[1] **Dr. Tejaskumar P. Bhatt**

[2*] **Dr. Yagnik A Rathod**

[3] **Dr. Virendra K Barot**

[4] **Prof. Ashok K Rathva**

[5] **Prof. Vanraj D Baria**

[6] **Prof. Salman Y Bhimla**

Design and Implementation of AMI Network for Smart Grid using MQTT Protocol

JES Journal of Electrical Systems

Abstract: - In a Smart Grid, Smart Meters (SM) is an essential component and are used to realize the actual-time information series. Advanced Metering Infrastructure (AMI) a network infrastructure with a variety of Smart Energy Meters connected to a distributed system and will provide flexible control, transmission. The Smart Grid has great benefits, but cyber and physical security, and privacy concerns are arising as critical concerns. Smart Grid may suffer from a variety of threats, including both cyber-attacks and physical attacks from potential customers who disrupt Smart Meters to generate low power consumption costs. Due to the resource-restrained nature of IOT suitable approach for AMI, a lightweight communication protocol is required. Message Querying Telemetry delivery (MQTT) is one of the lightweight communication protocols that use submit and subscribe technique but senses the poosibilities of cyber threat. Most recent MQTT protocols are susceptible to a denial of provider attack and by utilizing those abilities it is possible to make those devices potential and feasible objectives for adversaries. Middleware-based IoT software protocols play a key position in permitting two-manner verbal exchange and faraway manage of IoT devices. Feasible threats in MQTT-based IOT environments need to be identified before appropriate countermeasures may be implemented. We are presenting the MQTT risk model and evaluate a DoS assault that targets MQTT brokers. The proposed strategy reduce the threat or attack on end-to-end system and to provide solution to the issues of physical and cyberattack such as distributed denial-of-service (DDoS) attack, especially on a smart grid system and to provide information access solutions using cloud storage and using firewall services or security services on AMI as a part of Smart Grid. Hence, The MQTT protocol, deployed in the cloud using Kubernetes, which can provide a real-time application and transport layer protocol along with appropriate attack protection, suits the AMI network the best for the development and production workings of SMs and the AMI-Network.

Keywords: MQTT, AMI, Smart Grid, DDoS attack

1. Introduction

Over a period of time, Energy demand / consumption has increased manifold due to rise in the population, but energy supply has not increased accordingly [1]. Globally, the energy system meets a number of inspired innovations that are essential to decarbonizes the energy, transform the old grid through incorporation of rapidly developing Information and Communication Technologies (ICTs). The existing power grid is probably the largest commercial discovery of the 20th century. However, it is outdated and exploited, which is very important in extinguishing and costing energy. For this and various other reasons, requires to create a cyber-physical energy system known as a Smart Grid (SG) in which the cyber-layer that controls the transmission, production and distribution of power, handles data exchange, communication and calculation, is firmly integrated into the virtual system [2,3]. Smart grid connections include local area networks (HANs), Neighborhood Area Networks (NANs), Wide Area Network (WAN), Data Centers, and flexible integration systems. The Smart Grid is a vision of electrical networks of growing challenges and opportunities, bringing benefits to all consumers.

An Advanced Metering Infrastructure (AMI) is a network, operating on a wireless mesh network and multi-hop communication is possible with a different intelligent meter until it reaches the concentrator. The AMI network is used for data collection, measurement, and analysis, from networks connected to next-generation electricity meters, or, smart AMI communication network and new computer capabilities for smart grid devices add

[1] Dr. Tejaskumar Bhatt, *Faculty of Engineering, GLS UNIVERSITY,Ahmedabad, Gujarat, tejas.bhatt@glsuniversity.ac.in*

[2] * Dr. Yagnik Rathod, *Government Engineering College, Dahod, Gujarat, India, rathod.yagnik@gmail.com*

[3] Dr. Virendra K Barot , *Government Engineering College, Bhavnagar, Gujarat, India, viren.rao82@gmail.com*

[4] Prof. Ashok K Rathva , *Government Engineering College, Dahod, Gujarat, India, ashok.gecd@gmail.com*

[5] Prof. Vanraj D Baria , *Government Engineering College, Dahod, Gujarat, India, vdbaria.ce@gmail.com*

[6] Prof. Salman Y Bhimla , *Government Engineering College, Dahod, Gujarat, India, sbhimla.comp@gmail.com*

