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

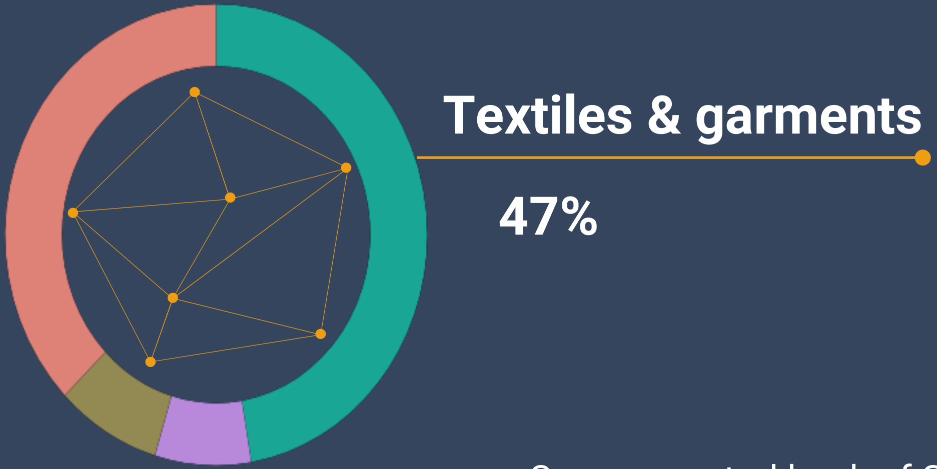
Co - Supervisor
Ms. Wellalage Sasini Nuwanthika

External – Supervisor
Mr. Gamini De Alwis

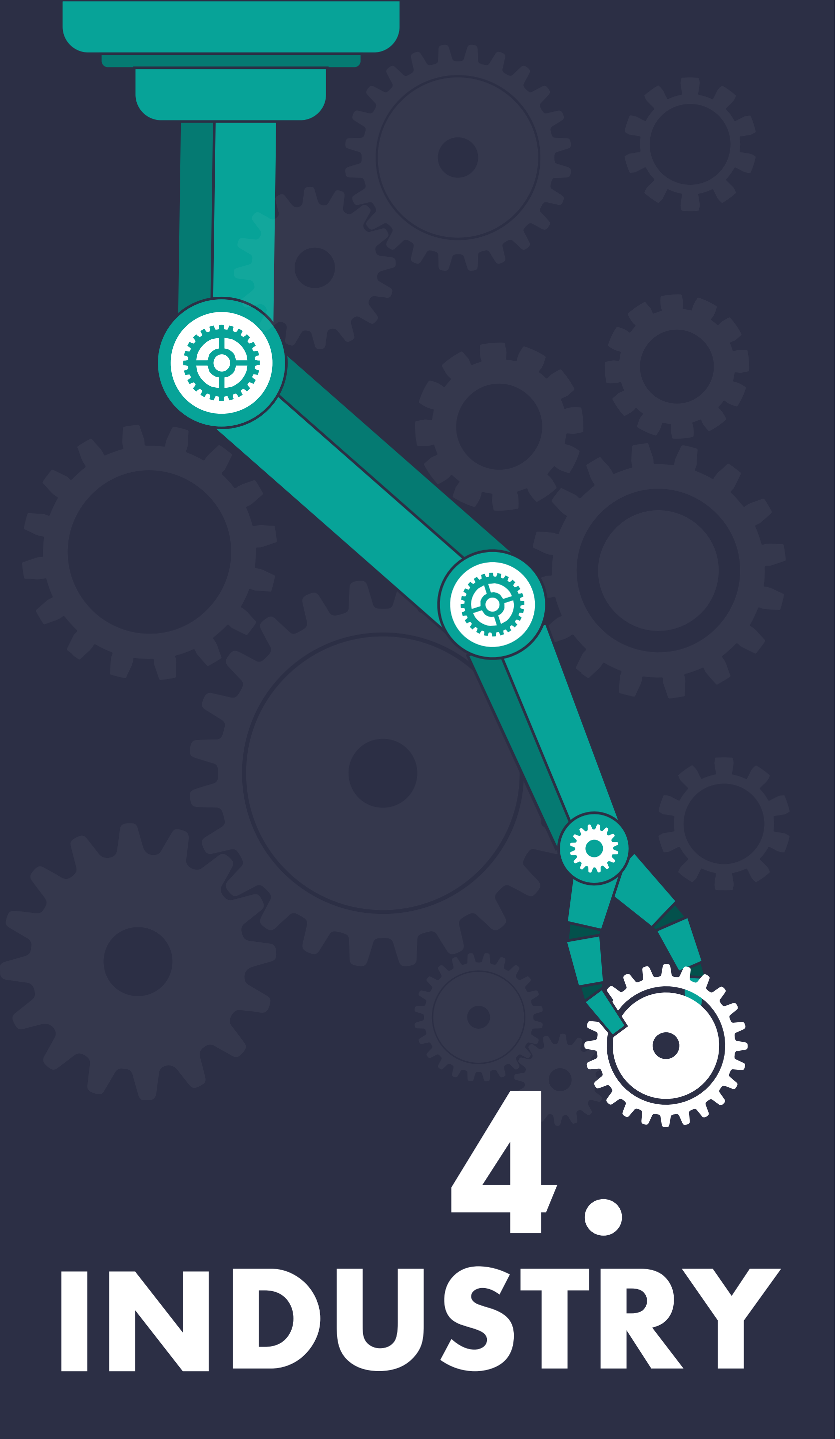
Introduction

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

- **Why Garment Industry ?**



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

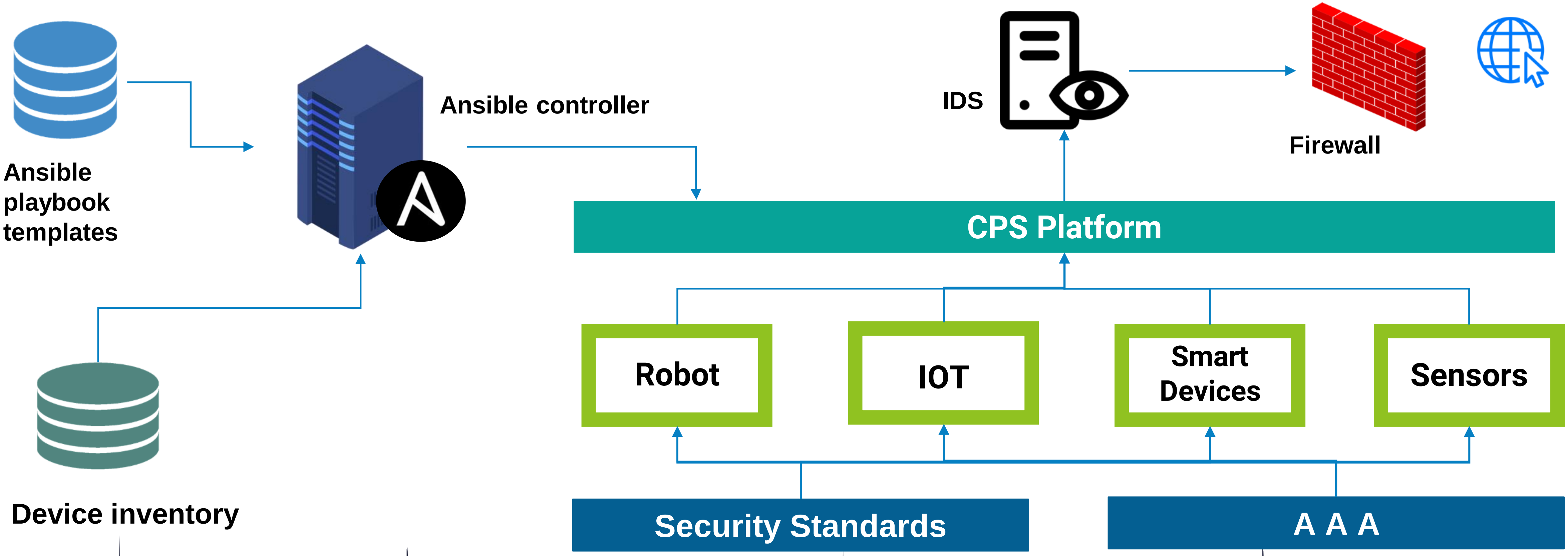
Authentication & Access Monitoring

Policy Development & Update Management

Security Configurations

Intrusion Detection

Overall System Diagram



Dasunpriya Kalhara

IT18139440

Cyber Security

Research Question

Dasunpriya Kalhara
IT18139440

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

Specific & Sub Objectives

Dasunpriya Kalhara
IT18139440

Specific Objective :

A tool for Automating security configurations

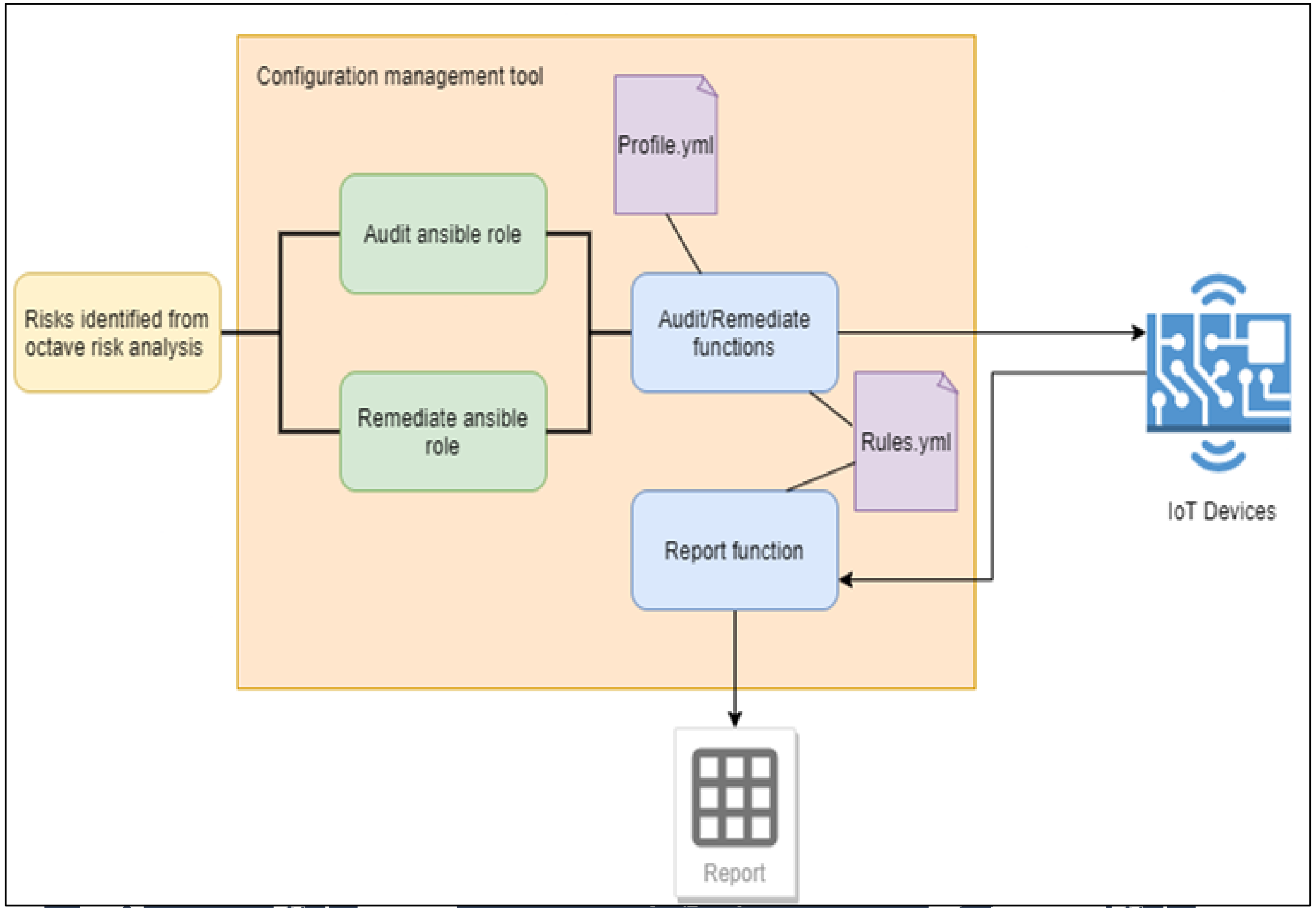
Sub Objectives :

- 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

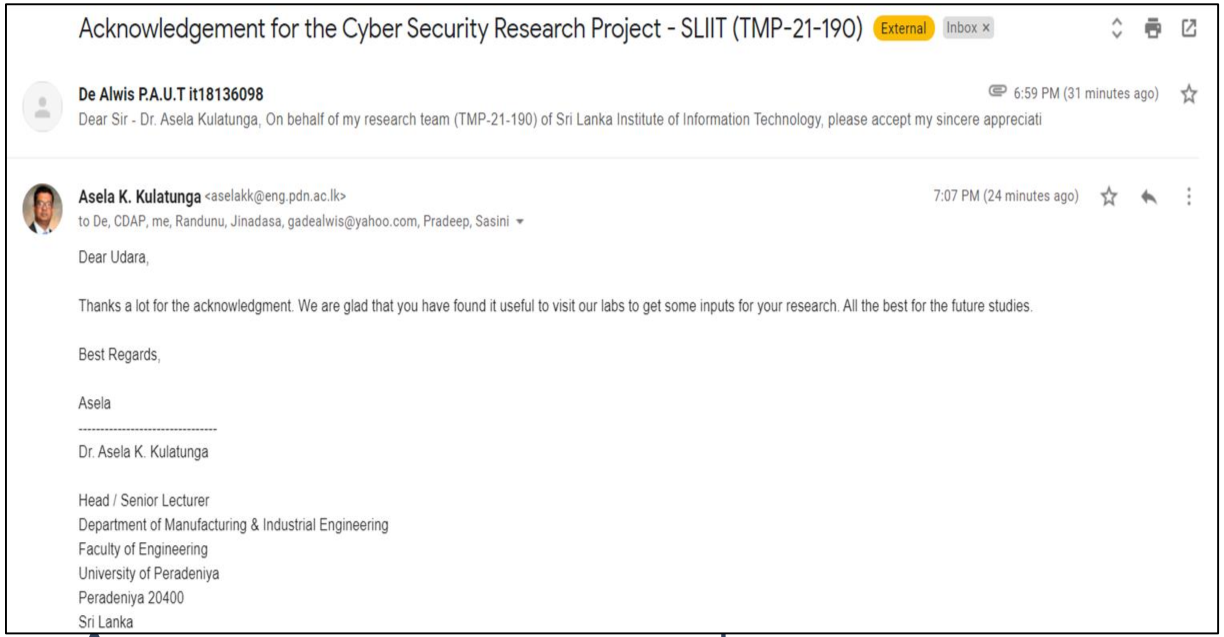

Configuration management tool
Profile.yml
Audit ansible role
Risks identified from octave risk analysis
Audit/Remediate functions
Remediate ansible role
Rules.yml
Report function
IoT Devices
Report

