Tanzania Journal of Engineering and Technology 2024, **43(4)**:164-175

Websites: https://ajol.org/tjet; https://tjet.udsm.ac.tz

ISSN 1821-536X (**print**); ISSN 2619-8789 (**electronic**)
https://doi.org/10.52339/tjet.v43i4.1089

Regular Research Manuscript

Design and Implementation of Secured Hybrid Gateway Node for Securing IoT - Enabled Distribution Automation

Ally Bitebo

Department of Computer Science and Engineering, University of Dar es Salaam, Dar es Salaam, Tanzania
Corresponding author: allybitebo@udsm.ac.tz; ORCID: 0000-0002-9599-4399

ABSTRACT

The integration of smart grid and Internet of Things (IoT) technologies plays a crucial role in enhancing the quality of services provided by traditional electrical grids. This combination has enabled the introduction of new services, such as demand response, automatic meter reading, and IoT-enabled Distribution Automation (IoT-DA), which incorporates sensors, actuators, intelligent electrical devices (IEDs), and information and communication technologies to monitor and control the grid. However, this integration also introduces network security risks, including Denial of Service (DoS) attacks, false data injection, and masquerading attacks, such as system node impersonation that can transmit incorrect readings, trigger false alarms, and lead to improper node control. To address these challenges, a secure hybrid gateway node was designed and implemented to safeguard communication networks. This solution uses Datagram Transport Layer Security (DTLS) for Constrained Application Protocol (CoAP) to transmit historical data and mutual Transport Layer Security (TLS) for Message Queuing Telemetry Transport (MQTT) to send switching messages. The results demonstrate that the secured hybrid gateway node successfully ensures data confidentiality, integrity, and resilience against DoS attacks. In the future, this study will measure the efficiency of the implemented of the secured hybrid gateway node in terms of the security and performance in IoT devices by analyzing energy and memory usage.

ARTICLE INFO

Submitted: Oct. 25, 2024

Revised: Dec. 27, 2024

Accepted: Dec. 31, 2024

Published: Feb. 2025

Keywords: *Internet of Things, Hybrid Gateway, Security, Message Queuing Telemetry Transport*

INTRODUCTION

There are significant efforts towards the adoption of Internet of Things (IoT) technologies in the smart grid domain. This is because of the advanced technological mechanisms and flexibility offered by IoT devices and the technology itself. Several studies have proposed the adoption of IoT technologies in smart grid systems, where an IoT Cloud architecture has been proposed adopted and deployed. This includes the integration of Information and Communication Technologies (ICT) to the electrical distribution network to automate electrical distribution system services which is known as Distribution Automation (DA) (Sorebo & Echols, 2011; Yan *et al*., 2012; Elkadeem *et al*., 2018). Moreover, the integration Internet of Things technologies to the DA which is called Internet of Things Enabled Distribution Automation Distribution (IoT-DA). These IoT-DA initiatives have been deployed to improve the efficiency of the electrical distribution system (Iglesias-Urkia *et al*., 2019, 2017; Aghenta & Iqbal, 2019). One of the notable proposed distribution

automation services is the fault monitoring system for the secondary electrical distribution network (Zidan *et al*., 2016; Andegelile *et al*., 2019).

These IoT-DA systems are implemented by following IoT cloud architecture as presented in Figure 1 (Rani *et al*., 2024). The architecture has three main layers which are IoT layer, fog layer and cloud layer. The IoT layer is composed of resource-constrained devices like wireless sensors and actuators. The fog layer plays an important role in interconnecting IoT layer and cloud layer, and the cloud layer is composed of high-performance computing devices for processing and analysing data. Also, it has large storage capacities for storing processed and collected data (Diro *et al*., 2020). The fog layer is composed of lightweight fog computing devices like microcontrollers or low-powered computing devices like Raspberry Pi, which act as aggregators or gateway devices. They perform some intermediate computations (Mnyanghwalo *et al*., 2019; Diro *et al*., 2020). These fog devices can be deployed as aggregators to collect information from different IoT devices installed in the field (Tom & Sankaranarayanan, 2017; Hossain *et al*., 2019). On the other hand, can be deployed as a broker or gateway to process and manage communication between communicating devices using different protocols, where each deployed protocol supports a certain application as presented in Figure 1. Moreover, the fog devices can be deployed as proxy servers to support data transmission from field devices to the cloud server over the Internet (Thantharate *et al*., 2019). Therefore, the deployment of the fog devices depends on the supporting applications to be deployed and targeting quality of service (QoS) goals to be attained in the given system.