Corresponding author: Dr. Yagnik Rathod, *Email: rathod.yagnik@gmail.com*

significant threat of external attacks in the old power style or power delivery systems such as cyber-attack that will need physical access to a server or network system by using the remote access. Here, there are three main security features integrated into the smart grid system: 1) Accessibility, which is a continuous power supply that provides user needs, 2) integrity, relevant information, and 3) confidential, user friendly data [4-8]. In an Advance Meter Infrastructure Network, SMs are not only connected to a server or grid but also shall not be easily accessible to customers or participants, allowing them to use the methods that attack the system. Security threats are growing exponentially, from within and outside the AMI network system where a DDoS attack falls on a denial of service on the AMI network. In an AMI network, a DDoS attack is selected for one or more common or common sites or devices as a victim node or tool where the attacker sends multiple packets of data or requests to these standard nodes or devices for specific details or details of these nodes or devices. When these target devices receive this attack data or packets, they form a large number of route data or packets. This AMI network has restricted communication bandwidth on the mesh network and router data packets which are the most important of all data packets. Here, where unwanted path data packets will override or terminate an inadequate network and the network result will be disrupted or flooded due to DDoS attacks on the AMI network. Here's where you need to identify and introduce new and complex denials of service attacks on the AMI network and the first in depth investigation of the impact [9-12]. The MQTT (Message Queue Telemetry Transport) is a binary protocol mainly designed for Machine-to-Machine (M2M) communications, with the aim to be lightweight and message oriented, for transferring information using very few computational resources. It is based on a publish-subscribe paradigm and it works well in unreliable scenarios, where the bandwidth is limited and latency is high, since it can guarantee the delivery of messages to IoT environment with its inherent simplicity, lack of a complex management, Quality of Service (QoS) support, flexibility in the payload format, last-will-and-testament mechanism, possibility of broker federation, etc. [13]. The inclusive analysis of the current vulnerabilities/attacks, security and privacy challenges associated with the smart metering data and network systems, its open concerns, and imminent track is discussed in paper [14]. The communication networks in the AMI have shaped a susceptibility to cyber-attacks over the ages. The dependability of the power grid to patrons trusts on the interpretations from the SM, and this takes about the necessity to protected the SMe data [15]. The foremost assistances of this review paper resides as the AMI vulnerabilities, AMI up-to-the-minute security arrangements with their aces and ploys, its communication protocols investigation, and its evolving security processes. The authors in [16] discussed several cybersecurity coercions to SG like Denial-of-service attack and its alleviation practices are examined and shows concerns towards threat to the communication channel. There is good findings by refererning the [17] which disussed various cyber security outbreaks and prevention methods in SM Metering Network Founded on the prevailing review threat models, a quantity of projected traditions have been intended to deal with all intimidations in the preparation of the secrecy and privacy provisions of SG measurement network. The offerings of [18] are like susceptibilities that may occur in all components of an AMI are described, summarizing and analyzed. Further, it reflects attacks that exploit these weaknesses and the effect on the performance of discrete apparatuses and the complete AMI system. It also provides disfferent approaches which can prevent an AMI system. Finally it helps in finding the research scope interms of the open challenges connecting to AMI security as well as future research directions. An intrusion detection scheme by combining feature dimensionality reduction and improved Long Short-Term Memory (LSTM) using the Stacked Autoencoder (SAE) has shown excellent performance in feature dimensionality reduction and has suggest obvious advantages in performance metrics such as accuracy and False Alarm Rate (FAR). The experimental results demonstrate that it can effectively identify the intrusion attack of communication in AMI[19]. A fruitful smart grid infrastructure needs the integration of a cyber-machine with a bodily energy machine. Smart meters are gadgets like virtual meters that bring the modern features of far-off analysing or gathering statistics or facts from smart meters. In addition, it directs, accepts, and implements instructions for distant creation and disconnection manipulation. As a result, a community of smart meters known as Smart Metering Networks (SMN) is created or formed by various smart meters. The Smart Grid includes this kind of network, which is also known as improved Meter Infrastructure. SM records, including petition and response records, as well as SM request records, billing records, and order records, are the responsibility of the SG. Here, these facts or data may be sent to public service earners' servers or offices as well as clients or customers for evaluation and promotion. Because it is at the heart of the SG, AMI is being conceptualized appropriately.

2. Methodology

2.1 Impression of DDOS Attacks

A malware described by Ping Yiet al [1] as a DDoS attack results in a denial of service within the AMI community. The attacker typically selects one or more common nodes as dupe nodes in this attack. The attacker then sends record packets to the target nodes that contain specific assault information. The victim nodes gain an enormous capacity for direction packets when they acquire those attack packs. In mesh networks, there is limited bandwidth for verbal exchange, and course packets have the highest priority of all packets. Additional route packets will use up a limited amount of communication bandwidth and ultimately result in device

obstruction. A DDoS attack causes a denial of service attack within the AMI network as a result. As depicted in Figure 1, the discern is an illustration of the DDoS outbreak in Advance Meter Infrastructure.