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 Peradeniya campus to get knowledge about CNC machines



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

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,

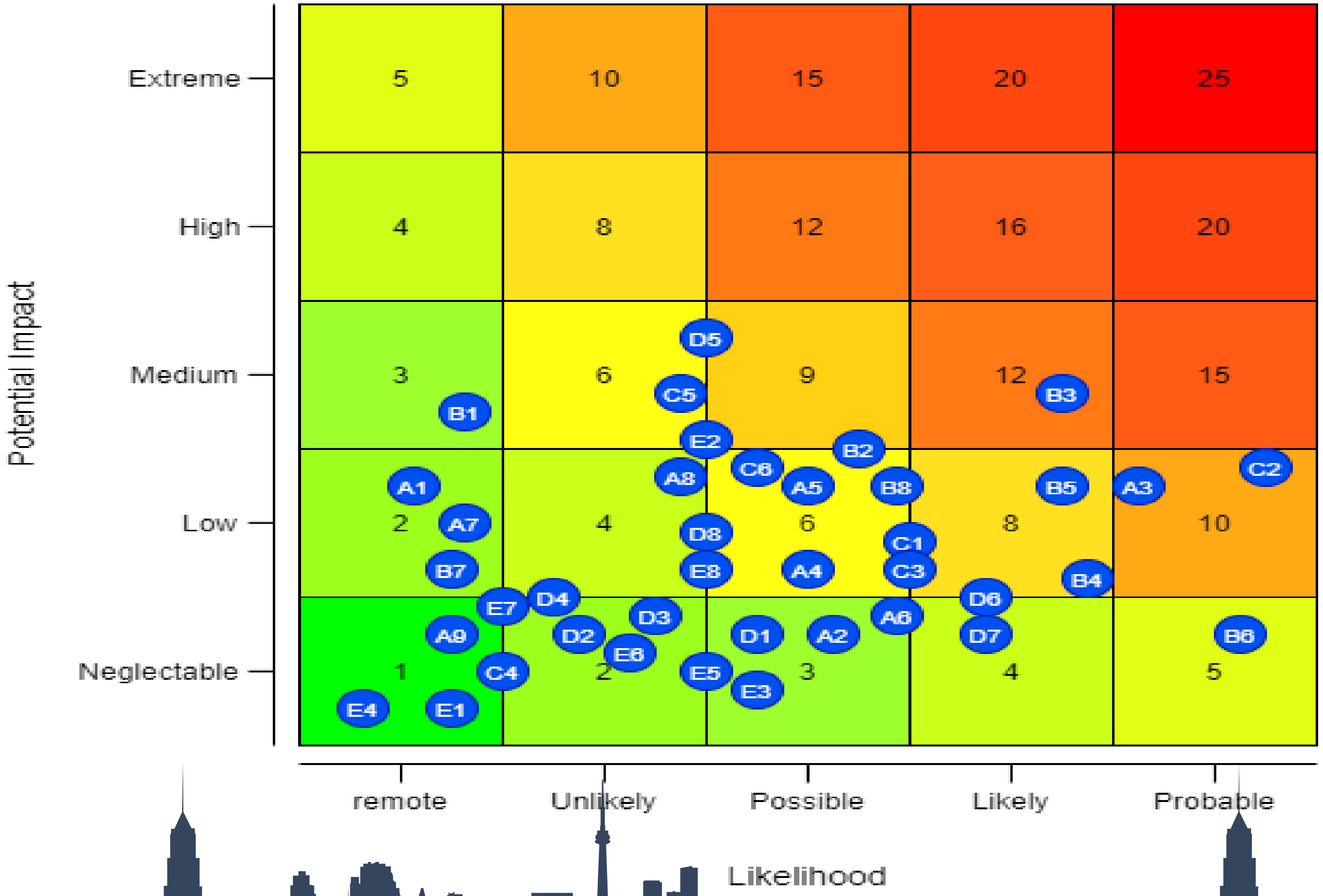
Asela

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.

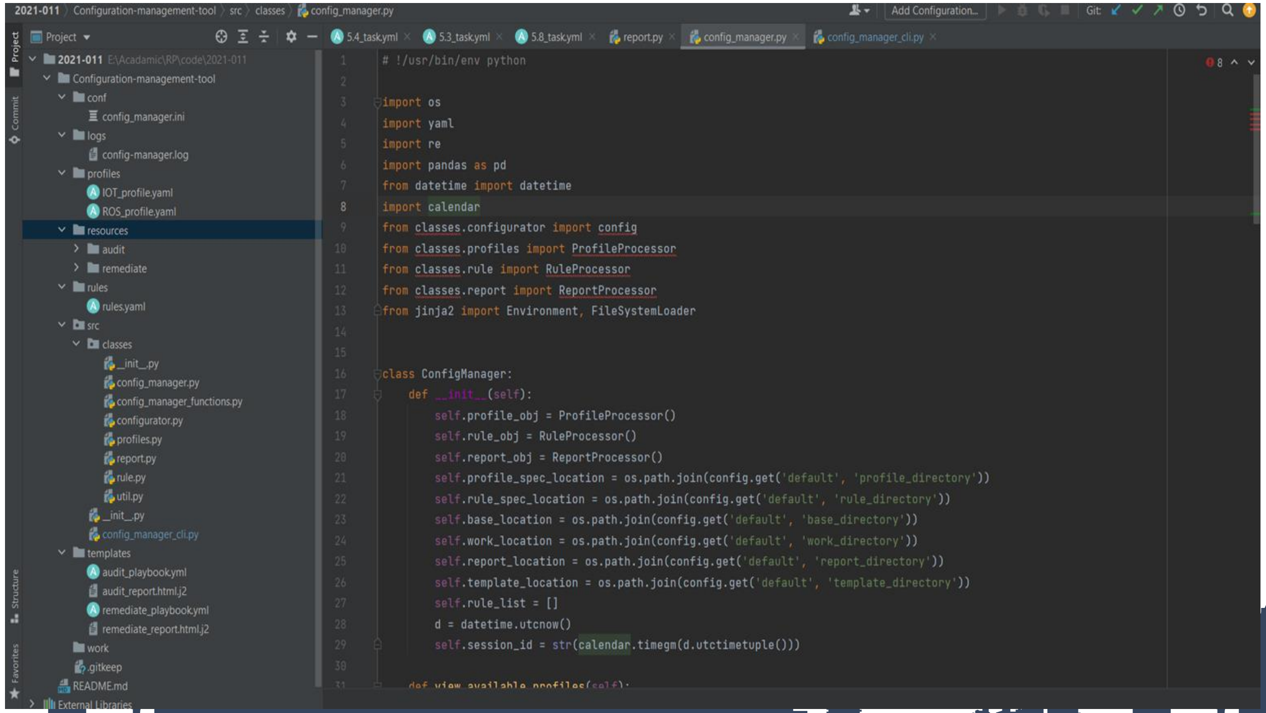
- Conduct octave risk analysis on IoT devices and ansible controller

Completion of the project

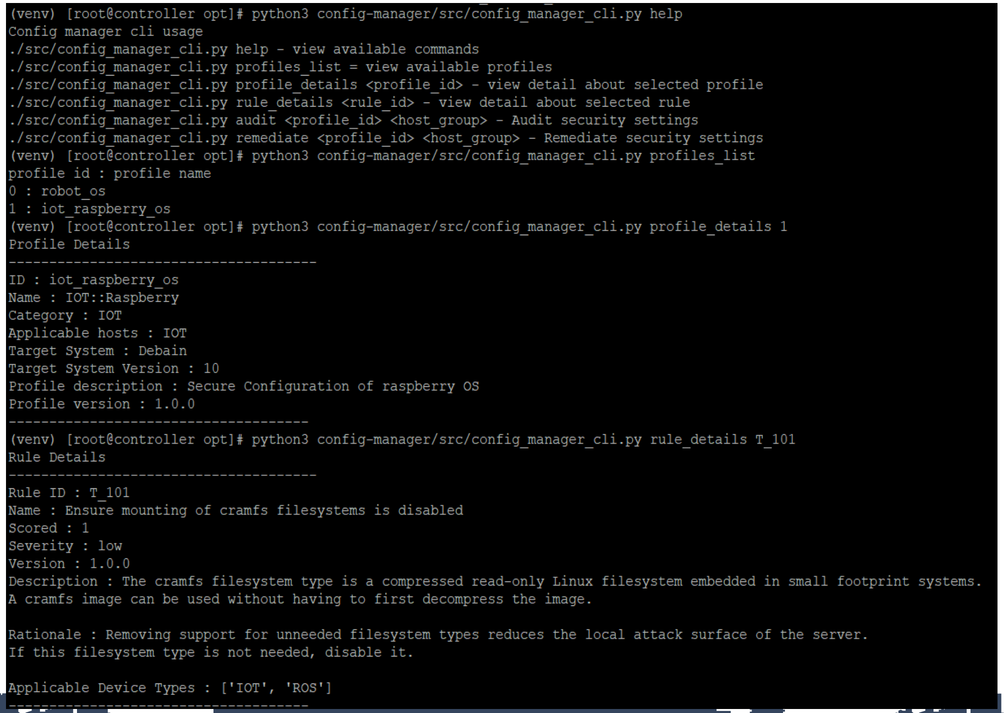
Dasunpriya Kalhara
IT18139440

Implement a tool to audit & remediate security configurations.

- Functional python cli tool to audit & remediate security configurations of raspberry OS (Debian 10).
- Ansible roles used for auditing and remediation.



```python
# !/usr/bin/env python

import os
import yaml
import re
import pandas as pd
from datetime import datetime
import calendar
from classes.configurator import config
from classes.profiles import ProfileProcessor
from classes.rule import RuleProcessor
from classes.report import ReportProcessor
from jinja2 import Environment, FileSystemLoader


class ConfigManager:
    def __init__(self):
        self.profile_obj = ProfileProcessor()
        self.rule_obj = RuleProcessor()
        self.report_obj = ReportProcessor()
        self.profile_spec_location = os.path.join(config.get('default', 'profile_directory'))
        self.rule_spec_location = os.path.join(config.get('default', 'rule_directory'))
        self.base_location = os.path.join(config.get('default', 'base_directory'))
        self.work_location = os.path.join(config.get('default', 'work_directory'))
        self.report_location = os.path.join(config.get('default', 'report_directory'))
        self.template_location = os.path.join(config.get('default', 'template_directory'))
        self.rule_list = []
        d = datetime.utcnow()
        self.session_id = str(calendar.timegm(d.utctimetuple()))

    def view_available_profiles(self):
```



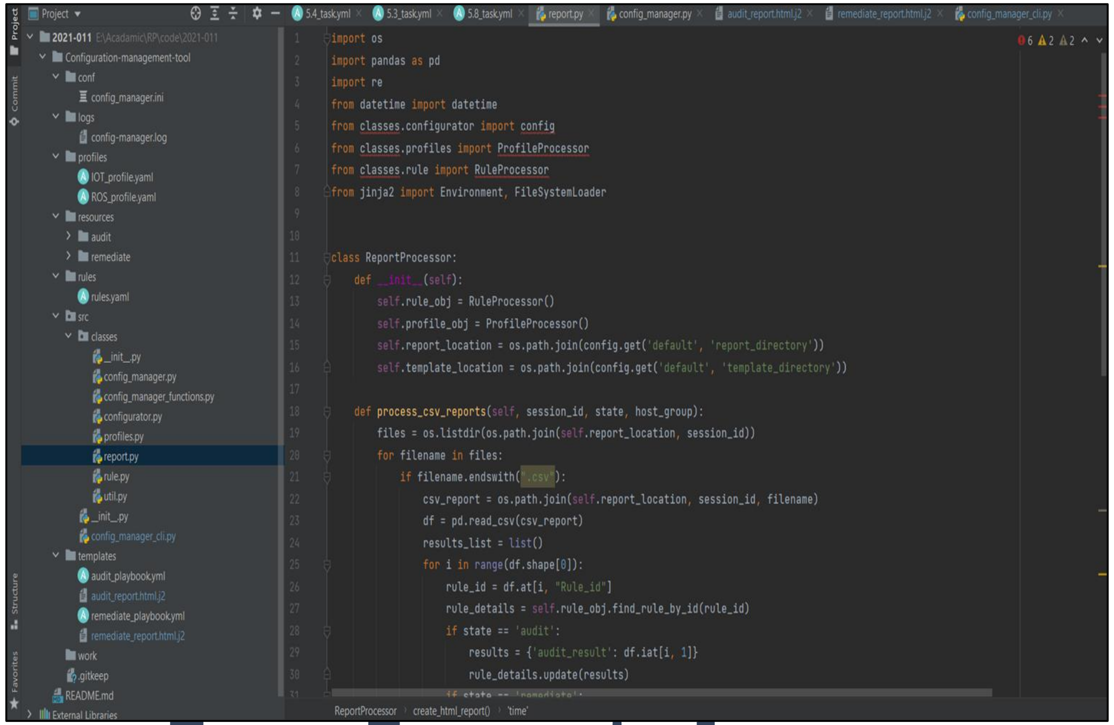
```
(venv) [root@controller opt]# python3 config-manager/src/config_manager_cli.py help
Config manager cli usage
./src/config_manager_cli.py help - view available commands
./src/config_manager_cli.py profiles_list = view available profiles
./src/config_manager_cli.py profile_details <profile_id> - view detail about selected profile
./src/config_manager_cli.py rule_details <rule_id> - view detail about selected rule
./src/config_manager_cli.py audit <profile_id> <host_group> - Audit security settings
./src/config_manager_cli.py remediate <profile_id> <host_group> - Remediate security settings
(venv) [root@controller opt]# python3 config-manager/src/config_manager_cli.py profiles_list
profile id : profile name
0 : robot_os
1 : iot_raspberry_os
(venv) [root@controller opt]# python3 config-manager/src/config_manager_cli.py profile_details 1
Profile Details
--------------------------------------
ID : iot_raspberry_os
Name : IOT::Raspberry
Category : IOT
Applicable hosts : IOT
Target System : Debain
Target System Version : 10
Profile description : Secure Configuration of raspberry OS
Profile version : 1.0.0
-------------------------------------
(venv) [root@controller opt]# python3 config-manager/src/config_manager_cli.py rule_details T_101
Rule Details
--------------------------------------
Rule ID : T_101
Name : Ensure mounting of cramfs filesystems is disabled
Scored : 1
Severity : low
Version : 1.0.0
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 Device Types : ['IOT', 'ROS']
-------------------------------------
```

