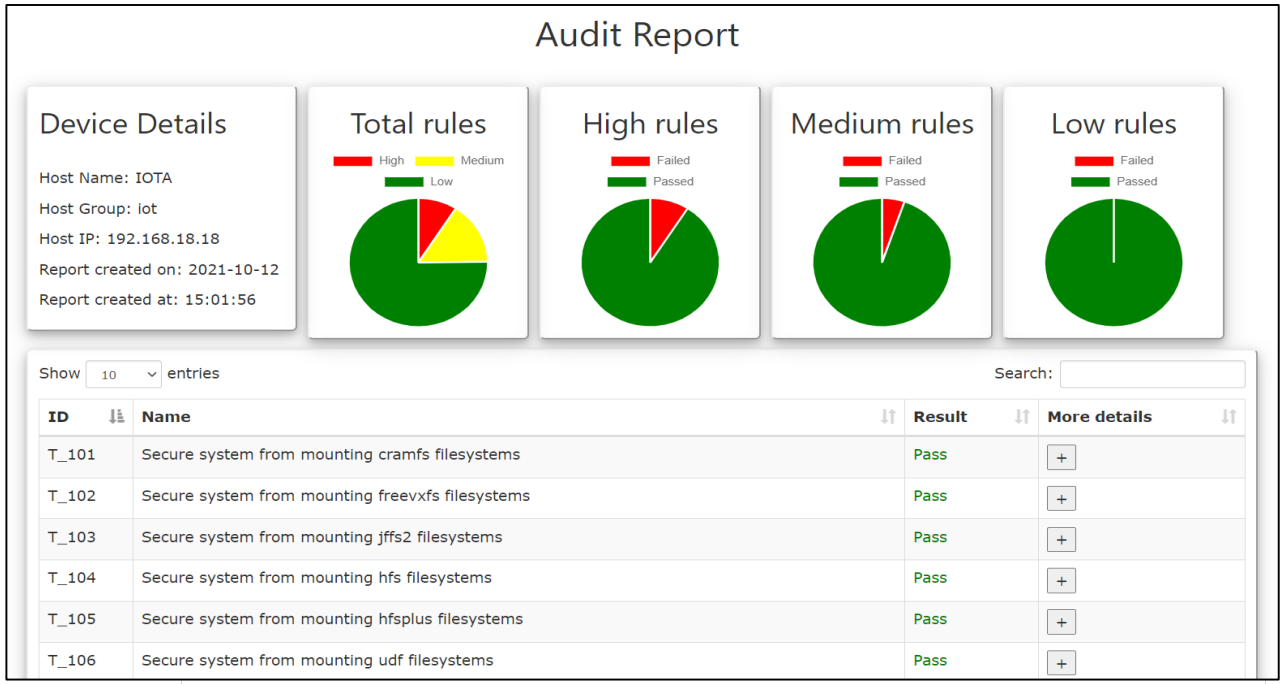


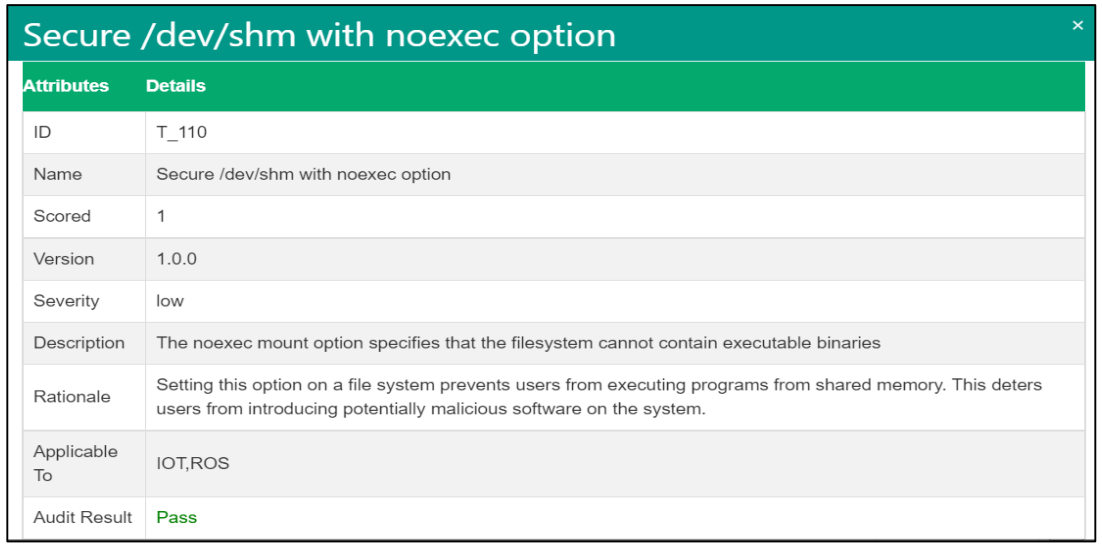

```python
def process_csv_reports(self, session_id, state, host_group):
    files = os.listdir(os.path.join(self.report_location, session_id))
    for filename in files:
        if filename.endswith(".csv"):
            csv_report = os.path.join(self.report_location, session_id, filename)
            df = pd.read_csv(csv_report)
            results_list = list()
            for i in range(df.shape[0]):
                rule_id = df.at[i, "Rule_id"]
                rule_details = self.rule_obj.find_rule_by_id(rule_id)
                if state == 'audit':
                    results = {'audit_result': df.iat[i, 1]}
                    rule_details.update(results)
                if state == 'remediate':
                    results = {'before_result': df.iat[i, 1], 'after_result': df.iat[i, 2]}
                    rule_details.update(results)
                results_list.append(rule_details)
            self.create_html_report(session_id, state, filename, host_group, results_list)
```

Completion of the project

Dasunpriya Kalhara
IT18139440

Implement Report functionality





Completion of the project

Dasunpriya Kalhara
IT18139440

Task	Status
Identify required CPS devices for cutting process and categorize.	Completed
Identify security requirements and evaluate based on severity.	Completed
Implement a tool to audit & remediate security configurations.	Completed
Implement report generating function based on audit results.	Completed
Implement and Test security configurations on the devices.	Completed
Integrate the tool to main system and test the tool.	In Progress

Results

Dasunpriya Kalhara
IT18139440

- Tests were conducted in a virtual environment
  - Audit and remediate performed on 3 Raspbian OS and 2 ROS systems
  - Used security profile for tests contains 120 security rules

- Audit took,
  - 12 minutes on Raspbian OS systems
  - 13 minutes on ROS systems
  - Total audit time = 25 minutes

- Remediate took,
  - 23 minutes on Raspbian OS systems
  - 25 minutes on ROS systems
  - Total Remediate time = 48 minutes

Achievements

Dasunpriya Kalhara
IT18139440

- An automated tool for security hardening on IoT based Operating Systems such as Raspbian OS and ROS
- Simultaneous security auditing and remediating
- Centralized security configuration management tool

Pros vs Cons

Dasunpriya Kalhara
IT18139440

Pros	Cons
Flexible	More memory intensive on the Server
Scalable	Single point of failure
Efficient	
Reduces labor cost	
Reduces human error	
Reduces system down time	
Does not require agent programs on client devices	
Less memory intensive on client devices	
Ease of use	

References

Dasunpriya Kalhara
IT18139440

- [1] “OWASP Internet of Things Project OWASP. ” https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 (accessed Mar. 06, 2021).
- [2] H. Wang, Z. Zhang, and T. Taleb, “Editorial: Special Issue on Security and Privacy of IoT,” World Wide Web, vol. 21, no. 1, pp. 1–6, Jan. 2018, doi: 10.1007/s11280-017-0490-9.
- [3] “SCAP Workbench | OpenSCAP portal.” https://www.open-scap.org/tools/scap-workbench/ (accessed Mar. 06, 2021).
- [4] “CIS Benchmarks™,” CIS. https://www.cisecurity.org/cis-benchmarks/ (accessed Mar. 06, 2021).

Udara De Alwis

IT18136098

Cyber Security

Research Question

Udara De Alwis
IT18136098

How to identify and create security policies according to standards suitable for IoT and CPS devices.

How to Integrate security strategies and policies suitable for IoT and CPS devices.[5]

How to implement proper security update mechanism.

Research gap

Udara De Alwis
IT18136098

- When implementing security for IoT and CPS there are layered and decentralized approaches.
- A centralized security approach based on proper standardization for IoT and CPS garment manufacturing system will close the gap of decreased efficiency occurred by layered and decentralized approaches.