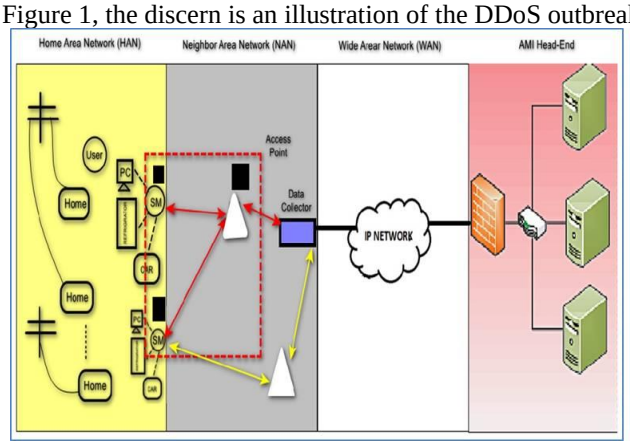

Figure 1:Intangible DDoS outbreak earlier Meter Infrastructure community

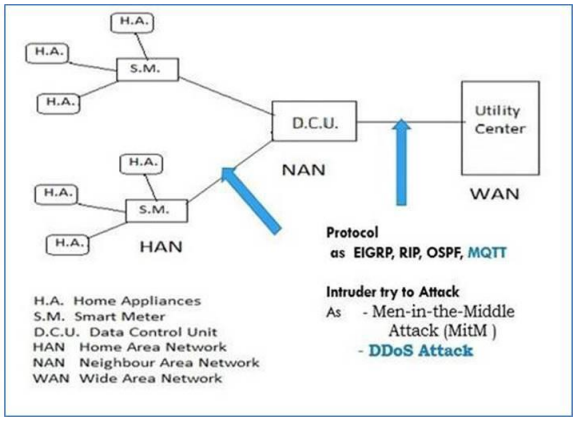

Figure 2: Proposition Archetypal in AMI network with attack

The attack, which is known as a DDoS attack, is basically carried out using an attack that is demonstratively friendly to fulfilling scheme obligations, which is a good way to trace the appropriateness of organizational capabilities and policies. Due to the vulnerability of the SM community to internet-based diverse attacks like DDoS, replay, overhearing, false statistics injection, repudiation, and node compromise, the increasing trustworthiness of the SM Infrastructure, which is based on online communication, needs to be modified. These kinds of attacks are extremely volatile for the SG machine or network, and they could signal the beginning of problems like strength instability and significant financial losses. In this version, the primary objective of the attackers is to empty the bandwidth and distribution strength of the vulnerable nodes as SM, which is probably connected to the AMI. During the initial stage of a DDoS attack on this AMI network, the frail node or strategies are discovered. There are three sorts of attacks that have been likely in the AMI community an attack on internet bandwidth, an assault on directing internet protocols, and an attack on community substructure. An assault like a DDoS assault essentially takes region the usage of a demonstrative attack that satisfies the duties of a fulfillment scheme that will screen the appropriateness of the employer's talents and policies. The increasing trustworthiness of the SM infrastructure, that's primarily based on net verbal exchange, should adapt to the vulnerability of the SM community to diverse net attacks, consisting of DDoS, replay, eavesdropping, spoofing, denial, and node compromise. Those sorts of assaults are very risky to the SG network or gadget and can reason issues including electricity instability and large financial losses. In this version, the attacker's predominant bias is to exhaust the bandwidth and dispensation electricity of defenseless sufferer nodes which includes SM which can be connected to the AMI. There may be a vulnerable factor or strategy on this AMI community that is detected at the very primary degree of inciting a DDoS attack. Three sorts of assaults are possibly in an AMI community, which include community bandwidth assault, community protocol routing attack, and community substructure assault.

2.2 Proposed system for AMI in Smart Grid with attack and Protocol

The proposed AMI network in Figure 2 in which SM are used as the main devices and are accountable for recording the power consumption of home appliances. Home area networks are provided for communication between various household appliances or devices or other integrated devices or systems such as smart thermostats, electric cars, home screens, photovoltaic roof systems, and smart meters. These devices or systems, power line communication (PLC), and wireless communications such as ZigBee, Z-Wave, and others can be used. Neighborhood area networks provide communication between individual meters or between separate contractors or data collection units via Wi-Max or mobile systems or technology. A unit that collects various data is connected to a central system such as a server or system center via WAN. A WAN is basically connected to two or more networks with a large network and a backhaul network. Here, content networks are primarily provided that communication between a service center or a control center such as a server or service center is operated via a wireless network or fiber optics cable with high data rates and low latency. During the reversal, the networks are primarily used and manage broadband communication with the Neighborhood Area Network, and are used for monitoring across all the sectors. A state-of-the-art infrastructure was developed which uses the number of Intelligent Meter devices connected to a network such as wireless network and in between, network elements are directly connected to servers in the cloud environment, attempting a malicious node by creating an attack as DDoS attacks and the server as a help center and using a cloud environment. Where, this DDoS attack clogs the entire AMI network and sends multiple requests to the server as a help center from network traffic, we should use a firewall to protect the AMI network. For this, measure and test wireless Smart Meter via AMI Network using a routing protocol such as EIRGP, RIP, OSPF, MQTT, using these processes and various

network elements such as access point, routers, servers over the cloud environment. The author in [2] classifies the AMI community via SM as a critical device accountable for receiving power for home programs and its heavy protection. Domestic networks are pre-prepared for conversation between one-of-a-kind home appliances and preserving the peace, which includes smart thermostats, electric automobiles, home displays, sun roof structures, Smart Meters, or different incorporated gadgets and structures. These gadgets or systems may use percent and wireless connectivity which include Zigbee, and Z-Wave. An adjacent community that offers communication among exclusive meters independently or one by one from concentrators or data series units thru WiMAX or cellular structures or technology.

The MQTT protocol is based on the construction of a communication network with a hop-by-hop data aggregation and a forwarding scheme. The research objective of this concept is part of the life-threatening Advance Meter Infrastructure in Smart Grid communication, and a different type of cyber security threat that discriminates against efficiency and reliability will focus on Smart Grid methods. Therefore, we are investigating a separate cyber security concern in the smart grid AMI system and proposing Google Cloudflare Security and MQTT protocol for collecting metered data and message distribution in AMI communications management. Therefore, measurements from SM and administrative messages from the SCADA center and/or local administrative offices may apply encryption and messaging methods tailored to security needs and system problems. Performance results show that the MQTT protocol has low latency and low packet loss and uses a firewall that provides the most secure and efficient data collection and delivery of management messages between smart meters and the local collector.

