Ransomware Detection and Mitigation for Smart Business Management System IoT Networks: Control and Security

Dhin Islam Md
University of Greenwich | Department of Computer Science

Abstract

This dissertation focuses on the crucial issues of detecting and mitigating the impact of ransomware in Smart Business Management System (SBMS) that are enhanced by Internet of Things (IoT) networks. The system creates a solid cybersecurity framework by using Cisco Packet Tracer for simulations and combining advanced security technologies like Firewalls, Software-Defined Networking (SDN), and Intrusion Detection and Prevention Systems (IDPS). This defence-in-depth strategy enhances operational efficiency and strengthens defences, ensuring stability and security of smart business operations against increasing ransomware attacks.

Introduction

As businesses adopt Internet of Things (IoT) technologies into their management systems more and more, they are exposed to greater threats of cyber threats, specifically ransomware. These attacks have the potential to significantly disrupt operational efficiencies and compromise data security. This project aims to create an advanced cybersecurity framework by using simulations in Cisco Packet Tracer. The framework will consist of multiple layers of security systems, including Firewalls, Software-Defined Networking (SDN), and Intrusion Detection and Prevention Systems (IDPS). This method not only strengthens the defences of Smart Business Management Systems (SBMS) against ransomware but also improves their operational integrity. This study confirms the success of our comprehensive security procedures, providing strong protection for IoT-driven business environments.

In order to tackle these issues, the research uses a defence-in-depth approach, leveraging the capabilities of a number of security technologies to establish a strong barrier against future breaches. The study systematically evaluates the adaptability of different security setups to various ransomware attack scenarios by demonstrating a realistic SBMS IoT network environment. This methodology not only highlights the weaknesses in present systems but also demonstrates the crucial importance of adaptive, integrated security solutions in protecting advanced IoT networks from increasingly sophisticated cyber-attacks.

Research of IoT Vulnerabilities and Effective Security Solutions

There are critical security concerns due to the rise of ransomware in IoT-enhanced Smart Business Management Systems (SBMS). The growth of IoT devices increases the attack surface, and ransomware might cause broad damage by taking advantage of their connectivity (**Nizˇetic´ et al., 2020**). Current cybersecurity defences against such advanced attacks are frequently insufficient, including intrusion detection systems and standard firewalls (**McIntosh et al., 2021**).To increase network resilience and defend against these dynamic threats, the literature emphasises the need for a strong, multi-layered defence that includes developments in firewall technologies and Software-Defined Networking (SDN) (**Pagán & Elleithy, 2021**).

Main Objectives

- Build a strong framework to protect the IoT-enhanced SBMS from ransomware attacks, adopting advanced security technologies.
- Implement a defence-in-depth strategy by employing a combination of firewalls, SDN, and IDPS to enhance network security.
- Utilise Cisco Packet Tracer to simulate a practical SBMS IoT network environment for the purpose of evaluating and analysing the effectiveness of multi layered security setups in mitigating ransomware threats.
- Methodically evaluate the strength of the suggested security framework against ransomware attacks to determine its effectiveness in protecting IoT-driven operations.
- Optimise the operational efficiency and continuous operation of the SBMS by establishing strong security measures against cyber threats, thereby lowering downtime and the risk of data loss.

