Cyber security automation for an industrial 4.0 garment manufacturing system

2021-11

Our Team

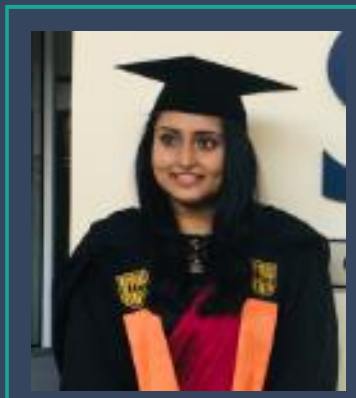
Dasunpriya Kalhara
IT18139440
Cyber Security

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



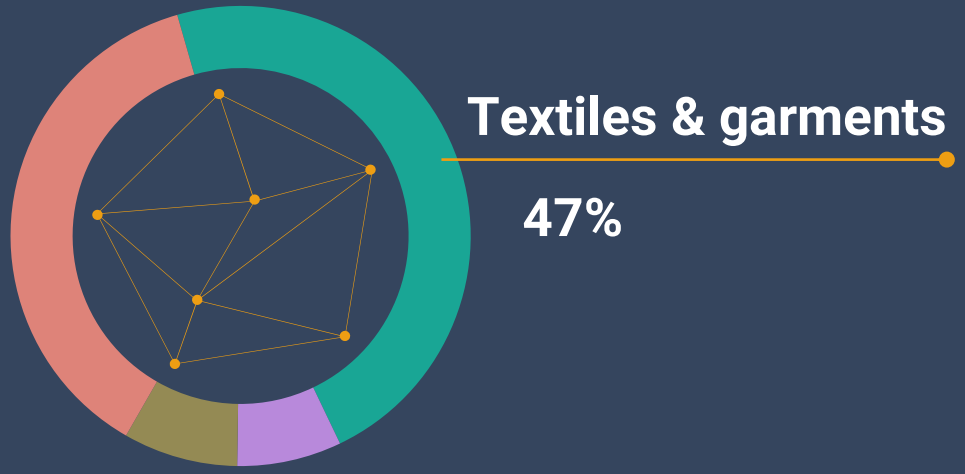
Co - Supervisor
Ms. Wellalage Sasini Nuwanthika

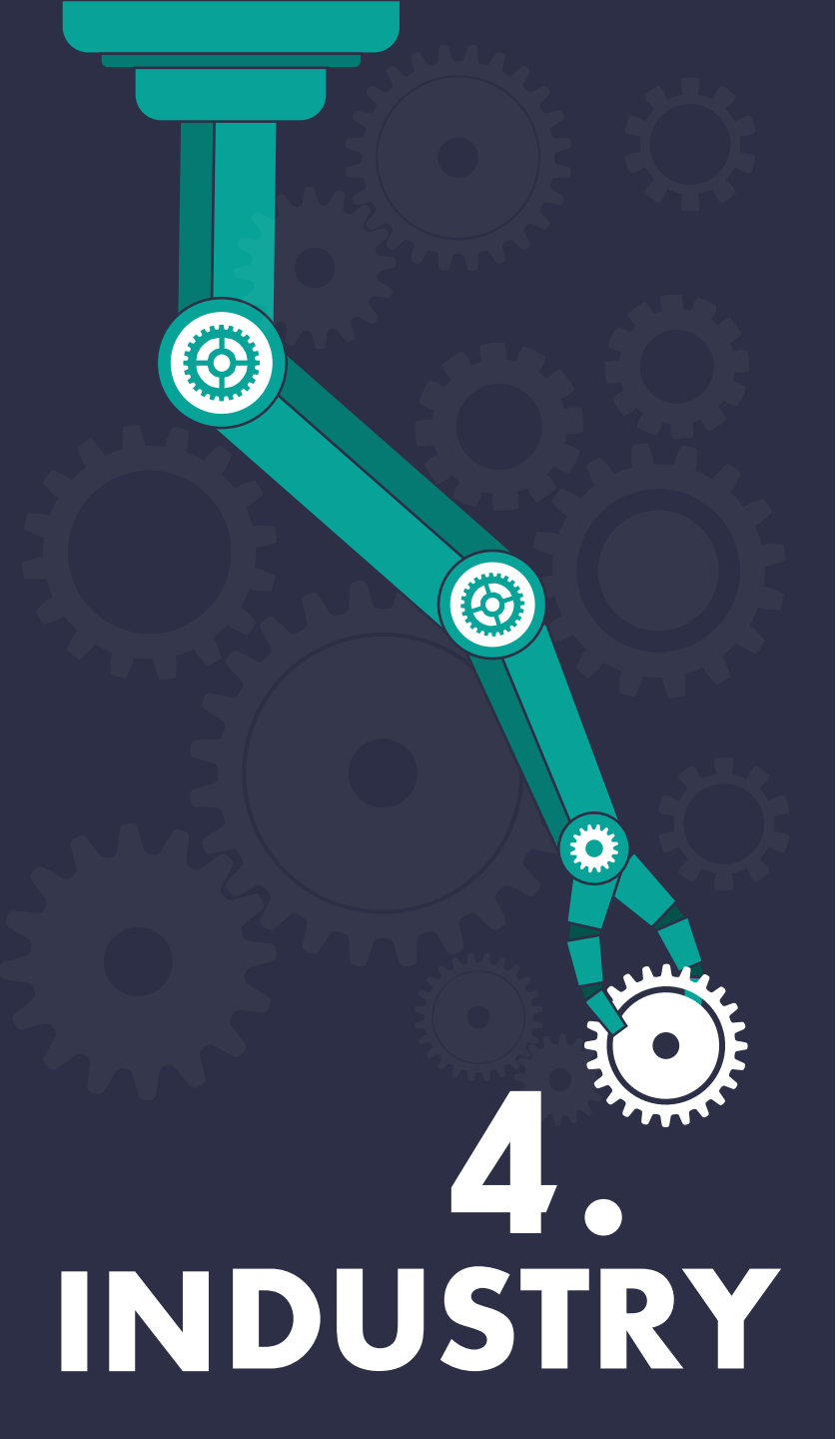
External – Supervisor
Mr. Gamini De Alwis