Specific & Sub Objectives

Udara De Alwis
IT18136098

Specific Objective :

- Create security policies for IoT and CPS
- Update management

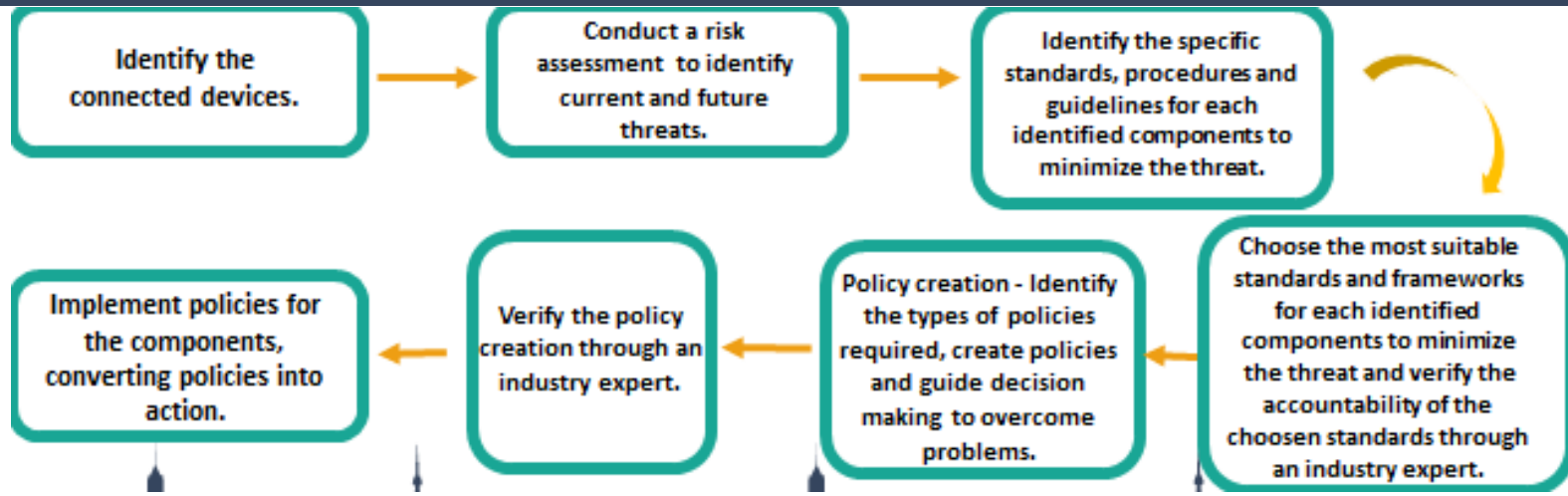
Sub Objectives :

- **Policy creation according to chosen standards:**
  - Mandatory and non-mandatory documentation required by the chosen standards.
  - Creation of password policy, access control policy, acceptable use policy, firewall policy Creation of Standard Operating Procedures(SOPs)
- **Update Management:**
  - Implementation and configuration of update management system.

Methodology

Udara De Alwis
IT18136098

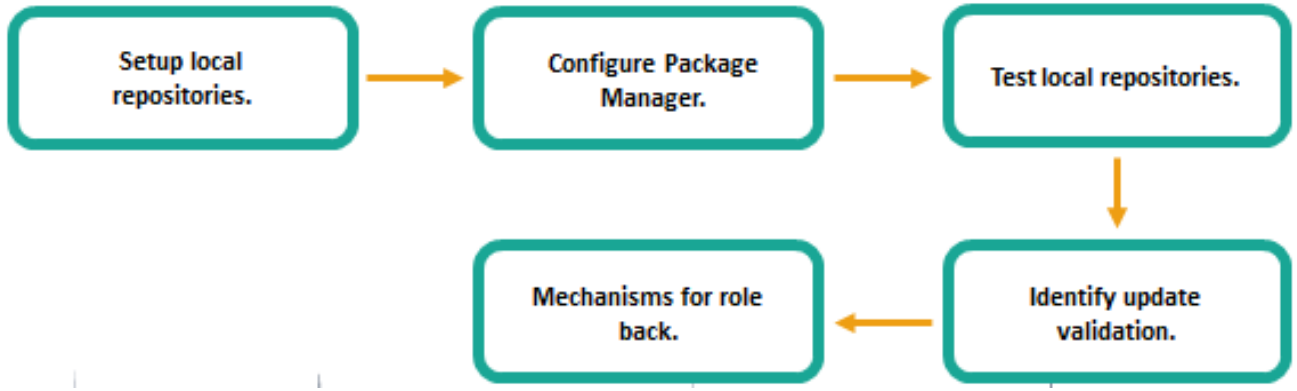
Security standards and policy development



- After identifying the devices through information gathering and observation according to the research requirement, a risk assessment was conducted using OCTAVE framework. ISO 27001 : 2013 and IEC 62443 standards were chosen according to the industry experts' consultation for the research. Compare the chosen standards and verify accountability for each standard.
- Creating access control, password, firewall policies and procedures.
- Verify policies and procedures through an industry expert.
- Integrate policies into actions and observe where we are still at risk.

Methodology

Udara De Alwis
IT18136098



Update management

- Set up local APT repository server on Ubuntu.
- Configure update manager to setup a central local repository in the server by Creating a local Apache Web Server, so that the clients can install, update and upgrade the packages from the central repository over a LAN.
- Create Catalog file for APT use in directory
- Copying all DEB files from installation media for a directory. Identify update validation.
- Scan all deb files and create the local repository in the server.
- Configure Server sources list.
- Test repositories.
- Configure clients by adding the server repository location.
- Identify update validation.
- Mechanisms for role back

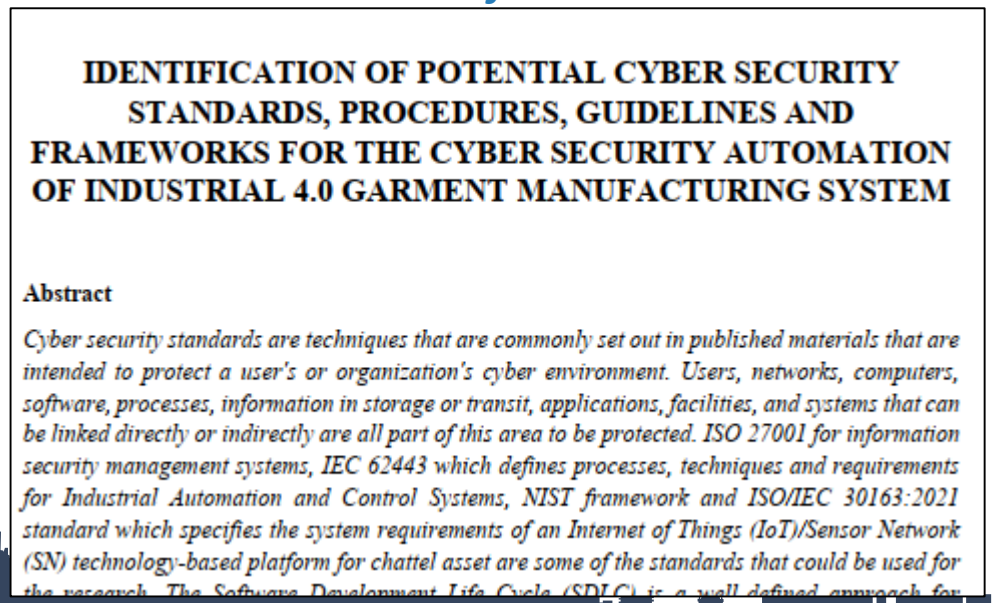
Completion of the project

Udara De Alwis
IT18136098

Identify the suitable standards to create policies.

- Potential cyber security standards, procedures, guidelines and frameworks for the cyber security automation of industrial 4.0 garment manufacturing system were identified and documented.
- ISO 27001:2013 and IEC 62443 standards were chosen according to the requirements.
- Documentation of comparison of chosen standards.

Potential standard identification documentation

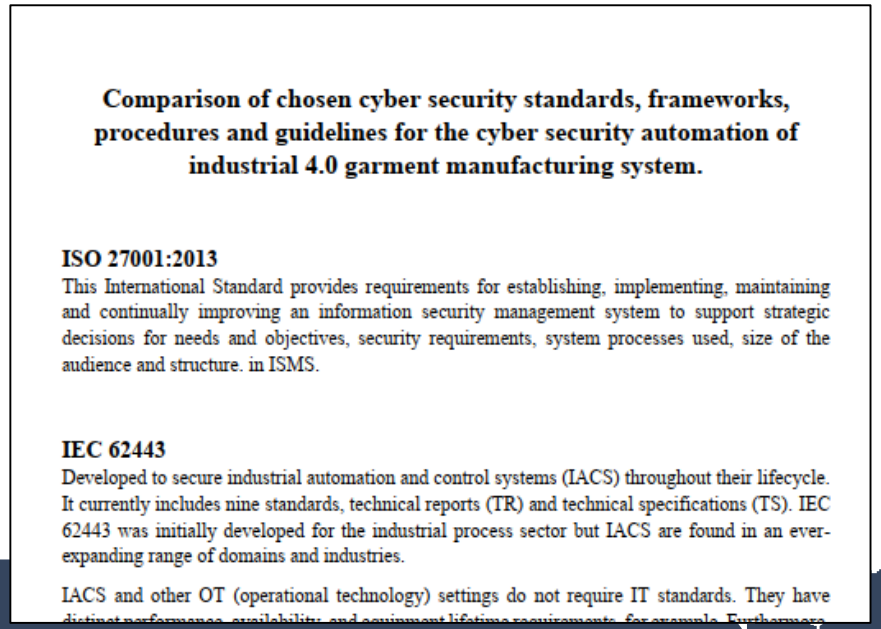


IDENTIFICATION OF POTENTIAL CYBER SECURITY STANDARDS, PROCEDURES, GUIDELINES AND FRAMEWORKS FOR THE CYBER SECURITY AUTOMATION OF INDUSTRIAL 4.0 GARMENT MANUFACTURING SYSTEM

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

Comparison of chosen standards



Comparison of chosen cyber security standards, frameworks, procedures and guidelines for the cyber security automation of industrial 4.0 garment manufacturing system.

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.