Completion of the project

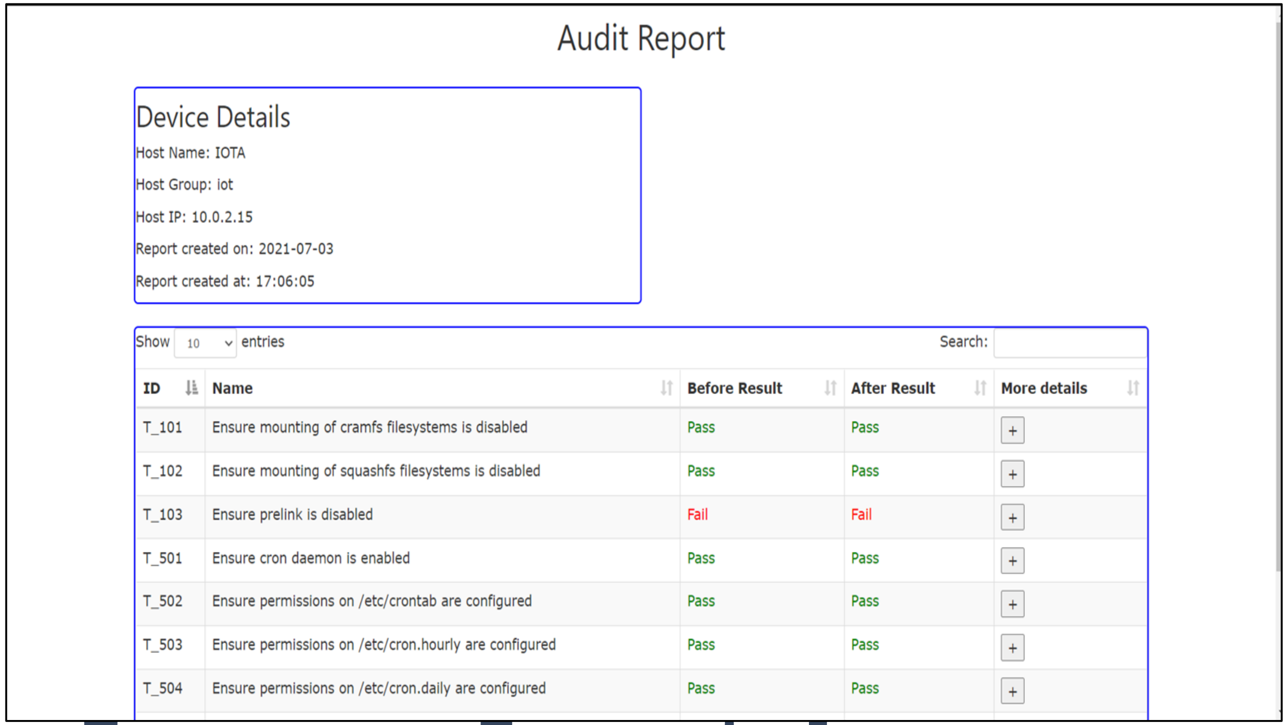
Dasunpriya Kalhara
IT18139440

Implement report generating function based on audit results.

- Currently in progress



```python
import os
import pandas as pd
import re
from datetime import datetime
from classes.configurator import config
from classes.profiles import ProfileProcessor
from classes.rule import RuleProcessor
from jinja2 import Environment, FileSystemLoader


class ReportProcessor:
    def __init__(self):
        self.rule_obj = RuleProcessor()
        self.profile_obj = ProfileProcessor()
        self.report_location = os.path.join(config.get('default', 'report_directory'))
        self.template_location = os.path.join(config.get('default', 'template_directory'))

    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':
```



Audit Report

Device Details

Host Name: IOTA

Host Group: iot

Host IP: 10.0.2.15

Report created on: 2021-07-03

Report created at: 17:06:05

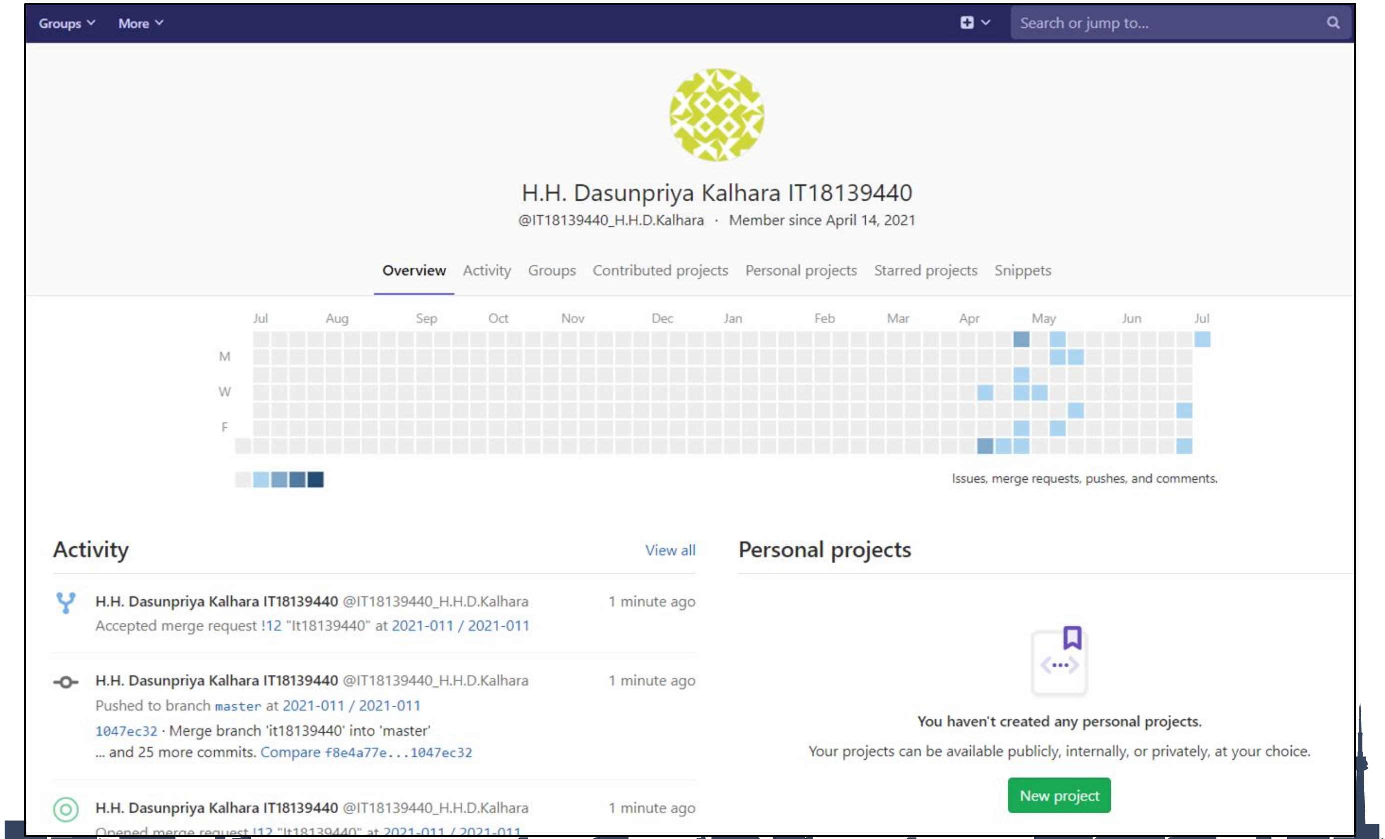
Show 10 entries Search:

ID	Name	Before Result	After Result	More details
T_101	Ensure mounting of cramfs filesystems is disabled	Pass	Pass	+
T_102	Ensure mounting of squashfs filesystems is disabled	Pass	Pass	+
T_103	Ensure prelink is disabled	Fail	Fail	+
T_501	Ensure cron daemon is enabled	Pass	Pass	+
T_502	Ensure permissions on /etc/crontab are configured	Pass	Pass	+
T_503	Ensure permissions on /etc/cron.hourly are configured	Pass	Pass	+
T_504	Ensure permissions on /etc/cron.daily are configured	Pass	Pass	+

Completion of the project

Dasunpriya Kalhara
IT18139440

- Gitlab commits



H.H. Dasunpriya Kalhara IT18139440

@IT18139440_H.H.D.Kalhara · Member since April 14, 2021

Issues, merge requests, pushes, and comments.

Activity

View all

H.H. Dasunpriya Kalhara IT18139440 @IT18139440_H.H.D.Kalhara 1 minute ago
Accepted merge request !12 "It18139440" at 2021-011 / 2021-011

H.H. Dasunpriya Kalhara IT18139440 @IT18139440_H.H.D.Kalhara 1 minute ago
Pushed to branch `master` at 2021-011 / 2021-011
`1047ec32` · Merge branch 'it18139440' into 'master'
... and 25 more commits. Compare `f8e4a77e...1047ec32`

H.H. Dasunpriya Kalhara IT18139440 @IT18139440_H.H.D.Kalhara 1 minute ago
Opened merge request !12 "It18139440" at 2021-011 / 2021-011

Personal projects

You haven't created any personal projects.

Your projects can be available publicly, internally, or privately, at your choice.

New project

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.	In Progress
Implement and Test security configurations on the devices.	In Progress
Integrate the tool to main system and test the tool.	Not Started

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.

Udara De Alwis

IT18136098

Cyber Security

Research Question

Udara De Alwis
IT18136098

How to identify and create security policies 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.

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. According to the area of concern, actor, means of the threat, motive, outcome, security requirements, probability, consequences and severity the heat map is generated.
- Risk assessment report and risk treatment plan will be created according to chosen standards after integrating the components.
- 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

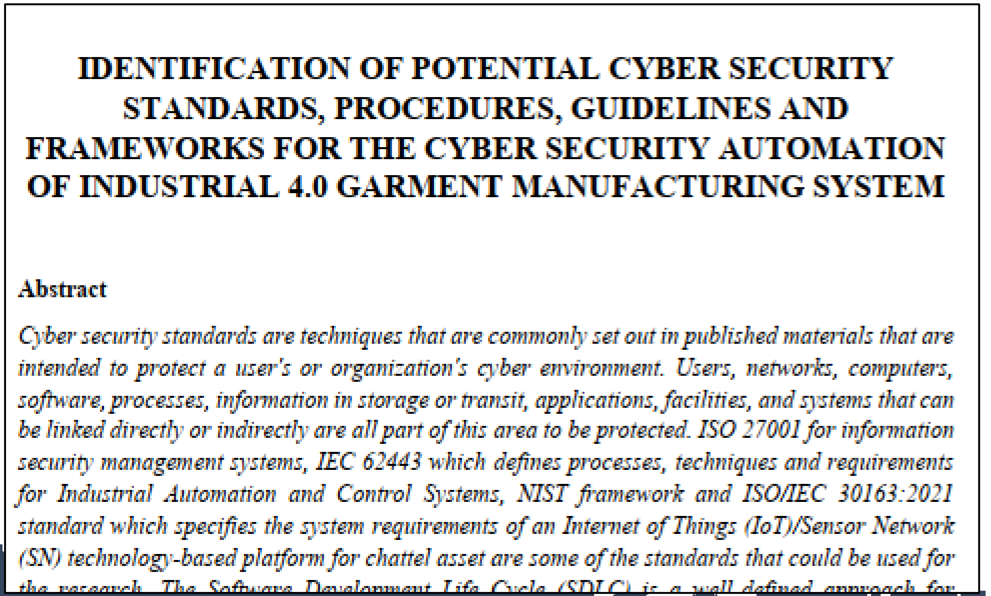
- Set up local APT repository server on Ubuntu using Installation CD
- Configure update manager to setup a central local repository in the server by Creating a local Apache Web Server, so that the clients can install, update and upgrade the packages from the central repository over a LAN.
- Create Catalog 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.

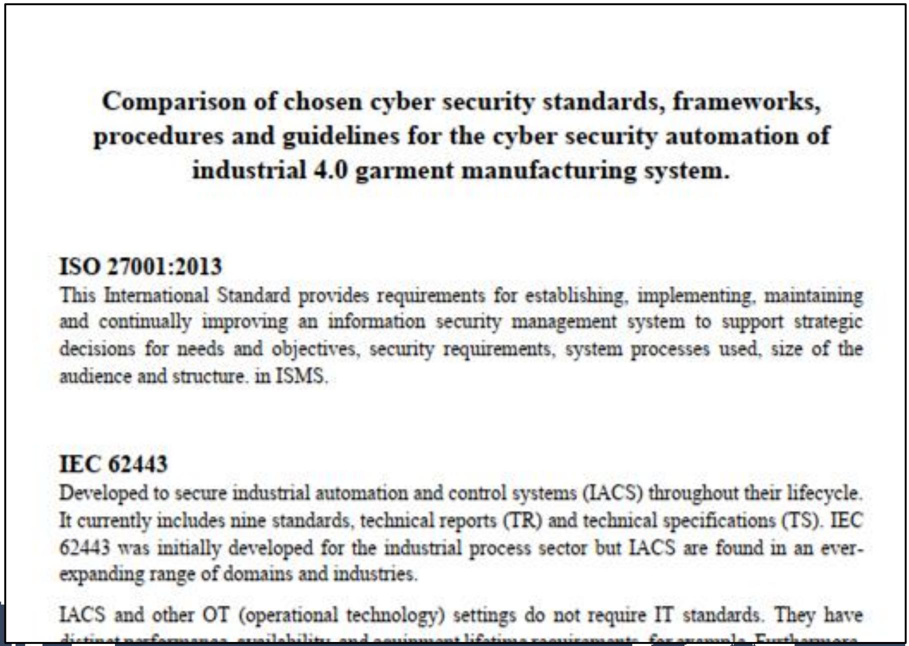
- Potential cyber security standards, procedures, guidelines and frameworks for the cyber security automation of industrial 4.0 garment manufacturing system were identified and documented.
- ISO 27001:2013 and IEC 62443 standards were chosen according to the requirements.
- Documentation of comparison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



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



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.