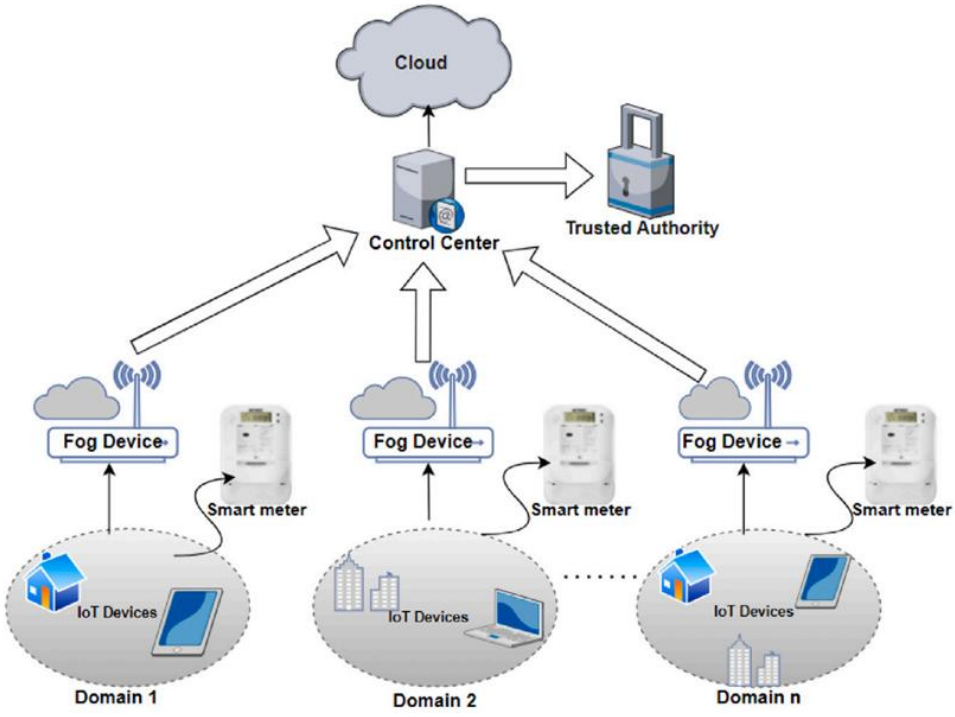

Figure 1: The IoT Cloud Layered Architecture (Rani *et al*., 2024).

These gateways are middleware devices installed between field devices and high-performance computers installed in the cloud infrastructure at the control center. They perform computational tasks immediately after receiving data from sensors and provide immediate feedback to reduce communication latency, computational delays and utilize less bandwidth. However, IoT technologies are facing interoperability, scalability and connectivity challenges for both devices

and platforms. It is hard to have a universal solution to support all services which leads to delaying of development or adoption of new emerging services (Thantharate *et al*., 2019). Furthermore, cyber-physical systems like Distribution Automation (DA) are heterogeneous systems with multiple services supported by multiple protocols. Moreover, the development of a single standard solution seemed unlike. However, there is a need to develop an interoperable, scalable and reusable IoT platform to support current and future services. It has been identified that; the middleware is the key part of the IoT stack to support interoperability (Akasiadis *et al*., 2019).

