ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

Developing Robust Cyber Defense Strategies for Zambian Smart Grids: Insights from a Simulation Study

Bruce Byamungu[1]; Moses Mupeta[2]

[1]Author, [2]Supervisor

[1]Department ICT Information and Communications University, Lusaka, Zambia.
[2]Department ICT Information and Communications University, Lusaka, Zambia.

Publication Date: 2026/07/02

Abstract: The critical infrastructures cybersecurity must be guaranteed as Zambia's adoption of Smart Grid technology progresses. While improving the efficiency and dependability of electricity distribution smart grids also make the power grid more vulnerable to cyberattacks on communication protocols like Modbus. In this paper, a virtualized Smart Grid environment based on the Zambian Grid is used to simulate and analyze Modbus protocol cyberattacks. A variety of cyberattacks were launched using a virtualized infrastructure to mimic possible threats and the corresponding grid responses were tracked. According to the findings, the Modbus protocol is vulnerable, and strong cybersecurity measures are required to safeguard the availability and integrity of Smart Grids. We validate the proposed testbed architecture by performing and analyzing a representative cyberattack in the developed environment, thus showing the principles for the analysis of other possible cybernetic attacks. The findings suggest future work for improving cybersecurity in Smart Grid implementations and offer a framework for bolstering cyber defense tactics in Zambian power systems.

Keywords: *Smart Grid, Cyber-Attacks, Modbus Protocol, Virtual Environment, Zambian Grid, Cybersecurity, Supervisory Control and Data Acquisition (SCADA), Denial of Service (DoS), Man-in-the-Middle (MitM).*

How to Cite: Bruce Byamungu; Moses Mupeta (2026) Developing Robust Cyber Defense Strategies for Zambian Smart Grids: Insights from a Simulation Study. *International Journal of Innovative Science and Research Technology*, 11(6), 2080-2096. https://doi.org/10.38124/ijisrt/26jun263

I. INTRODUCTION

The integration of Smart Grids into power distribution systems has transformed the energy sector by enhancing control, real-time monitoring, and efficiency(Khalid, 2024). However, this evolution brings new challenges, notably the increased risk of cyber-attacks on critical infrastructure(Admass et al., 2024). Zambia's electricity grid, which is undergoing modernization, faces significant threats from cyber intrusions targeting key communication protocols such as Modbus(Phiri and Tembo, 2022),(Bhajekar and Gupta, 2024).

Modbus, a widely used communication protocol in Industrial Control Systems (ICS), plays a crucial role in facilitating data exchange between devices in Smart Grids(McLaughlin et al., 2015). Its widespread use in Supervisory Control and Data Acquisition (SCADA) systems, coupled with inherent security weaknesses, makes it a prime target for cyber-attacks(Parian et al., 2020). As the Zambian grid adopts Smart Grid technology, simulating and understanding the potential threats posed by cyber-attacks on the Modbus protocol becomes critical(Lukumba Phiri, 2023),(Anon, n.d.).

Both fossil fuels like petroleum and renewable energy sources including biomass, solar, wind, and water are used in Zambia(Anon, n.d.). Zambia has the potential to be energy self-sufficient due to its large untapped renewable resource reserves, except for petroleum, which is imported into the nation entirely. Water, however, continues to be Zambia's primary energy source despite the variety of these sources(Chitandula1 et al., n.d.). An estimated 40% of the water resources in the SADC area are found in Zambia, which also has a hydropower potential of over 6,000 MW, of which 2,354 MW have been developed(Entwisle et al., n.d.). The nationwide installed generation capacity in the electrical subsector grew from 3,811.32 MW in 2023 to 3,871.32 MW in 2024. With an 82 percent share, hydroelectric plants remained the dominant force in the electricity generation landscape. At 9% and 5%, respectively, coal and solar power plants also made contributions to the energy mix(Anon, n.d.). In the SAPP region, Zambia has authorized power traders that import and export electricity. These include GreenCo, which

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

imports from Mozambique and South Africa, Kanona, which exports to both South Africa and the Democratic Republic of the Congo, and EN Power, which exports to the former(Anon, n.d.).

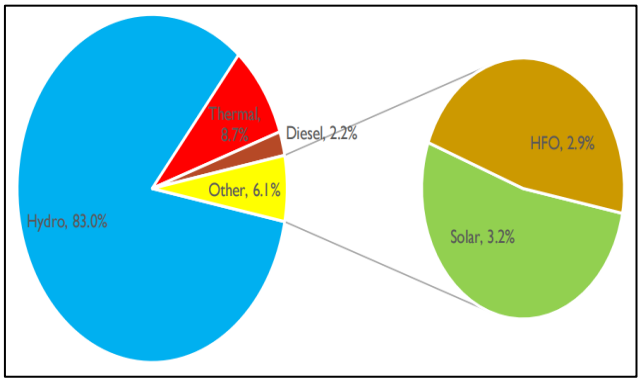

Fig 1 Summary of Power Generation in Zambia

The Zambia Electricity Supply Corporation (ZESCO) is the dominant player in Zambia's energy sector. Electricity is produced, transmitted, distributed, and supplied to both national and regional markets by ZESCO, a vertically integrated national utility(Bayliss and Pollen, 2021). Two other significant participants are the Lunsemfwa Hydro Power firm and the Copperbelt Energy Corporation (CEC), a transmission firm that buys high-voltage electricity from ZESCO and supplies it to the mining sector in the Copperbelt region(Bayliss and Pollen, 2021). Additionally, there are two rural concessions: North West Energy Corporation(Anon, n.d.), which provides energy to a mining settlement in the country that is not connected to the ZESCO system, and Zengamina Hydro Power Company (ZHPC)(Anon, n.d.), which operates a remote rural network in the Northern Province.

Zambia's population was projected to be 20.8 million in 2023. Out of the entire population, 40.8 percent lived in cities and 59.2 percent lived in rural areas. According to official statistics, 53.6% of households had access to electricity. Additionally, compared to 80.3 percent of households in urban areas, 34.0 percent of homes in rural areas had access to electricity(Anon, n.d.).

For families nationwide, the national grid accounted for 34.4 percent of all energy use, followed by dry batteries (24.3 percent), and solar home systems (18.6 percent). Just 0.2% of the houses reported getting their energy from a nearby mini-grid(Anon, n.d.).

Internet-based data transmission and remote control are features of smart grid energy monitoring devices(Jahid et al., 2023). SCADA technology integrates sensors, actuators, and software such as Human Machine Interface (HMI) for data collecting, networked communication, display, and monitoring/control(Anon, n.d.). It also obtains data from distant facilities and gives restricted control orders. Along with communication networks, it makes use of Master Terminal Units (MTUs) like the Arduino IoT Cloud and Remote Terminal Units (RTUs) like microcontrollers(Anon, n.d.). Generally speaking, SCADA systems fall into one of two categories: proprietary or open source. Because proprietary systems only use parts from one manufacturer, they may be less flexible and vulnerable to supplier failure(Anon, n.d.).

The Internet of Things (IoT) uses software and sensors to link physical objects so that data may be shared online. IoT, which started in the RFID community, has grown as cloud computing and connectivity technologies have advanced(Anon, n.d.),(Gopal et al., 2022). IP networks facilitate communication across billions of objects, ranging from domestic appliances to industrial machinery, allowing for intelligent decision-making, improved security, and real-time monitoring(Mouha and Mouha, 2021). This facilitates event automation, monitoring, location tracking, and real-time identification(Anon, n.d.). Smart sensors, PLCs, actuators, and IEDs from SCADA networks and industrial control systems (ICS) are all integrated into the IoT platform(Upadhyay et al., 2024).

Cyberattacks against vital infrastructure have increased in frequency in recent years. These attacks can have a wide range of effects, from physical destruction to financial loss and crucial service interruption. The growing digitization of critical infrastructure sectors and the confluence of operational technology (OT) and information technology (IT) have made these attacks easier(Cremer et al., 2022).

Smart grid vulnerabilities have been revealed by recent, intermittent cybersecurity incidents around the world, highlighting the critical need for strong cybersecurity safeguards, as seen in Table 1. The risk of smart grid cyberattacks increases as technology becomes more pervasive in daily life and cyber-physical systems become more complex. Implementing preventive steps that reduce these risks and maintain the dependability and security of our power systems requires cooperation between governments, utility corporations, and cybersecurity experts(Paul et al., 2024).

Table 1 List of Attacks on Smart Grids

Incident Title	Date	Incident
Stuxnet Worm	July 2010	The first known example of malware was the Stuxnet worm, which initially targeted Iranian uranium enrichment facilities before spreading to other countries(Anon, n.d.),(Knapp and Langill, 2015).
Saudi Aramco Systems Interruption	2012	Saudi Aramco, the biggest oil corporation in the global and a Saudi Arabian enterprise, had its systems interrupted by the Shamoon ransomware(Alghamdi, 2021).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

Ukrainian Power Grid Attack	2015	The timing of the attack on Ukraine's electrical grid, which resulted in blackouts, was ideal(Anon, 2024).
Russian Hackers Power Grid Break-in	2016	During the Christmas season, Russian hackers gained access to an electrical system in northern Ukraine. They caused OT (automatic control system) problems in the substations, resulting in multiple hours of power outages, and they hacked an IT-based data network (Pollard, n.d.).
US Power Utilities Spear-phishing Attack	March 2018	By spear-phishing personnel, Russian hackers were able to penetrate the control systems of US power utilities, jeopardizing grid security. Although there were no confirmed outages, the incident sparked worries about how susceptible US infrastructure is to cyberattacks (Alawida et al., 2022).
Cyber Espionage Campaign	2017–2018	Russian hackers compromised the grid's security by using spear-phishing attacks on employees to infiltrate the control systems of US power firms. The event sparked worries about how susceptible US infrastructure is to cyberattacks, even though no failures were recorded (Alawida et al., 2022).
Petrochemical Facility Malware Attack	2017–2018	A malware attack targeting the safety systems of a Saudi Arabian petrochemical company was designed to undermine industrial control systems and result in bodily harm. This illustrates how, in addition to data disruption or theft, cyberattacks can have practical consequences(Abdelkader et al., 2024).
Water Treatment Plant Hack Attempt	February 2021	Remote attackers were successful in gaining unauthorized remote access to the control system of a water treatment facility in Florida. By increasing the quantities of sodium hydroxide (lye) to dangerously high levels, they aimed to regulate the water supply(Anon, n.d.).
SolarWinds Supply Chain Attack	2020	The SolarWinds supply chain assault was identified as a cyberattack in December 2020. Customers of SolarWinds, a provider of network and device management software, received an update that contained malware that might have compromised thousands of networks(Ghanbari et al., 2024).