Summary of Design and Implementation

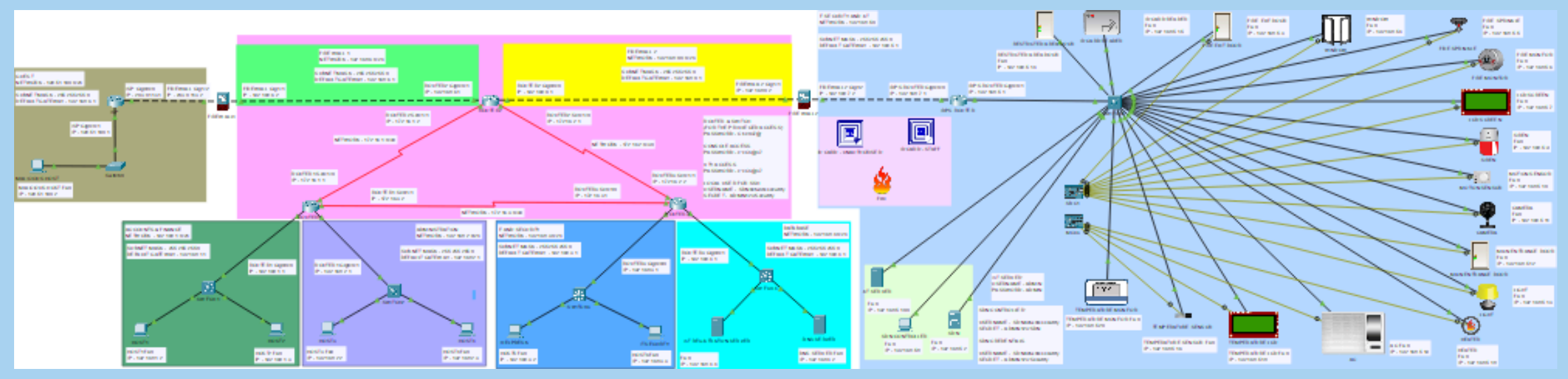


Figure 1: Smart Business Management System IoT Network Topology

The project involves creating a simulated SBMS-IoT network using Cisco Packet Tracer. The focus is on implementing a layered security architecture that includes firewalls, SDN, and IDPS. The implementation involves installing security measures and programming IoT devices using Python to strengthen defence against ransomware in different network scenarios. This combination offers a dynamic and adaptable security environment that extensive simulations have thoroughly evaluated to confirm its effectiveness.

Simulation Testing Result

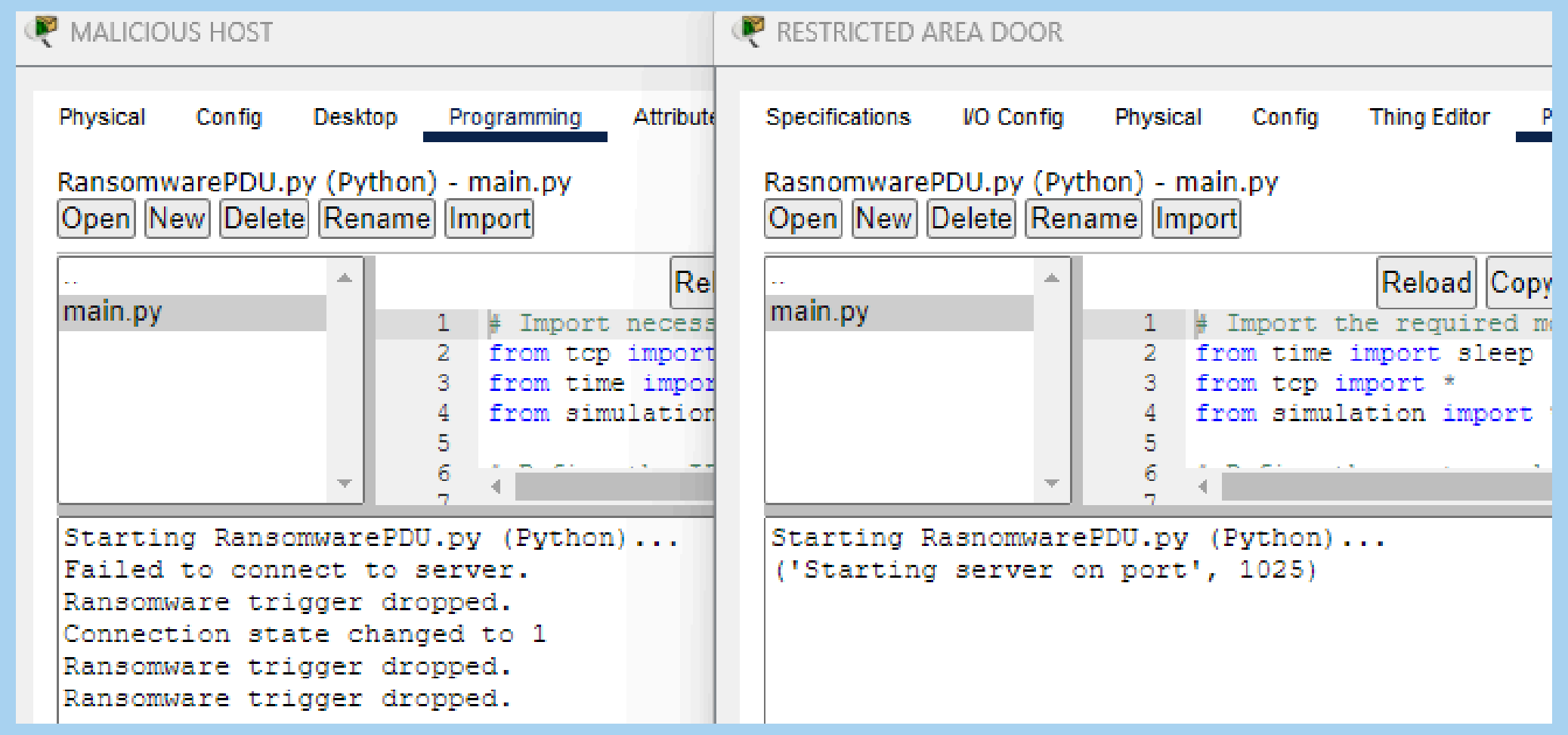
The effectiveness of the implemented different devices and nodes, IoT interconnections, and security measures was thoroughly evaluated across thirteen separate scenarios. These scenarios aimed to evaluate the strength of the SBMS network, its IoT interconnect setup, and its security framework in effectively dealing with ransomware threats. The testing covered various methods of attack, such as direct attacks on network access points and insider attacks, with both scenarios involving the manipulation of encrypted traffic.