2.3 MQTT Protocol

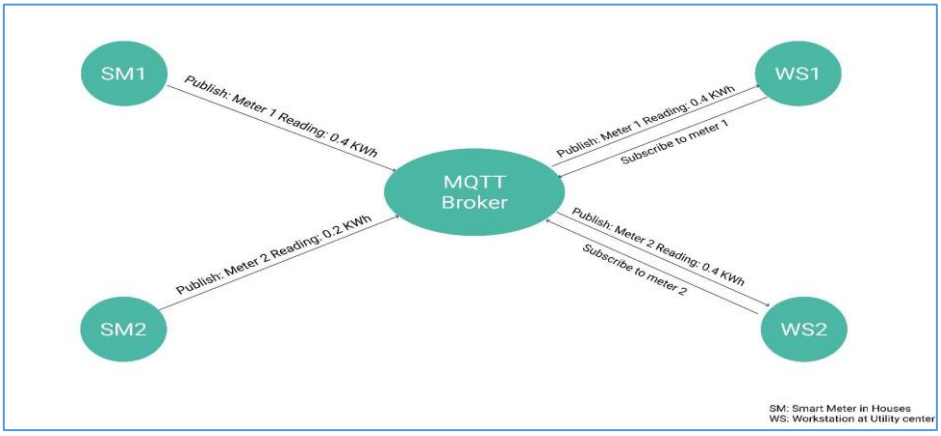

Figure 3: MQTT workflow

MQTT is a real-time publish subscribe protocol that's well suited for efficient distribution of data. Using a series of microservices, we can convert existing open data power grid into an open, real-time streaming service. MQTT provides various kind of security as MQTT Payload Encryption, MQTT Message Data Integrity, Prevention of sniffing attack, MQTT connect packets for credentials.The work structure is based on a single central server, called a broker, and multiple clients. Each customer can publish and / or subscribe to data within each topic shown in Figure 3. The big advantage is that customers do not need to get to know each other so that their software is very simple and requires minimal resources. All uploaded by a broker who receives published data and distributes it to all subject subscribers.

The advantage of publishing / subscribing a program is that the data sender (publisher) and the data receiver (client) do not know each other because there is a broker between the two of them. In addition, there is a time separation that allows the publisher and client to be able to connect simultaneously so that the client can always receive previously delayed data. The DoS attack status considered in this task is shown in Figure 3. It is a barebone MQTT server that can run on any stream servers.

MQTT (MQ Telemetry shipping or Message Queuing Telemetry transport) is an open OASIS and ISO general (ISO/IEC 20922) lightweight submit/subscribe community protocol that allows for similar conversation in an IoT-based completely AMI network. Based on a put-up-subscription architecture, it is an open-source TCP protocol. Put up-subscribe, also known as "pub-sub," allows customers to work with a trusted dealer and "subscribe" to topics of interest. All subscribed client nodes receive the posted message when a client "publishes" this topic. MQTT is a complete TCP-based proto-col with one-to-one and one-to-many messaging as well as low overhead and high quality of service (QoS). Stretching in accordance to embedded systems to connect with the M2M (machine to device) broker, connect with additional embedded structures via cloud servers, and be configurable via cloud network services are all hypo-thetical. This is a fundamental MQTT server that could direct to any spouting server. Aedes is basically an MQTT broker with basic functionality that can be extended using extensions. We've used Aedes to make the real-time broker. Aedes is a node.js library and a command-line interface. It provides various extensions such as statistic generation and logging. We can

connect to any middleware realtime database with a preferred database as MongoDB. Aedes is essentially an MQTT broker with undeveloped systems that can be suspended for an extended period of time. With Aedes, we developed a real-time trading system. Aedes is a command-line interface and Node.js library. It offers numerous de-lays, including record generation and logging. Utilize your preferred database, such as MongoDB, to connect to any middleware database in real-time. MQTT.Js is a Java Script based client library for Node.js and the browser for the MQTT protocol. It's a connected open-source library that makes the switch easier and lets you get MQTT data online. For a similar analysis, we have developed an MQTT client that makes use of this library to log MQTT data obtained from its broker. A simple submit/subscribe messaging client with servers that provide MQTT is provided by this library. In NodeMCU, the C/C++ library is used to send data to brokers. The MQTT package is a great library for publishing MQTT-based complete packages to agents via NodeMCU because it is a light package and ses a put-up-and-subscribe model to send programs.

2.4 Implementation

For developing a Smart Meter, we have used the ACS712 modern sensor that uses the Hall Effect to calculate AC equal voltage, which necessitates the smart meter connection and also shown in figure 4 and 5. The fee is sent as an analog signal from this voltage, and the open-source IoT platform NodeMCU. It started with hardware that was entirely based on the ESP-12 module and included firmware that runs on the ESP8266 wi-fi SoC from Es-press of systems. Support for the 32-bit ESP32 MCU was laterly added. It has a single analog pin on which the MUX is connected to three to four current sensors, which represent packages. In order to guarantee that we receive the correct price for the contemporary sensor, the Voltmeter has been linked. Arduino was utilized as the relationship's power source. The analog value of the modern-equal voltage is then sent to the NodeMCU via the MUX by the ACS712 current sensors., The MQTT broker receives the acquired statistics via wireless transmission from NodeMCU.