In this study a virtual environment model of the Zambian grid will be used to simulate Modbus-based cyberattacks evaluate the effects of these attacks and suggest countermeasures. A variety of efforts have been made by academia to address the growing perceived cybersecurity threat to smart power plants. Among the recommendations in this field are supply chain safety measures cyber-physical protection systems best practice proposals risk assessments and cyberattack scenario studies. The study assesses the effectiveness of cybersecurity measures that are currently in place by simulating real-world situations.

- Particularly in light of the Zambian power grid the study will methodically identify and classify the unique vulnerabilities present in the Modbus protocol.
- The research will measure the possible risks connected to these vulnerabilities and evaluate their effect on the security and dependability of the grid by modeling different attack scenarios. Access control encryption network segmentation intrusion detection systems (IDS) regular security audits and penetration testing are just a few of the cybersecurity measures that the study will suggest to reduce the risks that have been identified. By focusing on these important areas this research will help make Zambia's power grid more secure and resilient safeguarding vital infrastructure and guaranteeing that customers will receive electricity on time.

The remainder of the article is organized as follows: Chapter 2 provides background information and relevant literature Chapter 3 presents the methodology Chapter 4 presents the findings and analysis and Chapter 5 wraps up the study.

II. BACKGROUND AND RELATED WORK

Numerous studies have been conducted on the simulation of cyberattacks on smart grids with a focus on protocols such as DNP3 IEC 61850 and Modbus. Research conducted in nations such as China Europe and the United States has demonstrated the catastrophic consequences of coordinated cyberattacks on national power systems. Fewer studies though have examined the African context and even fewer have modeled the Zambian grid to determine how cyberattacks would affect this particular infrastructure.

In 2015, J. Z. Thornton(Thornton, 2015) created a virtual SCADA lab where the Simulink/Matlab software(Anon, n.d.) was used to represent the physical process (gas pipeline) using intricate mathematical equations. The control logic stated in the ladder language was emulated using Python programming, and Modbus/TCP communication was accomplished using Python libraries (modbus_tk). A proprietary solution (GE iFix) and Python libraries (TKInter) were used in part to create the SCADA. Despite its budgetary benefits, the extensive usage of Python on the testbed might have diminished the realism of the suggested virtual lab. Furthermore, we think that proprietary software ought to be avoided at all costs.

A SCADA testbed for cybersecurity research was introduced by M. Andrey Teixeira et al. in 2018(Teixeira et al., 2018). Their concept focused on using the Modbus protocol to regulate a water storage tank in an HIL setup. To create an automated intrusion detection system, machine learning (ML) algorithms were trained on the testbed's responses to reconnaissance industrial network cyberattacks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

However, the model's potential real-world applications are limited by the overly simple selection of the industrial subprocess to be emulated. Additionally, it uses specialized commercial equipment, like the Schneider PLC type M241CE40, which limits the generalizability of the results and complicates experiment replication.

S. Figueroa-Lorenzo et al. (2019)(Figueroa-Lorenzo, 2019) constructed a virtual testbed of TCP/IP software network elements (firewall, routers, and switches) that Cisco has made available for use in the network simulator GNS3 to evaluate their proposal to enhance the security of the Modbus protocol. The authors assumed that the cybersecurity of the model was ensured by design because their method depended on including the Transport Layer Security (TLS) mechanism into the conventional Modbus TCP/IP protocol. The next step was to assess any issues brought on by poor performance and implementation errors, which the suggested configuration may confirm. This study demonstrates the strength and adaptability of virtualized testbeds for investigating a wide range of cybersecurity topics for industrial control systems (ICS).

A testbed architecture is described by F. Zhang et al., 2019 (Zhang et al., 2019) to illustrate a multilayered defense-in-depth-based intrusion detection system. This featured a data storage unit, a National Instruments cDAQ9188 Ethernet chassis, an engineering workstation for the SCADA, and a malicious PC running Kali Linux. This configuration made it possible for many assaults, including man-in-the-middle (MITM) and denial-of-service (DoS) attacks. However, only a theoretical simulation of the physical process that represents a nuclear reactor subsystem was made. In 2020, F. Zhang et al.(Zhang and Coble, 2020) suggested a HIL testbed constructed with the Asherah NPP Simulator (ANS), which can simulate realistically, addressing this problem. Additionally, it includes a PLC for data collection and fake data injection attacks.

Motivated by the dearth of high-quality real data in the volumes and features needed for machine learning applications targeted at automating cybersecurity tasks, O. Pospisil et al., 2021(Pospisil et al., 2021) provide an overview of recent work in the field of industrial testbeds. The report continues by outlining several testbeds that were established in their university's lab to gather data. However, researchers with limited laboratory facilities may encounter challenges due to the abundance of possibilities examined. Specifically, concerning testbeds built using a wide range of proprietary protocols and physical equipment.

E. Aboah Boateng et al., 2022 (Aboah Boateng and Bruce, 2022) built a testbed based on open-source software to evaluate the efficacy of the ML one-class neural network (OCNN) training approach on a Modbus/TCP network with previous efforts aiming at establishing automated IDS for ICS. To find anomalies in PLC operation, the latter employed machine learning techniques such as isolation forest (IF) and one-class support vector machine (OCSVM). Fortunately, the authors were able to incorporate the traffic light operating software, which was originally developed for the Siemens S&-1212C PLCs, into the open-source soft PLC OpenPLC. Furthermore, ScadaBR, a free supervision system, was chosen to supply the human-machine interface (HMI).

Based on information obtained from smart meters (SM) placed at customers' residences, the authors in (Moghaddass and Wang, 2018) put into practice a real-time anomaly detection system. More specifically, in (Huitsing et al., 2008), P. Huitsing et al. provided a comprehensive theoretical analysis of the many cyberattacks against the Modbus protocol. To collect pertinent traces that machine learning algorithms could exploit, (Li et al., 2017) conducted four distinct cyberattacks on the Modbus protocol. To identify intrusions that share characteristics with known attacks the traffic generated by this simulated environment was classified using decision trees and neural networks. MTF, a Modbus/TCP Fuzzer, was designed and implemented by Voyiatz et al.(Voyiatzis et al., 2015).

The authors of (Wang et al., 2018) suggested an intrusion detection technique for the Modbus TCP protocol that makes use of a honeypot. An unsupervised clustering technique based on log sequence similarity to cluster assaulting actions is used in the suggested strategy. To take advantage of a series of attacks on a CPS testbed, the Modbus/TCP Attack-Tree model was put into practice (Bashendy et al., 2021). This model incorporates reconnaissance, denial-of-service, replay, and man-in-the-middle attacks. This blends assault time, detection time, and plant hazard-generating time to function as a formal risk assessment model. After analyzing 37 cases, the authors of the research (Radoglou-Grammatikis and Sarigiannidis, 2019) looked at the IDPSs' role in the SG paradigm.

An IDS that functions in two ways was proposed by the authors in (Radoglou-Grammatikis et al., n.d.). They started by researching and improving the cyberattacks that the Smod pen-testing tool offered. Secondly, they present an anomaly-based intrusion detection system (IDS) that can detect intrusions that result in Modbus/TCP denial of service (DoS). By analyzing and testing the current security countermeasures that are specific to SCADA systems, a case study describes various countermeasures that can enhance security for the Modbus/TCP protocol in SCADA systems (Luswata et al., 2018). A model for organizing information security in Modbus TCP was proposed in another work (Ametov et al., 2021).

III. METHODOLOGY

In this chapter, we present the requirements considered in building up the proposed testbed, and we discuss the idea that guided the validation of our design. Then, the testbed components are detailed and discussed. The following methodological process can be seen in the flowchart depicted in Figure 2.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

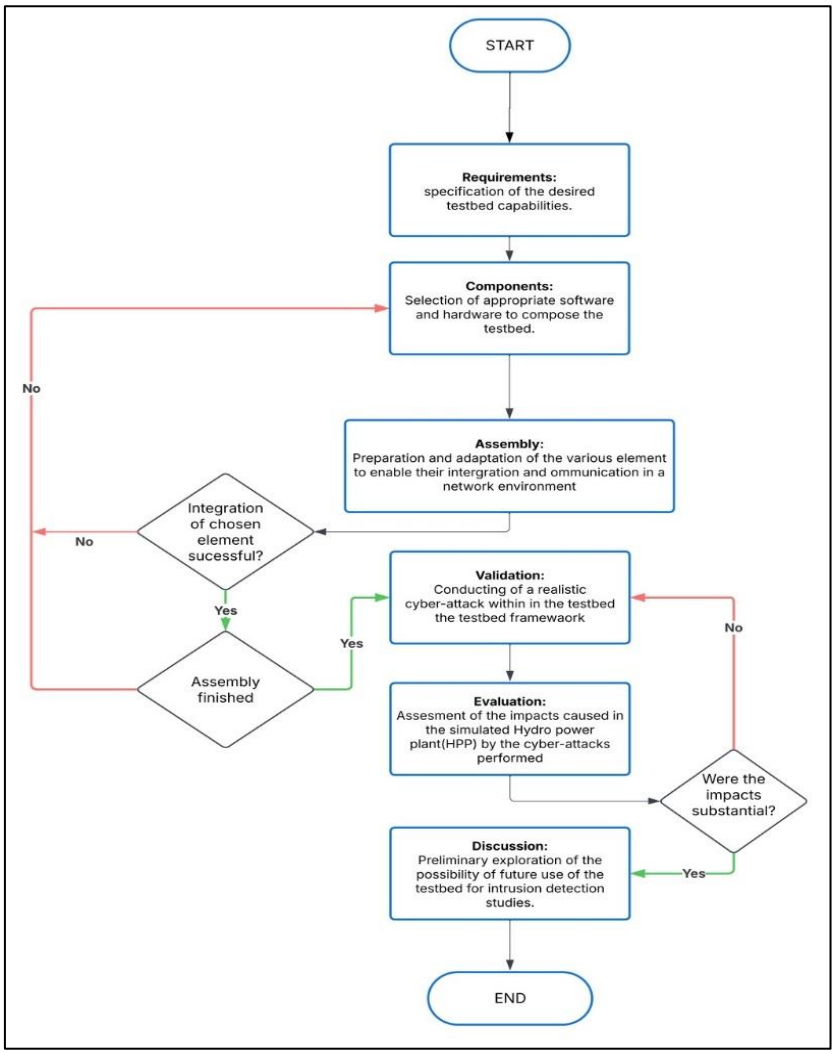

Fig 2 Methodological Process

➢ *The Modbus Protocol*

Devices in various network infrastructures can communicate with one another thanks to the Modbus protocol. The slave device in the master-slave architecture is linked to the outside world by sensors, actuators, or other PLC types(Anon, n.d.). A MODBUS Network Architecture sample can be found in Figure 3.