Introduction

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

- **Why Garment Industry ?**





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

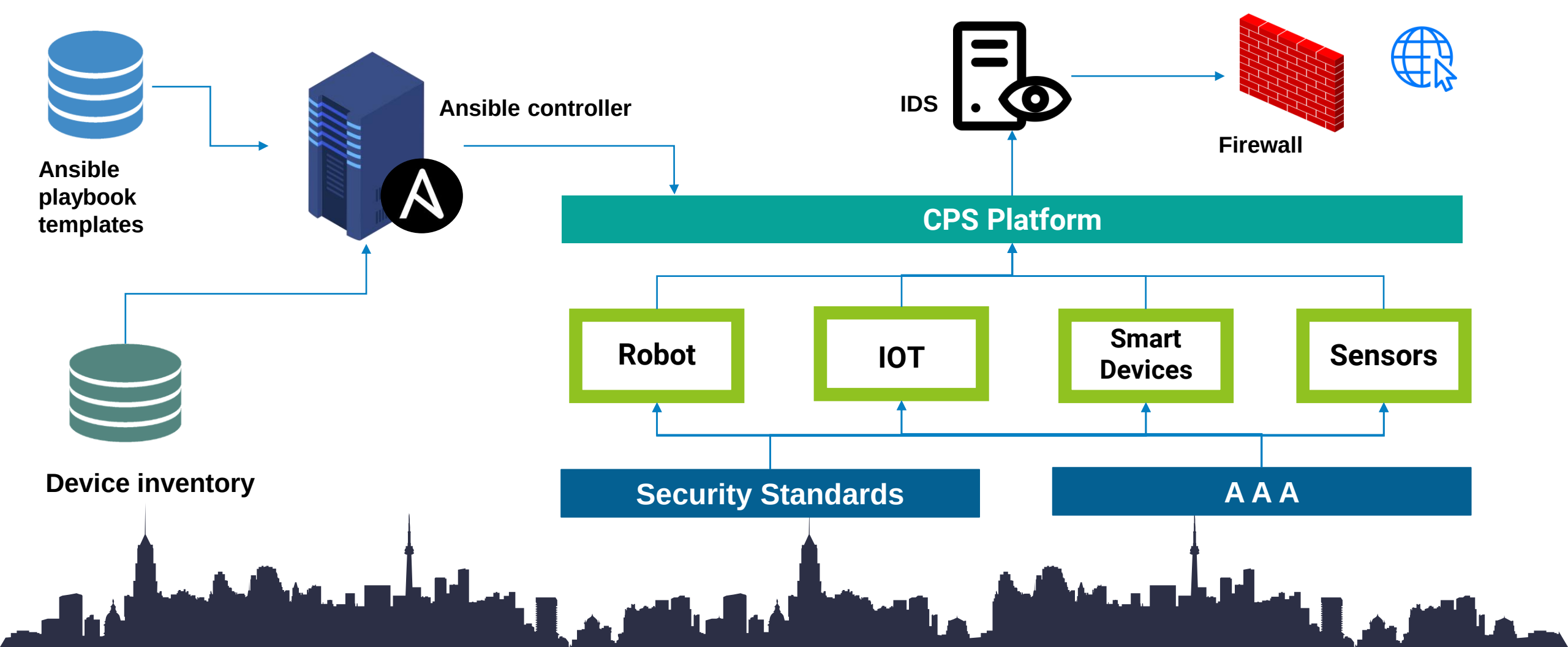
Authentication & access monitoring

Security updates

Security configurations

Intrusion Detection

Overall System Diagram



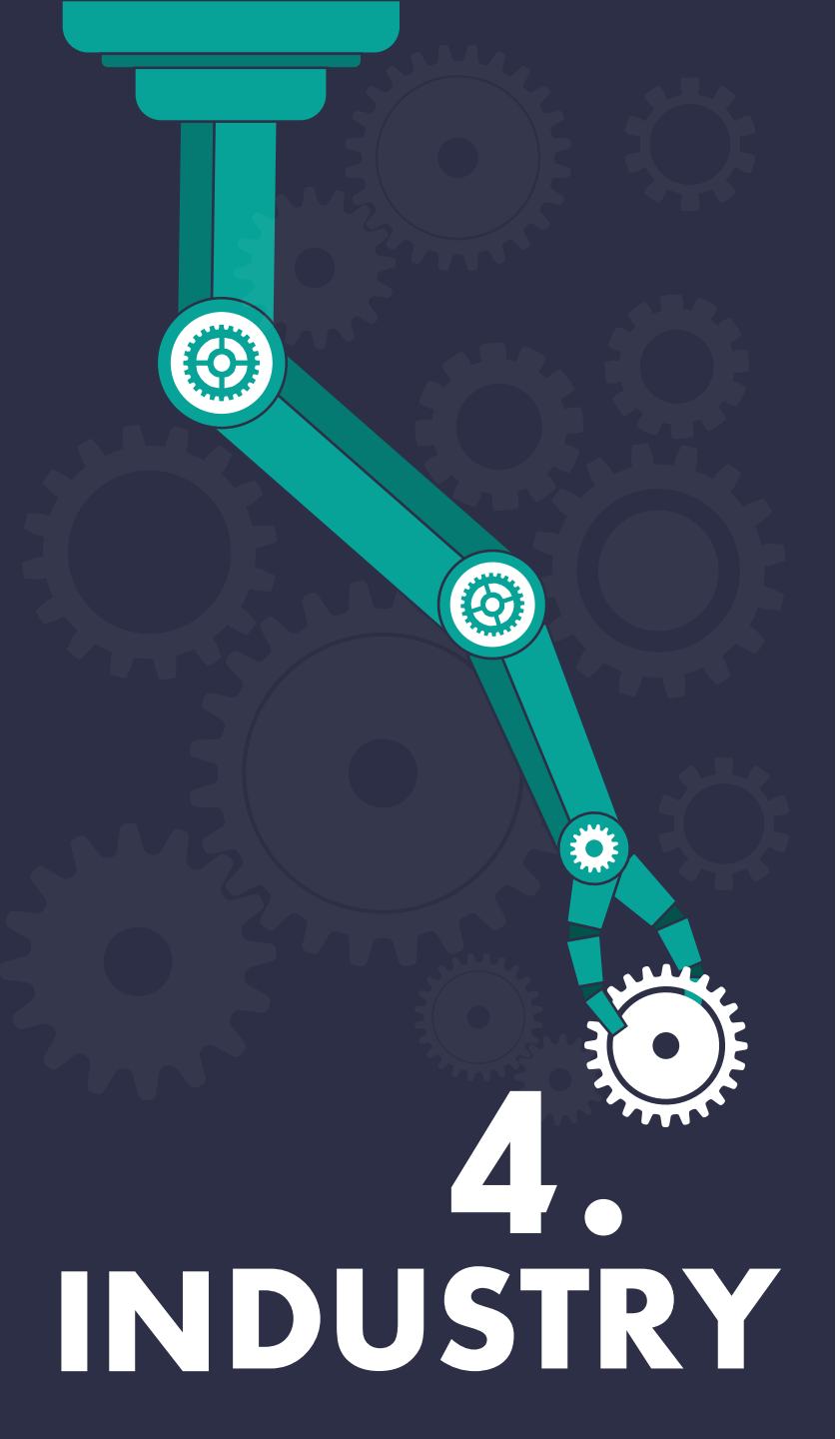
Dasunpriya Kalhara

IT18139440

Cyber Security

Dasunpriya Kalhara
IT18139440

Introduction



Background

Dasunpriya Kalhara
IT18139440

Insecure Default Settings

Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations [1].

Research Gap

	SCAP Workbench [2]	CIS-CAT Pro [3]	Proposed Tool
Ubuntu Linux	✗	✓	✓
Robot OS	✗	✗	✓
Raspberry OS	✗	✗	✓

Research Question

Dasunpriya Kalhara
IT18139440

How can we Automate Security configuration for CPS devices?

Specific & Sub Objectives

Dasunpriya Kalhara
IT18139440

Specific Objective :

A tool for Automating security configurations

Sub Objectives :

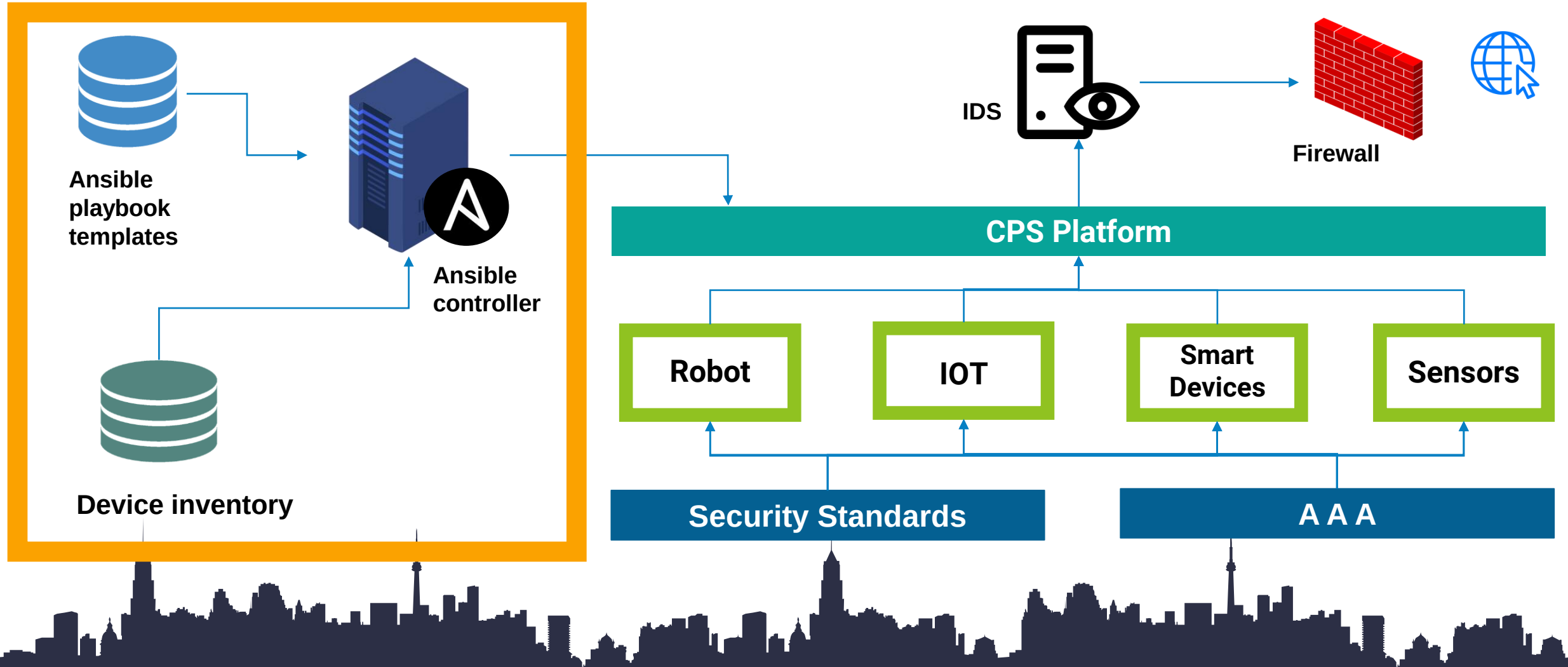
- Audit security configurations
- Centralized device configuration management
- Generate Audit reports