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 and other OT (operational technology) settings do not require IT standards. They have

Completion of the project

Udara De Alwis
IT18136098

ISO 27001 toolkit

- Mandatory documentation – business case, defining scope of ISMS, Statement of applicability.
- Policy creation

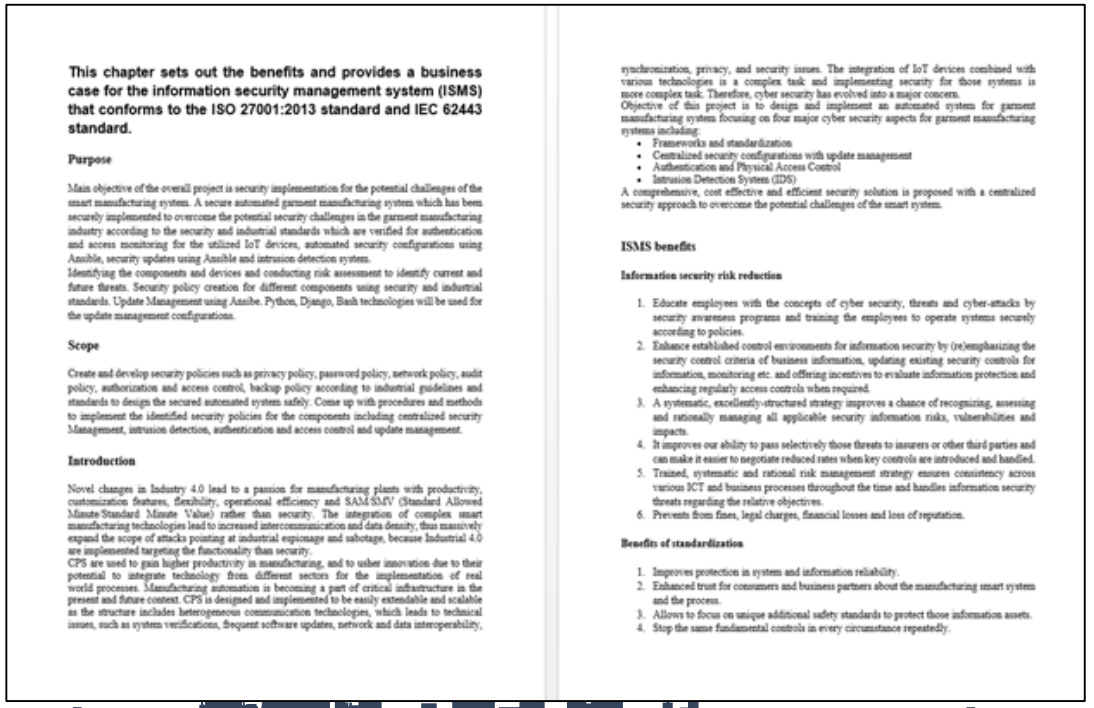
Statement of Applicability(SOA)

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

Click to add text

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							
	5.1	Management direction for information security							
5 Security Policies	5.1.1	Policies for information	TSE				x		As for the manufacturing automation ISMS to be controlled while preserving CIA to protect against cyber-attacks, it was clear that visible information policy for the automation system's entire life cycle has to be developed as best practice to demonstrate the outcome of the well secured system.
	5.1.2	Review of the policies for information security	Y				x		By reviewing current general policies, their weakness can be indentified and strenghtened. The Intrusion detection and prevention, authentication and access control, security configurations and audit components have implemented according to general policies. Reviewing them should be done to develop the policies to preserve CIA.

Business case Documentation



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 Ansibe. 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 safely. 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 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.

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 securely 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.

Completion of the project

Udara De Alwis
IT18136098

Policy documentation

Password Policy

Password Policy

1. Policy Statement

When restricting access, the systems should be safeguarded with passwords that are difficult to guess or derive. The importance of passwords in computer security cannot be underestimated. They serve as the first line of defense for systems. The entire system could be hacked if the password system is not strong. Therefore, secure password policy should be implemented in accordance with the guidelines indicated below. Password management systems must be interactive and ensure that passwords are of high quality.

2. Purpose

Ensure that security practices are introduced, implemented and maintained by all employees with respect to password-protected information infrastructure according to the standards ISO 27001:2013 and IEC 62443.

3. Scope

3.1 Applicability

The policy is applicable to the smart manufacturing system

3.2 Documentation

The documentation shall consist of Password Policy and related guidelines.

3.3 Document Control

The Password Policy document and all other referenced documents shall be controlled.

3.4 Records

Records being generated as part of the Password Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

Audit policy

Information Systems Audit Policy

1. Policy Statement

Audit controls and adequate security precautions are to prevent, control, and eliminate risks that can negatively impact the system and expose sensitive data. The policy confirms that the Information system is effectively implemented and maintained.

2. Purpose

The goal of this policy is to ensure that security configuration management system is configured in accordance with the security standards ISO 27001 and IEC 62443 as well as the best practices. The policy is also to confirm internal audits at planned intervals to provide information on whether the information security management system, conforms to requirements for its information security management system. Servers and other configuration devices must be audited four times a year and in accordance with appropriate regulatory compliance to ensure the integrity, confidentiality, and availability of information and resources. It also reduce risks of information systems, the data it manages, and the users it services.

3. Scope

3.1 Applicability

The policy is applicable to the smart manufacturing system and applies to all involved in the creation, deployment, operations, or support of the system.

3.2 Documentation

The documentation shall consist of information systems audit Policy and related guidelines.

3.3 Document Control

The information systems audit Policy document and all other referenced documents shall be controlled.

3.4 Records

Records being generated as part of the information systems audit Policy shall be retained for a period of

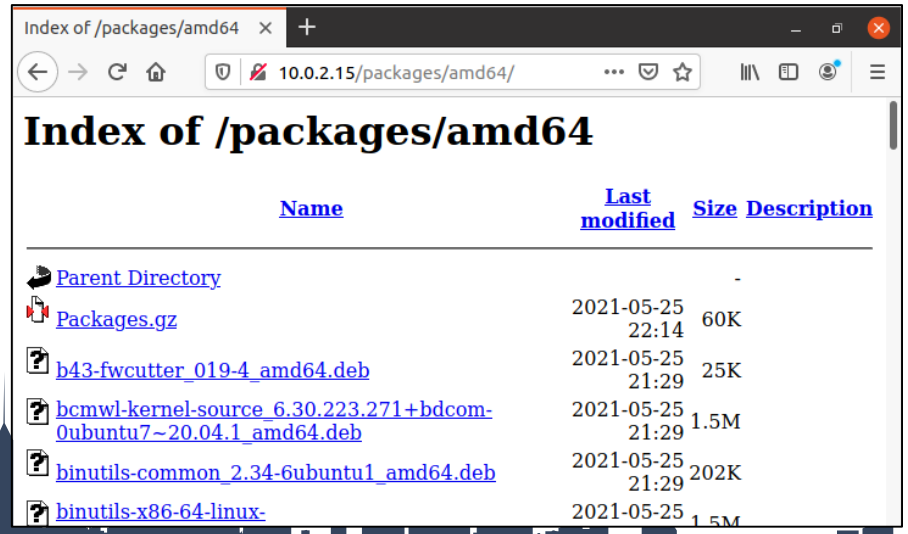
Completion of the project

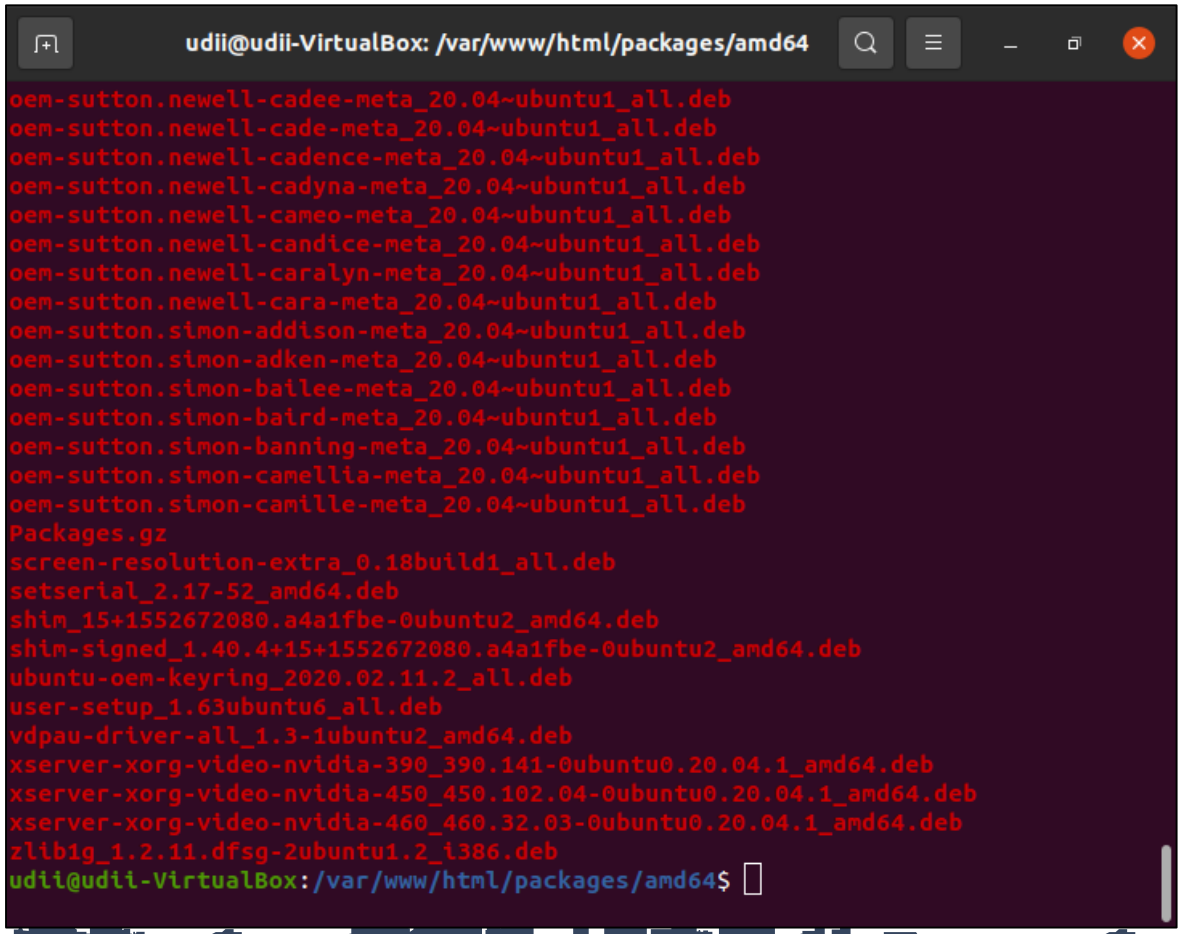
Udara De Alwis
IT18136098

Update Management

- Set up local repositories.
- Configure package Manager
- Test local repositories
- Identify update validation