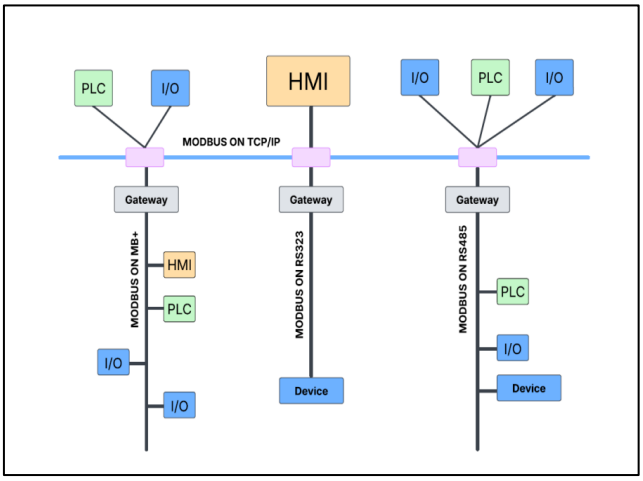

Fig 3. Example of MODBUS Network Architecture

To start a remote operation, all kinds of field devices, PLCs, HMIs, Control Panels, Drivers, Motion Control, and I/O devices connect to the same network utilizing various Modbus implementations, including Modbus+, serial, and Modbus TCP/IP. Modbus+ and serial gateways serve as intermediaries between various bus or network types that employ the Modbus protocol(Voyiatzis et al., 2015).

Modbus is commonly utilized in SCADA environments to offer request and answer message services, which enable the master to obtain data regarding the condition of the slave devices. Four different message kinds make up the very basic communication between the slave and the master(Voyiatzis et al., 2015):

- Request
- Response
- Message Confirmation
- Message Indication

Transactions can only be started by one device (the master) when a master-slave approach is employed. In response, the other devices (the slaves) either provide the master with the desired data or carry out the requested action.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

Any peripheral device that uses Modbus to process data and transmit its output to the master is referred to as a slave. A host computer with the proper application software installed is a typical master device; other devices can be both slaves and masters(Radoglou-Grammatikis et al., n.d.).

➢ *Data and Addressing Model*

Discrete inputs, coils, input registers, and holding registers are the four data types that form the foundation of the Modbus data stack. Discrete inputs are read-only, single-bit data values that serve as data buffers for the slave unit's sensory input. The same is true for the input registers; however, in that instance, the data value in the input register is 16 bits. While holding registers have 16-bit values and coils have single-bit data values, both can be written by the master device and configured to alter the slave's variables and settings if the operator so desires(Anon, n.d.). A summary of the various register types is provided in Table 2.

Table 2 Modbus Register Types

Register type	Description	Access Type
Coils	1-bit registers used to control discrete outputs (including Boolean values)	Read/Write
Discrete Inputs	1-bit registers used as inputs, representing status or conditions	Read-Only
Input Registers	16-bit registers used as inputs, storing numerical values	Read-Only
Holding Registers	16-bit registers used for inputs, outputs, configuration data, or holding data	Read/Write

Every one of the four data kinds has 10,000 assigned addresses and a unique register memory stack. The register memory spaces for the four data kinds are given in Table 3.

Table 3 Register Memory Intervals for Modbus Register

Register Type	Address Range
Coils	1-9999
Discrete Input	10000 -19999
Input Registers	30000 -39999
Holding Registers	40000 - 49999

➢ *MODBUS Frame*

A straightforward Protocol Data Unit (PDU) is defined by the Modbus protocol, regardless of the communication layers that underlie it. Some more fields of the Application Data Unit (ADU) may be introduced by the mapping of the MODBUS protocol on particular busses or networks. Modbus is merely a message structure that is independent of the underlying physical layer, but it specifies guidelines for data organization and interpretation(Anon, n.d.). In Figure 4, the general Modbus frame is shown.

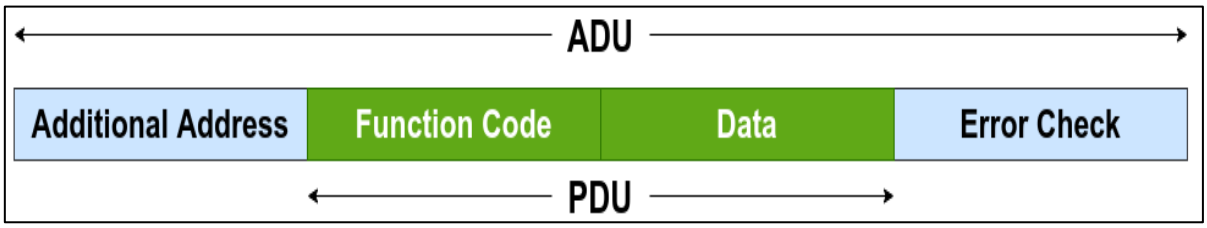

Fig 4 MODBUS Frame

The master device which initiates the transaction, builds the ADU. After the master unicast or multicast the request, the slaves return a response to all the requests that were addressed to them individually, while they cannot respond to broadcast requests and of course, they do not initiate messages on their own. A master's request consists of an address, a function code that defines the requested action, other required data, and an error-checking field. The function code field of a Modbus data unit is coded in one byte. The valid codes are included in a range of 1-255(Anon, n.d.).

The slave's response, on the other hand, is composed of fields that confirm the action taken, data to be returned, and an error-checking field. If there is no error, the slave's response contains the requested data; however, if the received request contains an error or the slave is unable to perform the requested action, the slave will return an exception message, which has a range of 128 to 255, as its response. The error check field, which is the final part of the message's frame, enables the master to verify that the message's contents are valid. For a typical response, the server merely duplicates the request for the original function code(Luswata et al., 2018),(Anon, n.d.).

➢ *Virtual Environment*

A virtual environment of the Zambian Smart Grid was developed to simulate cyberattacks using Kali Linux to initiate the attacks and the GNS3 network simulator. The distribution networks of SCADA control centers and generating units—all crucial components of the Zambian grid—were replicated using virtual machines and industrial control system emulation software such as OpenPLC, SCADABR, PFsense, and HPP.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

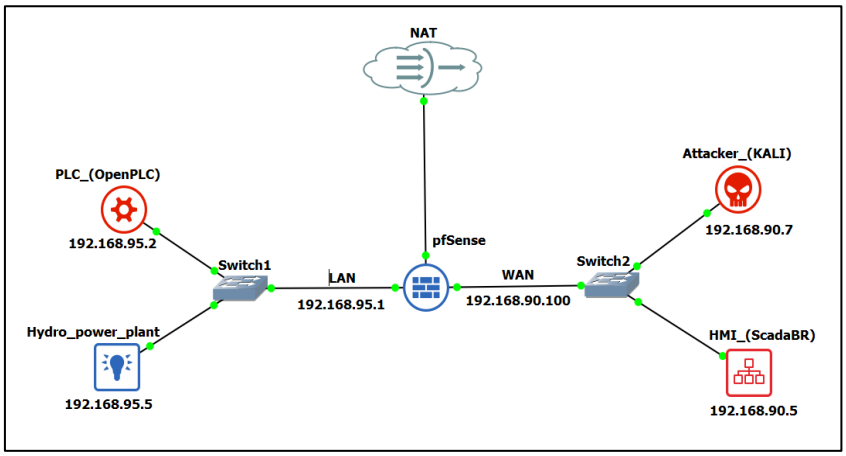

Fig 5 Experimental Setup Network.

➢ *Attack Scenarios*

Since Modbus lacks authentication, any system that looks to be a master can send orders to remote terminals. Messages can be intercepted, altered, and forwarded when integrity checking and encryption are not used. It is vulnerable to man-in-the-middle (MITM) attacks, which are particularly dangerous in SCADA critical control systems because they can simultaneously seize complete control of both protocol parties—the client and the server.

An MITM attack entails connecting a computer equipped with the necessary adapters to an unsecured communication channel. This MITM device can read, alter, and create Modbus messages to or from the device because it integrates a client and Modbus server [12]. The Modbus protocol is extremely susceptible to attacks like command injection, response injection, and measurement injection. Examining the Modbus protocol with different levels of injection attacks—from simple injections to sophisticated injections that target particular fields and values based on domain knowledge—reveals the potential outcomes, including irregular sensor readings, modified actuator states, and system control schemes. This may cause the gadget to completely shut off or only partially impair communication.

The following attacks fall into four general categories: denial of service, command injection, response injection, and reconnaissance. Information about the control system network is gathered via reconnaissance attacks, which also map the network architecture and determine the device's manufacturer, model number, supported network protocols, system address, and memory map. Response injection attacks try to show the controller of a feedback control loop inaccurate sensor data, process measurements, and process state. Attacks using command injection try to insert erroneous commands that result in improper control actions. Attacks known as denial of service aim to interfere with or destroy the communication channels that carry out the feedback control loops.

- *Reconnaissance*

Information about the control system network is gathered via reconnaissance attacks, which also map the network architecture and determine the device's manufacturer, model number, supported network protocols, system address, and memory map.

✓ *Address Scan:*

All legitimate Modbus addresses are sent Modbus queries in the address scan attack, which waits for answers. Modbus addresses that have been implemented will reply with either an error message or a success message. Addresses that are not implemented will not receive a response. To create a list of implemented addresses, the attack iterates through every valid address (0...247).

✓ *Function Code Scan:*

This attack is comparable to an address scan, but it builds a list of implemented function codes by connected addresses by going through all legitimate Modbus function code scans. The function code attack uses a device response to identify implemented function codes, just like the address scan attack does. A particular invalid function code exception is offered by invalid function codes.

✓ *Device Identification:*

To find out the PLC run status, vendor name, product code, major and minor revisions, vendor uniform resource locator (URL), product name, model name, user application name, and other device-specific information, the device identification attack leverages two read device identification functions that are built into the Modbus protocol. You can use this information to look up known flaws in vulnerability databases that have been made public.

✓ *Point Scan:*

For a recognized Modbus device address, the point scan attack generates a map of implemented Modbus data block addresses (coils, discrete inputs, holding registers, and input registers). Point scan attacks use Modbus response codes to identify which addresses are implemented and which are not, and then try to read from and write to every legitimate data block address.

✓ *Memory Dump:*

The goal of the memory dump assault is to read every PLC data block's contents.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

✓ *Modbus Network Scanning:*
To gather data about field equipment, this attack sends harmless messages to any address that could be on a Modbus network.

✓ *Passive Reconnaissance:*
An attack that reads network traffic or Modbus messages passively. By rebuilding the device application, this attack aids the attacker in profiling the process details.