Dasunpriya Kalhara
IT18139440

RESEARCH METHODOLOGY

System Diagram

Dasunpriya Kalhara
IT18139440



Technologies, techniques & algorithms

Dasunpriya Kalhara
IT18139440

Software specification

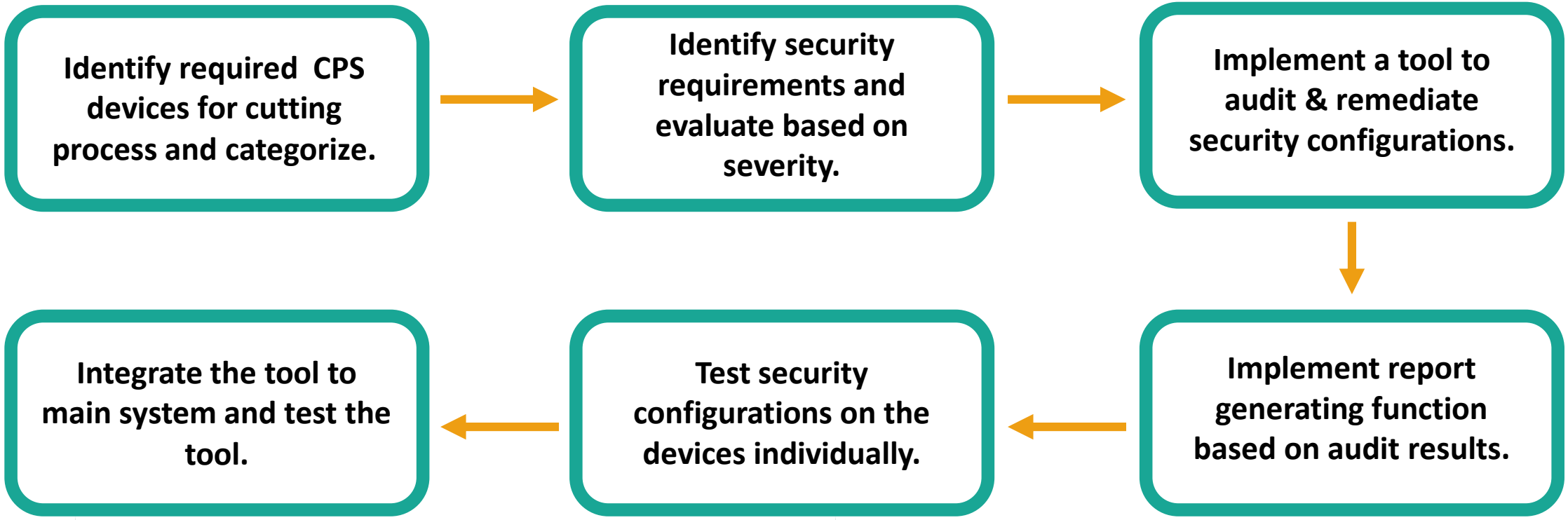
Dasunpriya Kalhara
IT18139440

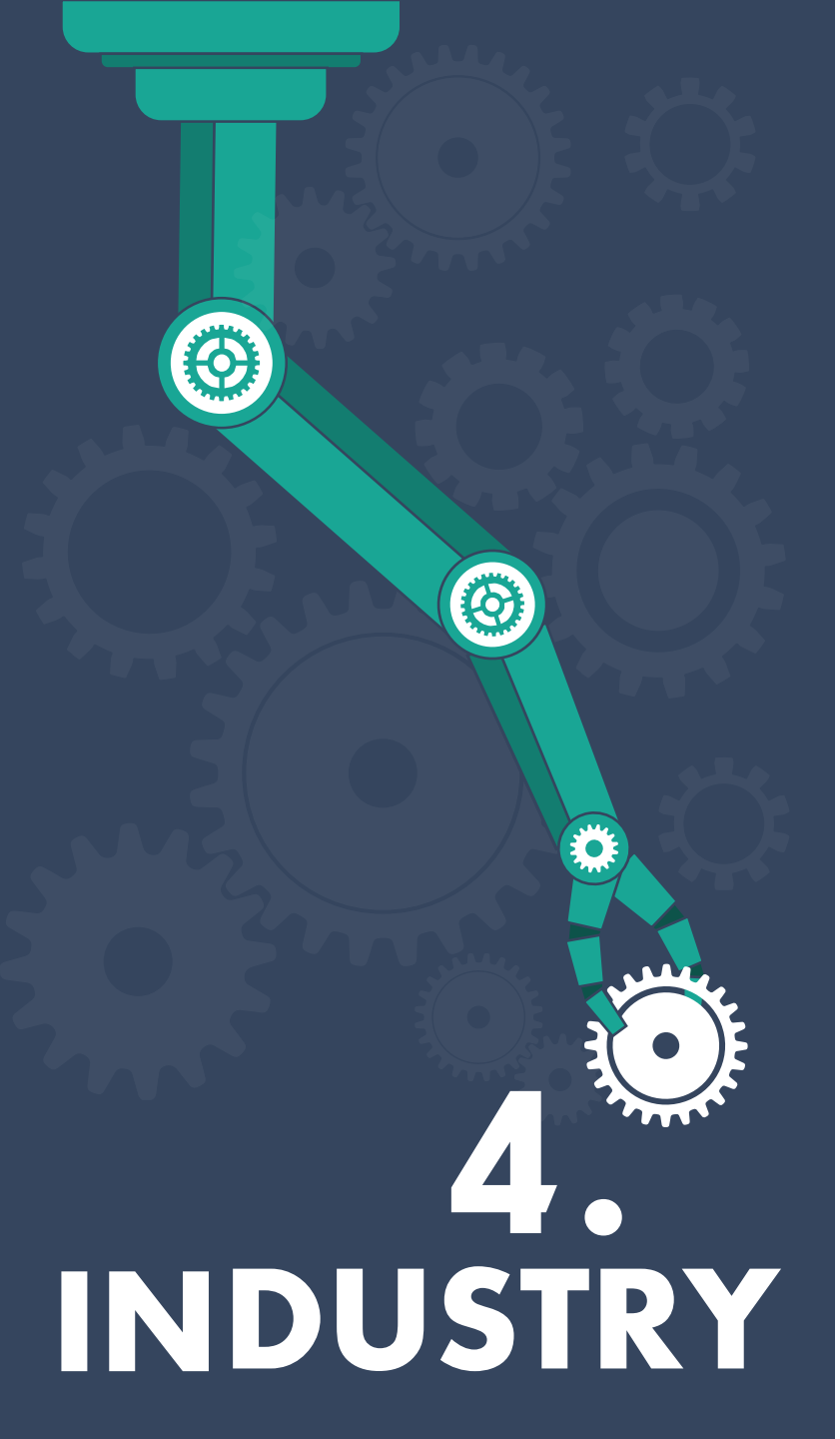
Requirements

- A Python tool to automate security configurations.
- Add new audit and remediations to the python tool.
- Select and deselect remediations to create optimize compliance profile based on resource usage of the devices.
- A report generating function to generate audit reports.

Work Breakdown Structure

Dasunpriya Kalhara
IT18139440





Dasunpriya Kalhara
IT18139440

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.

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] “SCAP Workbench | OpenSCAP portal.” https://www.open-scap.org/tools/scap-workbench/ (accessed Mar. 06, 2021).

•[3] “CIS Benchmarks™,” CIS. https://www.cisecurity.org/cis-benchmarks/ (accessed Mar. 06, 2021).

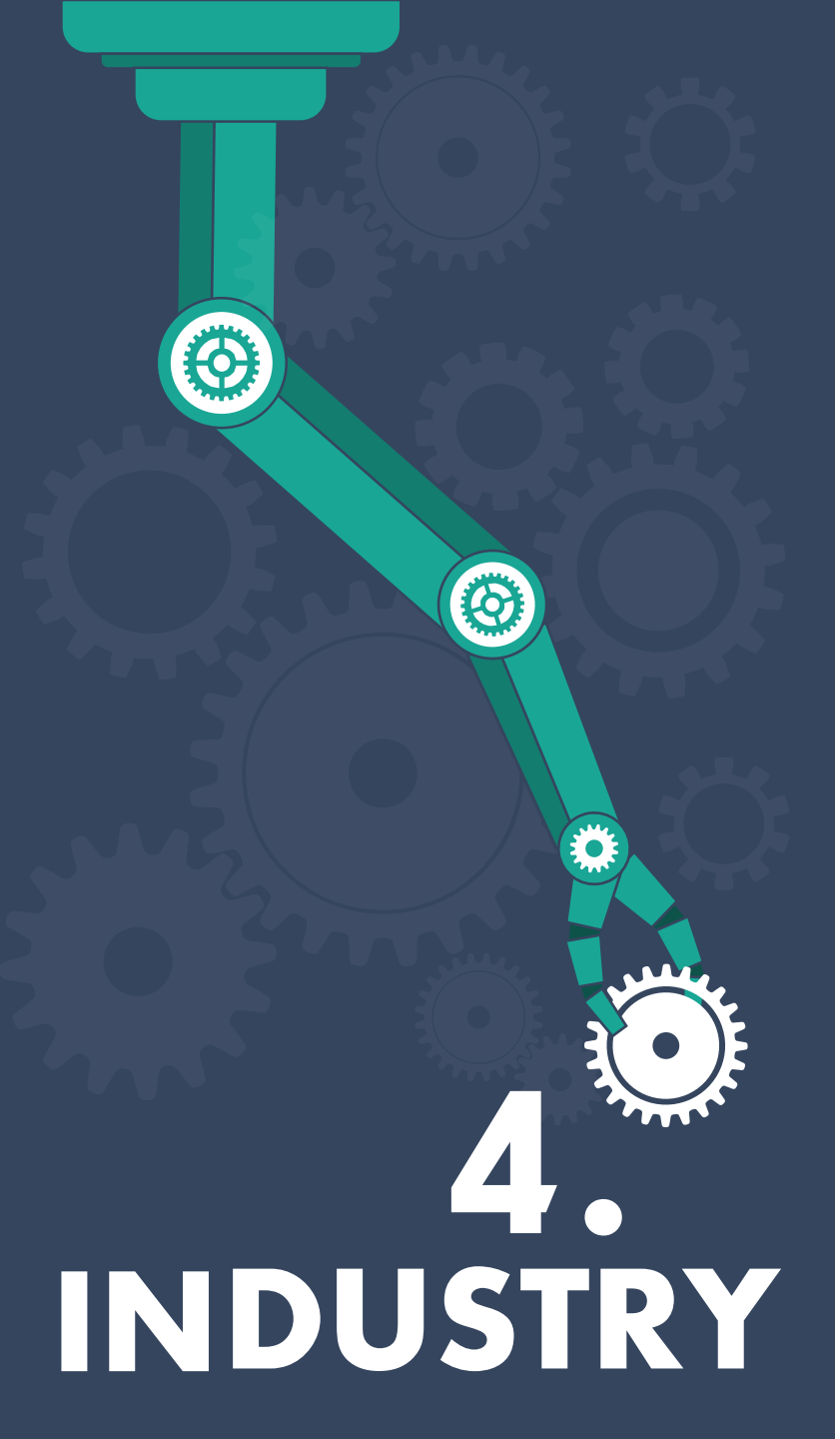
Udara De Alwis

IT18136098

Cyber Security

Udara De Alwis
IT18136098

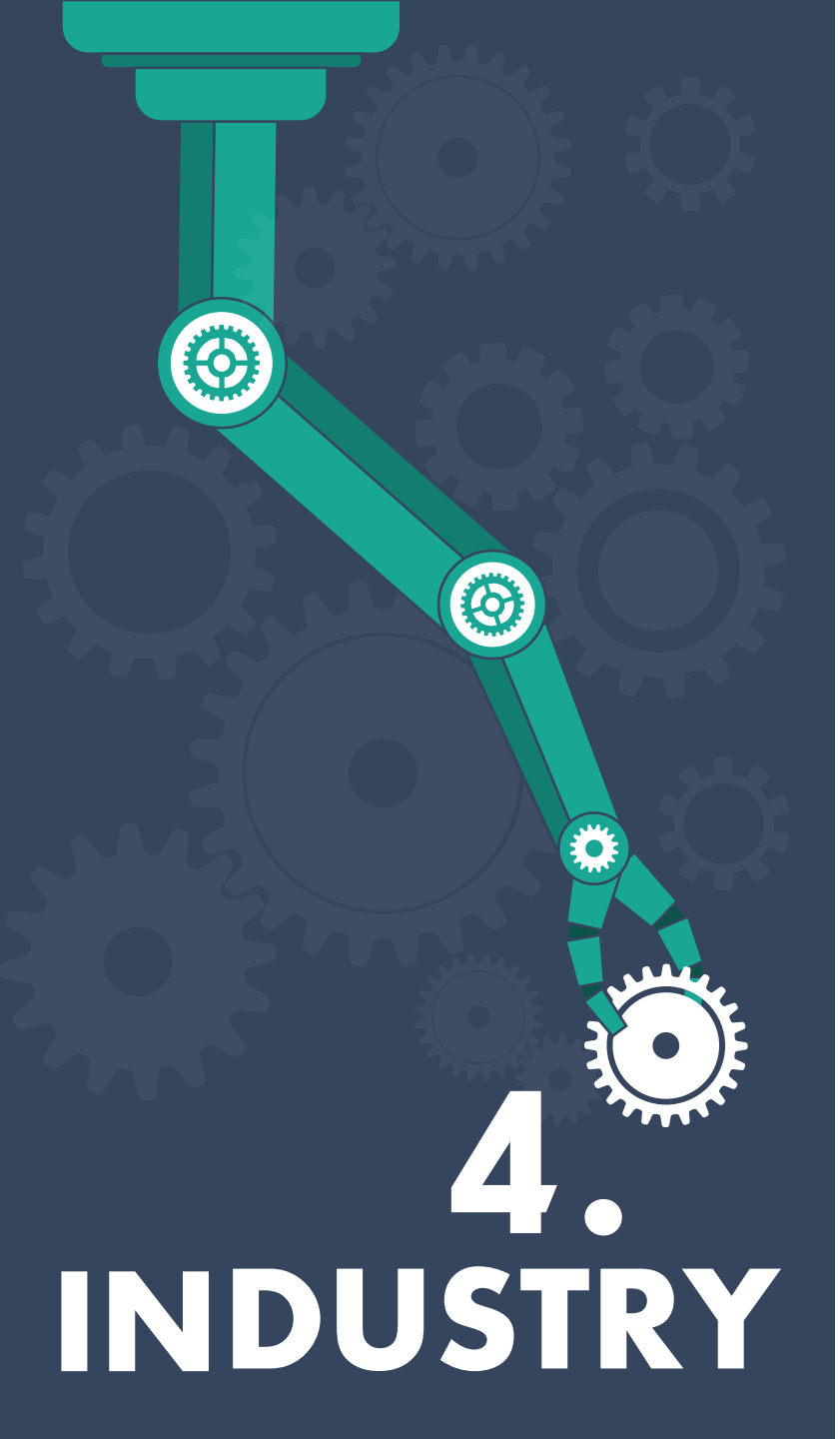
Introduction



Background

Udara De Alwis
IT18136098

- Manufacturing standards, are a challenge that IoT has to overcome. Manufacturers do not spend enough effort and resources on security[1].
- They are very industry specific and mostly just suggested best practices.
- IoT Devices lack having guidance for security policy enforcement.
- Policies are not been focused to enforce in the design stage.
- Lack of compliance.[1]
- Lack of secure update mechanism.[1]



Background cont'd

Udara De Alwis
IT18136098

Research Gap

- Industrial 4.0 automation is driven by focusing on the functionality and SAM/SMV(Standard Allowed Minute/ Standard Minute Value) rather than security.
- There are few IoT security frameworks in various stages of development. (ETSI(European Telecommunications Standards Institue)EN 303 645, IoT Security Compliance Framework, OWASP ISVS, ENISA, NIST)[2][3].