- In progress- Mechanisms for role back





Completion of the project

Udara De Alwis
IT18136098

TASK	STATUS
Identify the connected devices	Complete
Conduct a risk assessment to identify current and future threats	Complete
Identify the specific standards, procedures and guidelines for each identified components and their sub modules to minimize the threat.	Complete
Choose the most suitable standards, frameworks and best practices for each identified components and their sub modules	Complete
Policy creation and policy documentation	Complete
Verify the policy creation through an industry expert	Complete
Implement policies for the components, converting policies into action.	Complete
Setup local repositories	Complete
Configure package manager	Complete
Test local repositories	Complete
Identify update validation	Complete
Mechanisms for role back	In Progress

Results

Udara De Alwis
IT18136098

- The asset registry and the business case documentation was created and they were useful for the risk assessment to identify requirements and assets.
- The ISO 27001:2013 and IEC 62443 standards were chosen but when followed twos standards, NIST cyber security framework special publications were needed to create policies.
- The policy creation was verified by an industry expert.
- Update Management system was implemented in Ubuntu and for testing purposes Raspberry OS was used as client.

Discussion

Udara De Alwis
IT18136098

- 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.

Achievements

Udara De Alwis
IT18136098

- Implementing policies based on standardization for the industry 4.0 smart manufacturing system.
- An update management system was created giving a solution for consuming internet bandwidth when updating client devices often with security updates.

REFERENCES

Udara De Alwis
IT18136098

[1]“Top 10 IoT Security Issues: Ransom, Botnet Attacks, Spying,” *Intellectsoft Blog*, Jul. 30, 2020. https://www.intellectsoft.net/blog/biggest-iot-security-issues/ (accessed Mar. 07, 2021).

[2]“What Are the IoT Security Standards?,” *SDxCentral*. https://www.sdxcentral.com/5g/iot/definitions/what-are-iot-security-standards/ (accessed Mar. 07, 2021).“Comparison of IoT Security Frameworks,” *Comparison of IoT Security Frameworks*. https://www.eurofins-cybersecurity.com/news/comparison-iot-security-frameworks/ (accessed Mar. 07, 2021).

[3]“Comparison of IoT Security Frameworks,” *Comparison of IoT Security Frameworks*. https://www.eurofins-cybersecurity.com/news/comparison-iot-security-frameworks/ (accessed Mar. 07, 2021).

[4]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

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

Anuka Jinadasa

IT18132410

Cyber Security

Research Question

Anuka Jinadasa
IT18132410

How can we implement cost effective, lightweight yet fully capable firewall & IDS/IPS ?

Specific & Sub Objectives

Anuka Jinadasa
IT18132410

Specific Objective :

implement a firewall and IDS/IPS system

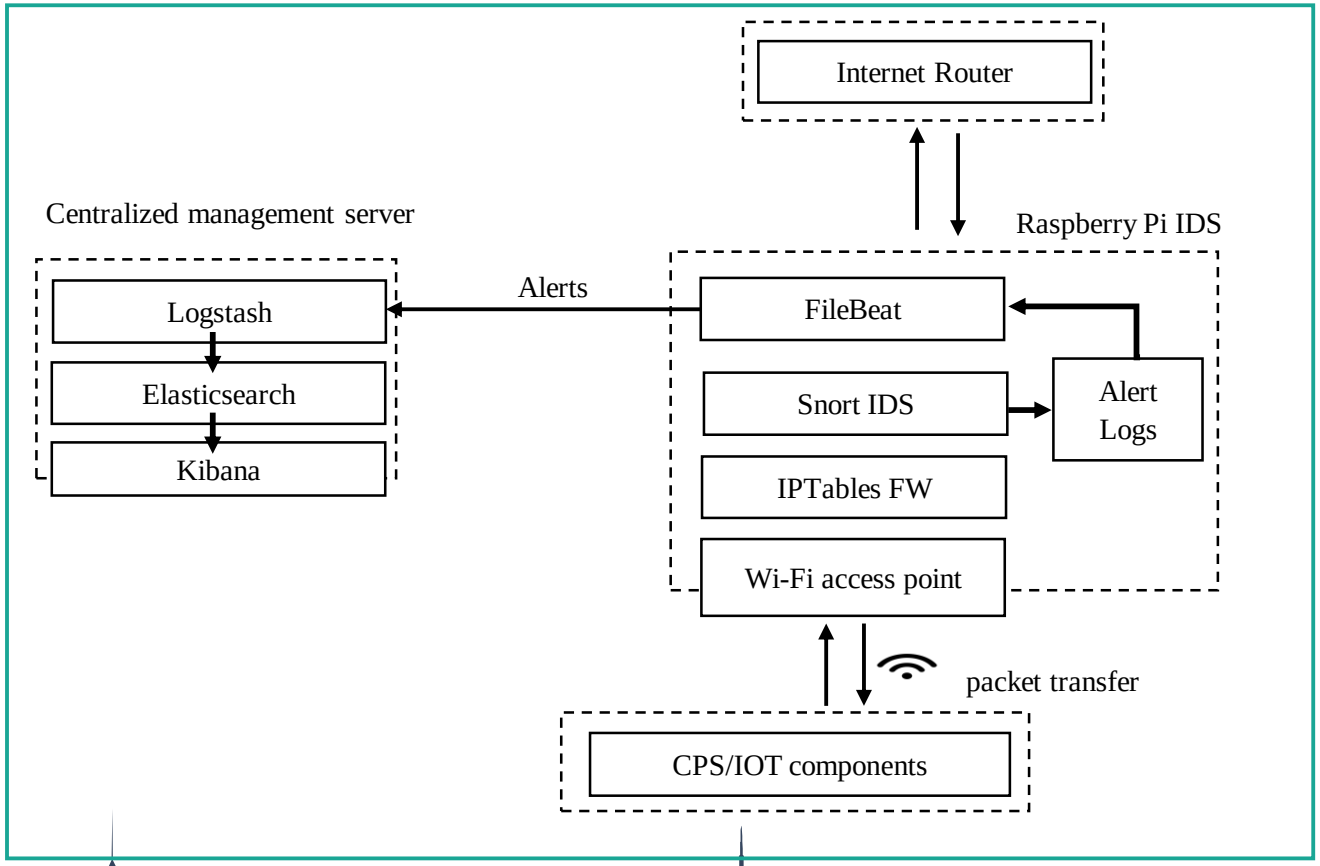
Sub Objectives :

- Provide easy access dashboard to the user.
- Visualize network behavior to user.
- Enable, add/ remove firewall rules according to the policies.
- Alert user when an anomaly occurs. [1]

Methodology

Anuka Jinadasa
IT18132410

- **Hardware –** Raspberry pi 4b
- **IDE** – Atom
- **Program Languages** - java script, bash scripts
- **Database** - MySQL
- **Risk assessment** – Octave
- **Elastic stack**