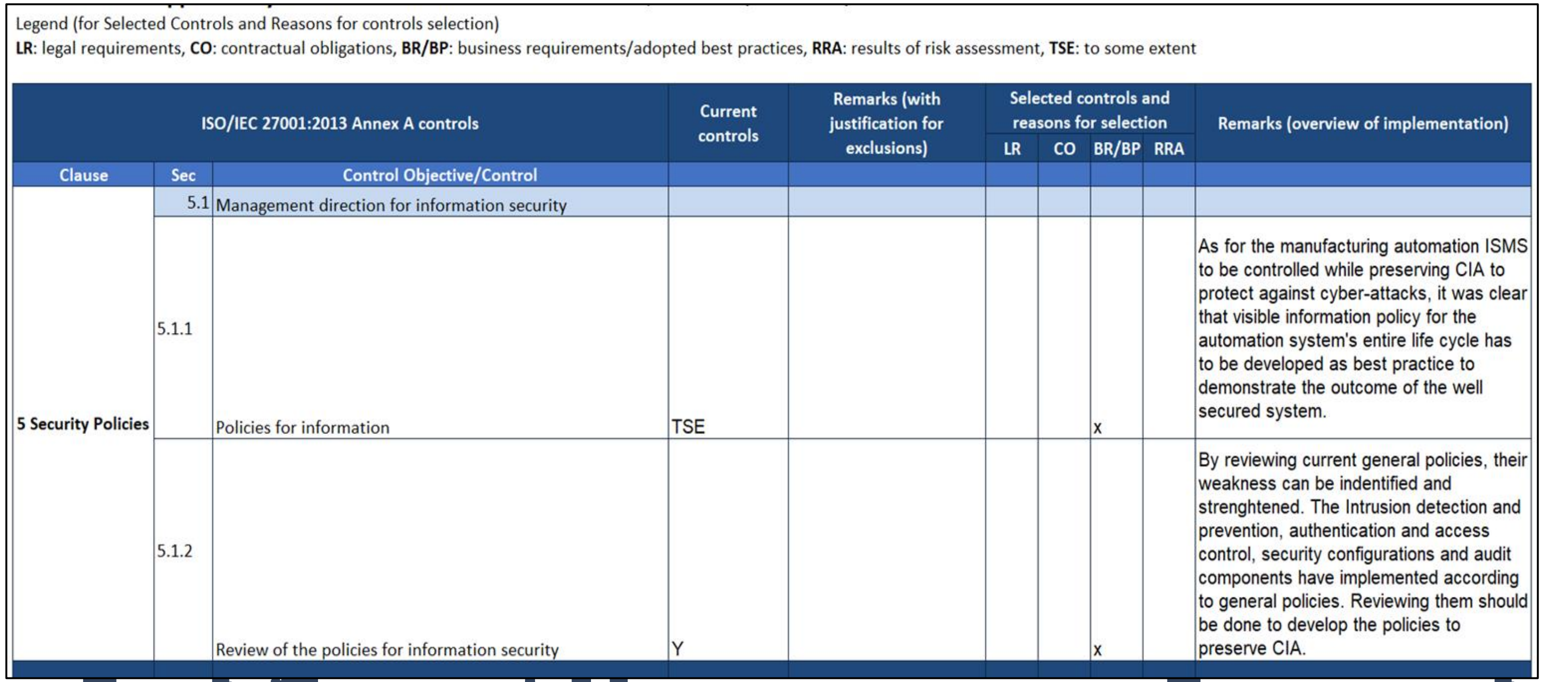
IACS and other OT (operational technology) settings do not require IT standards. They have distinct performance, availability, and equipment lifetime requirements, for example. Furthermore,

Completion of the project

Udara De Alwis
IT18136098

ISO 27001 toolkit

- Mandatory documentation – Defining scope of ISMS, Statement of applicability.
- Policy creation



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

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 Security Policies	5.1	Management direction for information security							
	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.

In progress –

- ISO 27001:2013 non-mandatory policy documentation.
- Creating SOP documents.

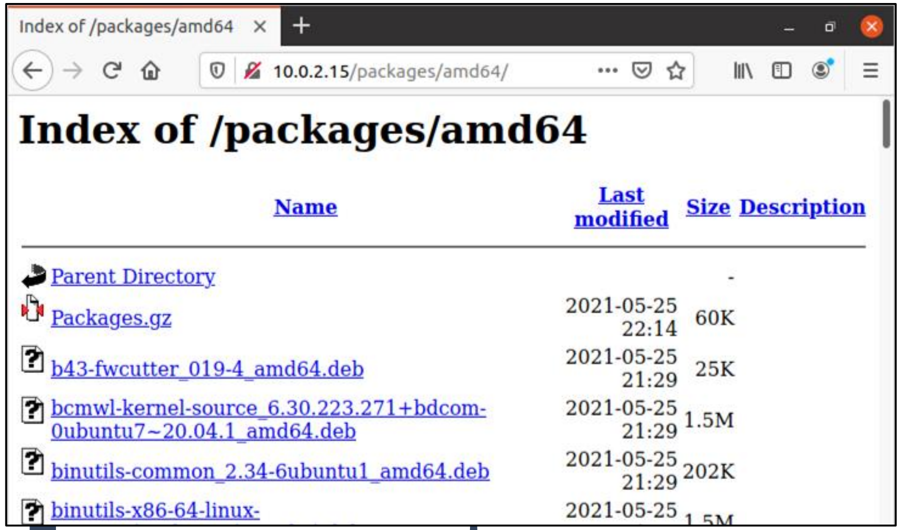
Completion of the project

Udara De Alwis
IT18136098

Update Management

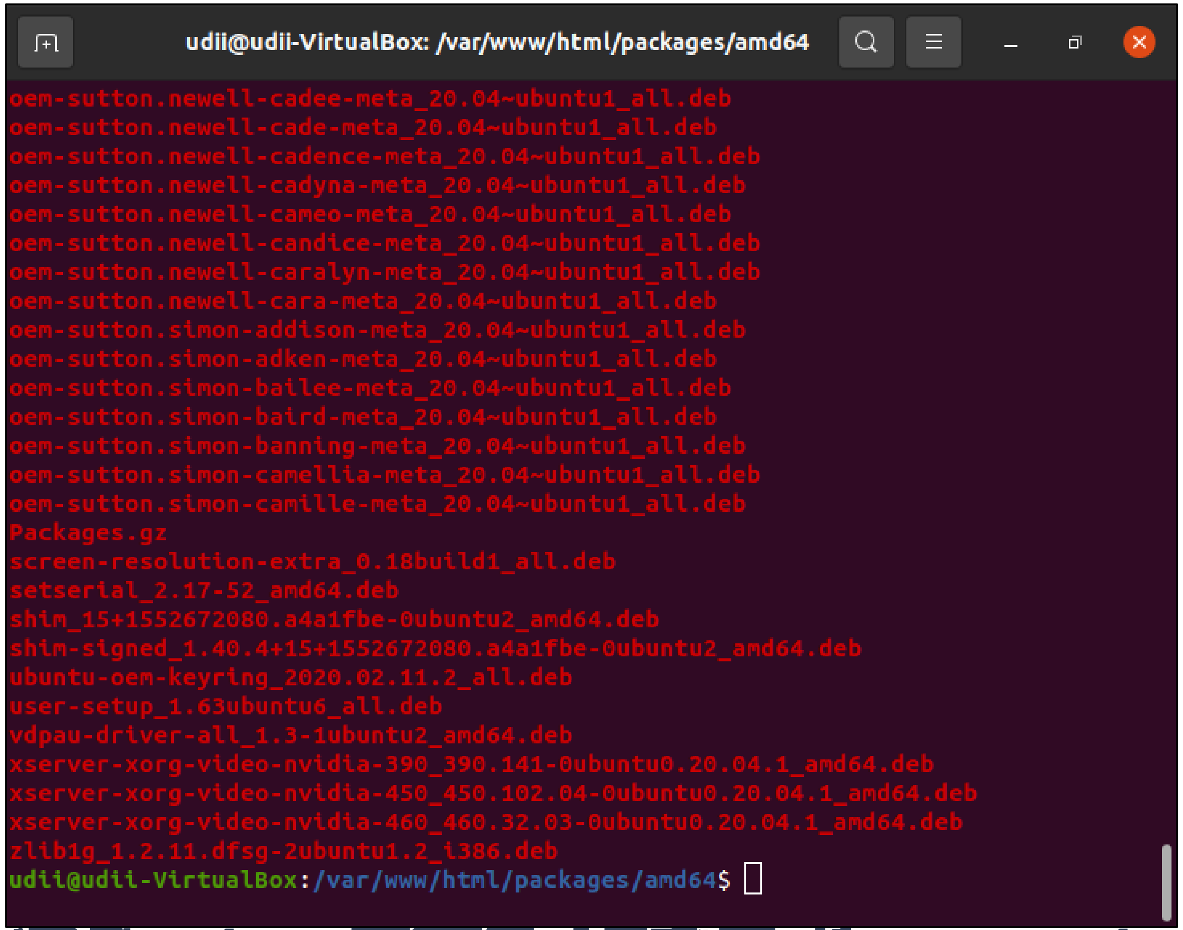
- Set up local repositories.
- Configure package Manager

- In progress- Test local repositories



Index of /packages/amd64

Name	Last modified	Size	Description
Parent Directory		-	
Packages.gz	2021-05-25 22:14	60K	
b43-fwcutter_019-4_amd64.deb	2021-05-25 21:29	25K	
bcmwl-kernel-source_6.30.223.271+bdcom-0ubuntu7~20.04.1_amd64.deb	2021-05-25 21:29	1.5M	
binutils-common_2.34-6ubuntu1_amd64.deb	2021-05-25 21:29	202K	
binutils-x86-64-linux-	2021-05-25	1.5M	

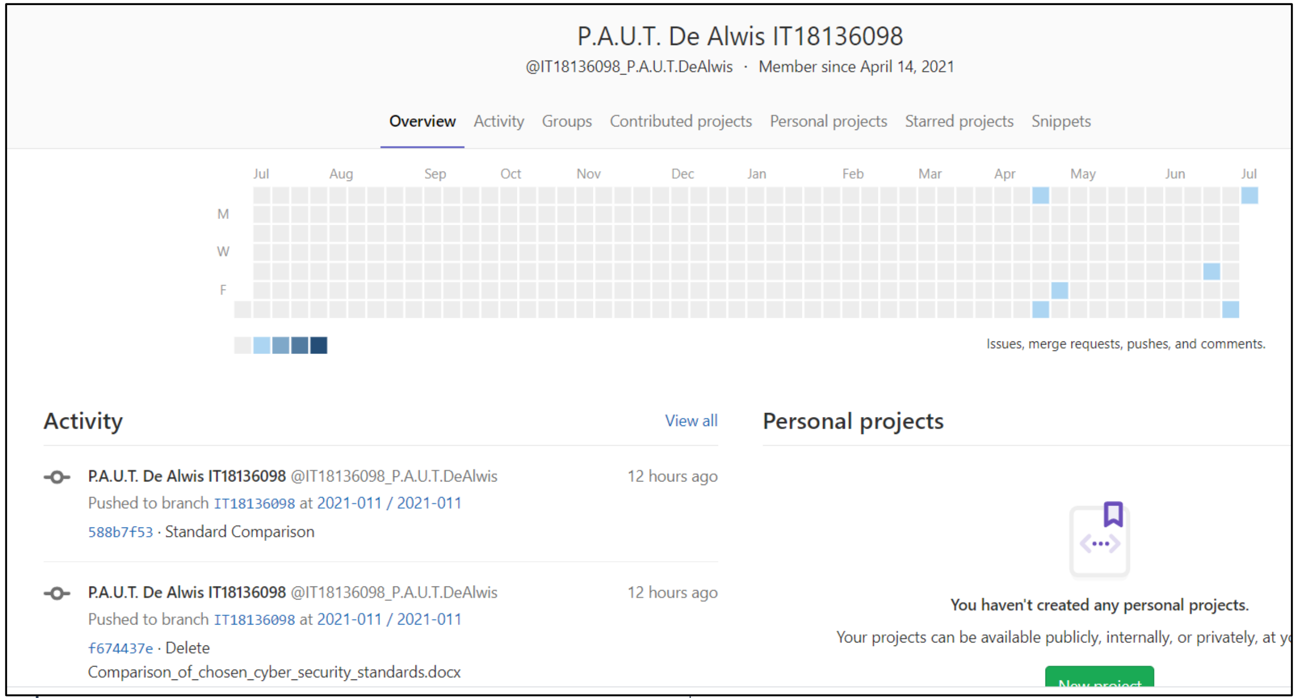


```
oem-sutton.newell-cadee-meta_20.04~ubuntu1_all.deb
oem-sutton.newell-cade-meta_20.04~ubuntu1_all.deb
oem-sutton.newell-cadence-meta_20.04~ubuntu1_all.deb
oem-sutton.newell-cadyna-meta_20.04~ubuntu1_all.deb
oem-sutton.newell-cameo-meta_20.04~ubuntu1_all.deb
oem-sutton.newell-candice-meta_20.04~ubuntu1_all.deb
oem-sutton.newell-caralyn-meta_20.04~ubuntu1_all.deb
oem-sutton.newell-cara-meta_20.04~ubuntu1_all.deb
oem-sutton.simon-addison-meta_20.04~ubuntu1_all.deb
oem-sutton.simon-adken-meta_20.04~ubuntu1_all.deb
oem-sutton.simon-bailee-meta_20.04~ubuntu1_all.deb
oem-sutton.simon-baird-meta_20.04~ubuntu1_all.deb
oem-sutton.simon-banning-meta_20.04~ubuntu1_all.deb
oem-sutton.simon-camellia-meta_20.04~ubuntu1_all.deb
oem-sutton.simon-camille-meta_20.04~ubuntu1_all.deb
Packages.gz
screen-resolution-extra_0.18build1_all.deb
setserial_2.17-52_amd64.deb
shim_15+1552672080.a4a1fbe-0ubuntu2_amd64.deb
shim-signed_1.40.4+15+1552672080.a4a1fbe-0ubuntu2_amd64.deb
ubuntu-oem-keyring_2020.02.11.2_all.deb
user-setup_1.63ubuntu6_all.deb
vdpau-driver-all_1.3-1ubuntu2_amd64.deb
xserver-xorg-video-nvidia-390_390.141-0ubuntu0.20.04.1_amd64.deb
xserver-xorg-video-nvidia-450_450.102.04-0ubuntu0.20.04.1_amd64.deb
xserver-xorg-video-nvidia-460_460.32.03-0ubuntu0.20.04.1_amd64.deb
zlib1g_1.2.11.dfsg-2ubuntu1.2_i386.deb
udii@udii-VirtualBox:/var/www/html/packages/amd64$
```

Completion of the project

Udara De Alwis
IT18136098

- Gitlab commits



P.A.U.T. De Alwis IT18136098

@IT18136098_P.A.U.T.DeAlwis · Member since April 14, 2021

Issues, merge requests, pushes, and comments.