- Comparison of the security standards and best practices for the different industrial automation domains are available.[4]
- There hasn't been a powerful enough push to make universal IoT security standards.

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 :

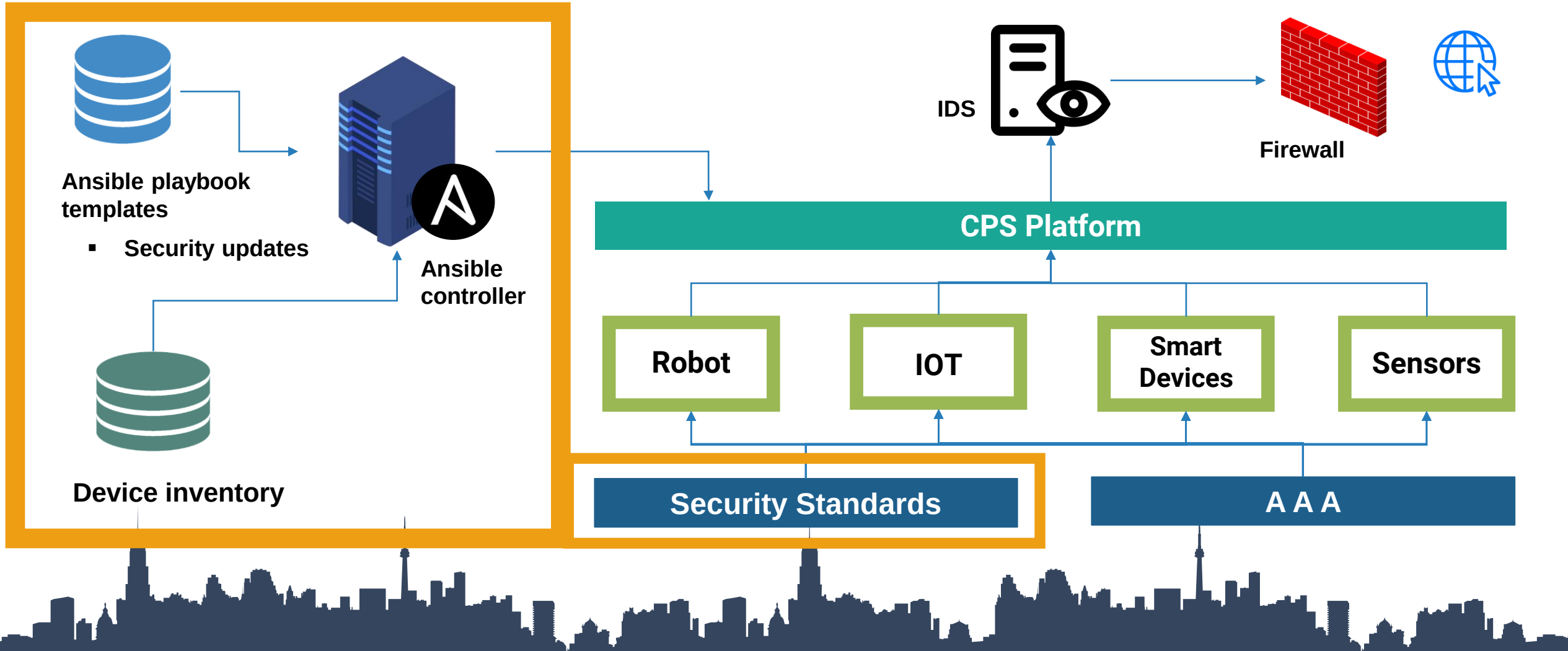
- Password policy creation
- Access policy creation
- Firewall policy creation
- Acceptable use policy creation
- Update policy implementation

Udara De Alwis
IT18136098

RESEARCH METHODOLOGY

System Diagram

Udara De Alwis
IT18136098



Technologies, techniques & algorithms

Udara De Alwis
IT18136098

Techniques

- NIST
- ENISMA

Requirements

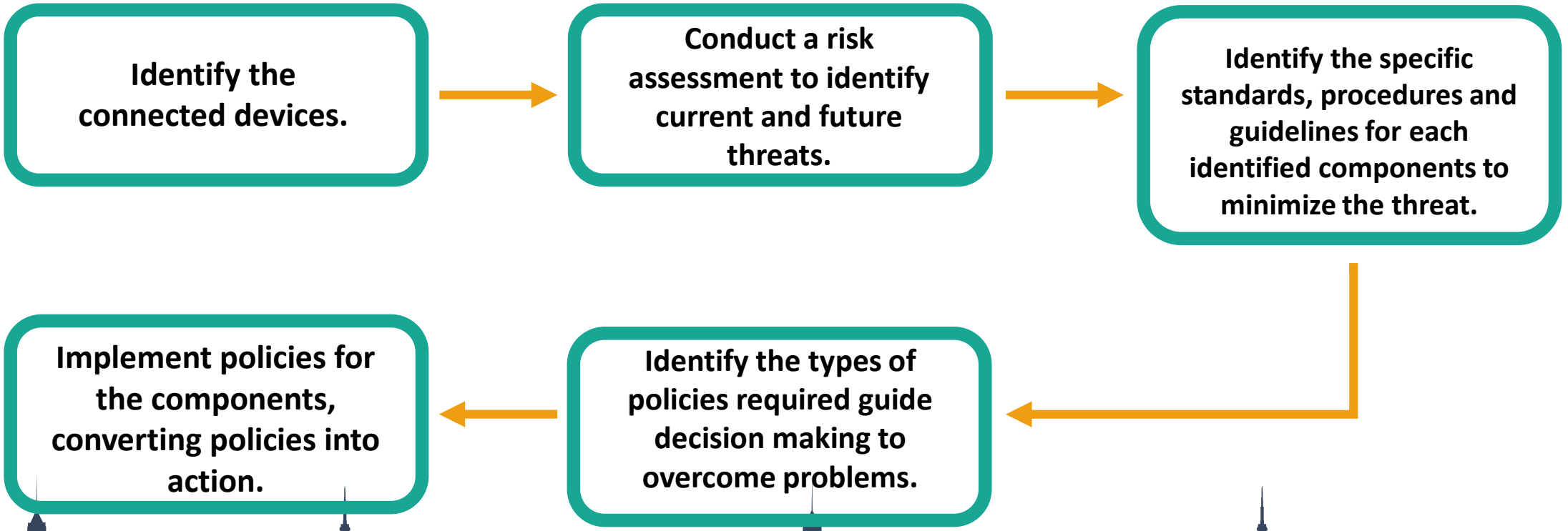
Udara De Alwis
IT18136098

- Meeting Stakeholder requirements.
- Risk identification and assessment.
- Security policy development and privacy by design.
- Hardware root of trust.