Main Results:

The testing showed a significant increase in network security, accompanied by a significant decrease in successful ransomware attacks. The multi layered security measures resulted in a strong defence system, effectively reducing the chance of vulnerability. Furthermore, the network connectivity and IoT interconnection performance were outstanding assuring the flawless connection of all components.

Specific Outcomes for Each Security Measure:

- Firewalls: Demonstrated exceptional performance in blocking unauthorised access attempts in every scenario, specifically preventing ransomware from exploiting network vulnerabilities at entry points. At the same time, insider threats attempting to introduce ransomware were effectively blocked at the entry points of the IoT network.



RansomwarePDU.py (Python) - main.py

```
# Import necess
from tcp import
from time impor
from simulation
```

```
Starting RansomwarePDU.py (Python)...
Failed to connect to server.
Ransomware trigger dropped.
Connection state changed to 1
Ransomware trigger dropped.
Ransomware trigger dropped.
```

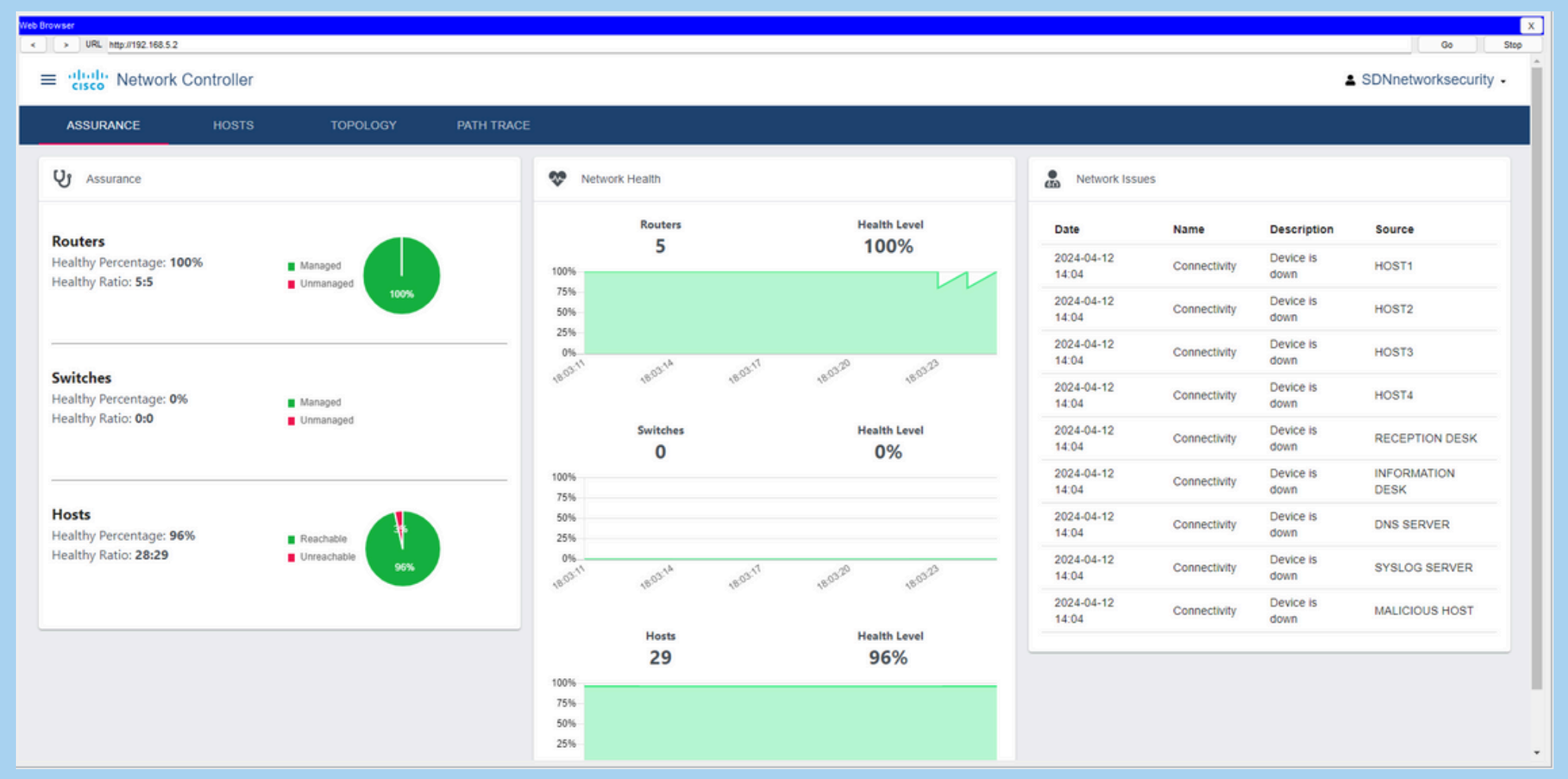
RasnomwarePDU.py (Python) - main.py

```
# Import the required m
from time import sleep
from tcp import *
from simulation import
```

```
Starting RasnomwarePDU.py (Python)...
('Starting server on port', 1025)
```