Activity

P.A.U.T. De Alwis IT18136098 @IT18136098_P.A.U.T.DeAlwis 12 hours ago
Pushed to branch IT18136098 at 2021-011 / 2021-011
588b7f53 · Standard Comparison

P.A.U.T. De Alwis IT18136098 @IT18136098_P.A.U.T.DeAlwis 12 hours ago
Pushed to branch IT18136098 at 2021-011 / 2021-011
f674437e · Delete Comparison_of_chosen_cyber_security_standards.docx

Personal projects

You haven't created any personal projects.

Your projects can be available publicly, internally, or privately, at y

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	In Progress
Creating SOP documents	In Progress
Verify the policy creation through an industry expert	Not Started
Implement policies for the components, converting policies into action.	Not Started
Setup local repositories	Complete
Configure package manager	Complete
Test local repositories	Not Started
Identify update validation	Not Started
Mechanisms for role back	Not Started

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

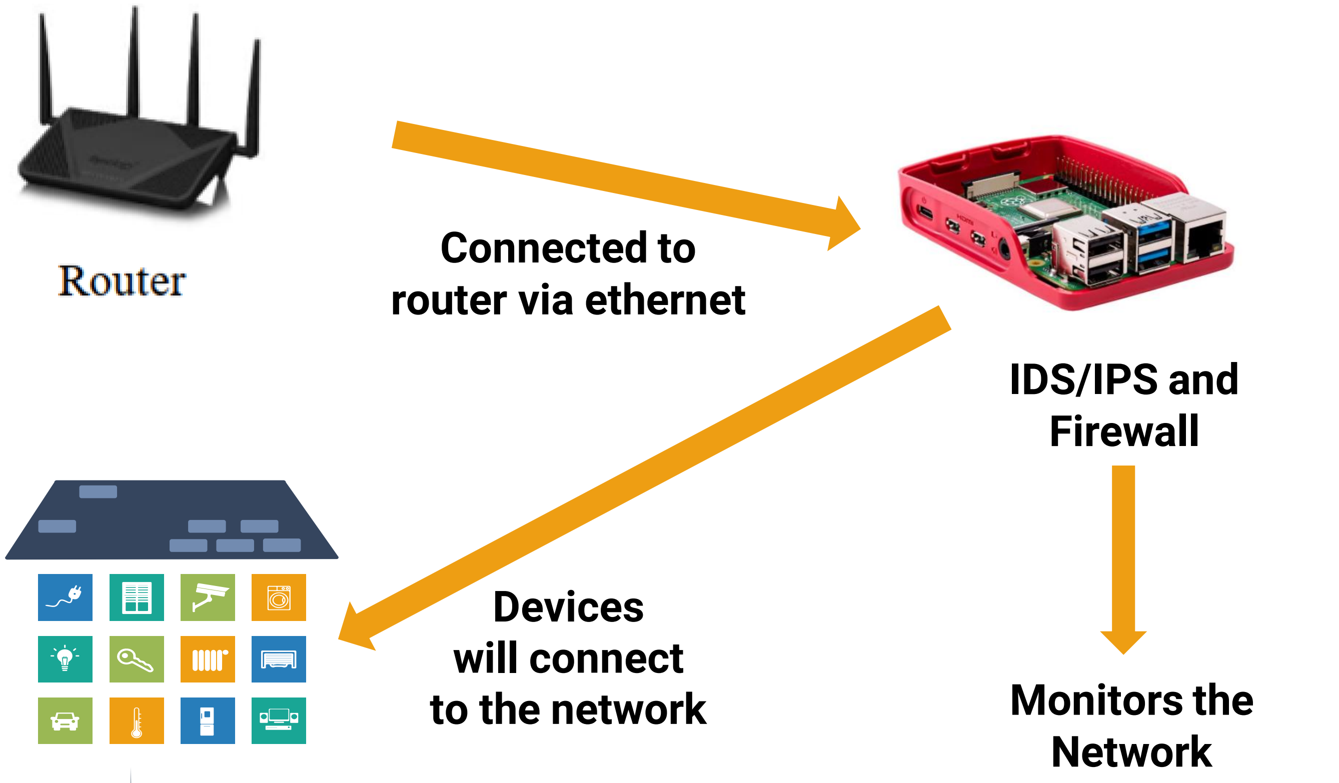
Sub Objectives :

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

Methodology

Anuka Jinadasa
IT18132410

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



Router

Connected to
router via ethernet

IDS/IPS and
Firewall

Devices
will connect
to the network

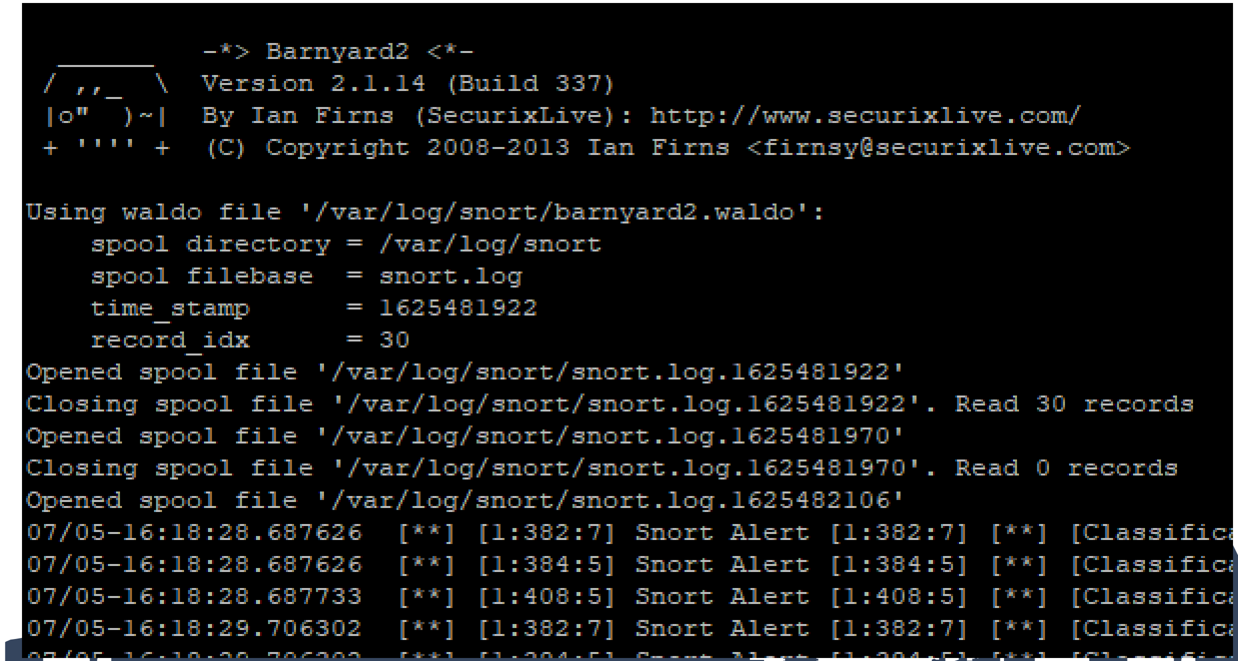
Monitors the
Network

Completion of the project

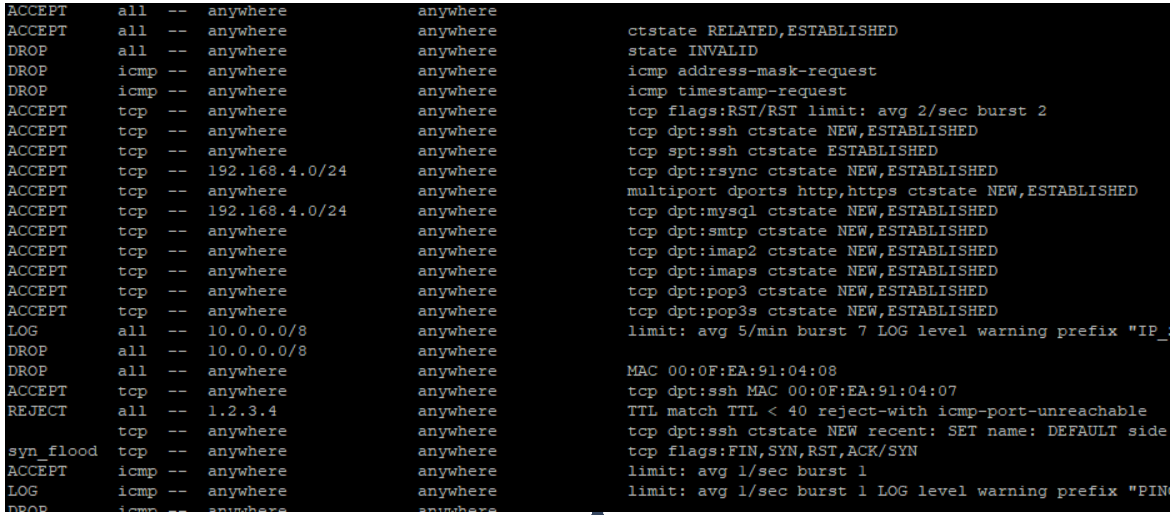
Anuka Jinadasa
IT18132410

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.



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

Using waldo file '/var/log/snort/barnyard2.waldo':
    spool directory = /var/log/snort
    spool filebase  = snort.log
    time_stamp      = 1625481922
    record_idx      = 30
Opened spool file '/var/log/snort/snort.log.1625481922'
Closing spool file '/var/log/snort/snort.log.1625481922'. Read 30 records
Opened spool file '/var/log/snort/snort.log.1625481970'
Closing spool file '/var/log/snort/snort.log.1625481970'. Read 0 records
Opened spool file '/var/log/snort/snort.log.1625482106'
07/05-16:18:28.687626  [**] [1:382:7] Snort Alert [1:382:7] [**] [Classifica
07/05-16:18:28.687626  [**] [1:384:5] Snort Alert [1:384:5] [**] [Classifica
07/05-16:18:28.687733  [**] [1:408:5] Snort Alert [1:408:5] [**] [Classifica
07/05-16:18:29.706302  [**] [1:382:7] Snort Alert [1:382:7] [**] [Classifica
```

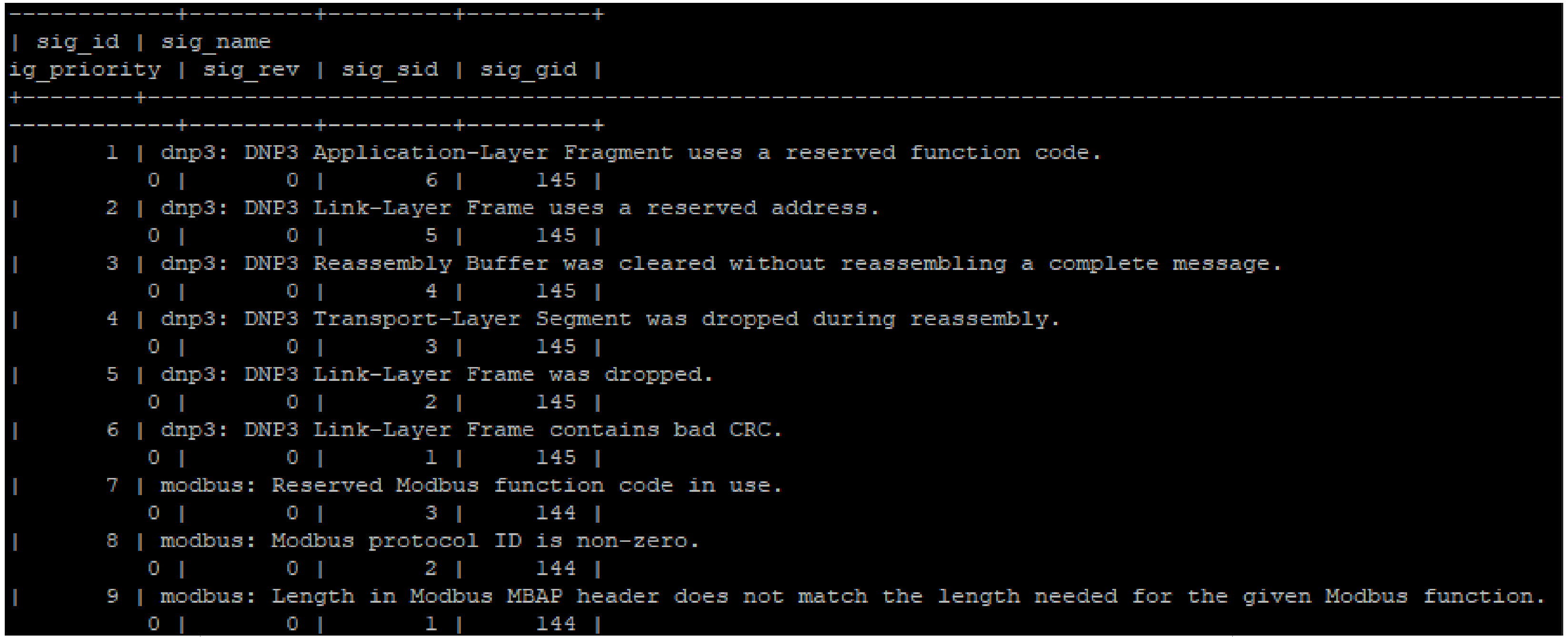


```
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DROP       all  --  anywhere             anywhere             state INVALID
DROP       icmp --  anywhere             anywhere             icmp address-mask-request
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 prefix "IP_
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-unreachable
           tcp  --  anywhere             anywhere             tcp dpt:ssh ctstate NEW recent: SET name: DEFAULT side
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 prefix "PIN
DROP       icmp --  anywhere             anywhere
```

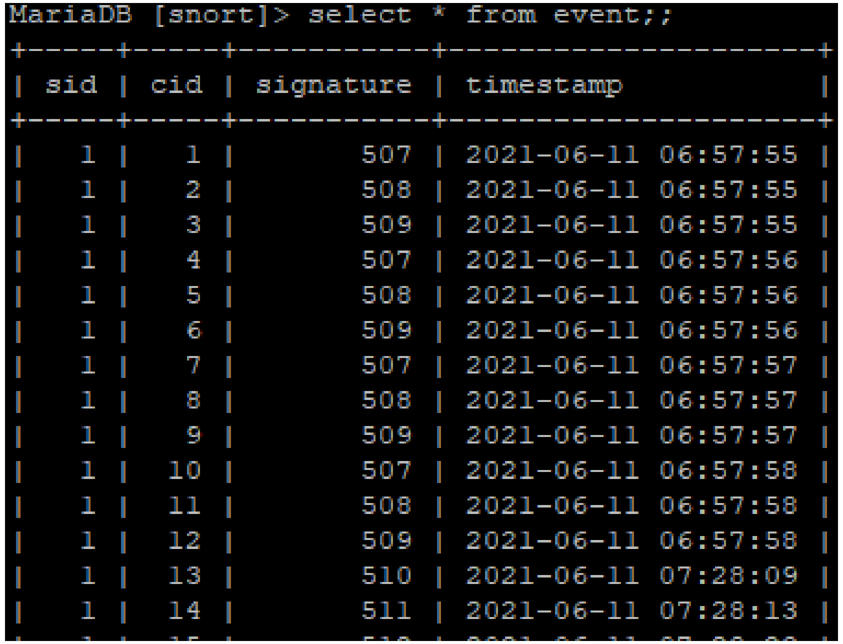
Completion of the project

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 |
```