Work Breakdown Structure

Udara De Alwis
IT18136098

❖ **Security standards and policy development**

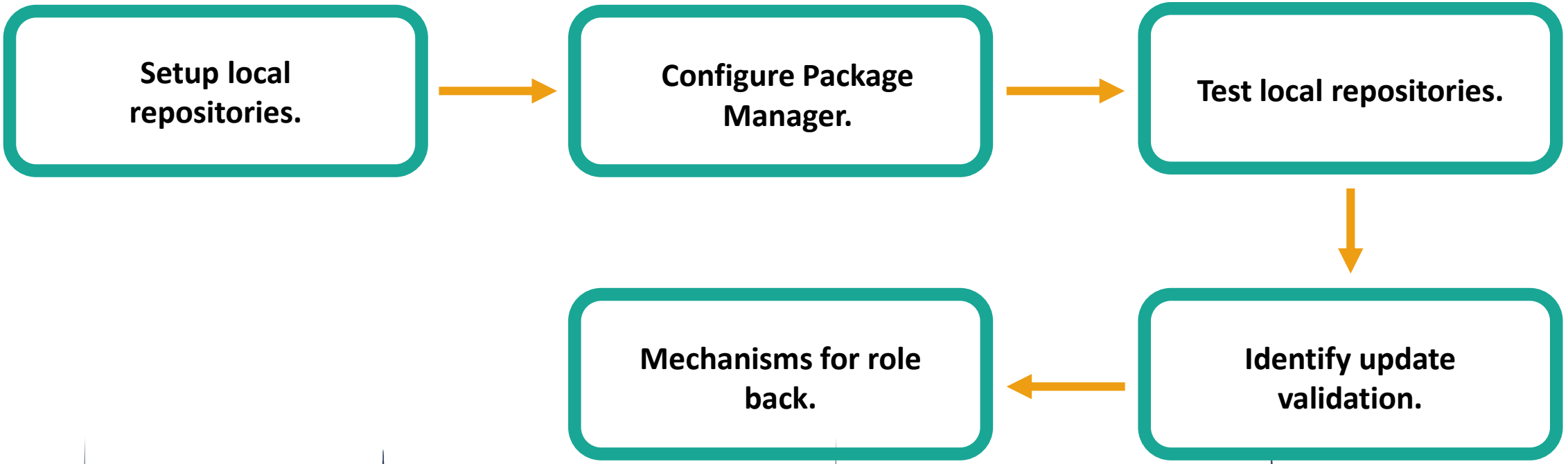


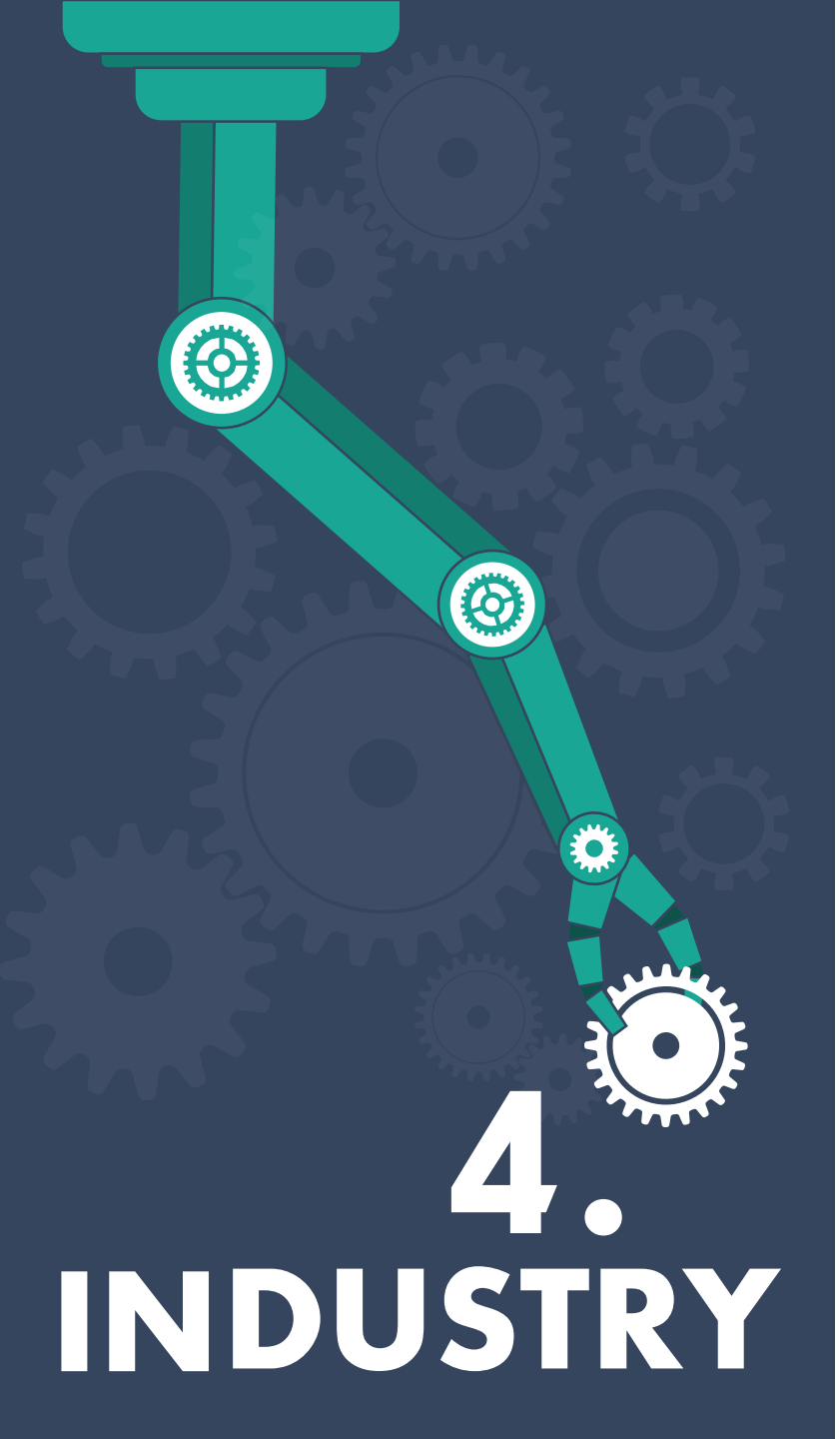
Work Breakdown Structure

cont'd

Udara De Alwis
IT18136098

- **Update management**





Udara De Alwis
IT18136098

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.

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.

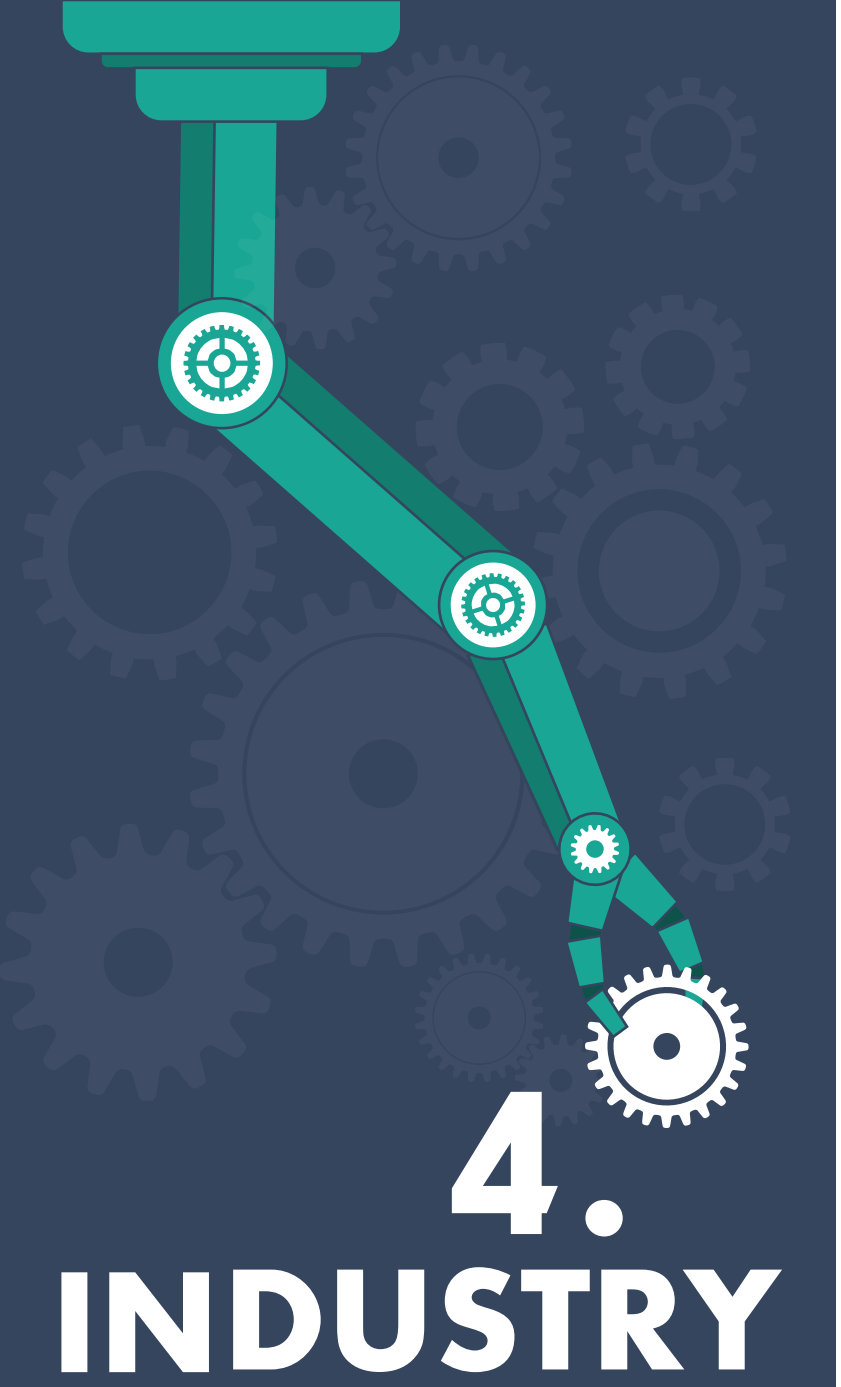
Anuka Jinadasa

IT18132410

Cyber Security

Anuka Jinadasa
IT18132410

Introduction



Background

Anuka Jinadasa
IT18132410

- securing smart devices is not a priority for vendors.
- Commercial security solutions are expensive to establish and maintain. [1] [2]

Research Gap

	McAfee NSP [3]	Cisco Firepower	Trend Micro TippingPoint	Proposed Solution
Signature based	✓	✓	✗	✓
Anomaly based	✓	✓	✓	✓
Base Price	$10,995	$100,000	$6,000	$500

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 :

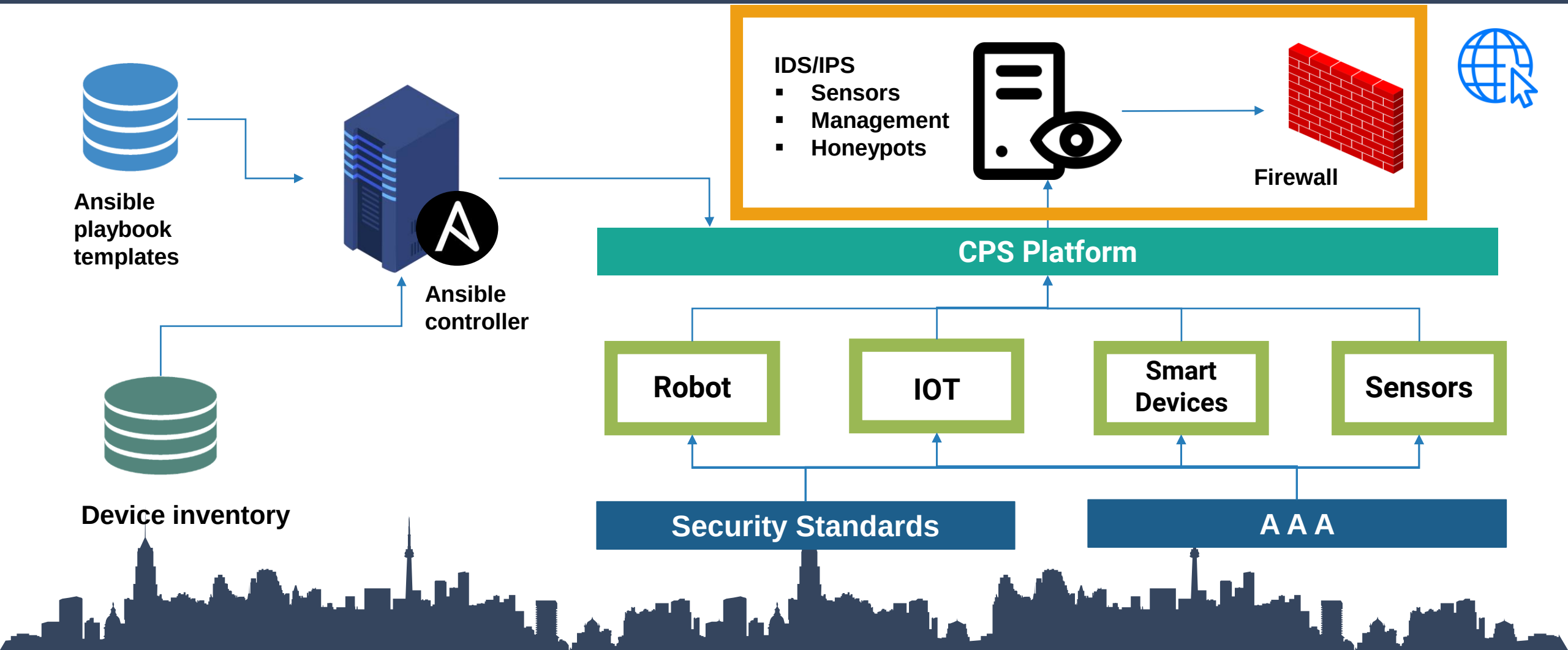
- Provide easy access dashboard to the user.
- Visualize network behavior to user.
- Enable add/ remove firewall rules through the dashboard.
- Alert user when an anomaly occurs. [1]