To support interoperability, multi-protocol gateway devices have been proposed to support multiple services. A mixture of Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT) protocols has been proposed to support several IoT applications such as software and security updates of the deployed remote devices (Thantharate *et al*., 2019; Zainudin *et al*., 2019; Akasiadis *et al*., 2019; Imran *et al*., 2024). Additionally, each of these deployed protocols poses different challenges in terms of quality of services and security mechanisms. Security is one of the important aspects in the integration and adoption of IoT technologies in smart grid systems like DA. This is because, the IoT technology involves millions of interconnected devices which increase the attacking interface compared to the legacy electrical grid systems (Bekara, 2014; Kimani *et al*., 2019).

In a study by (Thantharate *et al*., 2019), they proposed a hybrid gateway to support delivering on-air software security updates. However, their proposed models test the suitability of using CoAP, MQTT and a mixture of CoAP and MQTT (CoAP is encapsulated in the MQTT) when dispatching security updates without considering the security of the model itself. In such a way that any non-legitimate node can join the network and publish data to others as well as subscribe and receive software and security updates. Hence made the whole system vulnerable to cyber-attacks. Likewise, in a study by (Zainudin *et al*., 2019), they proposed a hybrid gateway node to support data transmission from sensors to the database server. The designed node supports three protocols which are CoAP, MQTT and web socket. However, the proposed node does not consider any security measure in its design and implementation which made the system to be vulnerable to cyber-attacks. For those reasons, it is important to design and implement these gateway nodes with security features to reduce the cyber security risk that might affect the whole DA system (Kimani *et al*., 2019).

The highlighted security challenges in IoT based smart grid are identity spoofing or impersonation, where a non-legitimate device acts on behalf of the legitimate device by using its identity. Eavesdropping is another security challenge, where an attacker can tap a communication channel to gain some knowledge of the transmitted data. This is because some of the smart grid system communication networks are using public communication infrastructure. Moreover, is tampering of data like state estimations, energy prices and power consumptions, where an attacker can modify these data to gain some advantages like reducing customer bill. Furthermore, an attacker can inject malicious code to compromise the operations of the smart grid devices like sensors, actuators and intelligent electronic devices (IEDs). Lastly, an attacker can launch denial of service (DoS) attacks to affect the availability of the system (Bekara, 2014; Kimani *et al*., 2019).

To protect the system from cyber-attacks, several approaches have been proposed to enhance the security of these gateway nodes. For example, a security architecture has been proposed to offer authentication and authorization of IoT-based healthcare devices by using smart gateway nodes. These nodes were implemented in a

distributed way to reduce the effects of Denial of Service (DoS) attacks. Moreover, a proposed architecture uses lightweight security protocols like certificated-based Datagram Transport Layer Security (DTLS) protocol. DTLS was applied to offer authorization and authentication of IoT devices, which are resource-constrained to reduce communication and computation overheads (Moosavi *et al*., 2015). Furthermore, these security features must be considered as main system components from the design stages.

Security of these gateway nodes plays an important role in the process of securing the whole cyber-physical systems like the smart grid. These gateway nodes are used to interconnect system components with different communication protocols, computation capabilities and application domains. They are main targets of cyber-attacks because they can be used as a medium of entrance to affect the whole system. Moreover, these gateway nodes are used to be connected to remote services like cloud services for storage or heavy-duty computation through the Internet. So, the interconnection to the Internet made these gateway nodes to be easy to be accessed by remote cyber-attackers. So, to address these challenges, proper security mechanisms/measures must be imposed or considered in the earlier stages of designing these gateway nodes.

To address the highlighted interoperability and security challenges facing IoT-based systems, this study proposes a secured hybrid gateway node to support data transmission on both CoAP and MQTT protocols. As well as, proposing a security mechanism to mitigate the security threats imposed when integrating IoT devices with the DA systems.