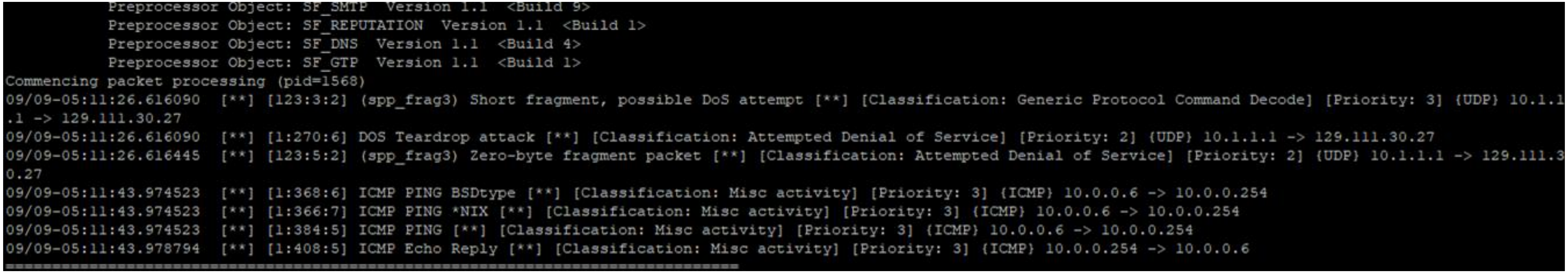


```
MariaDB [snort]> select * from event;;
+-----+-----+-----------+---------------------+
| sid | cid | signature | timestamp           |
+-----+-----+-----------+---------------------+
|   1 |   1 |       507 | 2021-06-11 06:57:55 |
|   1 |   2 |       508 | 2021-06-11 06:57:55 |
|   1 |   3 |       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 |
```

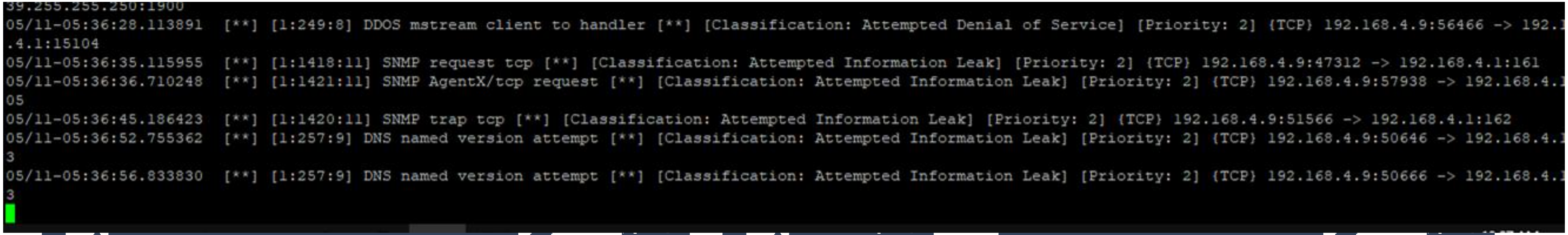
Completion of the project

Anuka Jinadasa
IT18132410

Initial testing of IDS & IPS & configured firewall rules



```
          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=1568)
09/09-05:11:26.616090  [**] [123:3:2] (spp_frag3) Short fragment, possible DoS attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.1.1
.1 -> 129.111.30.27
09/09-05:11:26.616090  [**] [1:270:6] DOS Teardrop attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 10.1.1.1 -> 129.111.30.27
09/09-05:11:26.616445  [**] [123:5:2] (spp_frag3) Zero-byte fragment packet [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 10.1.1.1 -> 129.111.3
0.27
09/09-05:11:43.974523  [**] [1:368:6] ICMP PING BSDtype [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.6 -> 10.0.0.254
09/09-05:11:43.974523  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.6 -> 10.0.0.254
09/09-05:11:43.974523  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.6 -> 10.0.0.254
09/09-05:11:43.978794  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.254 -> 10.0.0.6
```



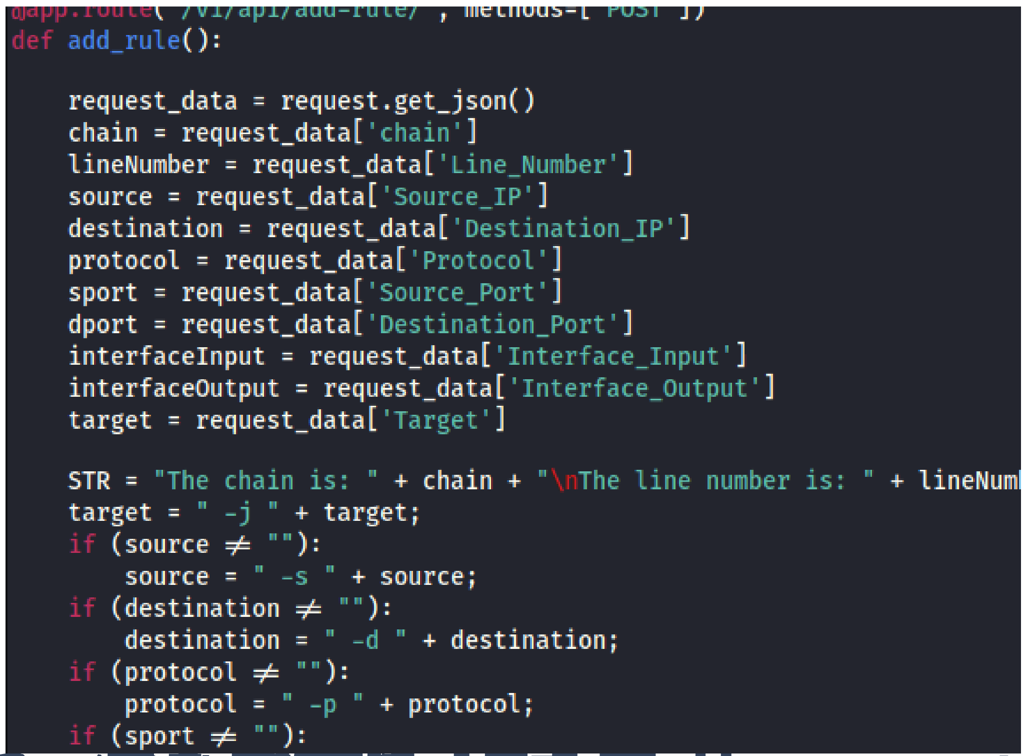
```
39.255.255.250:1900
05/11-05:36:28.113891  [**] [1:249:8] DDOS mstream client to handler [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 192.168.4.9:56466 -> 192.1
.4.1:15104
05/11-05:36:35.115955  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.4.9:47312 -> 192.168.4.1:161
05/11-05:36:36.710248  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.4.9:57938 -> 192.168.4.1
05
05/11-05:36:45.186423  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.4.9:51566 -> 192.168.4.1:162
05/11-05:36:52.755362  [**] [1:257:9] DNS named version attempt [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.4.9:50646 -> 192.168.4.1
3
05/11-05:36:56.833830  [**] [1:257:9] DNS named version attempt [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.4.9:50666 -> 192.168.4.1
3
```

Completion of the project

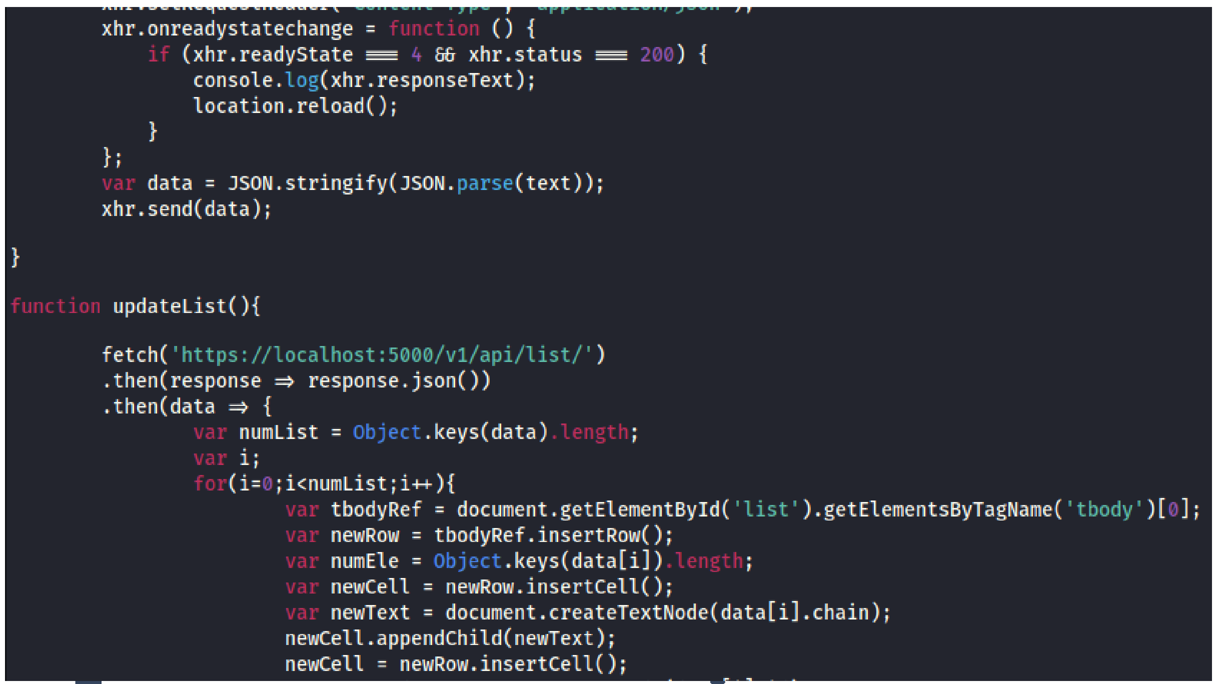
Anuka Jinadasa
IT18132410

Dashboard to add/remove firewall rules

- Currently in progress



```python
@app.route('/v1/api/add-rule/', methods=['POST'])
def add_rule():

    request_data = request.get_json()
    chain = request_data['chain']
    lineNumber = request_data['Line_Number']
    source = request_data['Source_IP']
    destination = request_data['Destination_IP']
    protocol = request_data['Protocol']
    sport = request_data['Source_Port']
    dport = request_data['Destination_Port']
    interfaceInput = request_data['Interface_Input']
    interfaceOutput = request_data['Interface_Output']
    target = request_data['Target']

    STR = "The chain is: " + chain + "\nThe line number is: " + lineNum
    target = " -j " + target;
    if (source != ""):
        source = " -s " + source;
    if (destination != ""):
        destination = " -d " + destination;
    if (protocol != ""):
        protocol = " -p " + protocol;
    if (sport != ""):
```

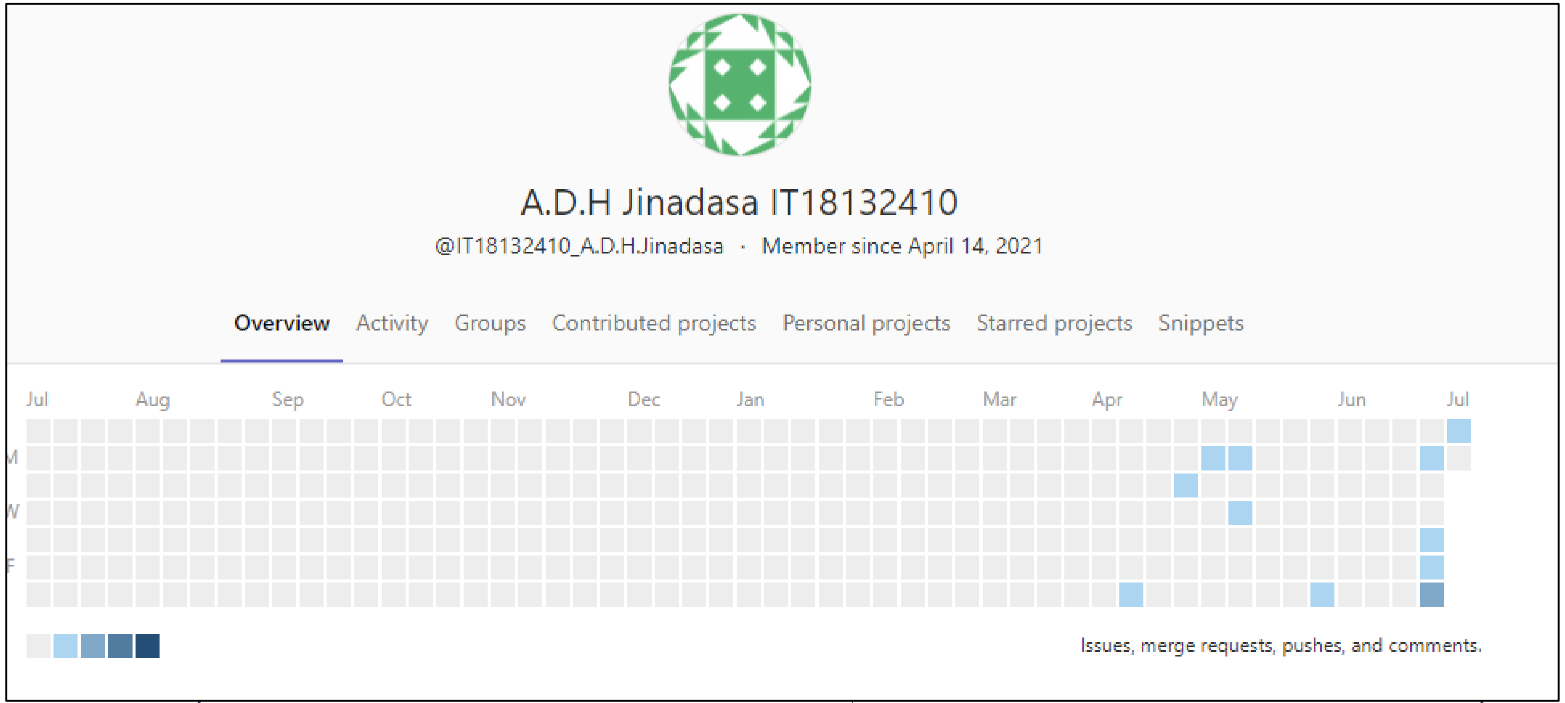


```javascript
        xhr.setRequestHeader('Content-Type', 'application/json');
        xhr.onreadystatechange = function () {
            if (xhr.readyState === 4 && xhr.status === 200) {
                console.log(xhr.responseText);
                location.reload();
            }
        };
        var data = JSON.stringify(JSON.parse(text));
        xhr.send(data);

}

function updateList(){

        fetch('https://localhost:5000/v1/api/list/')
        .then(response => response.json())
        .then(data => {
                var numList = Object.keys(data).length;
                var i;
                for(i=0;i<numList;i++){
                        var tbodyRef = document.getElementById('list').getElementsByTagName('tbody')[0];
                        var newRow = tbodyRef.insertRow();
                        var numEle = Object.keys(data[i]).length;
                        var newCell = newRow.insertCell();
                        var newText = document.createTextNode(data[i].chain);
                        newCell.appendChild(newText);
                        newCell = newRow.insertCell();
```

Completion of the project

Anuka Jinadasa
IT18132410

- Gitlab commits



A.D.H Jinadasa IT18132410

@IT18132410_A.D.H.Jinadasa · Member since April 14, 2021

Issues, merge requests, pushes, and comments.