Anuka Jinadasa
IT18132410

RESEARCH METHODOLOGY

System Diagram

Anuka Jinadasa
IT18132410



Technologies, techniques & algorithms

Anuka Jinadasa
IT18132410

Algorithms

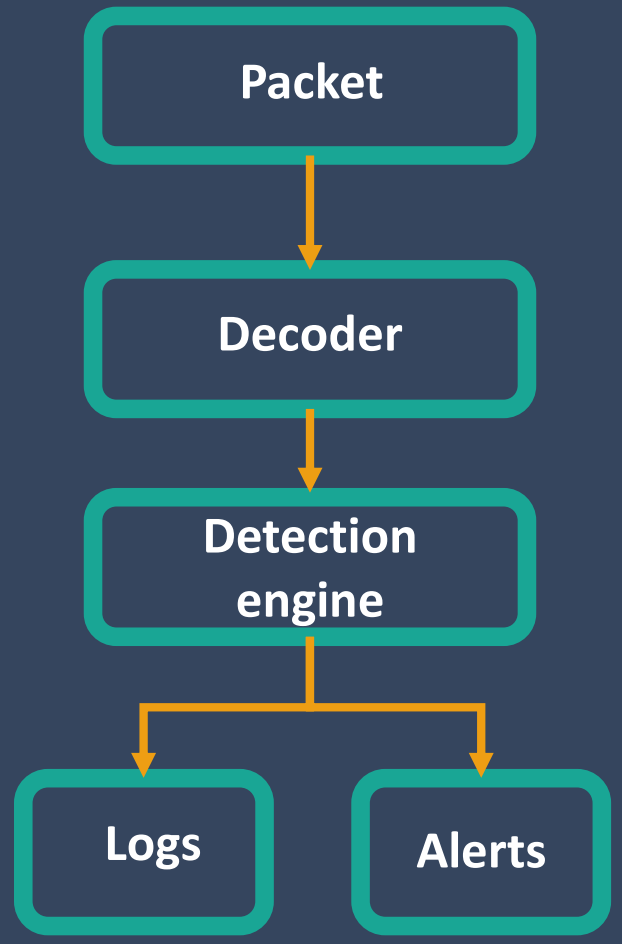
- Signature based detection
- Pattern based detection [4]

Software specification

Anuka Jinadasa
IT18132410

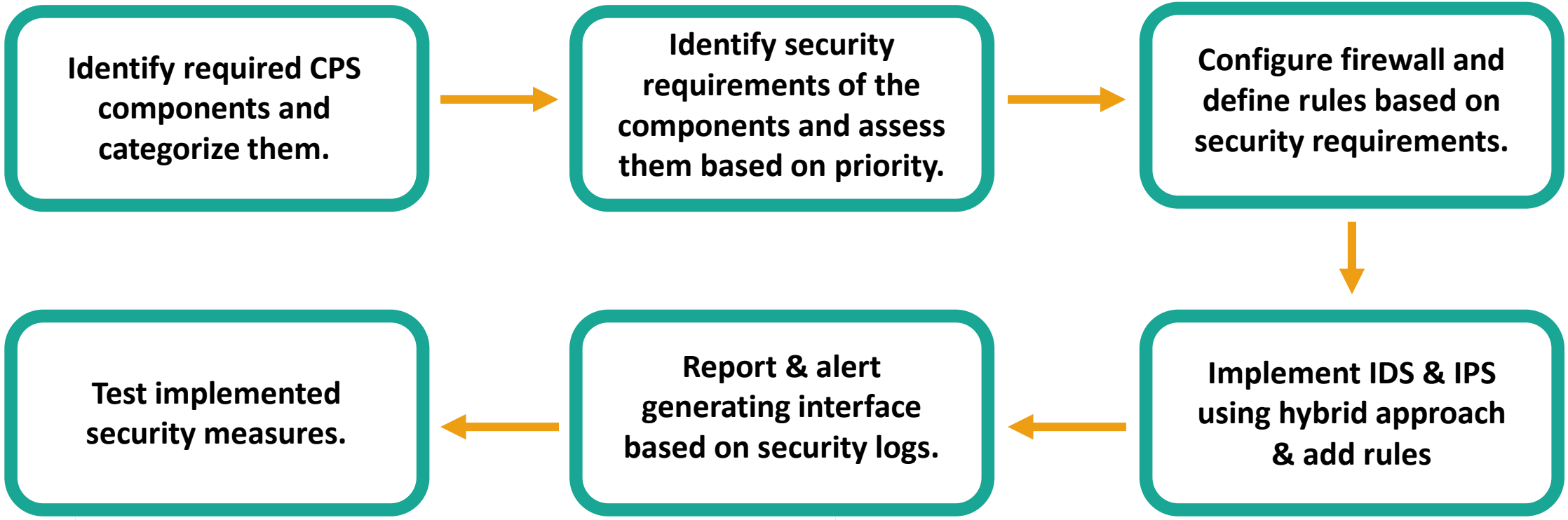
Requirements

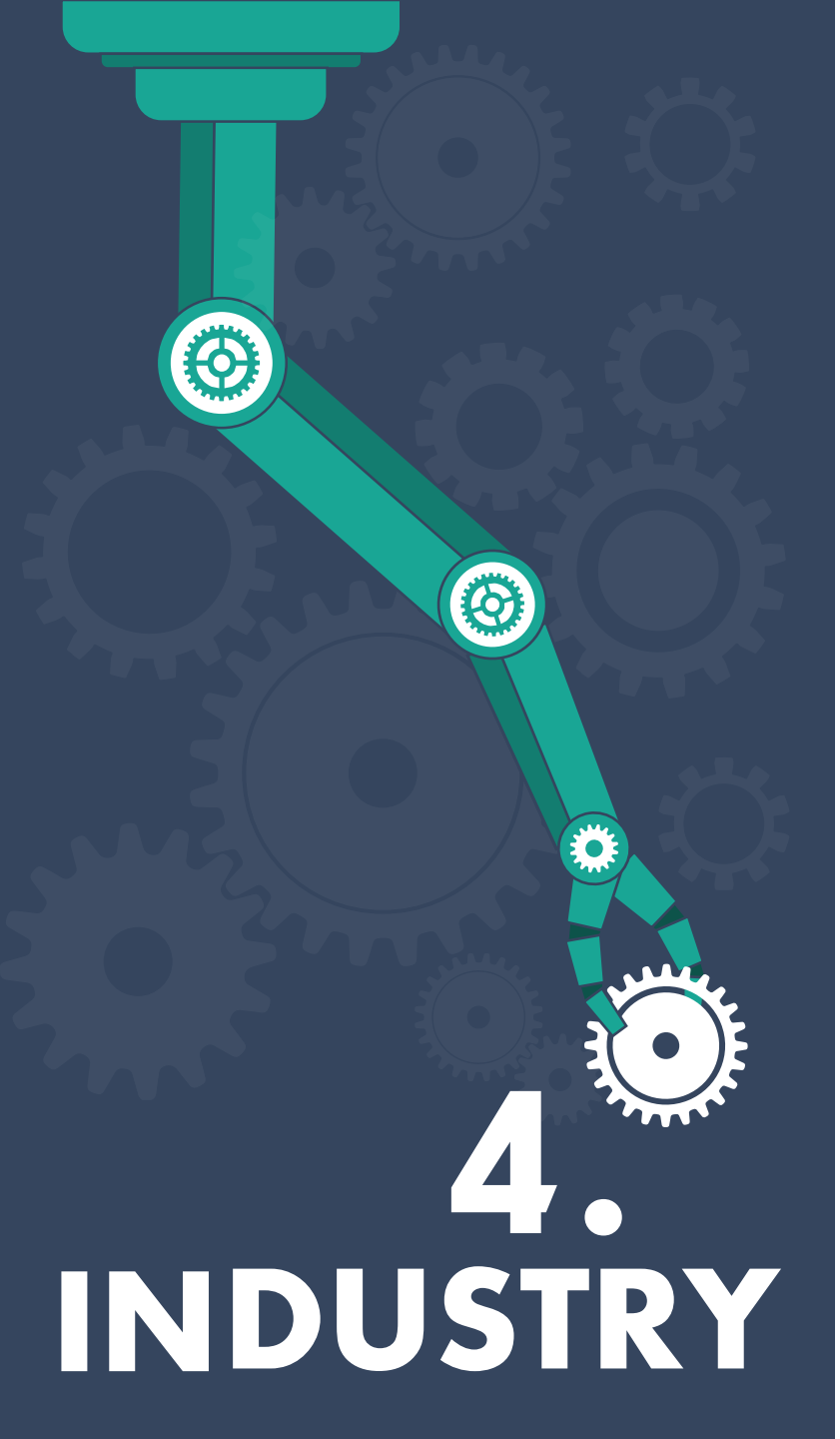
- Logging & alerting network behavior
- Packet decoder & Detection engine
- Visualize network behavior via dashboard.
- Add/ remove firewall rules via dashboard.
- Minimize false positive & false negative.
- Configure according to the security policies



Work Breakdown Structure

Anuka Jinadasa
IT18132410





Anuka Jinadasa
IT18132410

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.