- *Response Injection Attack*

There are three types of response injection attacks. First, programmable logic controllers, remote terminal units, and network endpoints—the servers that answer network client queries—can all be the source of response injection attacks. Second, during transmission from server to client, response injection attacks can intercept network packets and change their contents. Lastly, a third-party device within the network may create and send response injections. In this instance, a client query may receive more than one response, and the invalid response may become the more prominent one because it takes advantage of a race condition or a secondary assault like a denial of service Command Injection assault.

- *Command Injection Attacks*

Command introduces fictitious configuration and control commands into a control system. Control systems are managed by human operators, who also occasionally interfere with supervisory control activities. Hackers might try to introduce fictitious supervisory control activities into a network of control systems. Intelligent electronic devices and remote terminals are typically configured to automatically monitor and manage the physical process at a distant location. Ladder logic, C code, and registers—which store important control parameters like high and low limits and gating process control actions—are the programming formats used in this software. Ladder logic, C code, and remote terminal register settings can all be overwritten by hackers via command injection techniques. Malicious command injections may cause device communications to be interrupted, process control to be interrupted, device configurations to be altered without authorization, and process set points to be altered without authorization. Many industrial control system network protocols lack authentication mechanisms to confirm the packets' origin, as was indicated in the response injection discussion above. Attackers can now intercept and modify command packets thanks to this.

To prevent the real server from responding, attackers can also create unique command packets and insert them straight into the control system network service assault [35].Additionally, attackers can craft original command packets and directly inject them into the control system network service attack which stops the true server from responding [35].

- *Denial of Service Attacks*

Attacks known as denial of service (DOS) are used against industrial control systems to prevent specific parts of the cyber-physical system from operating normally, hence rendering the entire system inoperable. Because of this, DOS assaults can target either the physical or cyber system. DOS assaults on the cyber system try to stop programs that run on system endpoints that manage communications, log data, and control the system, or they target communication lines.

DOS attacks on the physical system can take many different forms, ranging from manually opening or closing switches and valves to destroying parts of the physical process that stop it from working.

IV. EXPERIMENTAL ATTACK ON MODBUS TCP

For the following experimental attack on Modbus TCP, we will use a lab setup that includes 4 virtual machines, They are all running on Ubuntu, We have the PLC with IP address 192.168.95.2 assigned. Next is the HPP(Hydro_Power_Plant) with an IP address 192.168.95.5 assigned, Next we have the HMI with IP address 192.168.90.5 assigned and Lastly we have Kali Linux which is our attacking machine with IP address 192.168.90.7 assigned.

All the machines were assigned an IP address by the PFSense, an open source firewall and router, It is also segregating the LAN network from and WLAN network.

➢ *OpenPLC*
OpenPLC is an open source PLC software that mimics real-world industrial controllers used in hydropower and other Industrial Control Systems.

➢ *ScadaBR*
SscadBR is an open source industrial system that acts as the Human-Machine Interface where operators monitor and control the industrial process.

➢ *HPP*
The hydropower plant is the critical infrastructure being controlles by the OpenPLC, But in this research, we used a Chemical Power Plant to simulate the attack

➢ *KALI*
Kali is an Open source linux distribution for penetration testing, We used it for scanning, exploiting, packet sniffing, and man-in-the-middle (MITM) attacks on the SCADA network.

➢ *PFSense*
PFSense was used to create segmented zones (DMZ) between the internal and external network (IT and OT).

It was also used to enforce firewall rules.

The other components used included two switches,Switch 1 and Switch 2. And a NAT network configuration was used when connecting the router (pfSense).

➢ *Attack on Registers*
We began by powering on all relevant devices: the attacker machine, SCADA HMI, the PLC server (OpenPLC),

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

and the chemical plant simulation system. Since these devices were preconfigured, we initiated the reconnaissance phase by running netdiscover to identify other active devices on the same network.

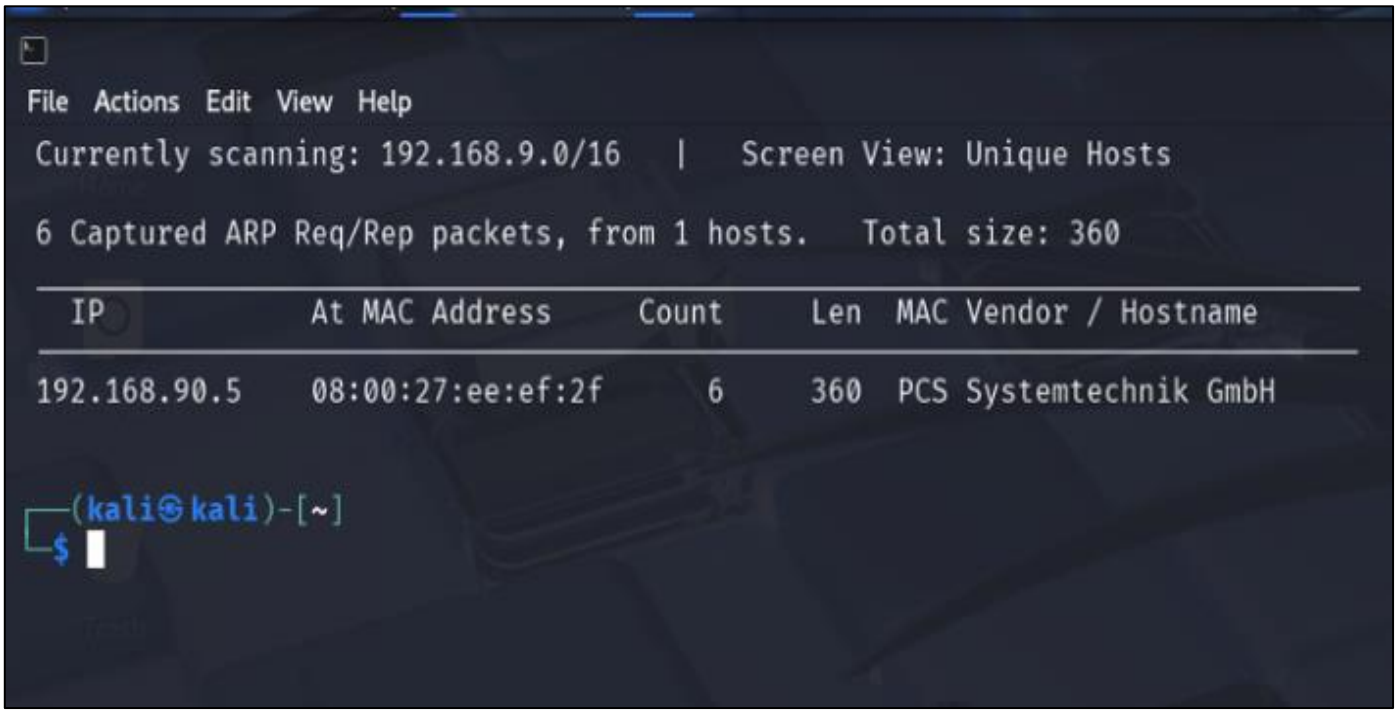

Fig 6 Attack on Registers

After discovering 192.168.90.5, which is our HMI, we pinged it to verify connectivity.

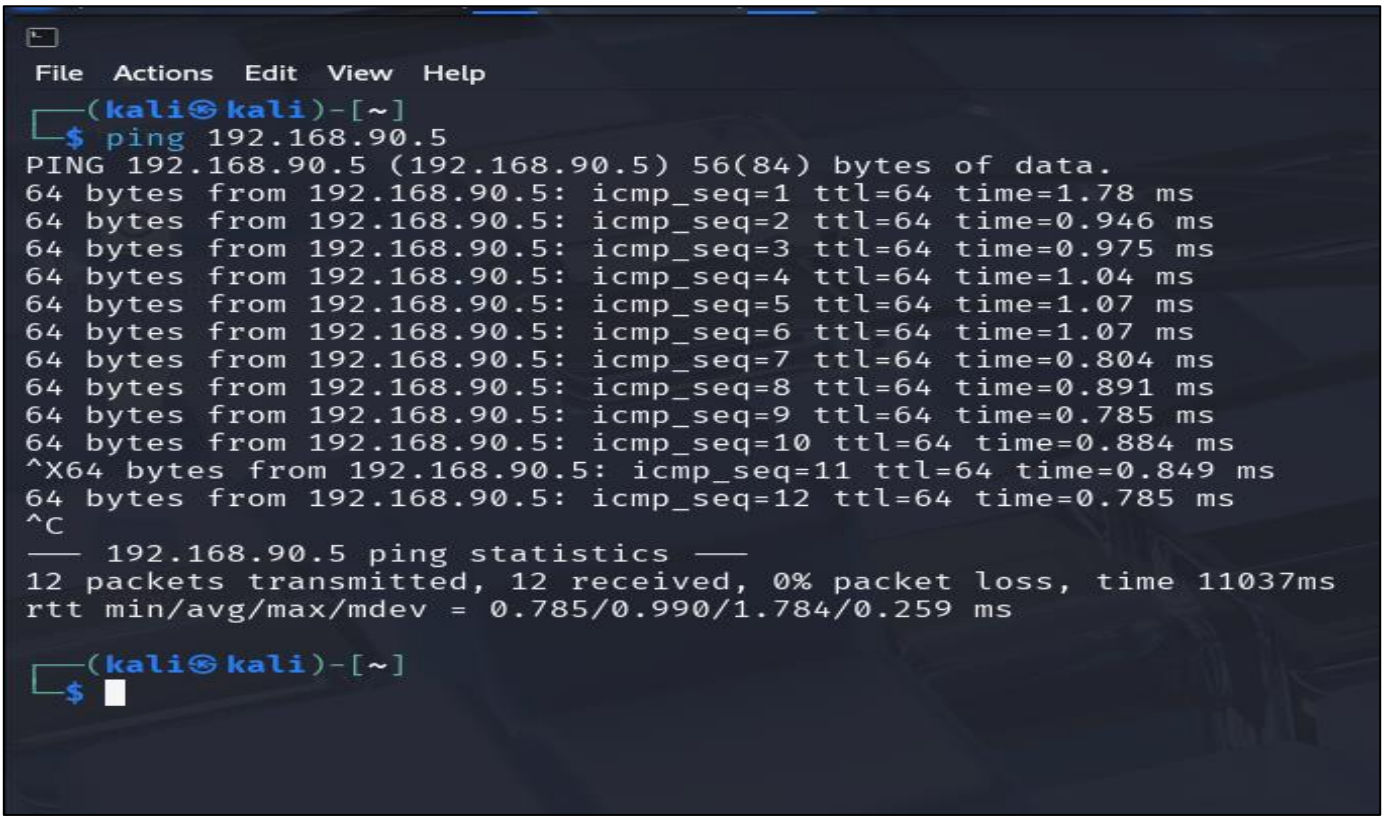

Fig 7 Attack on Registers

Next, we launched Wireshark, a network protocol analyzer, to observe communications between the HMI and other devices. During packet inspection, we noticed that the HMI was sending data to an IP: 192.168.95.2, which belonged to a different subnet.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