MATERIALS AND METHODS

Design of Secured Hybrid Gateway Node

The proposed overall system architecture is based on IoT cloud architecture, where IoT devices like sensors and actuators are installed in the field of electrical equipment. Next, the data are collected and pre-processed by gateways known as fog computers before being transferred to the high-performance computers at the control centre. The fog node operates as a hybrid gateway and supports three applications based on the nature of traffic transferred between system components. For IoT-enabled distribution automation, there is the bi-direction flow of data where there are sensor data transferred from electrical devices installed in the field to the control centre terming them as historical data, and control commands from the control centre to the actuators installed on the electrical devices in the field terming them as control data as shown in Figure 2.

Design of Secured Hybrid Gateway Node

The historical data are streamed using Constrained Application Protocol (CoAP) under/over User Datagram Protocol (UDP) protocol using the client-server architectural model. The control data are switching traffic by using Message Queuing Telemetry Transport (MQTT) under/over Transmission Control Protocol (TCP) protocol which uses using publisher-subscriber model. Thereafter, the Web Socket protocol is deployed to stream historical and control traffic to the control centre by using Hypertext Transfer Protocol (HTTP) protocol over the Internet as proposed in a study by (Zainudin *et al*., 2019; Imran *et al*., 2024). However, their study is missing security features which will be proposed and implemented by this study.

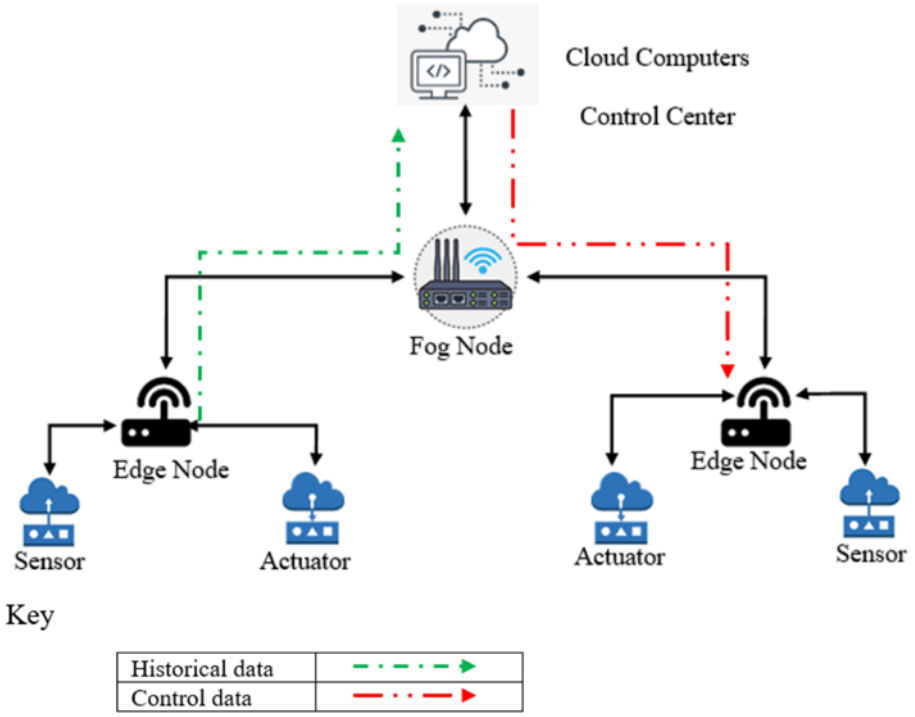

Figure 2: Overall System Architecture.

The secured hybrid gateway node design was carried out by considering the following factors: the nature of IoT devices its selves like sensors and actuators. the type of services or applications running to the gateway node, and the nature of traffic flow between system components. Those three factors act as the main building blocks towards designing the secured hybrid gateway node and each part has the following parameters as shown in Table 1. However, the gateway node designing process was motivated by the design proposed in this study (Zainudin *et al.*, 2019). But this work improved it by adding security features and containerizing the final design to compliment the port hiding mechanism by sing bridge technology proposed by (Akasiadis *et al.*, 2019, Rani *et al.*, 2024). The study utilized two modulation schemes
.