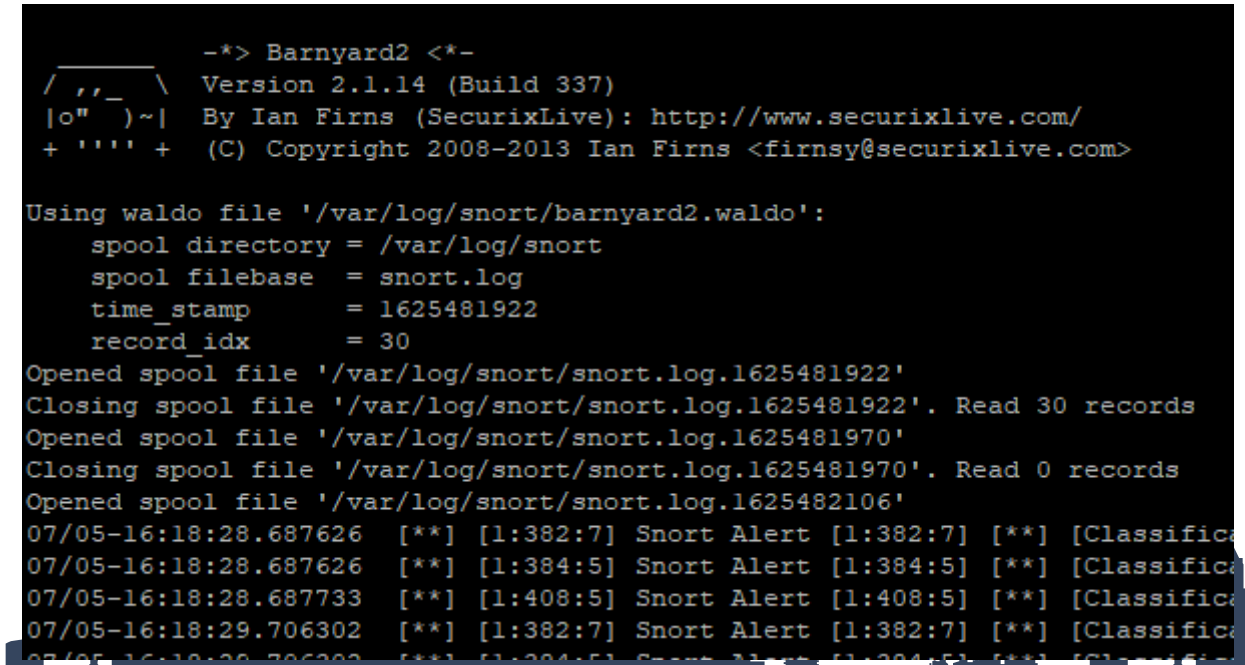


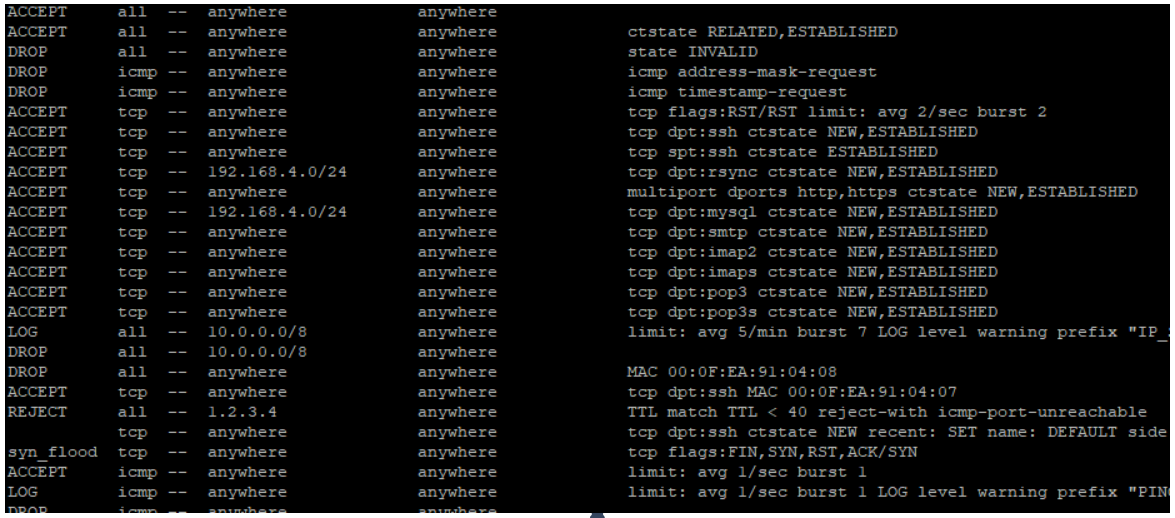
Completion of the project

Anuka Jinadasa
IT18132410

Implement IDS & IPS & configure firewall rules

- Barnyard2 & Pulledpork modules were used to decode alert logs & update rullset.
- Minimize false positive & false negative.
- Configured according to the security policies.





Completion of the project

Anuka Jinadasa
IT18132410

Signature database & saved IDS alerts

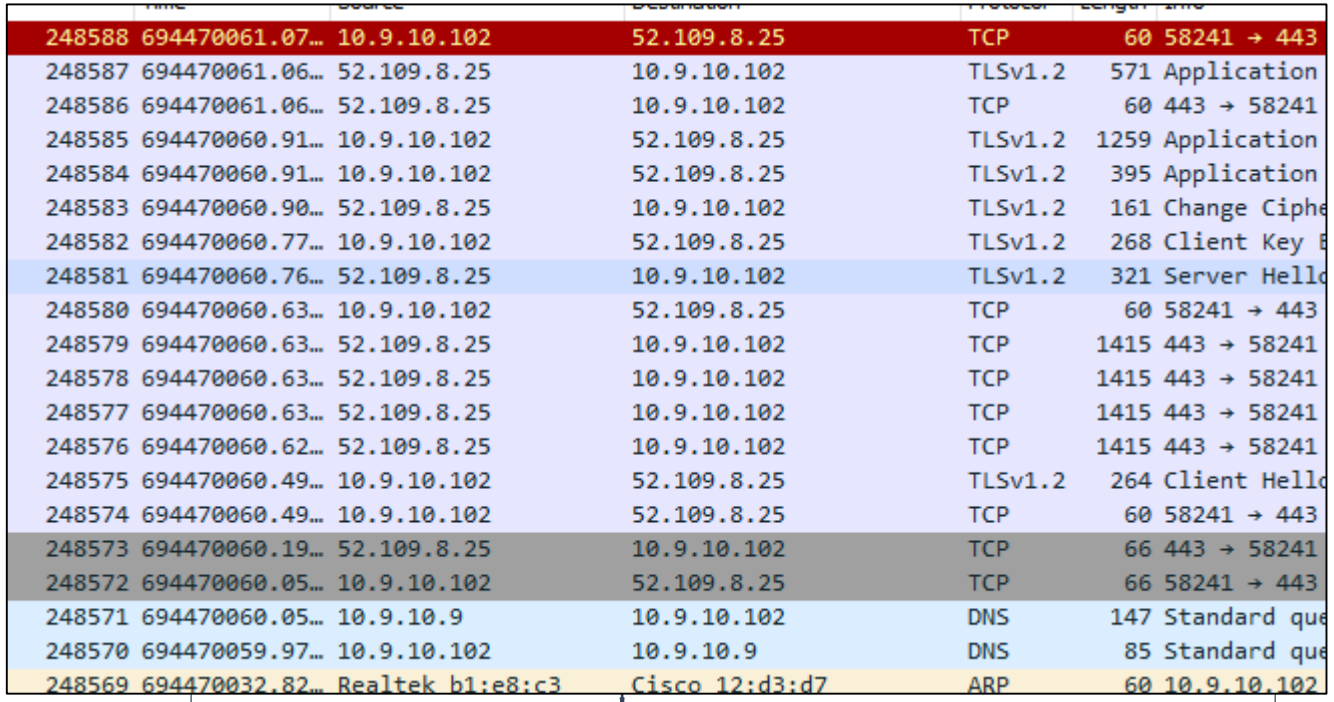
```
+-----------+---------+---------+---------+
| sig_id | sig_name
ig_priority | sig_rev | sig_sid | sig_gid |
+--------+-------------------------------------------------------------------------------------------------------
+-----------+---------+---------+---------+
|      1 | dnp3: DNP3 Application-Layer Fragment uses a reserved function code.
         0 |       0 |       6 |     145 |
|      2 | dnp3: DNP3 Link-Layer Frame uses a reserved address.
         0 |       0 |       5 |     145 |
|      3 | dnp3: DNP3 Reassembly Buffer was cleared without reassembling a complete message.
         0 |       0 |       4 |     145 |
|      4 | dnp3: DNP3 Transport-Layer Segment was dropped during reassembly.
         0 |       0 |       3 |     145 |
|      5 | dnp3: DNP3 Link-Layer Frame was dropped.
         0 |       0 |       2 |     145 |
|      6 | dnp3: DNP3 Link-Layer Frame contains bad CRC.
         0 |       0 |       1 |     145 |
|      7 | modbus: Reserved Modbus function code in use.
         0 |       0 |       3 |     144 |
|      8 | modbus: Modbus protocol ID is non-zero.
         0 |       0 |       2 |     144 |
|      9 | modbus: Length in Modbus MBAP header does not match the length needed for the given Modbus function.
         0 |       0 |       1 |     144 |
```

```
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 |
|   1 |  12 |       509 | 2021-06-11 06:57:58 |
|   1 |  13 |       510 | 2021-06-11 07:28:09 |
|   1 |  14 |       511 | 2021-06-11 07:28:13 |
```

Completion of the project

Anuka Jinadasa
IT18132410

Testing phase 1 of IDS



No.	Time	Source	Destination	Protocol	Length	Info
248588	694470061.07…	10.9.10.102	52.109.8.25	TCP	60	58241 → 443
248587	694470061.06…	52.109.8.25	10.9.10.102	TLSv1.2	571	Application
248586	694470061.06…	52.109.8.25	10.9.10.102	TCP	60	443 → 58241
248585	694470060.91…	10.9.10.102	52.109.8.25	TLSv1.2	1259	Application
248584	694470060.91…	10.9.10.102	52.109.8.25	TLSv1.2	395	Application
248583	694470060.90…	52.109.8.25	10.9.10.102	TLSv1.2	161	Change Ciphe
248582	694470060.77…	10.9.10.102	52.109.8.25	TLSv1.2	268	Client Key E
248581	694470060.76…	52.109.8.25	10.9.10.102	TLSv1.2	321	Server Hello
248580	694470060.63…	10.9.10.102	52.109.8.25	TCP	60	58241 → 443
248579	694470060.63…	52.109.8.25	10.9.10.102	TCP	1415	443 → 58241
248578	694470060.63…	52.109.8.25	10.9.10.102	TCP	1415	443 → 58241
248577	694470060.63…	52.109.8.25	10.9.10.102	TCP	1415	443 → 58241
248576	694470060.62…	52.109.8.25	10.9.10.102	TCP	1415	443 → 58241
248575	694470060.49…	10.9.10.102	52.109.8.25	TLSv1.2	264	Client Hello
248574	694470060.49…	10.9.10.102	52.109.8.25	TCP	60	58241 → 443
248573	694470060.19…	52.109.8.25	10.9.10.102	TCP	66	443 → 58241
248572	694470060.05…	10.9.10.102	52.109.8.25	TCP	66	58241 → 443
248571	694470060.05…	10.9.10.9	10.9.10.102	DNS	147	Standard que
248570	694470059.97…	10.9.10.102	10.9.10.9	DNS	85	Standard que
248569	694470032.82…	Realtek_b1:e8:c3	Cisco_12:d3:d7	ARP	60	10.9.10.102