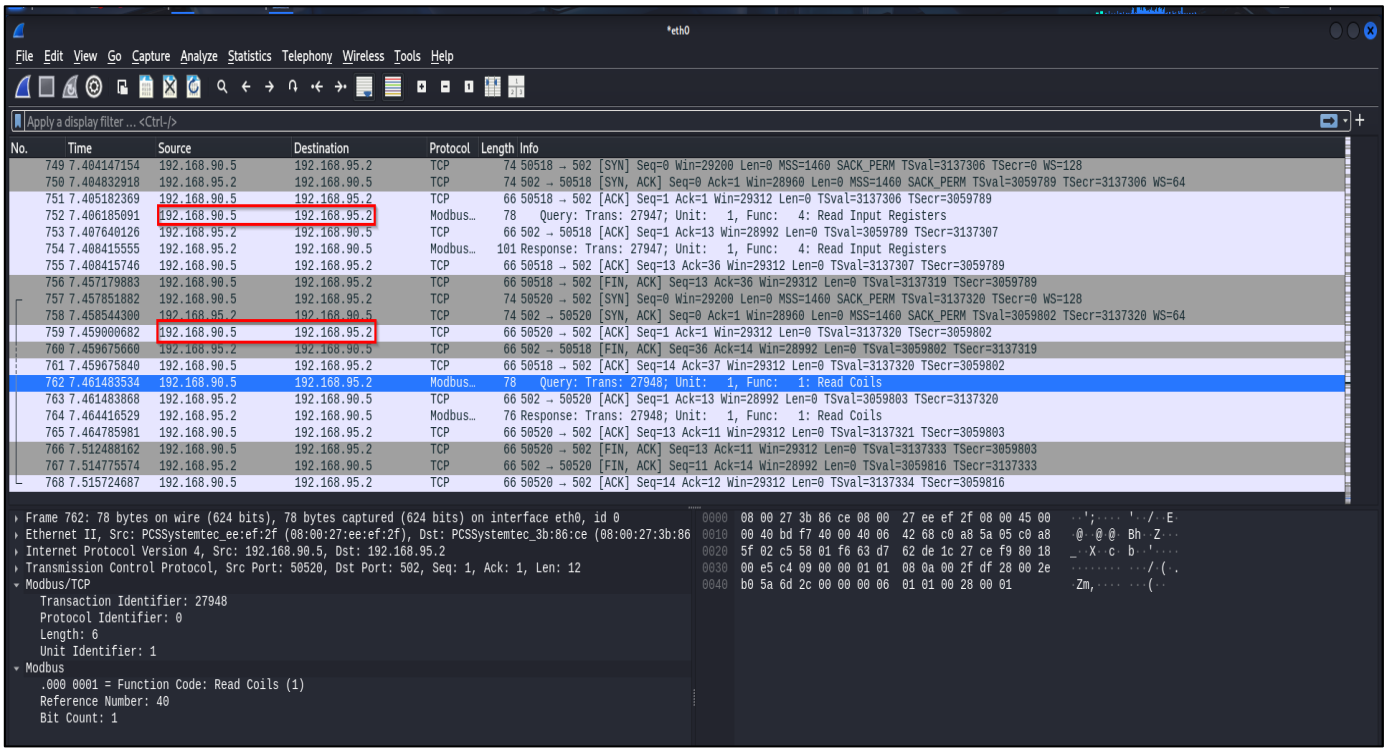

Fig 8 Attack on Registers

To interact with the target IP (192.168.95.2), we configured a new network route on our attacker machine, enabling communication with the 192.168.95.0/24 subnet.

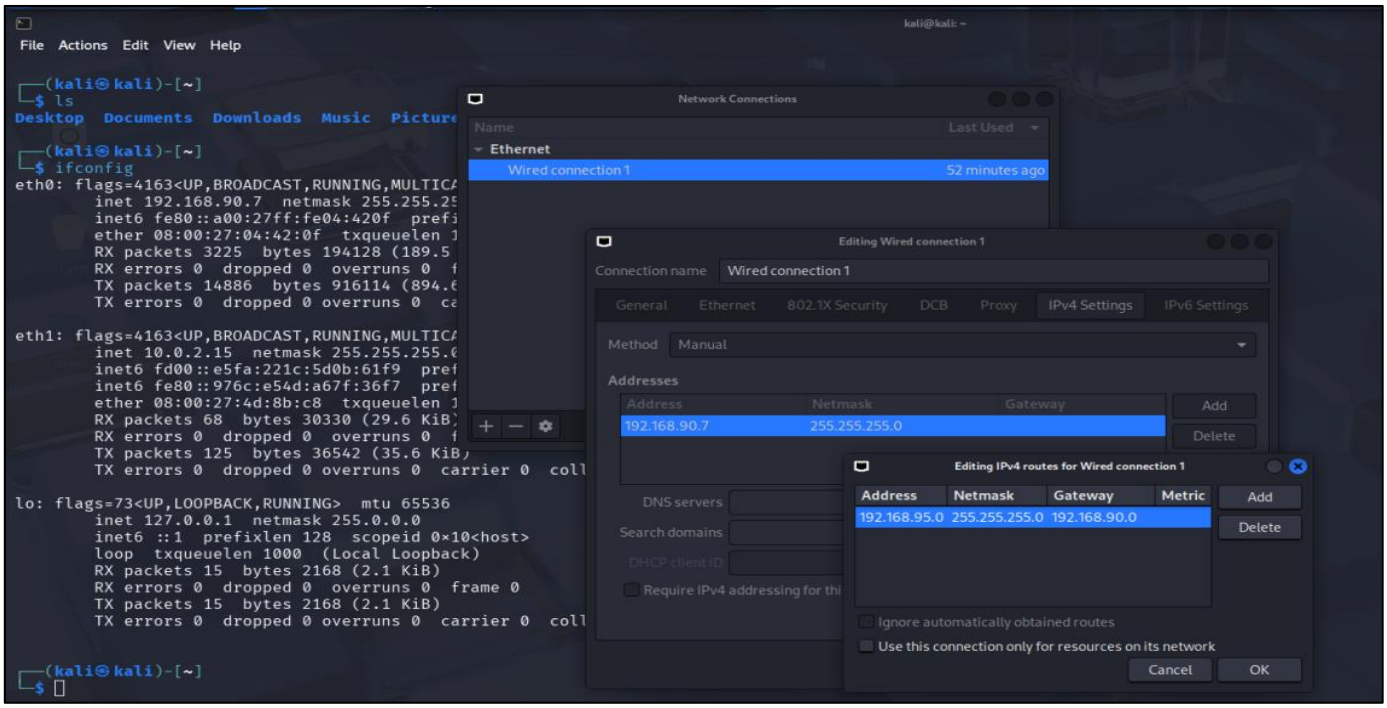

Fig 9 Attack on Registers

Once routing was set up, we confirmed connectivity by successfully pinging 192.168.95.2.

With connectivity established, we ran an Nmap scan on the target IP. The scan revealed the following open ports:

- Port 22 (SSH) – Secure Shell
- Port 80 (HTTP) – Web server
- Port 502 (Modbus) – Industrial control protocol used by PLCs

The presence of port 502 confirmed that the target was a PLC server.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 -sS -p- 192.168.95.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 06:06 EDT
Warning: 192.168.95.2 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.95.2
Host is up (0.0023s latency).
Not shown: 65435 closed tcp ports (reset), 97 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 19:c7:93:27:d7:fa:95:3c:d1:0e:c9:dd:9b:1f:f4:cf (RSA)
|   256 de:bc:c6:2d:2d:76:b2:b1:49:eb:c8:cf:81:4b:f5:40 (ECDSA)
|_  256 65:d6:e5:68:f2:be:ad:3e:0b:b3:44:4e:c0:28:26:ff (ED25519)
502/tcp  open  modbus  Modbus TCP
8080/tcp open  http    Node.js (Express middleware)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-open-proxy: Proxy might be redirecting requests
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.9
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Fig 10 Attack on Registers

Our objective was to manipulate the PLC's oils and registers using multiple attack methods. Tools used included:

- Metasploit's Modbus module
- Modbus Client (CLI-based tool)

From Wireshark, we gathered critical Modbus protocol parameters:

- Unit Identifier,
- Function Code: 1 (Read Coils)
- Reference Number: 40

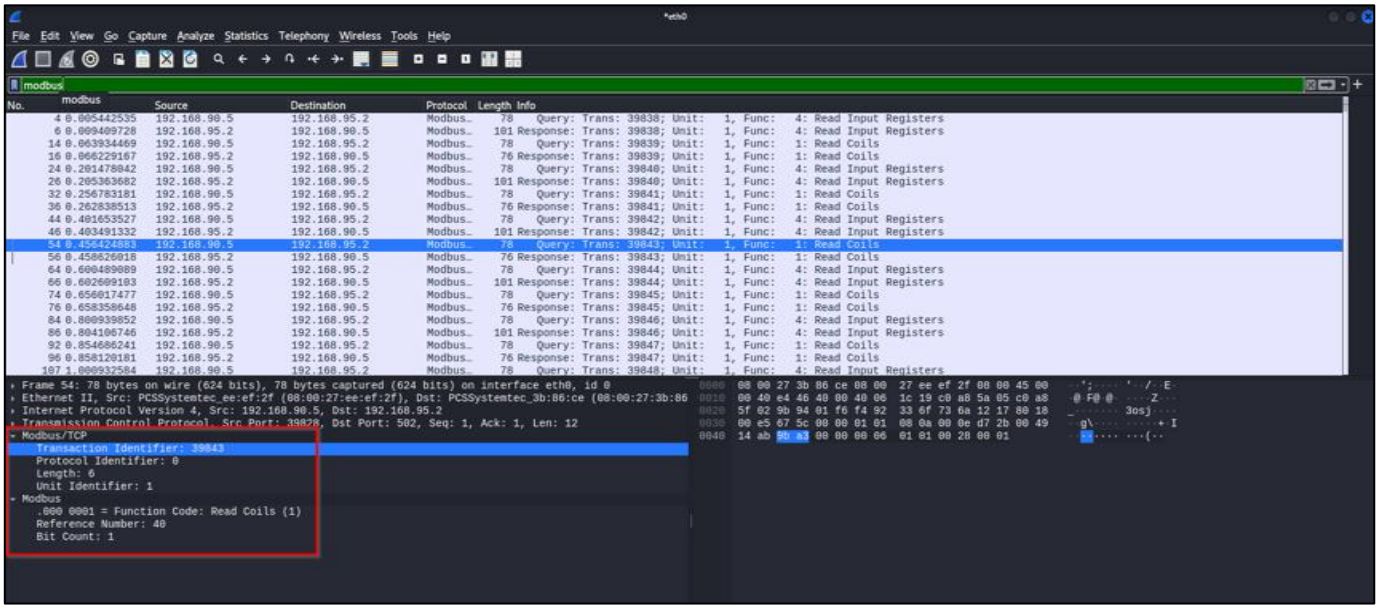

Fig 11 Monitoring Traffic in Wireshark

These parameters guided our register manipulation.