Figure 2: Firewalls Testing resultAgainst Ransomware Payload

- ***SDN***: SDN plays a crucial role in effectively controlling network traffic to control the paths through which ransomware attacks can propagate. This measure guaranteed the preservation of network reliability and uninterrupted operation in the face of threats. Even so, the use of Packet Tracer placed restrictions on the complete capability of SDN. However, the utilization of Python scripts simplified the obtaining of service tickets. Using these tickets allowed the inspection of network devices and hosts, offering an additional viewpoint on the entities connected within the network, which is crucial for network monitoring during security incidents.



Routers
Healthy Percentage: 100%
Healthy Ratio: 5:5

Switches
Healthy Percentage: 0%
Healthy Ratio: 0:0

Hosts
Healthy Percentage: 96%
Healthy Ratio: 28:29

Routers 5 Health Level 100%

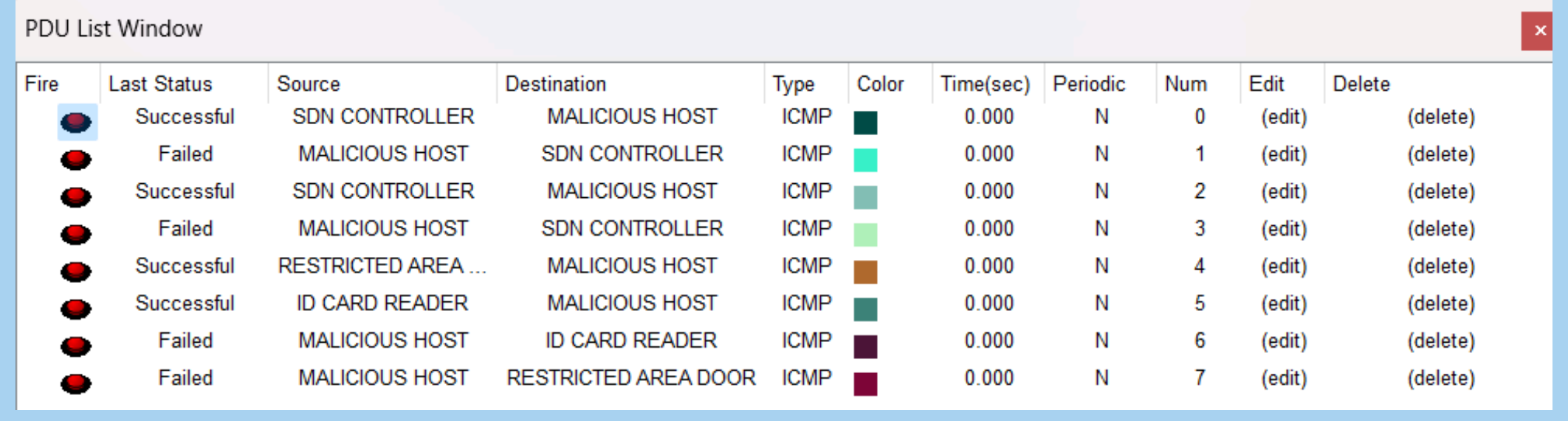
Switches 0 Health Level 0%

Hosts 29 Health Level 96%

Date	Name	Description	Source
2024-04-12 14:04	Connectivity	Device is down	HOST1
2024-04-12 14:04	Connectivity	Device is down	HOST2
2024-04-12 14:04	Connectivity	Device is down	HOST3
2024-04-12 14:04	Connectivity	Device is down	HOST4
2024-04-12 14:04	Connectivity	Device is down	RECEPTION DESK
2024-04-12 14:04	Connectivity	Device is down	INFORMATION DESK
2024-04-12 14:04	Connectivity	Device is down	DNS SERVER
2024-04-12 14:04	Connectivity	Device is down	SYSLOG SERVER
2024-04-12 14:04	Connectivity	Device is down	MALICIOUS HOST