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.	In Progress
Test implemented security measures.	Not Started

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

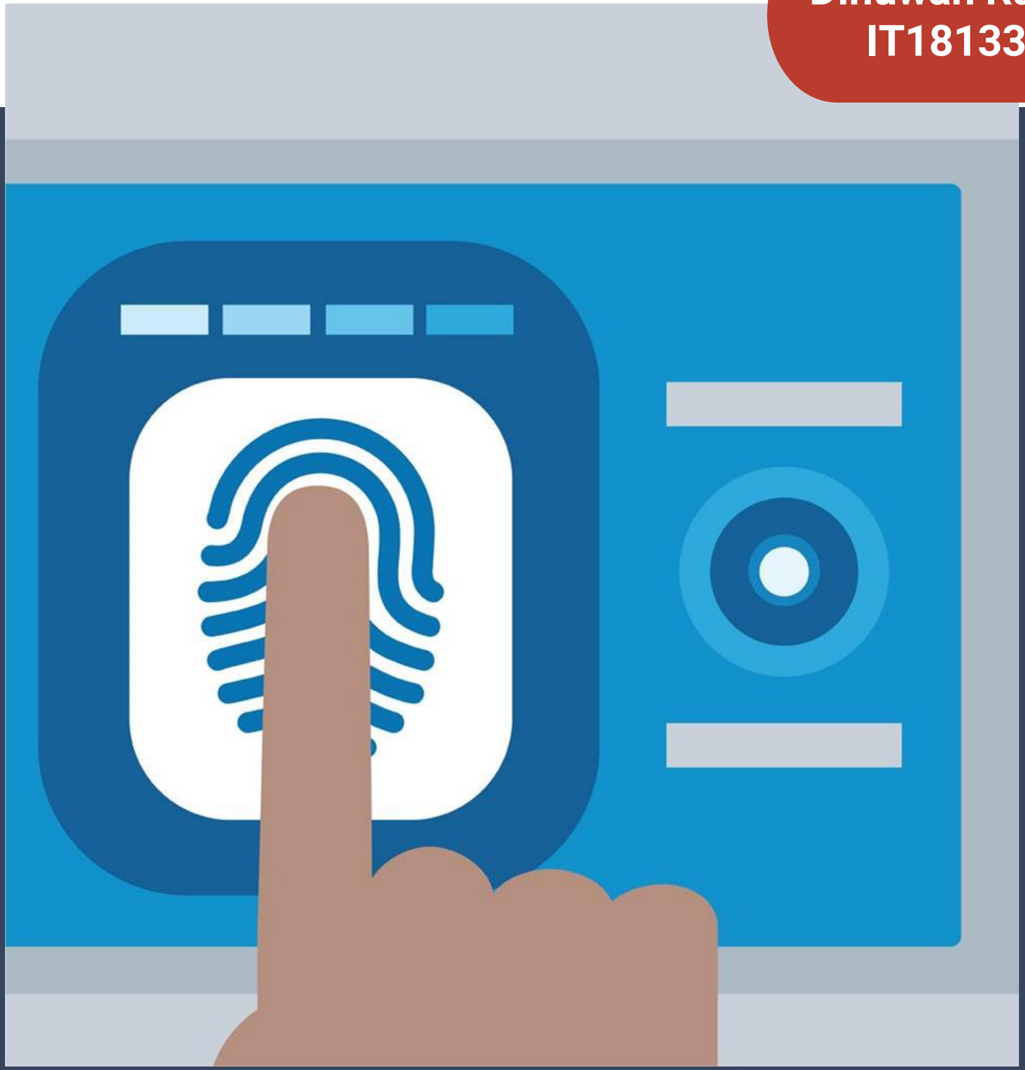
Research Question

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.

Sub Objectives :

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

Methodology

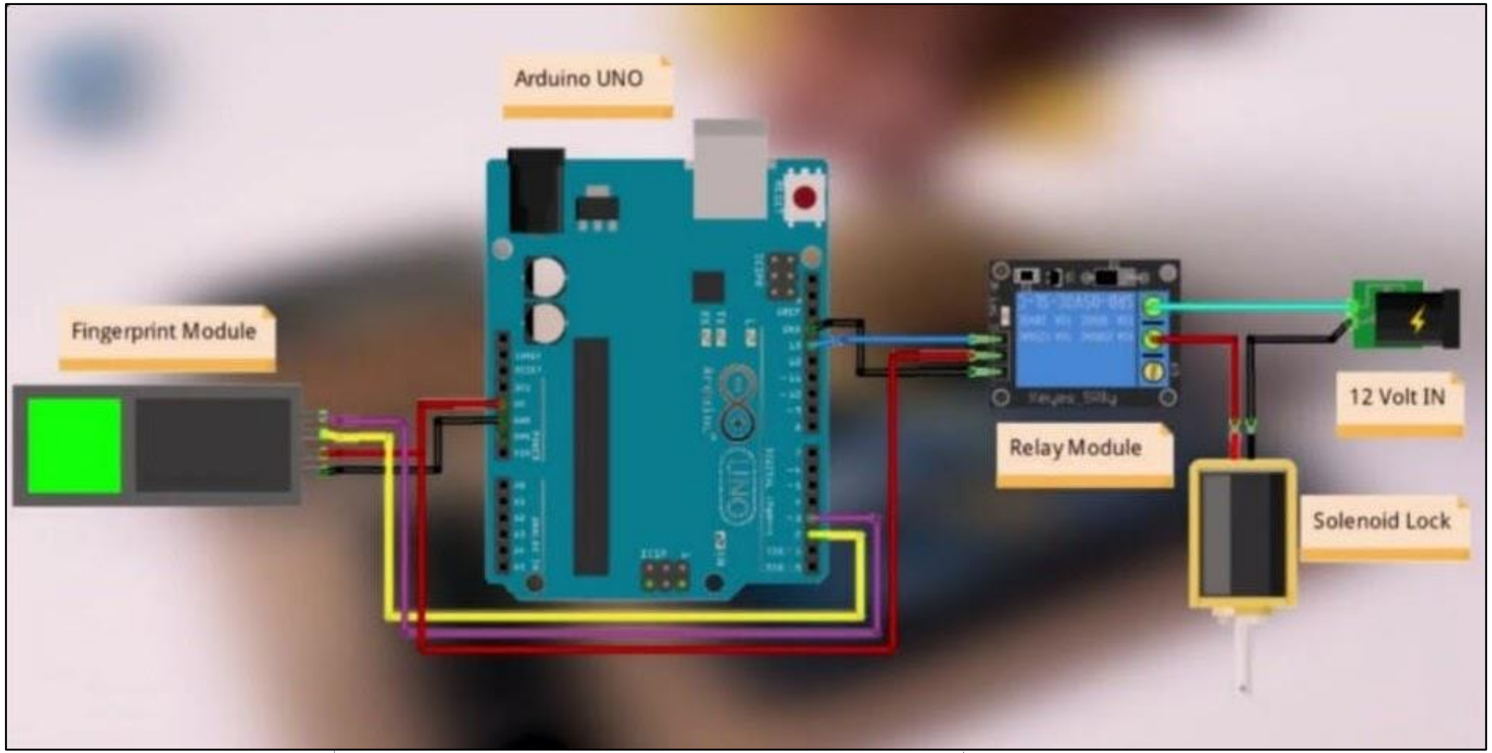
Dinuwan Randunu
IT18133578

Platform - Arduino

IDE – Arduino IDE

Language – C++

Risk Assessment - Octave

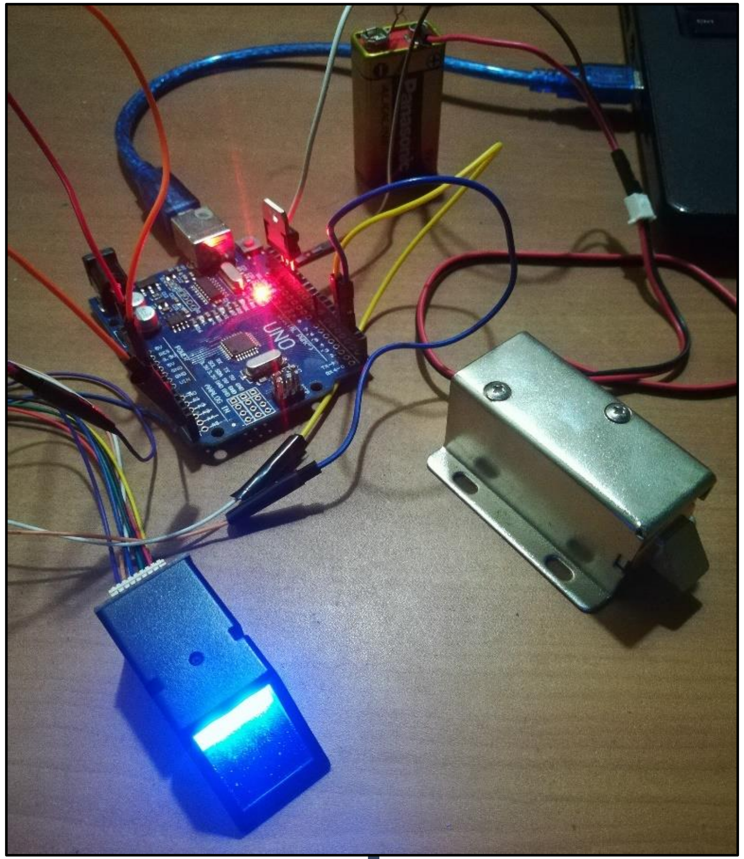


Completion of the project

Dinuwan Randunu
IT18133578

Implement smart lock physical system

- Hardware implementation

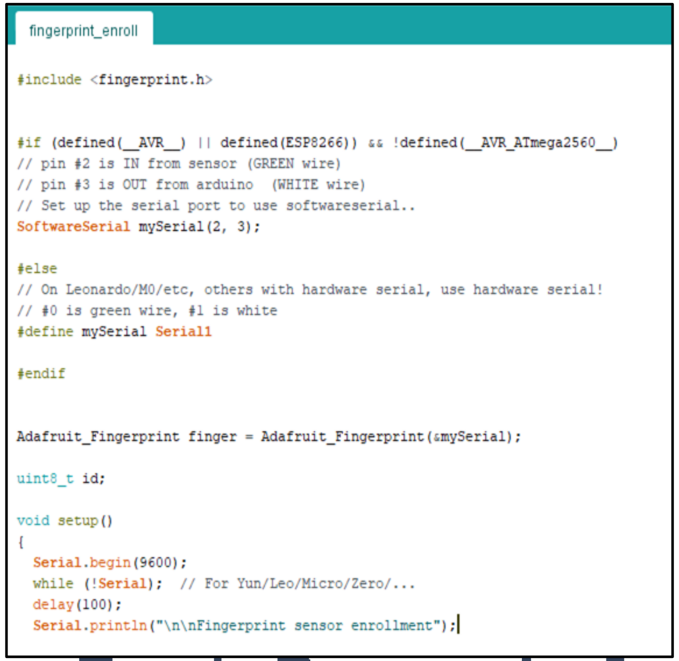


Completion of the project

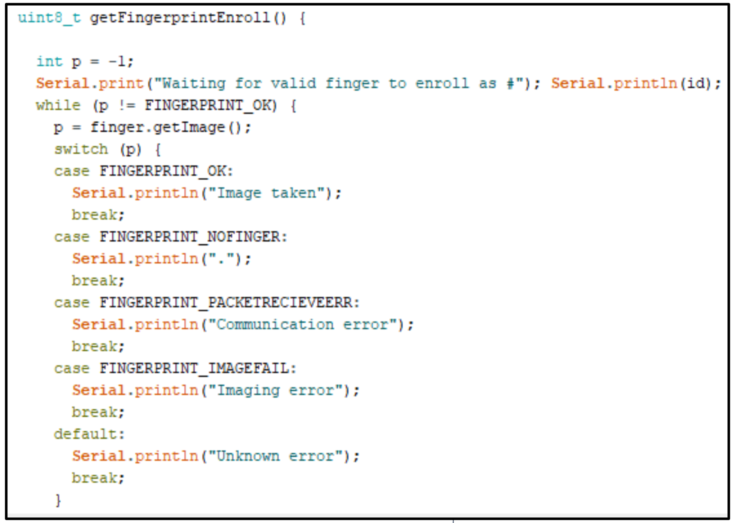
Dinuwan Randunu
IT18133578

Implement smart lock physical system

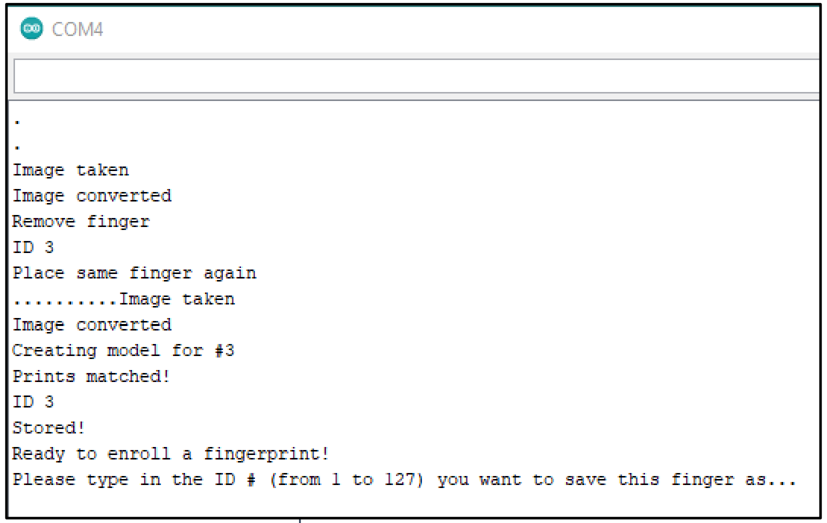
- Software implementation
- Fingerprint enrollment



```
#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;
    }
```