Launched the Metasploit Framework

Searched and selected the modbusclient module

Configured key options:

RHOSTS: 192.168.95.2

REF: 40

Action: WRITE_REGISTERS

Data_register: 65535, 65535, 65535

FUNC: Set to write coils or registers

Ran the module, which successfully wrote values to the PLC registers

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

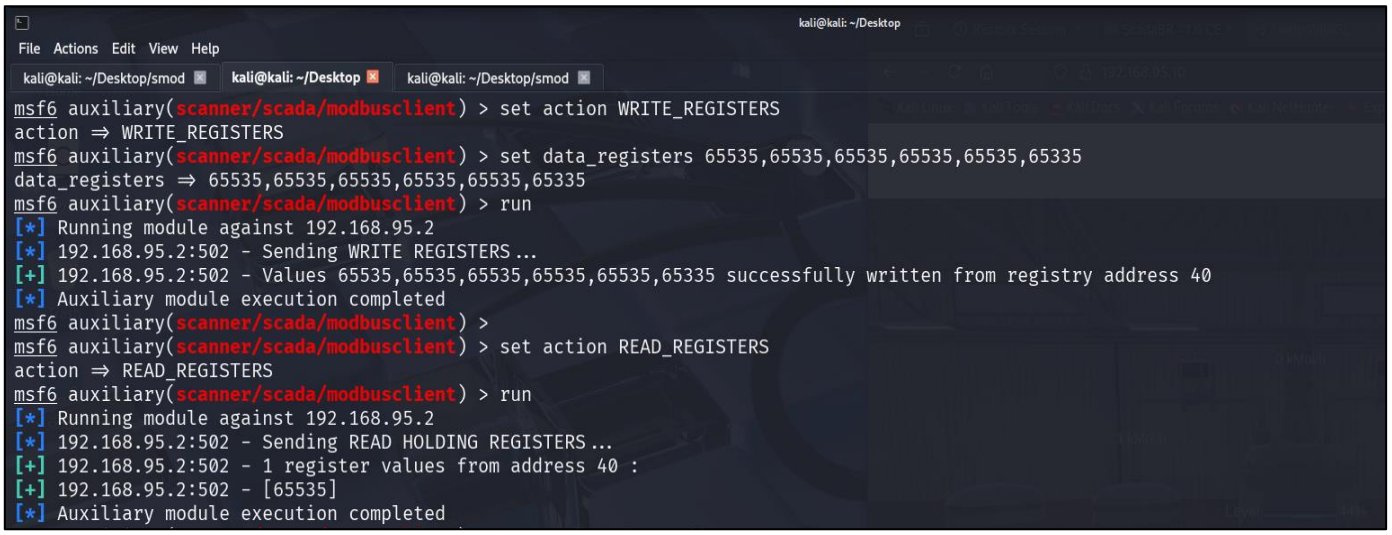

Fig 12 Setting Config in Metasploit

We changed the Function Code and reference address to read back the manipulated values. The output confirmed the registers were overwritten with values like 65535, from address 40. Validating the success of the exploitation of registers.

Fig 13 Exploiting in MSF Console

➢ *Attack on Coils*

The next phase of our attack involves attempting to change the values of the coils. Coils are binary — they can either be 1 (on) or 0 (off). These values control various aspects of the system, such as whether a component should be hot or cold, open or closed, or set to high or low. Essentially, they're used in simple if-condition logic.

For this task, we'll be using an open-source tool called modbus-client and metasploit modbus module. Our goal is to overwrite coil values at different addresses and observe how the plant responds to those changes.

We will start by installing the tool.

Fig 14 Installing Modbus Client

Since we've already established a connection to the Modbus server, we'll begin by reading the current coil values. Specifically, we'll read 30 coils starting from address 20 using the following command:

Modbus read 192.168.95.2 %M20 30

In this command:

- Modbus read: This is the command used to read coil data from a Modbus-compatible device.
- 192.168.95.2: This is the IP address of the target device we're communicating with.
- %M20 In Schneider Electric's Modbus notation, %M refers to memory bits, specifically coils. The number 20 is the starting address of the coil we want to access.
- 30 This indicates the number of consecutive coils to read, starting from address 20.

From the output, we can see that all 30 coils are initially set to 0.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

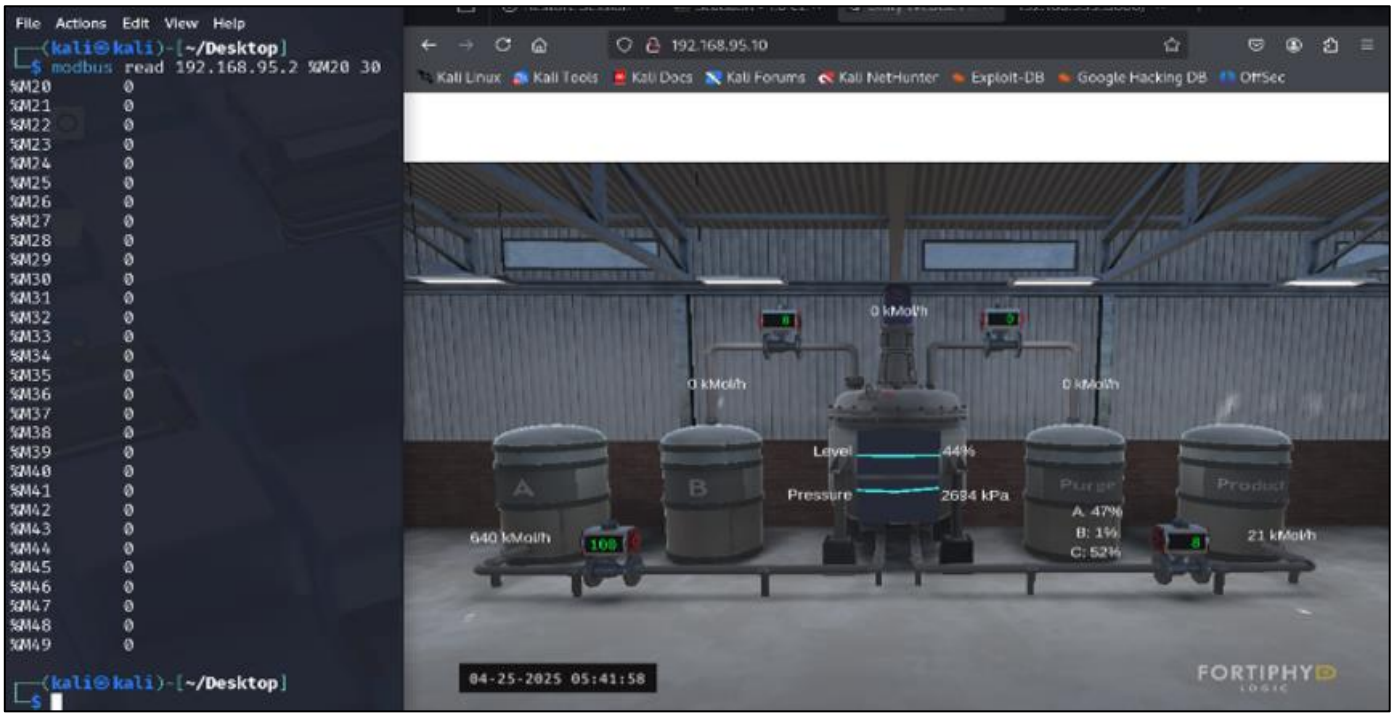

Fig 15 Reading the Number

Next, we'll try writing a value of 1 to coil address 39, 40 and 41 and observe what happens in the plant.

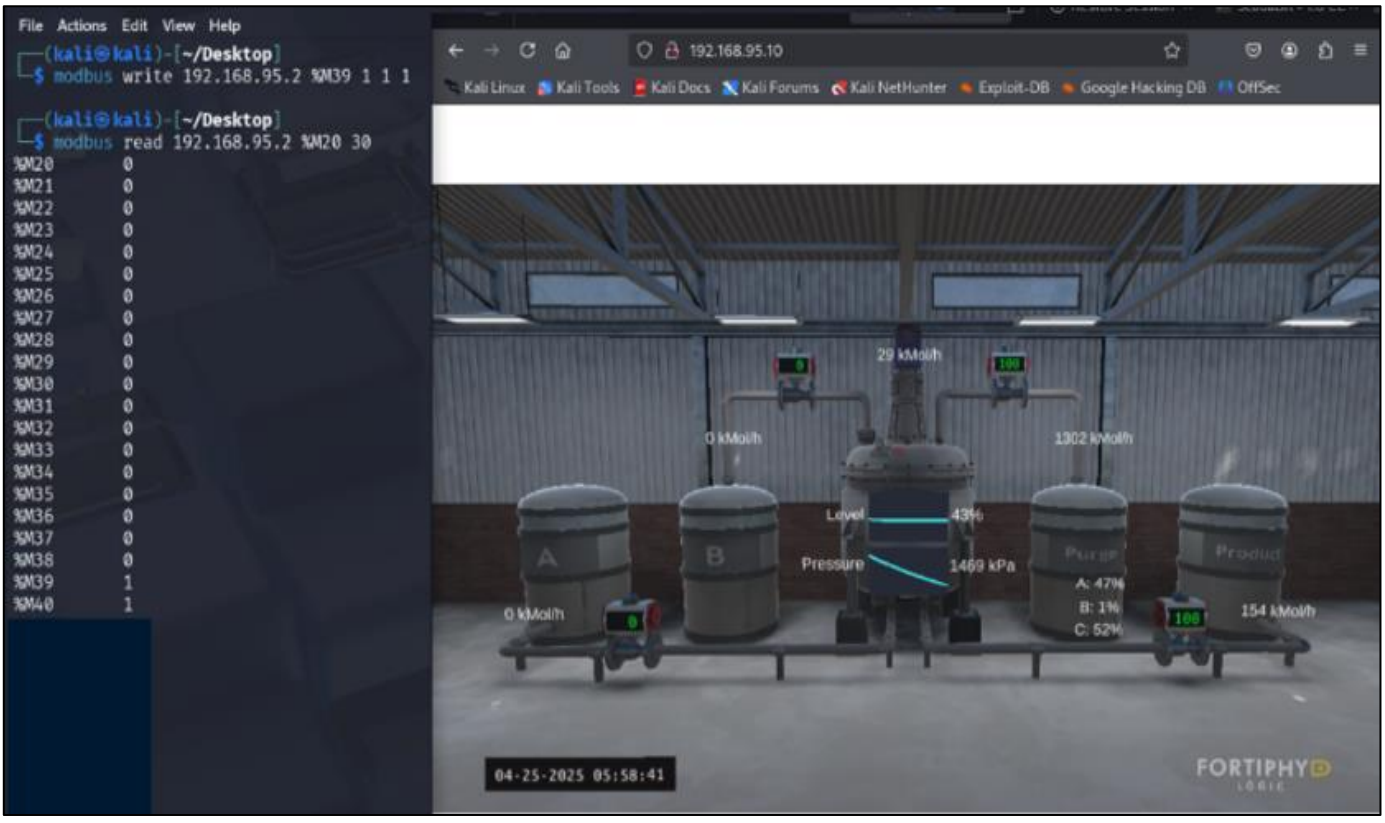

Fig 16 Testing Coil Addresses with Value 1

The results show that the plant's temperature begins to drop rapidly. This indicates that coil address 40 controls the cooling system.