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

Completion of the project

Anuka Jinadasa
IT18132410

Testing phase 2 of IDS

- Port scan
- DoS attack
  - LOIC simulation
  - Slowloris Dos attack
- Man in the middle attack
- Brute force attack

Completion of the project

Anuka Jinadasa
IT18132410

Testing phase 2 of IDS

	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			

Completion of the project

Custom rules

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SLR - DoS attempt"; flow: established,to_server ; uricontent:"id="; uricontent:"msg="; threshold: type thres

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SLR - DoS attempt (HTTP Mode)"; flow: established,to_server; content:"|47 45 54 20 20 48 54 54  50 2f 31 2e

alert udp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SLR -  possible dos attempt  - Behavior Rule (tracking/threshold)"; threshold: type threshold, track by_src,


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 tcp $HOME_NET any -> any 22 (msg:"SSH Brute-Force attack"; threshold:type both, track by_src, count 2000, seconds 60; classtype:trojan-activity;sid:1000281; rev:

alert tcp any any -> $HOME_NET 22 (msg:"Potential SSH Brute Force Attack";  flow:to_server; flags:S;threshold:type threshold, track by_src, count 3, seconds 60; classt


alert tcp any any -> any any (msg:"Possible Slow Loris attack"; classtype: denial-of-service; flow: to_server, established; pcre: !"/\x0D\x0A\x0D\x0A$/H"; threshold: t


alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP missing community string attempt"; content:"|04 00|"; depth:15; offset:5; reference:bugtraq,2112; reference:cve
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP null community string attempt"; content:"|04 01 00|"; depth:15; offset:5; reference:bugtraq,2112; reference:bug
alert udp $EXTERNAL_NET any -> $HOME_NET 161:162 (msg:"SNMP community string buffer overflow attempt"; content:"|02 01 00 04 82 01 00|"; offset:4; reference:bugtraq,40
alert udp $EXTERNAL_NET any -> $HOME_NET 161:162 (msg:"SNMP community string buffer overflow attempt with evasion"; content:" |04 82 01 00|"; depth:5; offset:7; refere
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP public access udp"; content:"public"; reference:bugtraq,2112; reference:bugtraq,4088; reference:bugtraq,4089; r
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP public access tcp"; flow:to_server,established; content:"public"; reference:bugtraq,2112; reference:bugtraq,408
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP private access udp"; content:"private"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132;
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP private access tcp"; flow:to_server,established; content:"private"; reference:bugtraq,4088; reference:bugtraq,4
alert udp any any -> 255.255.255.255 161 (msg:"SNMP Broadcast request"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve,2002-0012
```

Completion of the project

Dashboard log management – stored logs

_source

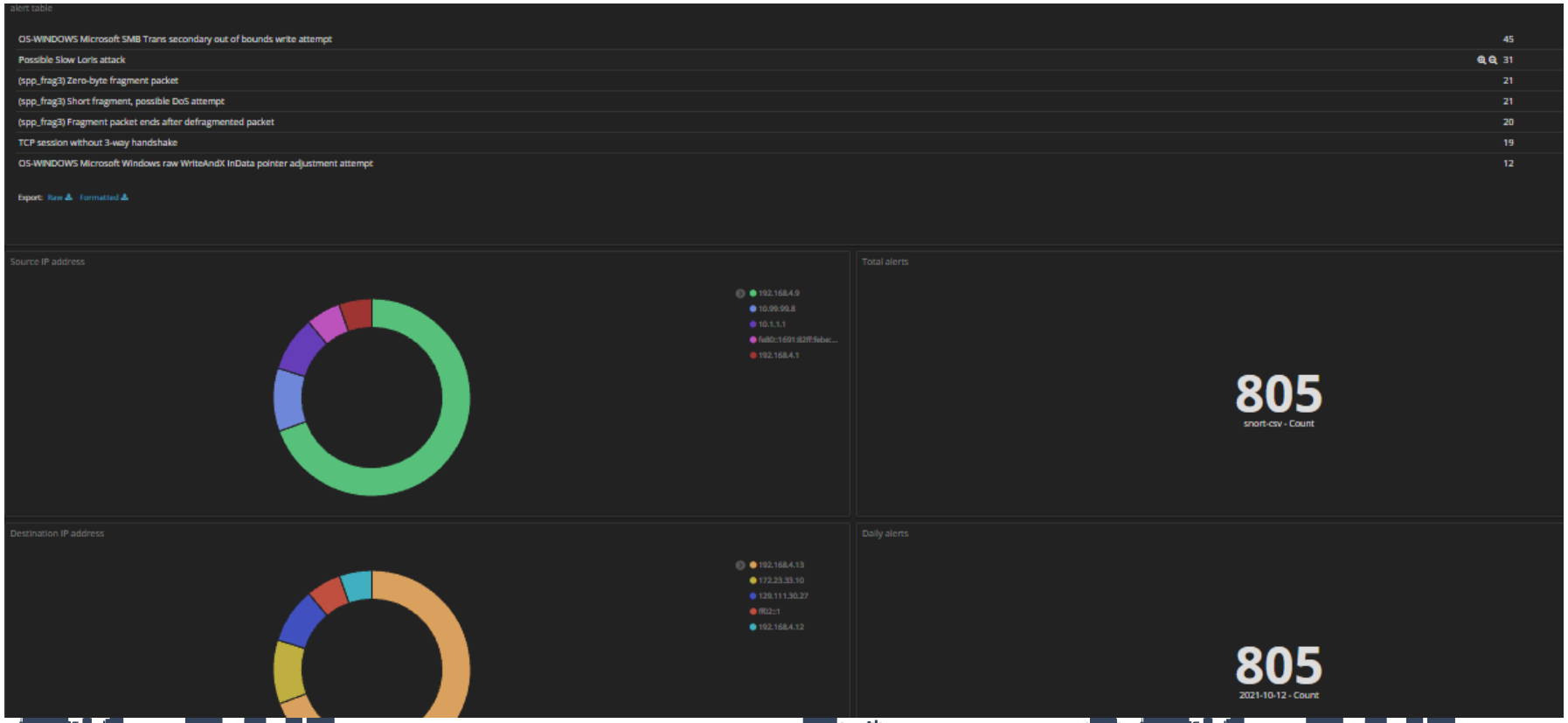
tags: snort, beats_input_codec_plain_applied agent.type: filebeat agent.id: a8f6871a-eaf9-4db4-8028-fd37a3190169
agent.version: 7.11.0 agent.ephemeral_id: 156300ed-da24-4eac-be3a-cf110574221d agent.hostname: raspberrypi agent.name: raspberrypi
msg: (spp_frag3) Fragment packet ends after defragmented packet dst: 129.111.30.27 @timestamp: October 12th 2021, 19:11:07.288
timestamp: 10/12-19:11:00.603971 message: "(spp_frag3) Fragment packet ends after defragmented packet",10/12-19:11:00.603971
,UDP,10.1.1.1,129.111.30.27 type: Snort host.name: raspberrypi input.type: log proto: UDP @version: 1 ecs.version: 1.6.0

log.file.path: /var/log/snort/snort.csv log.offset: 47,660 agent.type: filebeat agent.id: a8f6871a-eaf9-4db4-8028-fd37a3190169