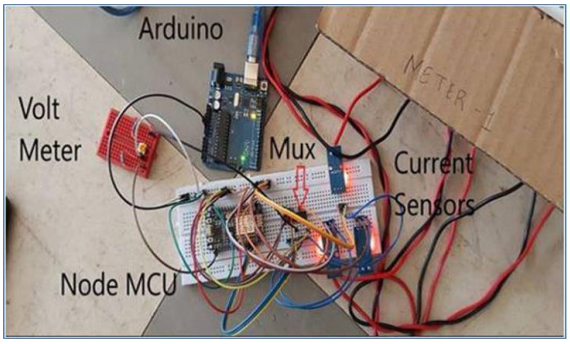

Figure 4: Smart Meter Construction Setup

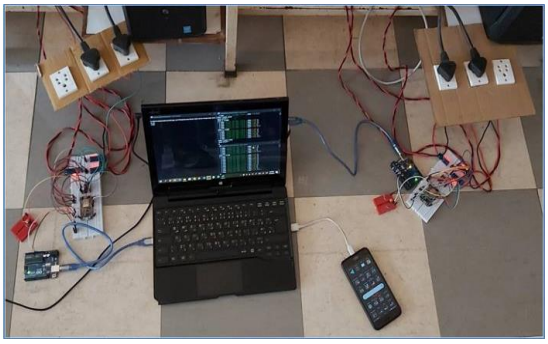

Figure 5: AMI Network Setup

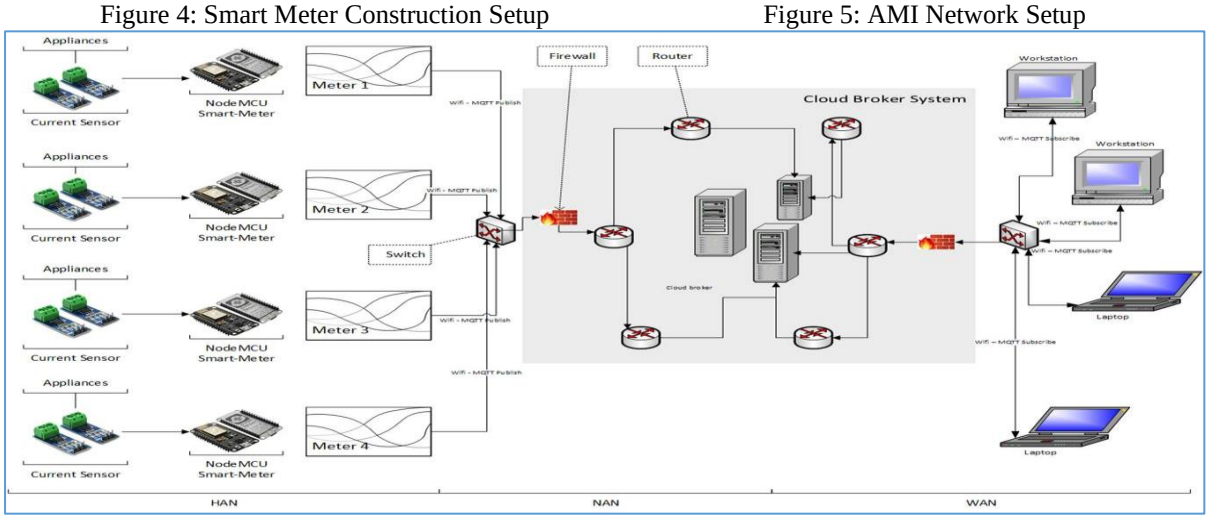

Figure 6 AMI Network Architecture

In this figure 6 AMI network Architecture, the current sensor (which is connected to the appliance) and the NodeMCU together comprises of the smart-meter. It sends the data to the broker, which is deployed on Kubernetes. The Kubernetes deployed broker runs 3 instances (minimum) so as to make sure it can load balance when a lot of requests are flooded. This data, when received by the broker, will be forwarded to everyone subscribed to that meter and will be discuss later in future work.