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

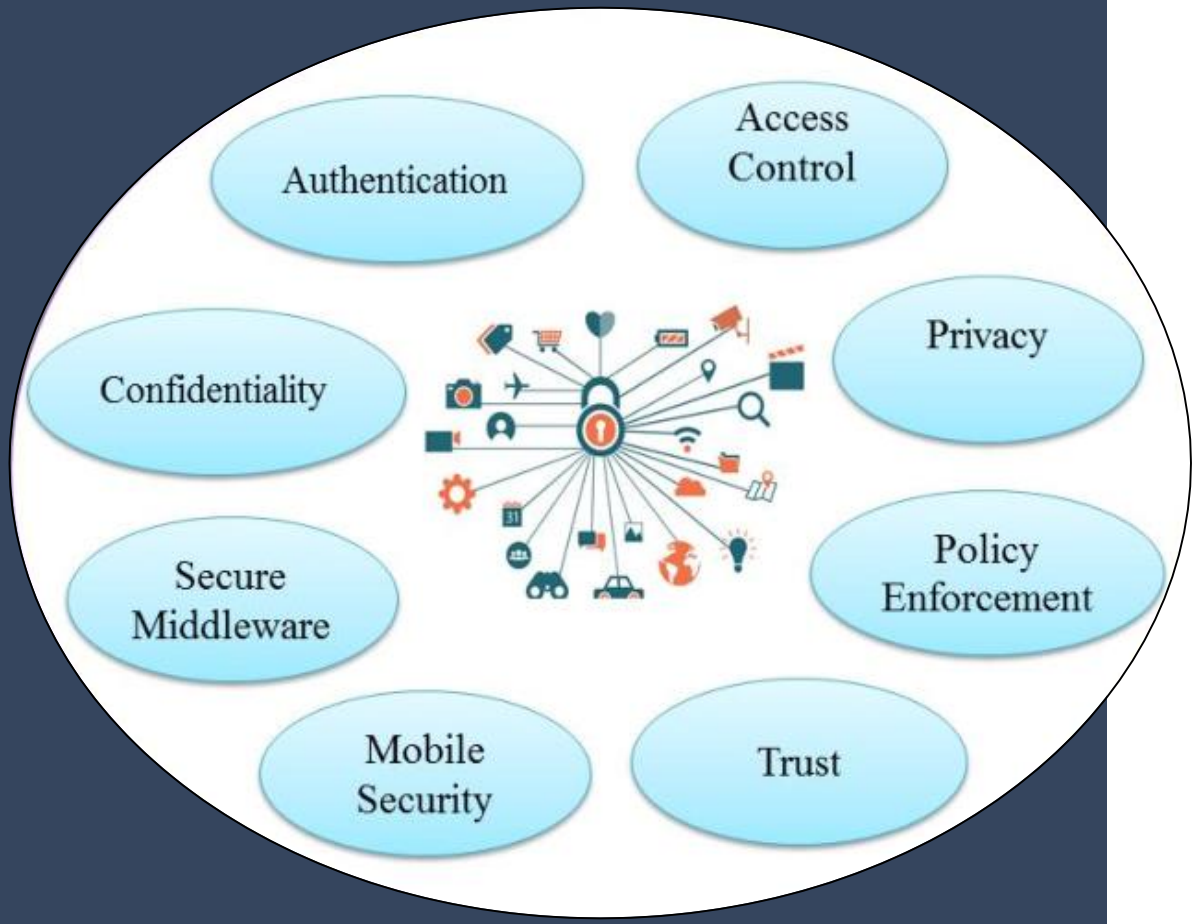
Dinuwan Randunu
IT18133578

Introduction

Background

Dinuwan Randunu
IT18133578

- Primarily focus only on functionality of industrial 4.0 automated systems.
- Security has been shared with a third party.
- Insecure Data
- Ethernet and the IP protocol stack are becoming a core part of plant and factory networks. [1]
- Connected to the internet over TCP/IP protocols without additional protection. [2]



Research Gap

Industrial 4.0 automation is driven by focusing on the functionality rather than 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 :

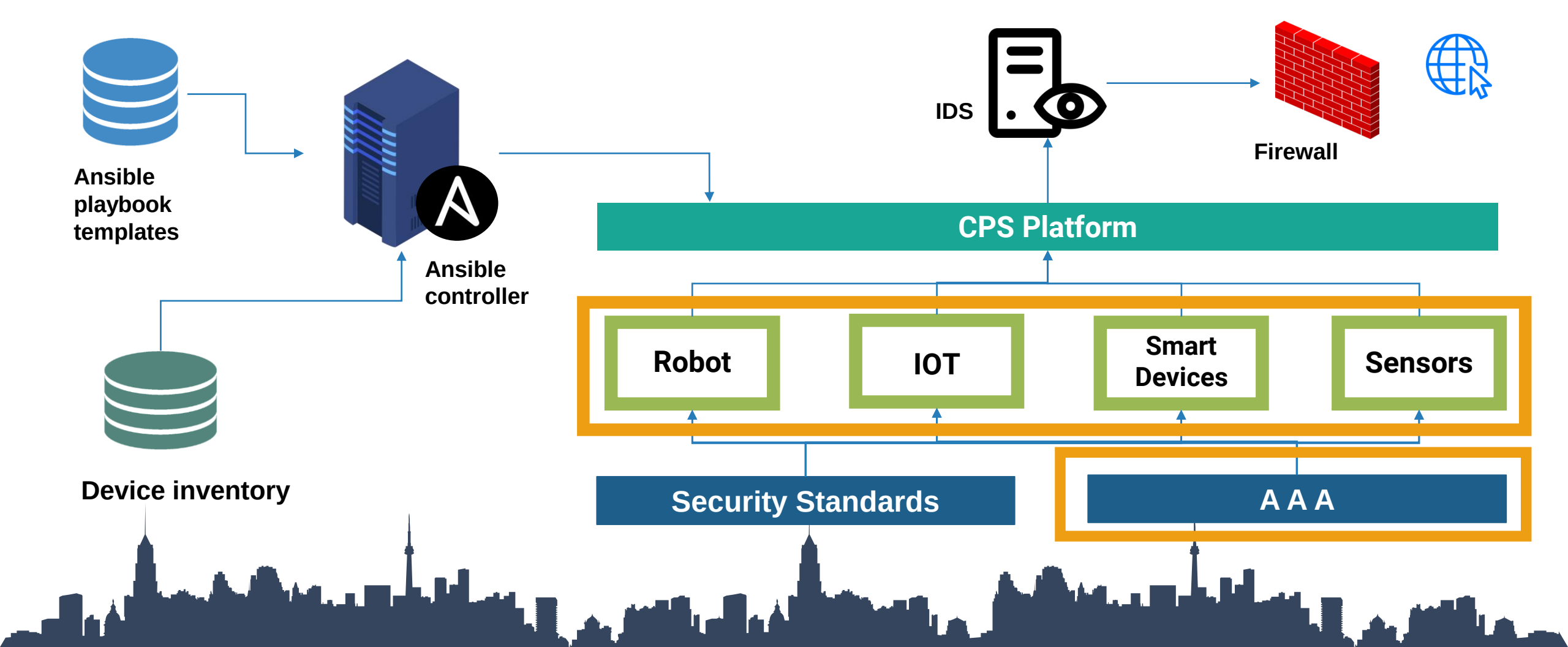
- Access log visualization.
- Report generation.
- Alert user when an anomaly occurs.