Table 1: Design parameters for the hybrid gateway node components

Components	Parameters
IoT devices	Sensors, actuators
Services	Streaming, publishing, subscription, authentication, authorization
Nature of traffic	Data streaming, message switching
Device registry	Devices information, roles

IoT Devices

The design has considered the role of IoT devices as sensors and actuators which are installed in the field. Sensors were used to read and record electrical system data like line current, line voltage and phase angle from substation transformers and send them to the control centre through the intermediate fog node. On the other hand, the actuators were used to receive control commands from the intermediate fog node or control centre.

Services or Applications

The design has considered five key services to be offered by the hybrid gateway node

by using CoAP and MQTT protocols. The CoAP protocol was used to support data streaming service from sensors to the control centre and is running at port number 5684. The MQTT protocol was used to support publishing and subscribing services where communicating devices are running at port number 1884. The web socket was used to support streaming real-time data to and from the control centre through HTTP/HTTPS and is running at port number 8080. Moreover, the fog gateway node is connected to a local database termed a device registry, where it stores the information of all communicating devices and users including their roles in supporting the authentication and authorization services. Finally, these components are controlled by a gateway controller operated like a proxy component termed as "igridnet" running at port number 1883.

Nature of Traffic

The design has considered two types of traffic flowing into the proposed system such as historical data streaming and control message switching data. Historical data streaming traffic is the one flowing from sensor nodes to the control centre. The control message switching traffic is fault data messages reported by intermediate fog devices to the control centre and control command messages from the control centre to actuators installed at the field.

Device Registry

The design has considered the system devices registry which is responsible for managing system device information such as device name, location data, MAC address and device roles. This information is stored in the local database called the device registry.

The main system operations started with the sensors connected to the field electrical equipment to sense and collect electrical field data like line current, line voltage and phase angle. Then, the collected data are sent to the control centre through the intermediate gateway node. The sensed data are streamed through the CoAP proxy server. However, once a fault occurs, the fault messages are transferred through the MQTT broker immediately to the respective defined topic. In the same way, once a fault message is translated and communicated to respective nodes for actions the actional command message is communicated back to actuators through a specific topic. All of these are achieved at the hybrid gateway nodes because of fault management algorithms running at the system nodes. Figure 3, shows the design of the secured hybrid gateway node to support IoT DA in SEPDN.

The operations of the proposed secured hybrid gateway node are intended to enhance the security of the proposed IoT DA by offering authentication and authorization of the communicating node. In addition, it creates secured communication channels between communicating system components. First, sensors are normally streamed historical data to the gateway. At the gateway node, the gateway controller authenticates and authorizes the sensor node with the help of the device registry. After a successful authentication and authorization process the sensor node is connected to the CoAP proxy server or MQTT broker for further processing as shown in Figure 4. Likewise, after a successful authentication and authorization process the sensor node can stream historical data to the control center for further analysis and computation as shown in Figure 4.

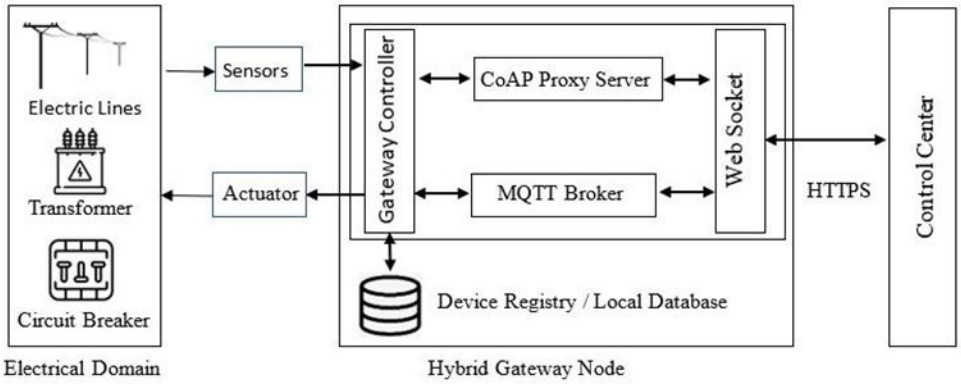

Figure 3: Design of the secured hybrid gateway with device registry.