3. Results and discussion

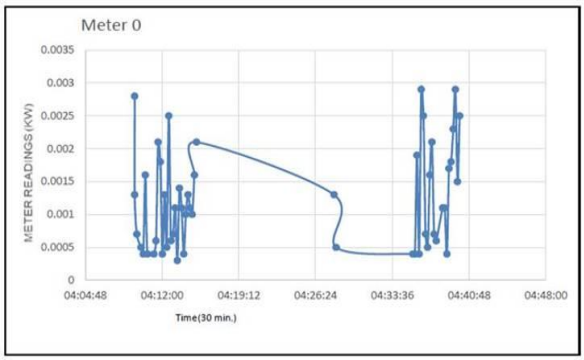

Figure 7: Meter 0 Reading with DDoS Attack

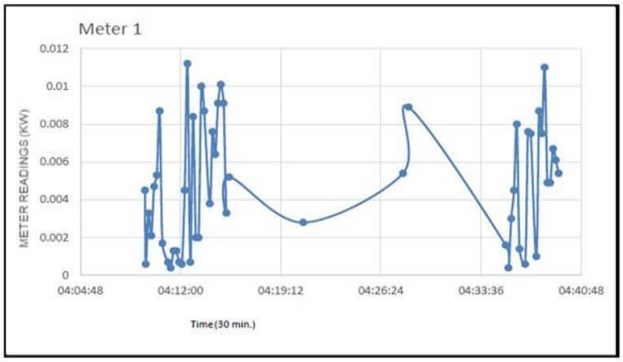

Figure 8: Meter 1 Reading with DDoS Attack

From determine 7 and parent 8 (Figure 7 and 8), we used MQTT Explorer to produce the standard streak graphs of meter estimations directed by using assorted meters and published via brokers. Meant for a half-hour, the overhead line charts designate facts from the broking when the attack turned into now not flung. Those consequences were critical to verify that each one networks are consistent and integral, to the ideal reason of all associated apparatuses. Observe the measured beliefs for reference for regular operating non-attacked surroundings of the system. Organizing a broker on a Kubernetes cluster have to confiscate the leeway of DDoS frightening the scheme, but seemingly that's the situation. The key motive turned into that an MQTT-based assault changed into unsuccessful in range a of variances, but a second standard DDoS attack that marks HTTP crashed our machine because of a cumbersome payload. The studying we did after the disposition, at some point of which we also made the MQTT DDOS assault, gave us unaffected and regular output for the MQTT DDOS attack however crashed our operating device with the HTTP DDOS assault. However, we word that the records aren't exactly secure, as other resources are intelligent to post packets as well as subscribe. So the question of records veracity ascends, to which a firewall seemed to be a fine solution.

3.1. Firewall

Every MQTT vendor communication must be able to pass through at least one fire-wall that supports multiple admissions instructions. If you can stop attackers at the firewall level, they might not be able to access other infrastructure-related packages. Sadly, there is no universal remedy. Every software example, in my opinion, needs firewall regulations. There are various open stock firewall arrangements accessible nowadays.

The MQTT provider may block the following traffic:

UDP: Because MQTT uses TCP, all UDP datagram packets can be blocked. At the MQTT provider, the following visitors may be blocked: UDP: Since MQTT uses TCP, UDP datagram packets can be blocked. The following website visitors may be blocked by MQTT sellers: UDP: Since MQTT uses TCP, all UDP datagram packets could be blocked. ICMP: ICMP visitors, ping, and traceroute ICMP packets should be investigated as they want to dam, despite the fact that blocking the entire ICMP road might not be the best idea. Damming traffic to any undesirable ports in your MQTT device is also a fantastic idea. Do not use your firewall to block the following MQTT ports: 1883: This is the MQTT replicate of choice. IANA refers to 1883 as MQTT over TCP. 8883: For MQTT over TLS, this is the default MQTT display screen. For easy MQTT, I am registered with IANA. Allow only the desired IP distance visitors if you know the IP addresses of your MQTT clients and have complete control over your MQTT system. Any clients out-side the specified IP range are not included in this tracking.

Policies for firewalls:

If (relationships. Listing. includes (request. Ip))
Packet equals a request Packet;
Packet = facts.
Information in the event of Proto equals MQTT and packet. Protocol.Mqtt.Dst equals 1883 and packet. Ip.Dst=="IP broker" and (information) search Records: "Measurement [0-9]:"))
Msg ("message valid") Else Drop(packet)

Configurations of firewalls:

- Match access lists for SYNHTTP, SYNHTTPS, and SYNMQTT;
- Set connection embryonic-con-max 256 in step with consumer-max 5 for HTTP, HTTPS, and MQTT;
- Cover provider OUT_POLICY interface outside

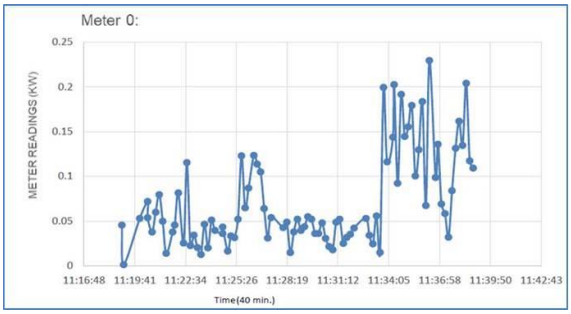

Figure 9: Meter Reading with Firewall(X-axis = 40 min,Y-axis = kW)

Figure 10: Meter Reading with Firewall (X-axis = 40 min,Y-axis = kW)

Figures 9 and 10 demonstrate that even after employing a firewall, the integrity of the data may still be in question due to the fact that the data remain in their raw, unencrypted form. However, the most common issues, such as the server crash caused by a network call overflow and the server being teased by unknown parties, have been resolved. As a result, our system will grow in strength and utility. We tested the machine by launching an HTTP DDoS attack, which had no effect because everything crashed prior to reaching the dealer close to the firewall.

3.2. System flow

1)Initialization:

I.The dealer starts up. opens a socket and listens on it for any subscription and post

II.It also sets up essential sources to generate queues. A connect (join) packet is sent to the broking by the subscriber (UC devices).

III.The Writer, which is a Smart meter, starts up and sends a connect packet to the brokering

IV.The broker acknowledges (CONNACK) each connect packet that it receives.

Consequently, documentation of a connection with Subscribers and publishers.

2) Values get submit from the smart-meter on the dealer:

I. Following initialization, the smart meter begins calculating the modern data it re-ceives from modern sensors

II. It also calculates the consumed electricity from the numerous modern values.

III. Through publishing the value, the smart meter transmits the generated energy value to the broker. placed)

IV. Upon receiving the published packet, the dealer does the following:

a. If the subject matter queue does not already exist, create one.

b. Adds the price to the subject matter queue.

c. Posts the cost to all subscribers by publishing the value as described below.