Dinuwan Randunu
IT18133578

RESEARCH METHODOLOGY

System Diagram

Dinuwan Randunu
IT18133578



Technologies, techniques & algorithms

Dinuwan Randunu
IT18133578

python™

django

elastic + logstash + kibana

BASH
THE BOURNE-AGAIN SHELL

octave®

NIST

Software specification

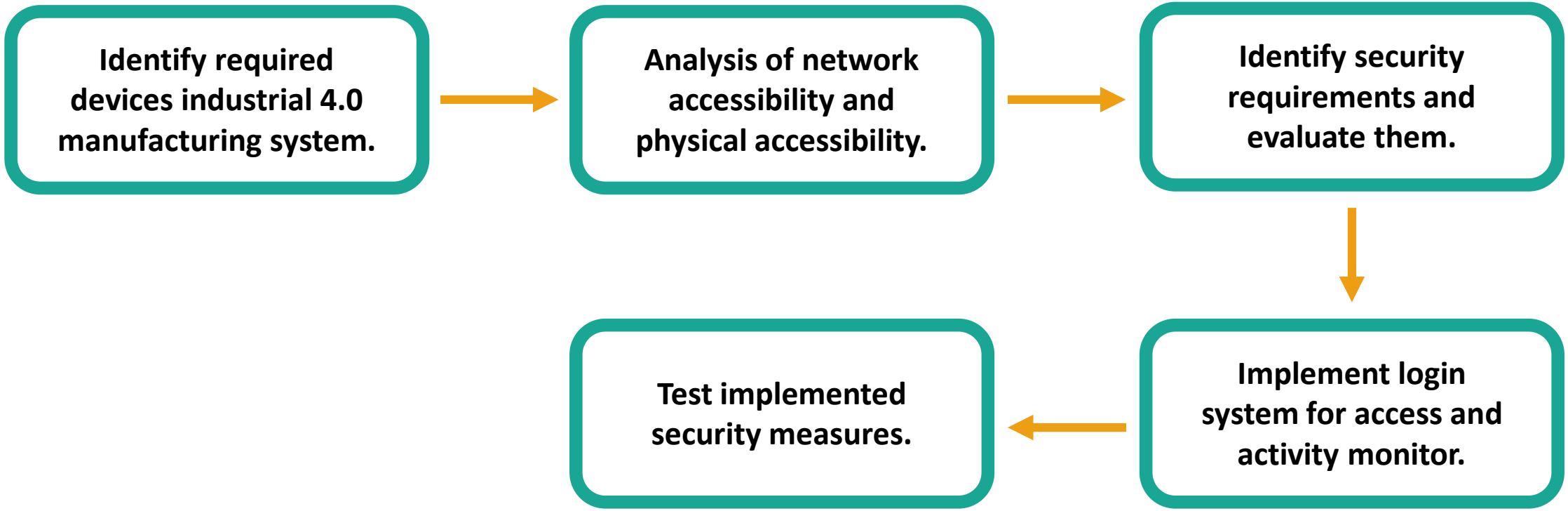
Dinuwan Randunu
IT18133578

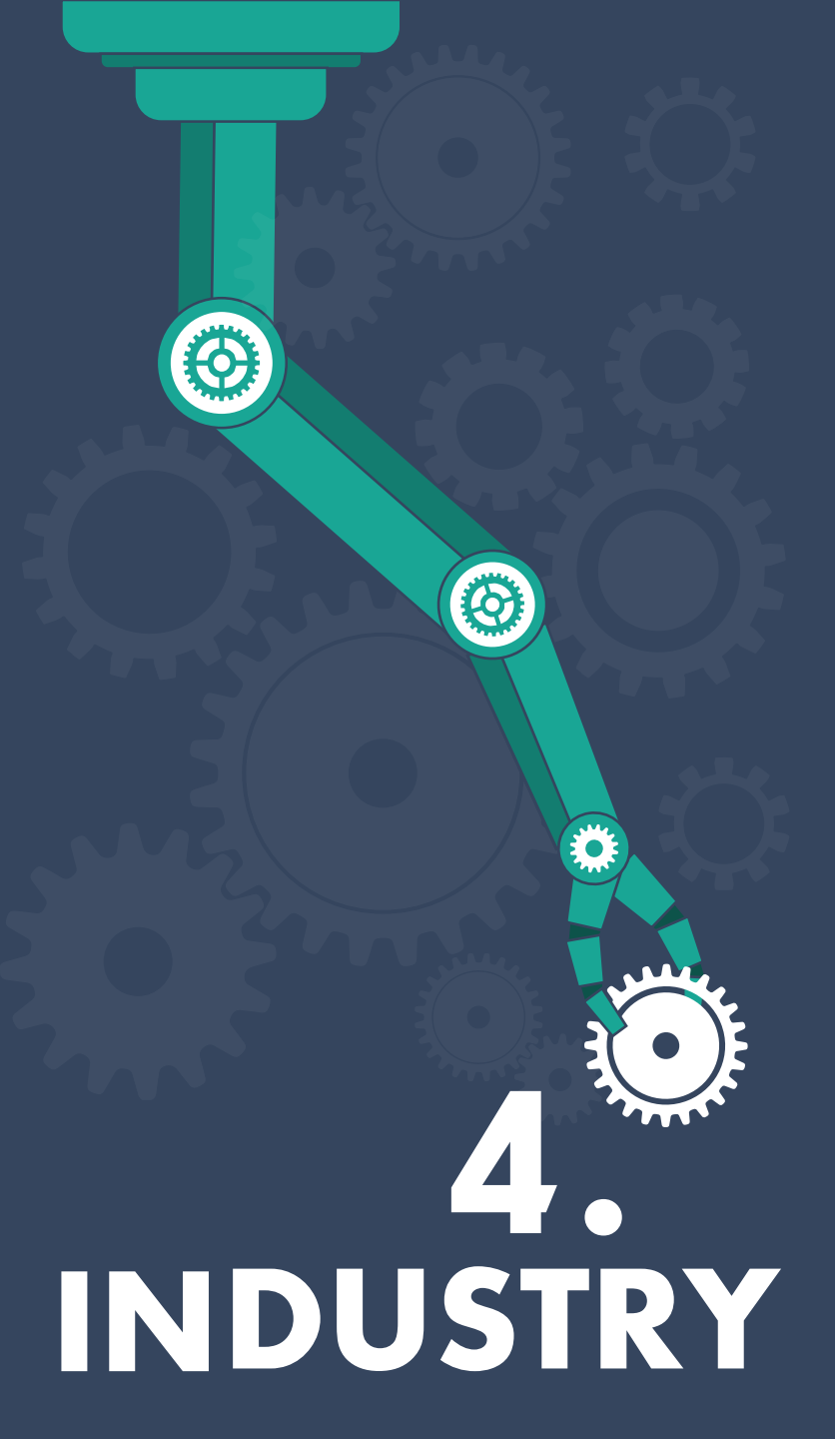
Requirements

- Database to store access logs and error logs.
- Implement a Physical Security System
- Data visualization from access logs.
- Report generation from access logs.

Work Breakdown Structure

Dinuwan Randunu
IT18133578





Dinuwan Randunu
IT18133578

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.

REFERENCES

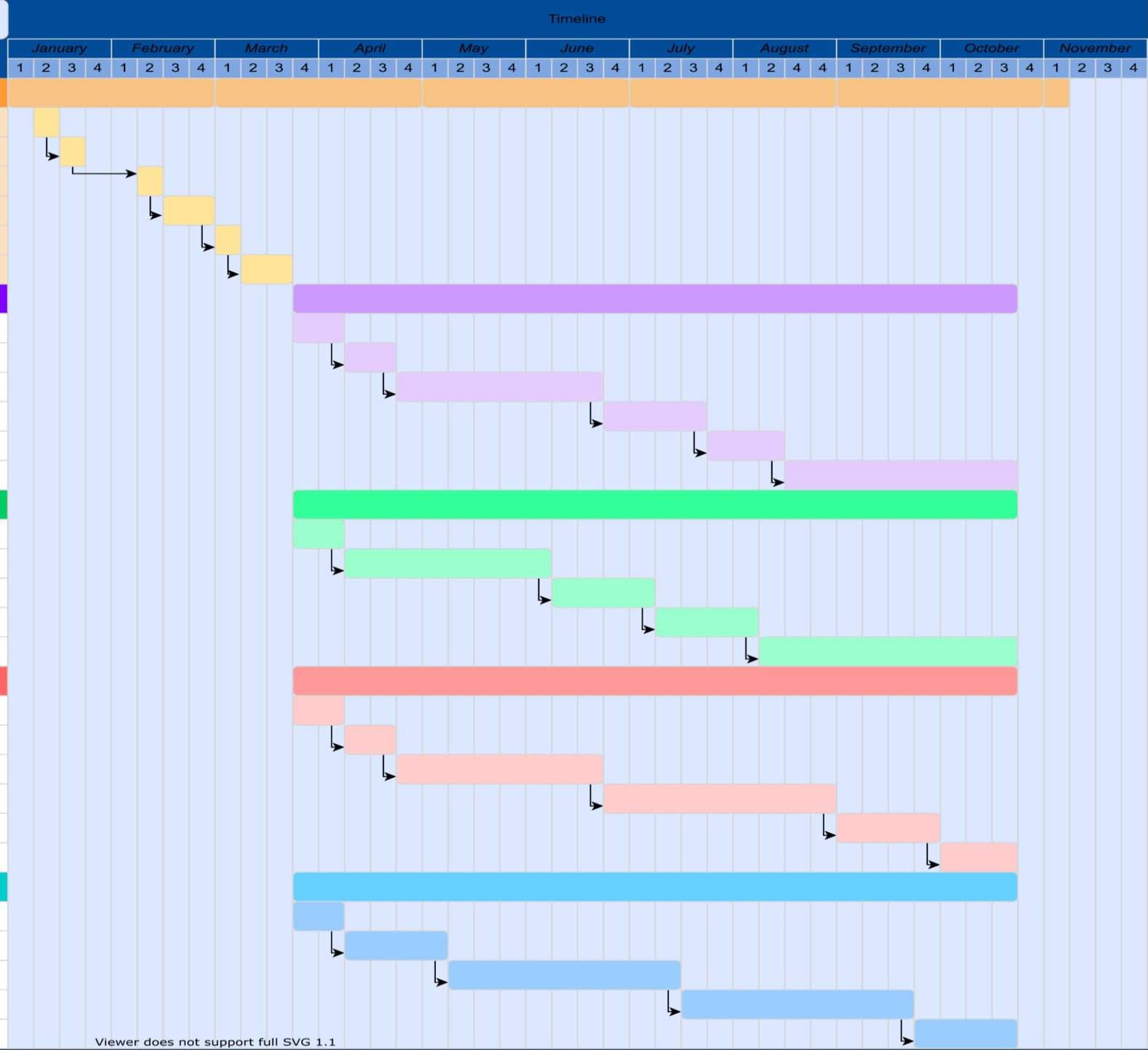
Dinuwan Randunu
IT18133578

[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

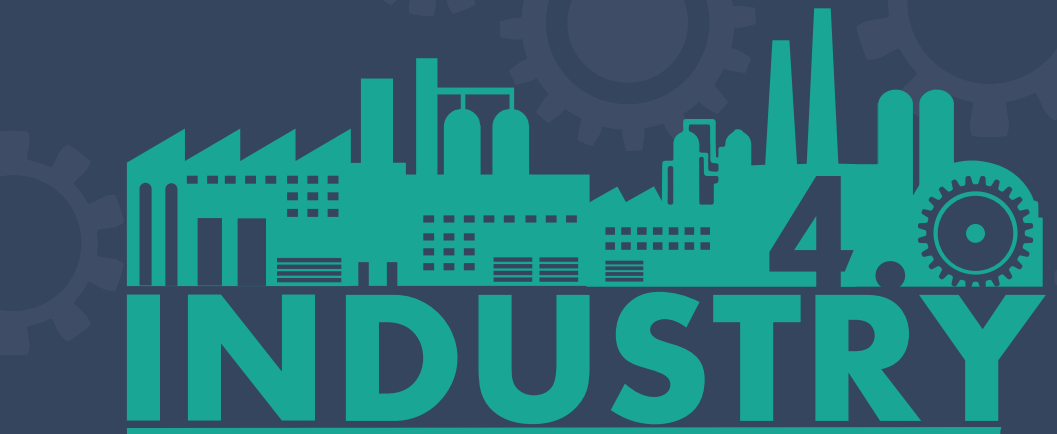
Gantt chart & Tentative budget allocation

#	Task Name	Duration	Start	ETA
Complete project execution		40 weeks	10-01-21	01-11-21
1	Online project Registration	1 week	10-01-21	17-01-21
2	Topic Assessment Form submission	1 week	18-01-21	22-01-21
3	Project Charter submission	1 week	08-02-21	12-02-21
4	Proposal report draft submission	2 weeks	15-02-21	26-02-21
5	Proposal presentation	1 weeks	28-02-21	08-03-21
6	Proposal report	2 weeks	08-03-21	21-03-21
7	Security Configuration	28 weeks	22-03-21	18-10-21
7.1	Identify required CPS devices	2 weeks	22-03-21	05-04-21
7.2	Identify and evaluate security requirements o...	2 weeks	06-04-21	20-04-21
7.3	Implement a tool for security hardening	8 weeks	20-04-21	15-06-21
7.4	Implement report generating tool	4 weeks	15-06-21	12-07-21
7.5	Test Security Configuration	3 weeks	13-07-21	02-08-21
7.6	Integrate hardening tool to the entire soluti...	9 weeks	03-08-21	18-10-21
8	Security standards and policy development	28 weeks	22-03-21	18-10-21
8.1	Identify the connected devices	2 weeks	22-03-21	05-04-21
8.2	Conduct a risk assessment	8 weeks	05-04-21	01-06-21
8.3	Identify the specific standards, procedures a...	4 weeks	01-06-21	28-06-21
8.4	Identify the types of policies required	4 weeks	28-06-21	26-07-21
8.5	Implement policies for the components	10 weeks	26-07-21	18-10-21
9	Implementations of Firewall & IDS	28 weeks	22-03-21	18-10-21
9.1	Identify required CPS components and categori...	2 weeks	22-03-21	05-04-21
9.2	Identify security requirements of the compone...	2 weeks	05-04-21	20-04-21
9.3	Configure firewall and define rules based on...	8 weeks	20-04-21	15-06-21
9.4	Implement IDS & IPS using a hybrid approach	9 weeks	15-06-21	09-08-21
9.5	Report generating tool based on audits and se...	4 weeks	09-08-21	06-09-21
9.6	Test implemented security measures	3 weeks	06-09-21	18-10-21
10	Authentication and access monitoring	28 weeks	22-03-21	18-10-21
10.1	Identify required devices	2 weeks	22-03-21	05-04-21
10.2	Identify security requirements	4 weeks	05-04-21	03-05-21
10.3	Analysis of network accessibility and physica...	9 weeks	03-05-21	05-07-21
10.4	Implement login system for access and activit...	9 weeks	05-07-21	06-09-21
10.5	Test implemented security measures	4 weeks	06-09-21	18-10-21



Item(s)	Cost(LKR)
Web server hosting	5000.00
Firewall + IDS/IPS hardware	1 8000.00
Physical security system hardware	5000.00
Raspberry Pi 3	1 2000.00
Total	**4 0000.00**


Q
&
A



Thank You