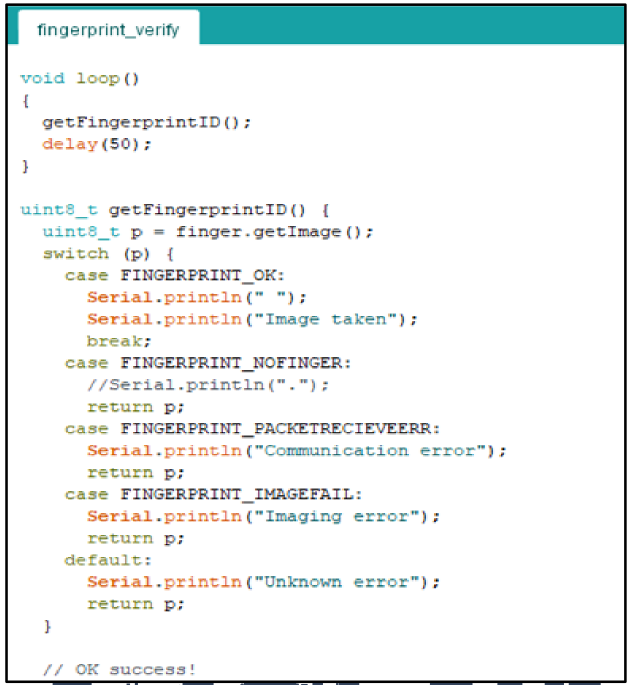
```
.
.
Image taken
Image converted
Remove finger
ID 3
Place same finger again
..........Image taken
Image converted
Creating model for #3
Prints matched!
ID 3
Stored!
Ready to enroll a fingerprint!
Please type in the ID # (from 1 to 127) you want to save this finger as...
```

Completion of the project

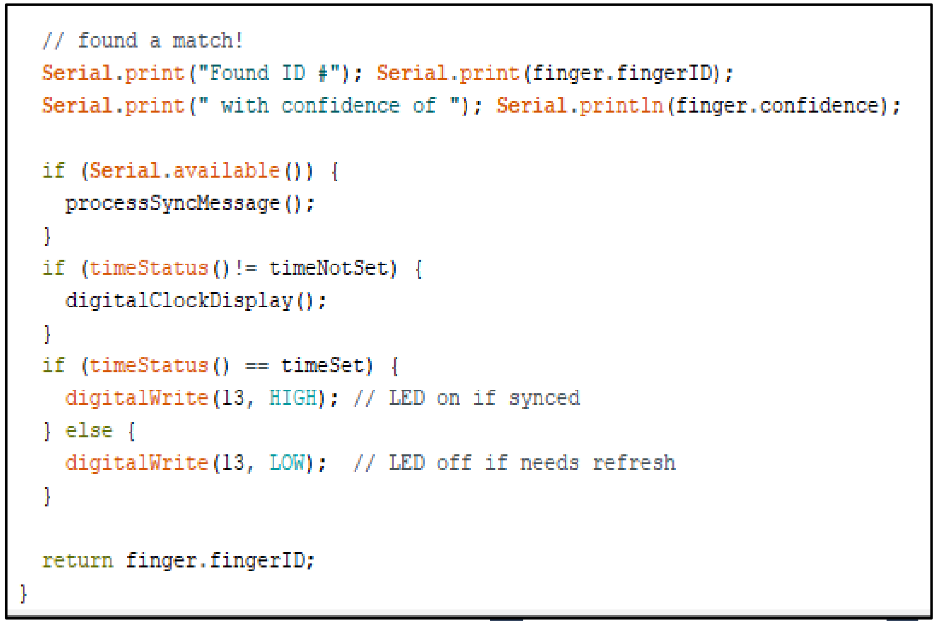
Dinuwan Randunu
IT18133578

Implement smart lock physical system

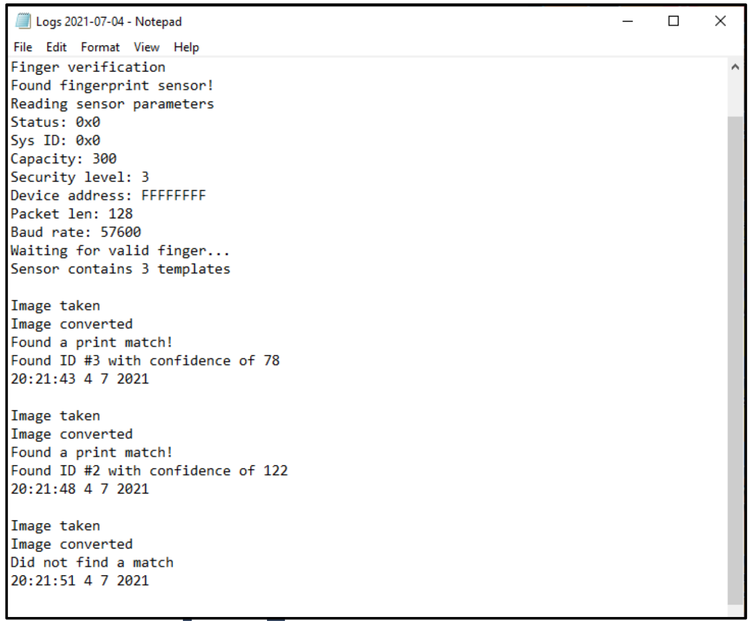
- Software implementation
- Fingerprint Verification



```
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;
}
```

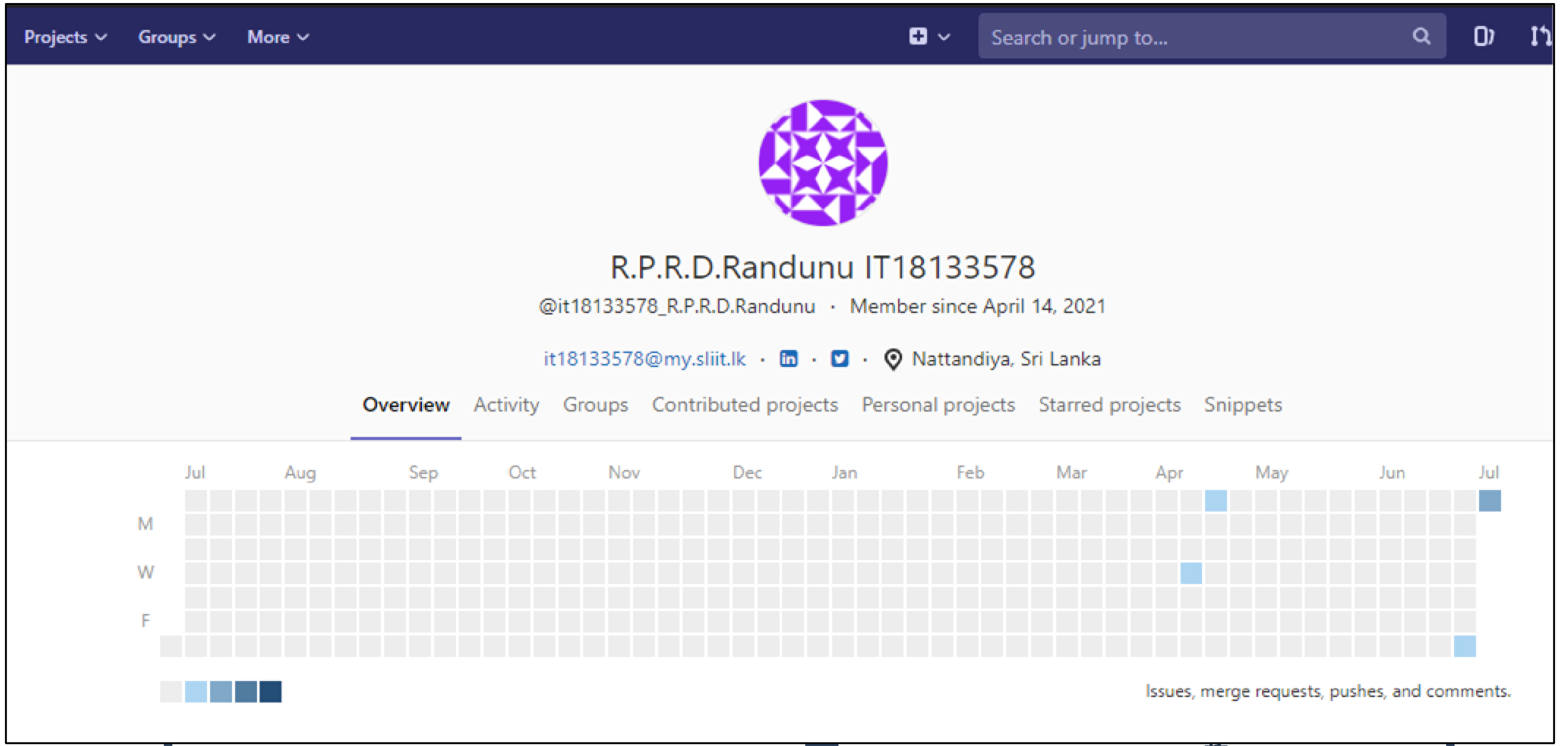


```
Finger verification
Found fingerprint sensor!
Reading sensor parameters
Status: 0x0
Sys ID: 0x0
Capacity: 300
Security level: 3
Device address: FFFFFFFF
Packet len: 128
Baud rate: 57600
Waiting for valid finger...
Sensor contains 3 templates

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

- Gitlab commits



R.P.R.D.Randunu IT18133578

@it18133578_R.P.R.D.Randunu · Member since April 14, 2021

it18133578@my.sliit.lk · · · Nattandiya, Sri Lanka

Issues, merge requests, pushes, and comments.

Completion of the project

Dinuwan Randunu
IT18133578

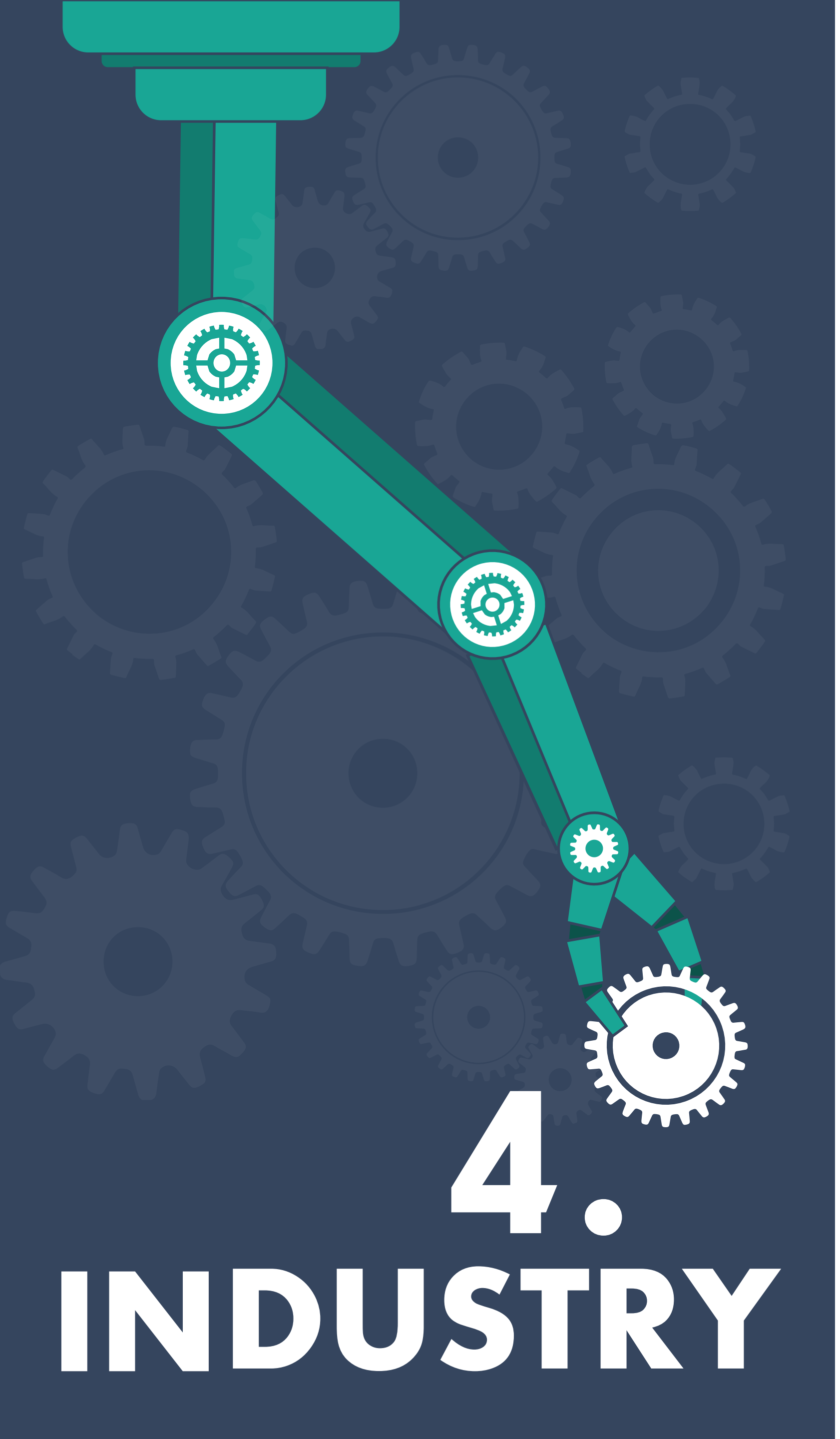
TASK	STATUS
Identify required devices industrial 4.0 manufacturing system	Complete
Identify security requirements and evaluate them	Complete
Analysis of network accessibility and physical accessibility	Complete
Implement smart lock physical system - Hardware implementation	In Progress
Implement smart lock physical system - Software implementation	In Progress
Implement login system for access and activity monitor	Not Started
Report generation	Not Started
Test implemented security measures	Not Started
Integration with the final product	Not Started

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

INDUSTRY 4.0

Thank You