Depending on the QOS (pleasant of provider), the broker may also decide to store it in its runtime or database if none are present.

d. Sends the author an acknowledgment (PUBACK).

3) Subscription:

I. The dealer subscribes to each subject by sending the broker to subscribe packets (SUBSCRIBE), each of which contains a distinct subject to be added to the sub-scribed packet

II. The dealer replies:

a. By sending subscribers a subscription acknowledgment (SUBACK);

b. By creating an empty topic queue if one does not already exist.

c. In addition, the subscriber's reference is added to the queue's subscriber list.

4) The values are sent to the UC devices by the brokerage

I. By publishing the information to everyone on the subscriber list for that queue, the brokerage sends the values gift to the UC devices.

II. After the dealer has received the post packet, the UC devices send an acknowl-edgment (PUBACK) to them.

5) The shutdown of UC devices:

I. It sends an un-subscription packet to unsubscribe from the subject while the UC devices are shutting down.

II. UNSUBSCRIBE. By removing them from the subscriber list, the broker responds by sending an acknowledgment (UNSUBACK).

3.3. Algorithms:

Algorithm 1: Generate a put up packet

I. Allow an appliance that is connected to a smart meter to be referred to as Ai

III. Let the initial cost of the RMS power that is needed through the house be: PRMS = 0;
IV. All home appliances that are connected to vid:
Vi = readCurrentEquivalentVoltage(Ai) PRMS += [220 ((Vi 0.707 500)/mVpA) 0.26]/1,000,
where mVpA is as follows: mVolt in Ampere), the cost of calibration for each sensor, and
V. The meter publishes the packet: MQTT (topic="Mesh $vid:"); value is PRMS)
VI Reset:

Algorithm 2: Receive and ship packets to subscribers

I. Allow post packet P to arrive at the dealer;
II. If P. Proto == MQTT and P. Destination. Port== 1883 && P. Destination. Ip ==
$Broker_IP && seek (P. Topic, "Meter [0-9] +: ")
a. If Queue.ofTopic(P. Subject matter)! = null;
III. ∀ subscriber inside the queue. OfTopic (P. Subject matter). Subscribers: Subscrib-er.
Post(P.Cost)
i. Let publish packet P arrive at broker;
ii. If P. proto == MQTT and P. destination. Port== 1883 && P. destination. ip ==
${Broker_IP} && search (P. topic,"\Meter [0-9] +: \")
a. If Queue.ofTopic(P. topic)! = null;
iii. ∀ subscriber in queue. Of Topic (P. topic). Subscribers:Subscriber. Publish (P.value)

Algorithm 3: UC Devices

I. Permit post packet P to arrive at UC tool;
II. If P. Proto == MQTT and P. Destination. Port== 1883 && P. Request. Ip == $Bro-ker_IP
a. Queue.Of(P. Topic). AddValue(P.Value)
b. LatestMeterReading = Queue.Of(P.Topic). Values.Sum ();
c. Analyse (latestMeterReading, P. Topic)

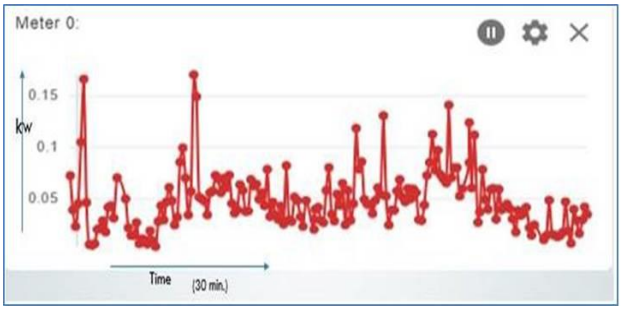

Figure 10 Smart Meter 0_without Attack

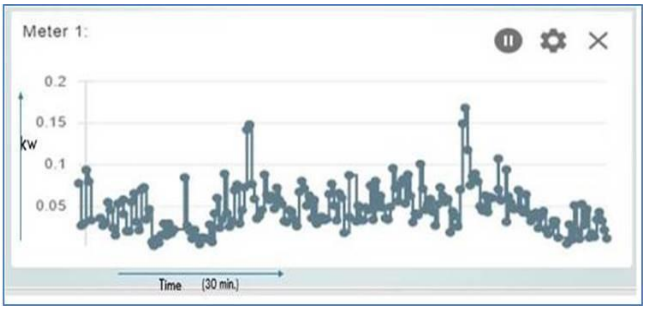

Figure 11 Smart Meter 1_without Attack

From figure 10, using MQTT Explorer, we generated a set of line chart graphs of the meter readings sent by the different meters, published to the broker. For 30 mins, the above line charts denote the readings from the broker when the attack was not initiated. These results were necessary to ensure that whether all connections were stable and intact, with proper functioning of all connected components. To note down the reading values for a reference for a normal working non-attacked environment of the system.

From figure 11, using MQTT Explorer, we generated a set of line chart graphs of the meter readings sent by the different meters, published to the broker. For 30 mins, the above line charts denote the readings from the broker when the attack was not initiated. These results were necessary to ensure that whether all connections were stable and intact, with proper functioning of all connected components. To note down the reading values for a reference for a normal working non-attacked environment of the system.