agent.version: 7.11.0 agent.ephemeral_id: 156300ed-da24-4eac-be3a-cf110574221d agent.hostname: raspberrypi agent.name: raspberrypi
msg: (spp_frag3) Short fragment, possible DoS attempt dst: 129.111.30.27 @timestamp: October 12th 2021, 19:11:07.289
timestamp: 10/12-19:11:00.611570 message: "(spp_frag3) Short fragment, possible DoS attempt",10/12-19:11:00.611570
,UDP,10.1.1.1,129.111.30.27 type: Snort host.name: raspberrypi input.type: log proto: UDP @version: 1 ecs.version: 1.6.0

log.file.path: /var/log/snort/snort.csv log.offset: 48,756 agent.type: filebeat agent.id: a8f6871a-eaf9-4db4-8028-fd37a3190169
agent.version: 7.11.0 agent.ephemeral_id: 156300ed-da24-4eac-be3a-cf110574221d agent.hostname: raspberrypi agent.name: raspberrypi
msg: (spp_frag3) Zero-byte fragment packet dst: 129.111.30.27 @timestamp: October 12th 2021, 19:11:07.290 timestamp: 10/12-
19:11:00.635704 message: "(spp_frag3) Zero-byte fragment packet",10/12-19:11:00.635704 ,UDP,10.1.1.1,129.111.30.27 type: Snort

Completion of the project

Dashboard log management server



Completion of the project

Anuka Jinadasa
IT18132410

Task	Status
Identify required CPS components and categorize them.	Completed
Identify security requirements of the components and assess them based on priority.	Completed
Configure firewall and define rules based on security requirements.	Completed
Implement IDS & IPS using hybrid approach & add rules	Completed
Report & alert generating interface based on security logs.	Completed
Test implemented security measures.	Completed
Securing IDS & Log management server	In Progress

Achievements

Anuka Jinadasa
IT18132410

We were able build a network monitoring solution for small industry 4.0 environments. Also can be easily tailored in for many different occasions & requirements.

Pros vs Cons

Anuka Jinadasa
IT18132410

Pros	Cons
Portability	Weak wireless bandwidth and range
Scalable	On premises log server
Minimum configuration	
Ease of use	
Versatility	
Low initial cost	

REFERENCES

Anuka Jinadasa
IT18132410

[1] N. Gupta, V. Naik and S. Sengupta, "A firewall for Internet of Things," 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, 2017, pp. 411-412, doi: 10.1109/COMSNETS.2017.7945418.

[2] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, “End-toend transport security in the ip-based internet of things,” in 2012 21st International Conference on Computer Communications and Networks (ICCCN). IEEE, 2012, pp. 1–5

[3] (Best Intrusion Detection & Prevention Systems 2021 | IDPS Guide, 2021)

[4] Ioulianou, Philokypros & Vassilakis, Vassilios & Moscholios, Ioannis. (2018). A Signature-based Intrusion Detection System for the Internet of Things.

Dinuwan Randunu

IT18133578

Cyber Security

Research Question

Dinuwan Randunu
IT18133578

How can we achieve

- Authentication
- Authorization
- Accounting

in cps devices ?

Specific & Sub Objectives

Dinuwan Randunu
IT18133578

Specific Objective :

Establish Authentication, authorization and accounting (AAA) and ensure security [1].

Sub Objectives :

- Access log visualization.
- Report generation.
- Alert user when an anomaly occurs.

Methodology

Dinuwan Randunu
IT18133578

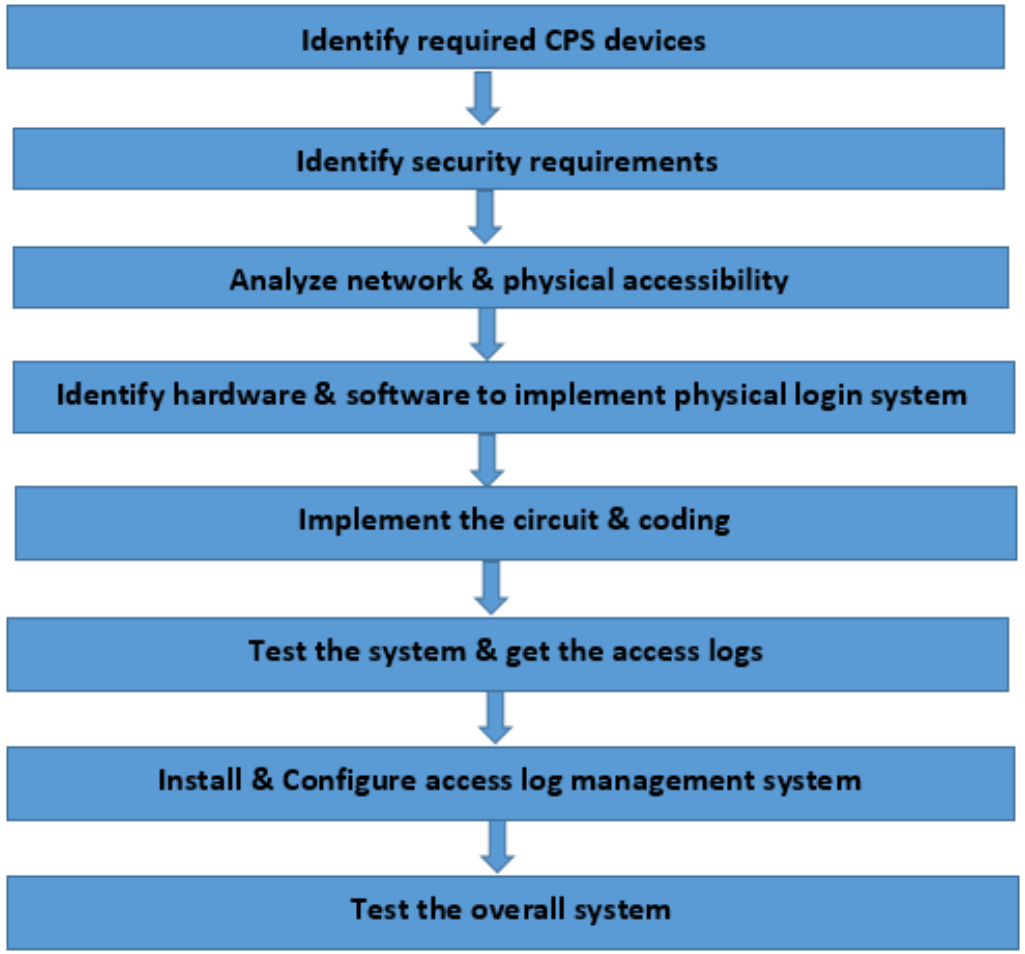
Platform – Arduino

IDE – Arduino IDE

Language – C++

Risk Assessment – Octave

Log Management – Elastic stack



Completion of the project

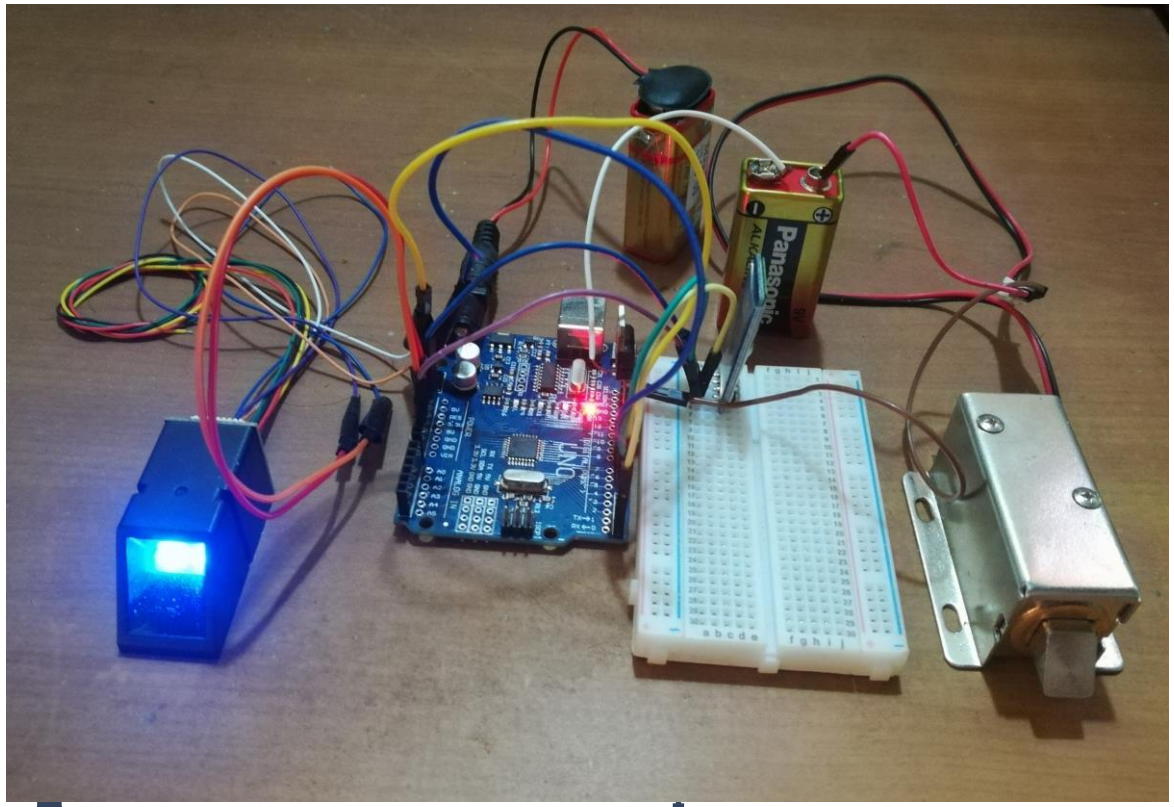
Dinuwan Randunu
IT18133578

Implement smart lock physical system

- Hardware implementation

Hardware requirements:

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



Completion of the project

Dinuwan Randunu
IT18133578

Implement smart lock physical system

- ❖ Software implementation
  - Fingerprint Enrollment using Arduino IDE

fingerprint_enroll