Figure 3: SDN Controller Testing Result

- ***IDPS***: Packet Tracer's lack of capability to create or modify IDPS signatures resulted in the system's failure to detect the ransomware signature. However, in tests using the ICMP protocol to replicate a ransomware attack, the IDPS successfully blocked these attempts. This indicates that if the IDPS had the ability to create or modify signatures, it would be possible to successfully detect and block ransomware signatures.



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	SDN CONTROLLER	MALICIOUS HOST	ICMP	■	0.000	N	0	(edit)	(delete)
●	Failed	MALICIOUS HOST	SDN CONTROLLER	ICMP	■	0.000	N	1	(edit)	(delete)
●	Successful	SDN CONTROLLER	MALICIOUS HOST	ICMP	■	0.000	N	2	(edit)	(delete)
●	Failed	MALICIOUS HOST	SDN CONTROLLER	ICMP	■	0.000	N	3	(edit)	(delete)
●	Successful	RESTRICTED AREA ...	MALICIOUS HOST	ICMP	■	0.000	N	4	(edit)	(delete)
●	Successful	ID CARD READER	MALICIOUS HOST	ICMP	■	0.000	N	5	(edit)	(delete)
●	Failed	MALICIOUS HOST	ID CARD READER	ICMP	■	0.000	N	6	(edit)	(delete)
●	Failed	MALICIOUS HOST	RESTRICTED AREA DOOR	ICMP	■	0.000	N	7	(edit)	(delete)

Figure 4: IDPS Testing Result

Table 1 summarizes the outcomes of all test scenarios, leading to an overall success rate of 92.3%

Test ID	Test Description	Expected Outcome	Actual Outcome	Pass/Fail
1	Network Connectivity	Ping Successful	Ping Successful	Pass
2	Smart Fire Alert System	Successfully working	Successfully working	Pass
3	Smart Motion Detection System	Successfully working	Successfully working	Pass
4	Smart Temperature Control System	Successfully working	Successfully working	Pass
5	Smart ID Card Reader	Successfully working	Successfully working	Pass
6	Ransomware Payload	Successfully sent	Successfully sent	Pass
7	Firewall 1 & 2	Detects Ransomware	Detects Ransomware	Pass
8	SDN	Successfully working	Successfully working	Pass
9	ServiceTicket.py	Successfully working	Successfully working	Pass
10	NetworkDevice.py	Successfully working	Successfully working	Pass
11	Host.py	Successfully working	Successfully working	Pass
12	IDPS - Ransomware Payload	Detect Ransowmare	Did not Detect	Faiil
13	IDPS - ICMP	Successfully blocks	Successfully blocks	Pass
11	Multi-Layered Security	Detects Ransomware	Detects Ransomware	Pass

Table 1: Simulation Testing Table Result

Conclusions

The project successfully achieved its objectives by implementing a strong security framework that incorporates firewalls, SDN, and IDPS. The system's resilience against simulated ransomware threats was proved through simulation testing using Cisco Packet Tracer. Although simulated environments have their limitations, the successful setup of advanced security components demonstrates significant progress in securing SBMS IoT networks. This cybersecurity method is an important contribution to the profession, especially in the context of the IoT network. It demonstrates a comprehensive understanding and successful strategies to combat ransomware attacks.

Future Work

This study establishes the groundwork for enhancing cybersecurity in IoT network enabled Smart Business Management Systems. Future study will shift from using simulated environments to actually implementing the security framework in a live SBMS IoT network, thereby increasing its practicality in real-world scenarios. In addition, the strategy will involve enhancing the IDPS to identify ransomware in encrypted data more effectively. This may be achieved by adding machine learning methods that analyse metadata and traffic patterns, bypassing the need for decryption.

References

McIntosh, Timothy et al. (2021). "Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions". In: ACM Computing Surveys (CSUR) 54.9, pp. 1–36.

Nizeti ˇ c, Sandro et al. (2020). "Internet of Things (IoT): Opportunities, issues and challenges towards a smart ´ and sustainable future". In: Journal of cleaner production 274, p. 122877.

Pagan, Alexander and Khaled Elleithy (2021). "A multi-layered defense approach to safeguard against ran- ´ somware". In: 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, pp. 0942–0947.