4. Conclusion and Future work

In this section, it is proposed to implement a cloud-based legal and secure framework for transmitting the customer's smart power meter data to the service provider and vice versa. Additionally, the stop-to-end device is reduced to reduce the risk of physical and cyber-attacks, particularly on smart grid devices, and information access solutions are provided by means of cloud storage and storage using hearth services or safety services on AMIs that include smart grid areas. Here, our primary objective is to provide information regarding our anticipated energy consumption, cyber-attack protection, authorization, and network parameters for transmitting data from the utility center to the customer smart meter and vice versa for the device level, which includes AMI in the smart Grid. In addition, we investigate the viability of the Google Kubernetes cloud platform and the Internet of Things (IoT) devices that can be a part of the smart Grid in both cloud and non-cloud environments. We believe that this work will make it easier to design and set some rules for the Cloudflare firewall to protect subscriber and post information from being stolen from the device. The answers are to be developed and implemented as the test bed for the AMI com-munity with the help of IoT devices. They will also simulate the

community with the different protocol's community layer routing protocols and also improve the cluster's firewall for security in order to keep these works for future work.

References

[1] Ping Yi, Ting Zhu, Qingquan Zhang, Yue Wu, Jianhua Li "A Denial of Service Attack in Advanced Metering Infrastructure Network" IEEE ICC 2014 pg. no 1029-1034

[2] Tejaskumar Bhatt, Chetan Kotwal, Nirbhaykumar Chaubey "Design and Implementation of Wireless AMI Network for Smart Grid using OPNET Riverbed " International Journal of Future Generation Communication and Networking Vol. 13, No. 4, (2020), pp. 777–787

[3] Muhammad Daniel Hafiz Abdullah, Zurina Mohd Hanapi, Zuriati Ahmad Zukarnain, Mohamad Afendee Mohamed "Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks" KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 9, NO. 4, Apr.2015 pg no. 1493-1515

[4] C Diovu and J.T Agee "A Cloud-Based Open flow Firewall for Mitigation Against DDoS Attacks In Smart Grid Ami Networks" 2017 IEEE PES-IAS Power Africa pg. no.28-33

[5] Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication Security for Smart Grid Distribution Networks," IEEE Communication Magazine, vol. 51, no. 1, pp. 42-49, 2013.

[6] M. Rahman, Amanullah Mto "Investigation of Bandwidth Requirement of Smart Meter Network Using OPNET Modeler" Smart Grid and Renewable Energy, 2013, 4, 378-390

[7] K. Brown and L. Christianson, "OPNET Lab Manual to Accompany Business Data and Communications," 2005

[8] D. Bian, Y. Wu, "Real-time Co-simulation Platform using OPAL-RT and OPNET for Analyzing Smart Grid Performance" 2015 IEEE

[9] Jun-Ho Huh, Kyungryong Seo "Smart Grid Framework Test Bed Using OPNET and Power Line Communication" 2016 IEEE DOI 10.1109/SCIS&ISIS.2016.192

[10] Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication Security for Smart Grid Distribution Networks," IEEE Communication Magazine, vol. 51, no. 1 2013 pp. 42-49.

[11] Jun-Ho Huh, Seung-Mo Je , Kyungryong Seo ―Design and Simulation of Foundation Technology for Zigbee-based Smart Grid Home Network System using OPNET Simulation‖ Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology Vol.5, No.4, August (2015), pp. 81-89

[12] Yonghe Guo, Chee-Wooi Ten, Shiyan Hu and Wayne W. Weaver, ―Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure‖ Innovative Smart Grid Technologies Conference (ISGT) 2015 IEEE Power and Energy Society, pp. 1-5.

[13] Hector Alaiz-Moreton, Jose Aveleira-Mata, Jorge Ondicol-Garcia "Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol" Hindawi, Wiley Volume 2019, Article ID 6516253, pp 1-11

[14] Ajiboye, P.O., Agyekum, K.OB.O. & Frimpong, E.A. Privacy and security of advanced metering infrastructure (AMI) data and network: a comprehensive review. J. Eng. Appl. Sci. 71, 91 (2024). https://doi.org/10.1186/s44147-024-00422-w

[15] Kebotogetse O, Samikannu R, Yahya A. Review of key management techniques for advanced metering infrastructure. International Journal of Distributed Sensor Networks. 2021;17(8). doi:10.1177/15501477211041541

[16] Gururaj, H.L., Swathi, B.H., Trupti, R. et al. Analysis of Preventive Measures Against DDoS Attacks in Smart Grid. J. Inst. Eng. India Ser. B 104, 297–303 (2023). https://doi.org/10.1007/s40031-022-00844-1

[17] Mostafa Shokry, Ali Ismail Awad, Mahmoud Khaled Abd-Ellah, Ashraf A.M. Khalaf,Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision,Future Generation Computer Systems,Volume 136,2022,Pages 358-377,ISSN 0167-739X, https://doi.org/10.1016/j.future.2022.06.013

[18] V. Kayalvizhy and A. Banumathi, "A Survey on Cyber Security Attacks and Countermeasures in Smart Grid Metering Network," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2021, pp. 160-165, doi: 10.1109/ICCMC51019.2021.9418303.

[19] Guanyu Lu, Xiuxia Tian, "An Efficient Communication Intrusion Detection Scheme in AMI Combining Feature Dimensionality Reduction and Improved LSTM", Security and Communication Networks, vol. 2021, Article ID 6631075, 21 pages, 2021. https://doi.org/10.1155/2021/6631075.