Now, let's try writing a 1 to coil address 41 and see what effect it has.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

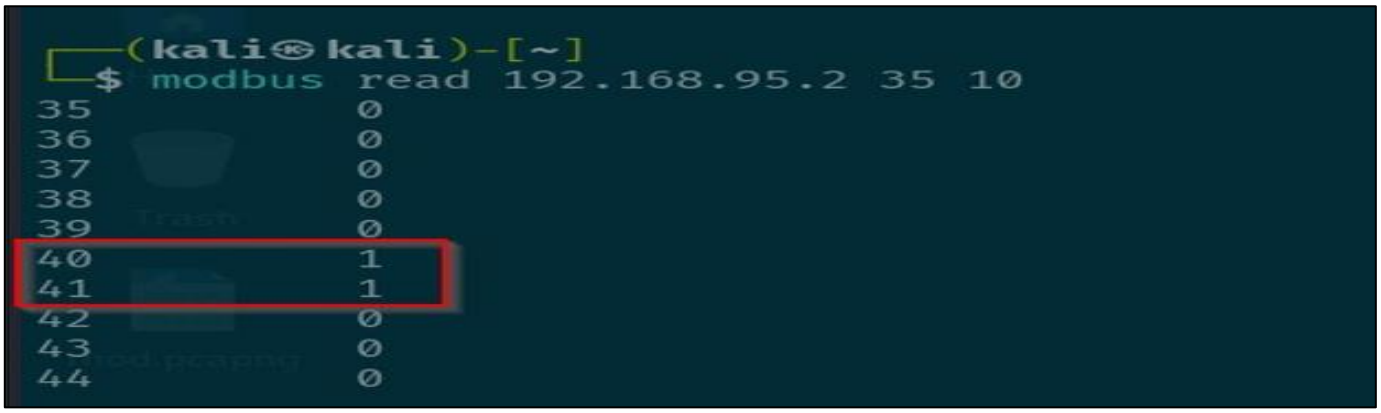

Fig 17 Obeserving Changes

And this is the result of the plant when address 41 coil value is written ti 1.

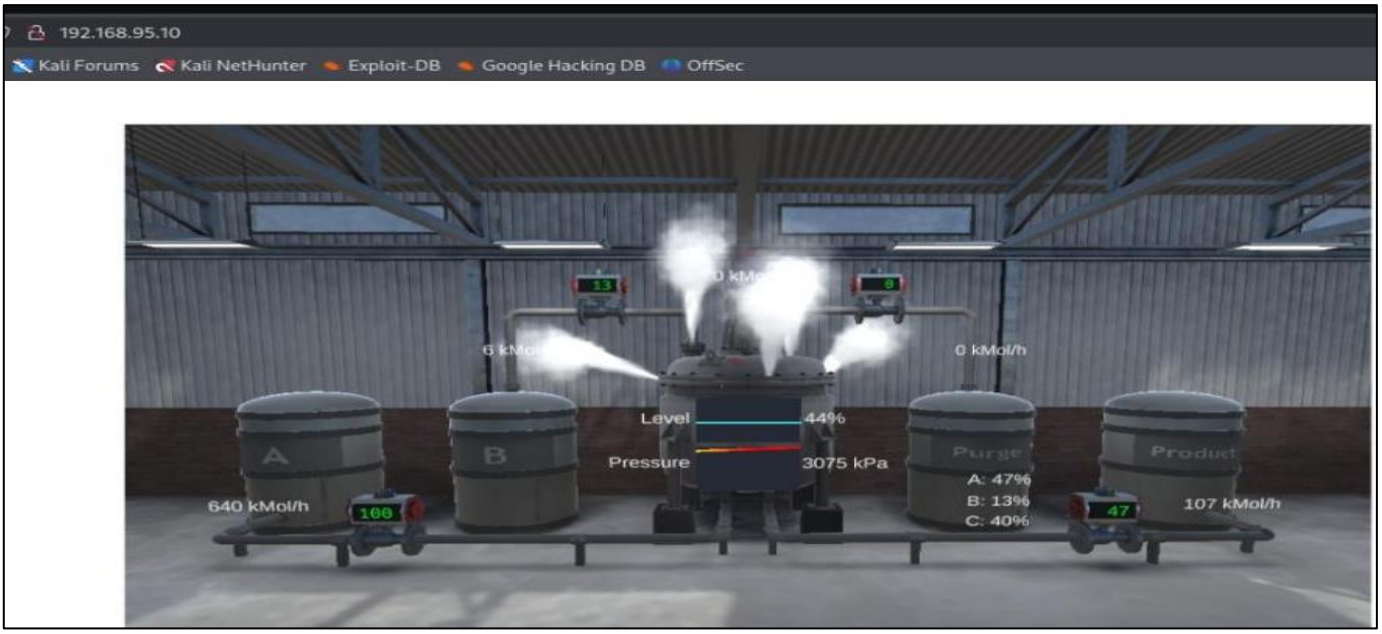

Fig 18 Temperature Changing

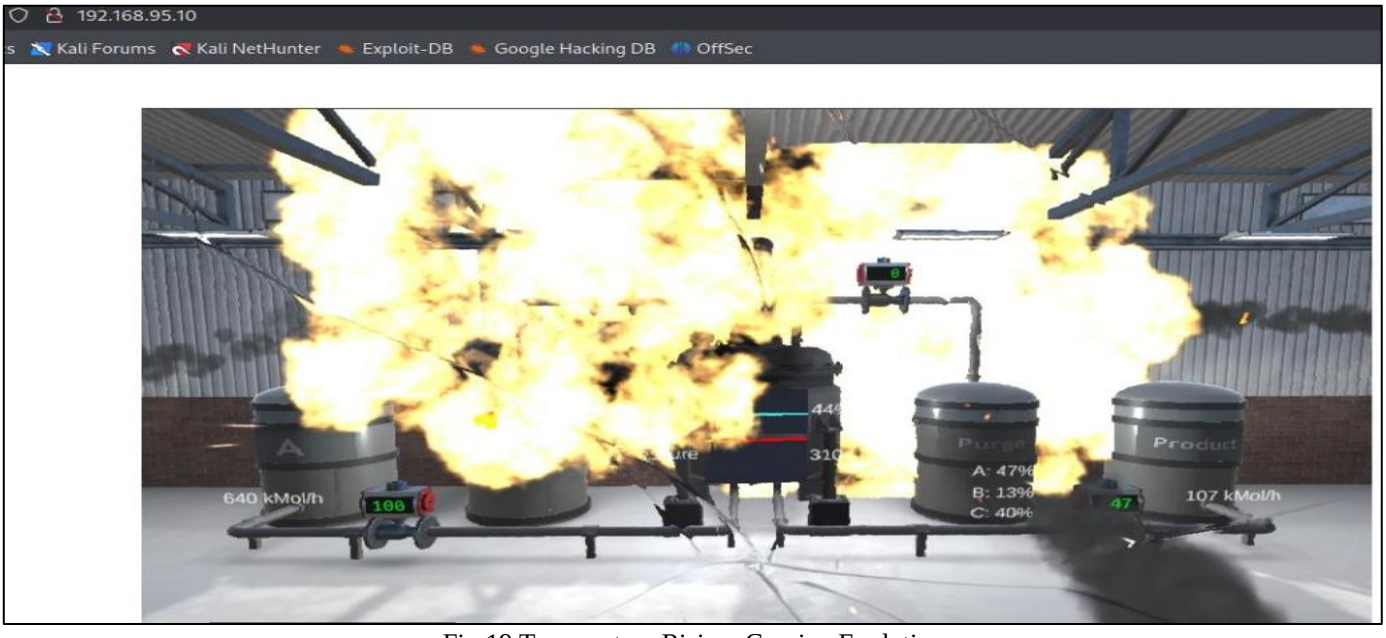

Fig 19 Temperature Rising, Causing Explotion

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

This time, the temperature rises extremely fast, so much so that the plant eventually explodes. This tells us that coil address 41 controls the heating system, and improper use can lead to catastrophic failure.

V. CONCLUSION

This study has demonstrated the vulnerability of the Modbus protocol to cyber-attacks in the context of Zambia's Smart Grid infrastructure. By simulating two types of cyber-attacks in a virtual environment, we have identified critical areas where cybersecurity measures need to be strengthened. The findings emphasize the need for the adoption of encryption, secure authentication mechanisms, and continuous network monitoring to protect the grid from potential attacks.

As Zambia continues to modernize its power infrastructure, it is crucial to prioritize cybersecurity in the Smart Grid ecosystem to ensure the reliable and safe distribution of electricity across the country.

VI. FUTURE WORK

Future work will focus on enhancing the simulation environment by incorporating additional communication protocols such as IEC 61850 and DNP3, which are also widely used in Smart Grids. Furthermore, the deployment of machine learning-based intrusion detection systems (IDS) will be explored to detect and mitigate cyber-attacks in real-time. Additionally, a more detailed model of the Zambian grid, including renewable energy sources, will be developed to assess how cyber-attacks affect the integration of distributed energy resources (DERs). Expanding collaboration with energy stakeholders and cybersecurity experts in Zambia will be key to advancing research in securing the nation’s Smart Grid infrastructure.

REFERENCES

[1]. Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.E.A., Bajaj, M., Blazek, V. and Prokop, L. 2024. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in Engineering. 23, p.102647.

[2]. Aboah Boateng, E. and Bruce, J.W. 2022. Unsupervised Machine Learning Techniques for Detecting PLC Process Control Anomalies. Journal of Cybersecurity and Privacy. 2(2), pp.220–244.