```
#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");
```

```
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_PACKETRECIEVEERR:
      Serial.println("Communication error");
      break;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      break;
    default:
      Serial.println("Unknown error");
      break;
    }
```

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...
```

Completion of the project

Dinuwan Randunu
IT18133578

Implement smart lock physical system

- ❖ Software implementation
  - Fingerprint Verification using Arduino IDE

fingerprint_verify

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

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

  // OK success!
```

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

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

  return finger.fingerID;
}
```

```
Finger verification
Found fingerprint sensor!
Reading sensor parameters
Status: 0x0
Sys ID: 0x0
Capacity: 300
Security level: 3
Device address: FFFFFFFF
Packet len: 128
Baud rate: 57600
Waiting for valid finger...
Sensor contains 3 templates

Image taken
Image converted
Found a print match!
Found ID #3 with confidence of 78
20:21:43 4 7 2021

Image taken
Image converted
Found a print match!
Found ID #2 with confidence of 122
20:21:48 4 7 2021

Image taken
Image converted
Did not find a match
20:21:51 4 7 2021
```

Completion of the project

Dinuwan Randunu
IT18133578

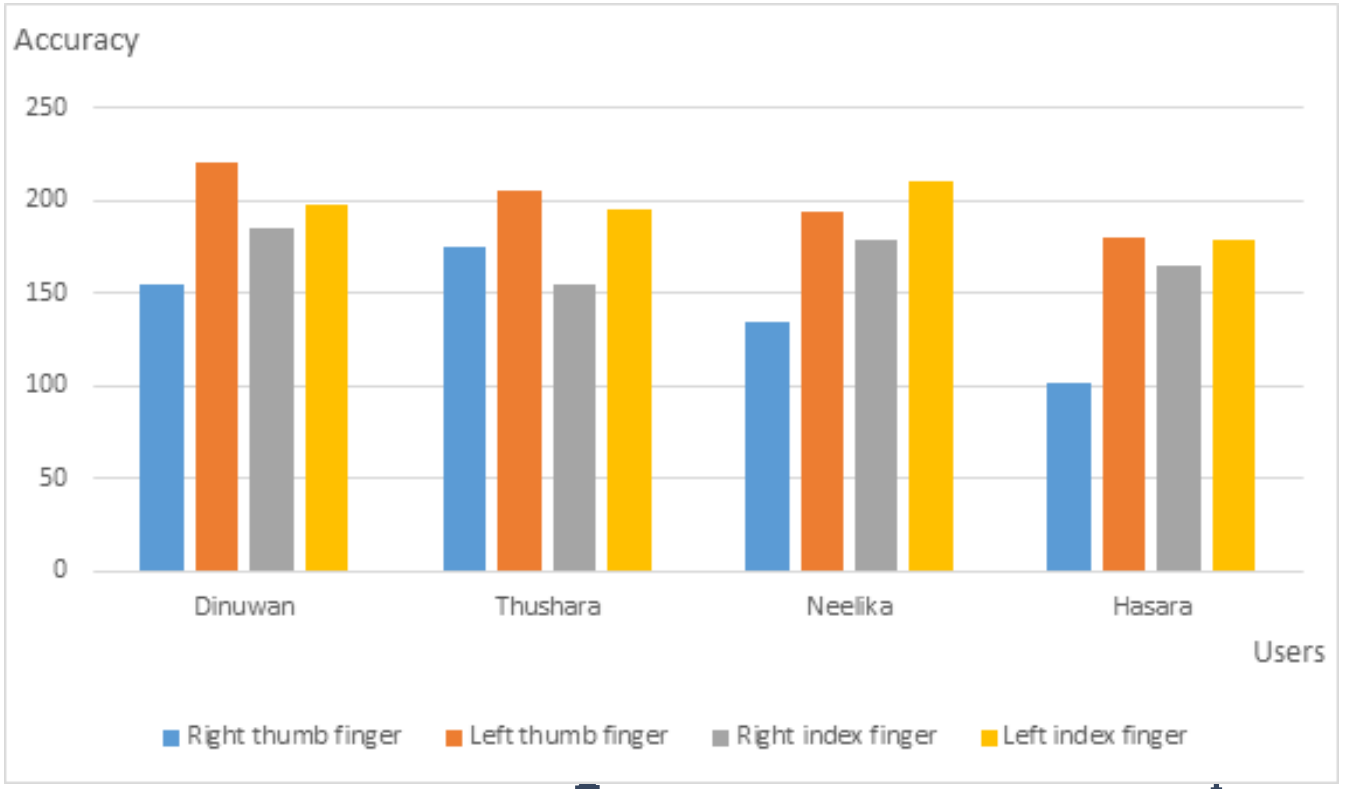
- For the testing purpose, matching and unmatching fingers are scanned using the fingerprint sensor and got the following results as access logs.

	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

Results

Dinuwan Randunu
IT18133578

- Accuracy Level



Achievements

Dinuwan Randunu
IT18133578

- Implement the fine-grained authentication and access control system for IIoT devices.
- Highly efficient as well as less vulnerable system.

Pros vs Cons

Dinuwan Randunu
IT18133578

Pros	Cons
Easy to use	Weak bluetooth communication range
Efficient	
Low cost	
High performance	
High stability	

Completion of the project

Dinuwan Randunu
IT18133578

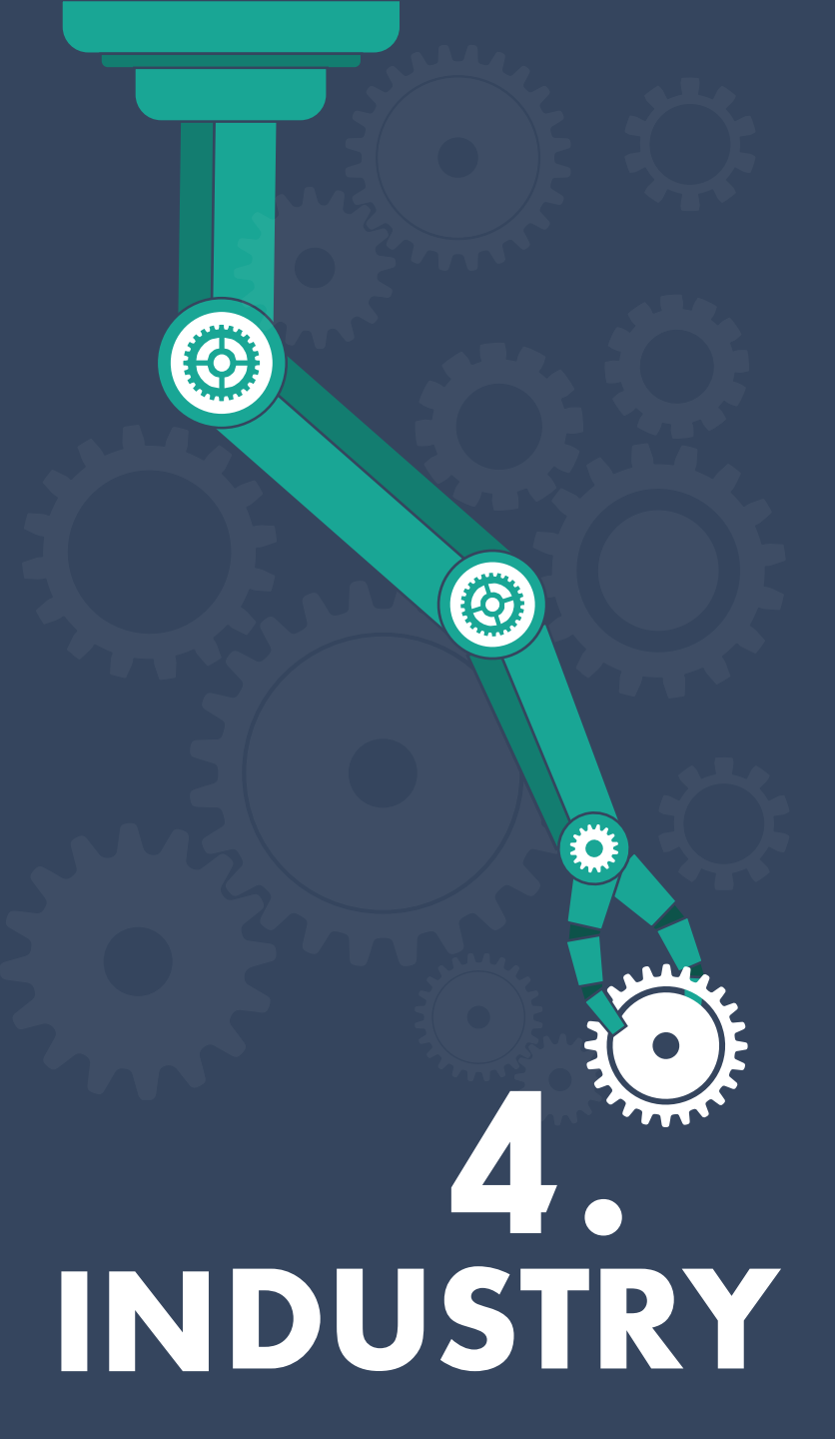
TASK	STATUS
Identify required devices industrial 4.0 manufacturing system	Complete
Identify security requirements and evaluate them	Complete
Analysis of network accessibility and physical accessibility	Complete
Implement smart lock physical system - Hardware implementation	Complete
Implement smart lock physical system - Software implementation	Complete
Test implemented security measures	Complete
Implement login system for access and activity monitor	In Progress
Integration with the final product	In Progress

REFERENCES

Dinuwan Randunu
IT18133578

[1]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.

[2]Francis Enejo Idachaba and Ayobami Ogunrinde, “Review of Remote Terminal Unit (RTU) and Gateways for Digital Oilfield delpoyments” International Journal of Advanced Computer Science and Applications(IJACSA), 3(8), 2012. http://dx.doi.org/10.14569/IJACSA.2012.030826



SUPPORTIVE INFORMATION

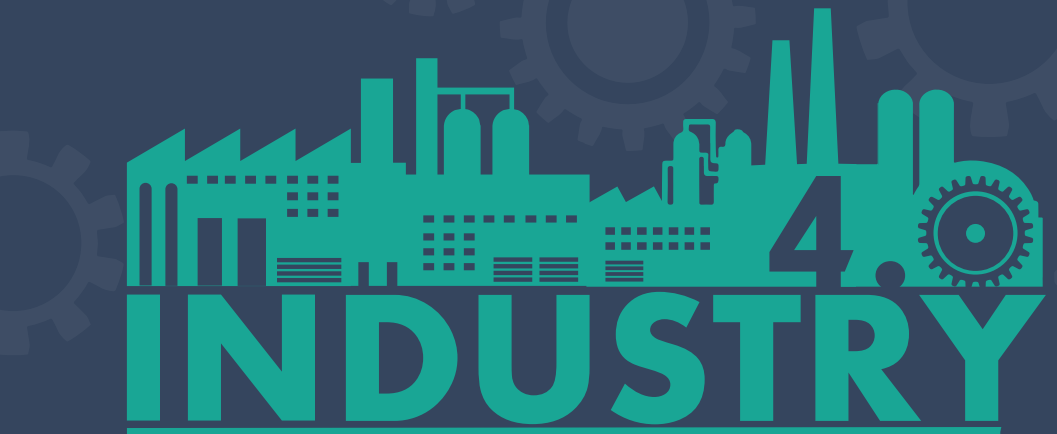
Commercialization

Targeted Audience: Small and medium 4.0 industries or industries that migrating into industry 4.0

Social Media - We will gauge our target audience through Facebook, Twitter, and Instagram campaigns.

Demonstration


Q
&
A



Thank You