[3]. Admass, W.S., Munaye, Y.Y. and Diro, A.A. 2024. Cyber security: State of the art, challenges and future directions. Cyber Security and Applications. 2, p.100031.

[4]. Alawida, M., Omolara, A.E., Abiodun, O.I. and Al-Rajab, M. 2022. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences. 34(10), pp.8176–8206.

[5]. Alghamdi, M.I. 2021. Impact of Cyber Attack on Saudi Aramco. Journal of Cybersecurity and Information Management (JCIM). 7(1), pp.13–21.

[6]. Ametov, F.R., Bekirov, E.A. and Asanov, M.M. 2021. Organization of Secure Communication between Programmable Logic Controllers Using the Open Platform Communications Protocol. Journal of Physics: Conference Series. 2096(1), p.012125.

[7]. Anon n.d. Africa GreenCo Granted Electricity Trading And Import/Export Licenses in South Africa – Africa GreenCo. [Accessed 1 February 2025a]. Available from: https://africagreenco.com/africa-greenco-granted-electricity-trading-and-import-export-licenses-in-south-africa/.

[8]. Anon 2024. Attacks on Ukraine’s Electric Grid: Insights for U.S. Infrastructure Security and Resilience.

[9]. Anon n.d. Beyond the Grid Fund for Africa signs its first projects with off-grid energy service companies in Zambia - BGFA. [Accessed 1 February 2025b]. Available from: https://beyondthegrid.africa/news/beyond-the-grid-fund-for-africa-signs-its-first-projects-with-off-grid-energy-service-companies-in-zambia/.

[10]. Anon n.d. Compromise of U.S. Water Treatment Facility | CISA. [Accessed 8 February 2025c]. Available from: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a.

[11]. Anon n.d. Energy Sector – Ministry of Energy. [Accessed 1 February 2025d]. Available from: https://www.moe.gov.zm/?page_id=2198.

[12]. Anon n.d. Internet of Things Device - an overview | ScienceDirect Topics. [Accessed 1 February 2025e]. Available from: https://www.sciencedirect.com/topics/computer-science/internet-of-things-device.

[13]. Anon n.d. MINISTRY OF ENERGY LAUNCHES 2023 NATIONAL ENERGY ACCESS SURVEY REPORT – Ministry of Energy. [Accessed 1 February 2025f]. Available from: https://www.moe.gov.zm/?p=3813.

[14]. Anon n.d. Modbus - an overview | ScienceDirect Topics. [Accessed 22 March 2025g]. Available from: https://www.sciencedirect.com/topics/computer-science/modbus.

[15]. Anon n.d. Northwestern Energy Corporation Ltd | Electricity | Zambia. [Accessed 1 February 2025h]. Available from: https://www.northwesternenergycorp.com/.

[16]. Anon n.d. Simulation Software - MATLAB & Simulink. [Accessed 8 February 2025i]. Available from: https://www.mathworks.com/discovery/simulation-software.html.

[17]. Anon n.d. Smart infrastructure solution transforming Zambia’s grid - Iskraemeco Corpo. [Accessed 26 October 2024j]. Available from: https://iskraemeco.com/news/smart-infrastructure-solution-transforming-zambias-grid/.

[18]. Anon n.d. Stuxnet - an overview | ScienceDirect Topics. [Accessed 5 February 2025k]. Available from:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

https://www.sciencedirect.com/topics/computer-science/stuxnet.

[19]. Anon n.d. Supervisory Control and Data Acquisition System - an overview | ScienceDirect Topics. [Accessed 1 February 2025l]. Available from: https://www.sciencedirect.com/topics/engineering/supervisory-control-and-data-acquisition-system.

[20]. Bashendy, M., Eltanbouly, S., Tantawy, A. and Erradi, A. 2021. Design and Implementation of Cyber-Physical Attacks on Modbus/TCP Protocol. , pp.38–45.

[21]. Bayliss, K. and Pollen, G. 2021. The power paradigm in practice: A critical review of developments in the Zambian electricity sector. World Development. 140, p.105358.

[22]. Bhajekar, A. and Gupta, Dr.S. 2024. CYBER SECURITY FOR POWER GRIDS: THREATS, MITIGATION, AND FUTURE OUTLOOK. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. 08(09), pp.1–4.

[23]. Chitandula1, A., Abuzayed, A., Nyoni, K.J., Solà Vilalta, A., Maliye5, R., Kabala6, E. and Cheelo7, C. n.d. STATUS QUO OF THE ENERGY SYSTEM AND CONSUMPTION IN ZAMBIA PART ONE OF A THREE PART SERIES FOR THE GoPRO-ZAMBIA RESEARCH PROJECT STATUS QUO OF THE ENERGY SYSTEM AND CONSUMPTION IN ZAMBIA Zambia Report Series STATUS QUO OF THE ENERGY SYSTEM AND CONSUMPTION IN ZAMBIA.

[24]. Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. 2022. Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance. Issues and Practice. 47(3), p.698.

[25]. Entwisle, B., Grieshop, A.P., Lloyd, S., Radin, M., Saparapa, R., Scott, S. and Sinai, C. n.d. ENERGY ACCESS EPPSA TEAM Energy Poverty PIRE in Southern Africa • STATE OF KNOWLEDGE ENERGY ACCESS IN ZAMBIA.

[26]. Figueroa-Lorenzo, S. 2019. A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach.

[27]. Ghanbari, H., Koskinen, K. and Wei, Y. 2024. From SolarWinds to Kaseya: The rise of supply chain attacks in a digital world. Journal of Information Technology Teaching Cases.

[28]. Gopal, S.B., Poongodi, C. and Nanthiya, D. 2022. Blockchain-based secured payment in IoE. Smart Energy and Electric Power Systems: Current Trends and New Intelligent Perspectives., pp.185–200.

[29]. Huitsing, P., Chandia, R., Papa, M. and Shenoi, S. 2008. Attack taxonomies for the Modbus protocols. Int. J. Crit. Infrastructure Prot. 1, pp.37–44.

[30]. Jahid, A., Alsharif, M.H. and Hall, T.J. 2023. The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap. Journal of Network and Computer Applications. 217.

[31]. Khalid, M. 2024. Smart grids and renewable energy systems: Perspectives and grid integration challenges. Energy Strategy Reviews. 51, p.101299.

[32]. Knapp, E.D. and Langill, J.T. 2015. Hacking Industrial Control Systems. Industrial Network Security., pp.171–207.

[33]. Li, S.C., Huang, Y., Tai, B.C. and Lin, C.T. 2017. Using Data Mining Methods to Detect Simulated Intrusions on a Modbus Network. Proceedings - 2017 IEEE 7th International Symposium on Cloud and Service Computing, SC2 2017. 2018-January, pp.143–148.

[34]. Lukumba Phiri, by 2023. A framework for cyber security risk modeling and mitigation in smart grid communication and control systems.

[35]. Luswata, J., Zavarsky, P., Swar, B. and Zvabva, D. 2018. Analysis of SCADA Security Using Penetration Testing: A Case Study on Modbus TCP Protocol. 29th Biennial Symposium on Communications, BSC 2018.

[36]. McLaughlin, K., Friedberg, I., Kang, B.J., Maynard, P., Sezer, S. and McWilliams, G. 2015. Secure Communications in Smart Grid: Networking and Protocols. Smart Grid Security: Innovative Solutions for a Modernized Grid., pp.113–148.

[37]. Moghaddass, R. and Wang, J. 2018. A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data. IEEE Transactions on Smart Grid. 9(6), pp.5820–5830.

[38]. Mouha, R.A. and Mouha, R.A. 2021. Internet of Things (IoT). Journal of Data Analysis and Information Processing. 9(2), pp.77–101.

[39]. Parian, C., Guldimann, T. and Bhatia, S. 2020. Fooling the Master: Exploiting Weaknesses in the Modbus Protocol. Procedia Computer Science. 171, pp.2453–2458.

[40]. Paul, B., Sarker, A., Abhi, S.H., Das, S.K., Ali, Md.F., Islam, M.M., Islam, Md.R., Moyeen, S.I., Rahman Badal, Md.F., Ahamed, Md.H., Sarker, S.K., Das, P., Hasan, Md.M. and Saqib, N. 2024. Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. Heliyon. 10(19), p.e37980.

[41]. Phiri, L. and Tembo, S. 2022. Evaluating the Security Posture and Protection of Critical Assets of Industrial Control Systems in Zambia International Journal of Advances in Scientific Research and Engineering (ijasre) Evaluating the Security Posture and Protection of Critical Assets of Industrial Control Systems in Zambia. Article in International Journal of Advances in Scientific Research and Engineering.

[42]. Pollard, M. n.d. Pepperdine Policy Review Pepperdine Policy Review A Case Study of Russian Cyber-Attacks on the Ukrainian Power A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States Grid: Implications and Best Practices for the United States. Pepperdine Policy Review. 16, pp.4–23.

[43]. Pospisil, O., Blazek, P., Kuchar, K., Fujdiak, R. and Misurec, J. 2021. Application Perspective on Cybersecurity Testbed for Industrial Control Systems. Sensors (Basel, Switzerland). 21(23).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun263

[44]. Radoglou-Grammatikis, P., Siniosoglou, I., Liatifis, T., Kourouniadis, A., Rompolos, K. and Sarigiannidis, P. n.d. Implementation and Detection of Modbus Cyberattacks.
[45]. Radoglou-Grammatikis, P.I. and Sarigiannidis, P.G. 2019. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. IEEE Access. 7, pp.46595–46620.
[46]. Teixeira, M.A., Salman, T., Zolanvari, M., Jain, R., Meskin, N. and Samaka, M. 2018. SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach. Future Internet. 10(8), pp.1–15.
[47]. Thornton, J.Z. 2015. A virtualized SCADA laboratory for research and teaching.
[48]. Upadhyay, D., Ghosh, S., Ohno, H., Zaman, M. and Sampalli, S. 2024. Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator. International Journal of Critical Infrastructure Protection. 47, p.100705.
[49]. Voyiatzis, A.G., Katsigiannis, K. and Koubias, S. 2015. A Modbus/TCP Fuzzer for testing internetworked industrial systems. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA. 2015-October.
[50]. Wang, P.H., Liao, I.E., Kao, K.F. and Huang, J.Y. 2018. An intrusion detection method based on log sequence clustering of honeypot for Modbus TCP protocol. International Conference on Applied System Innovation., pp.255–258.
[51]. Zhang, F. and Coble, J.B. 2020. Robust localized cyber-attack detection for key equipment in nuclear power plants. Progress in Nuclear Energy. 128.
[52]. Zhang, F., Kodituwakku, H.A.D.E., Hines, J.W. and Coble, J. 2019. Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Transactions on Industrial Informatics. 15(7), pp.4362–4369.