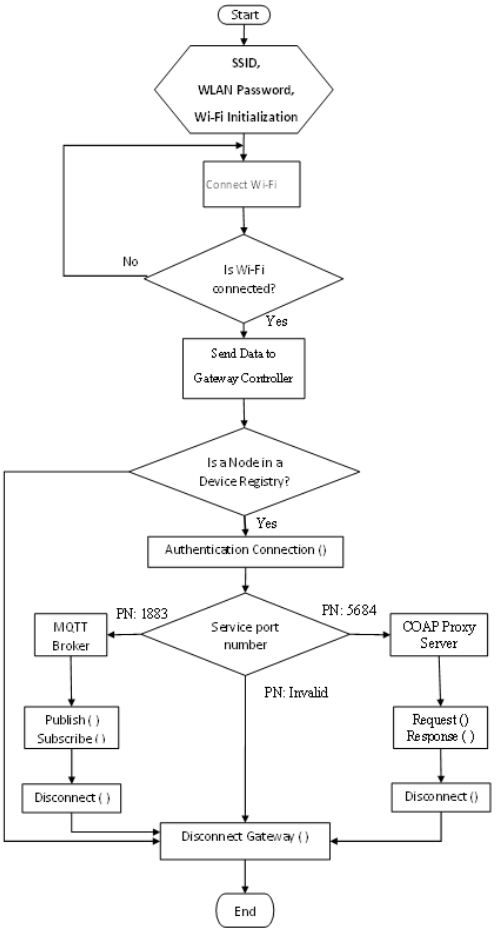

Figure 4: Flow chart to authenticate and authorize a system node before connected to the CoAP Proxy Server or MQTT broker.

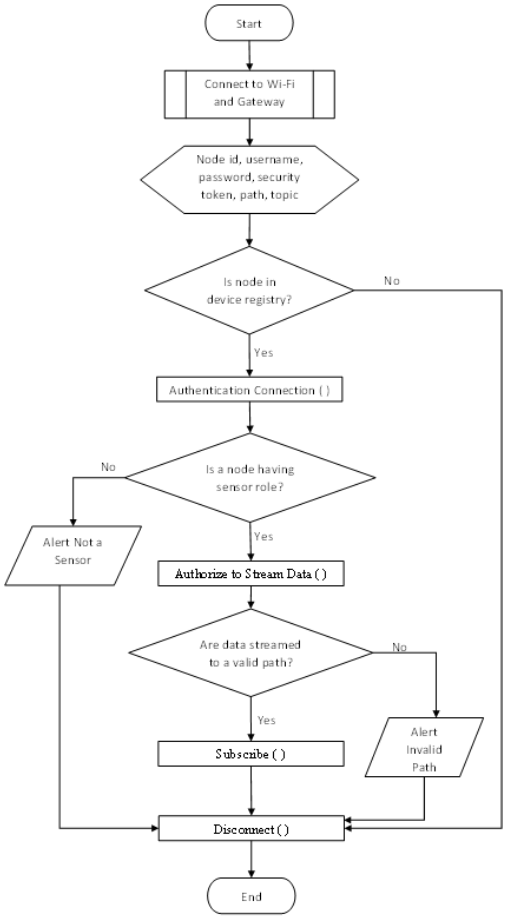

Figure 5: Flow chart to authenticate and authorize a system node before connected to the CoAP Proxy Server for streaming historical data.

Moreover, when faults occur the sensors, actuators, gateway nodes and control centre must operate together to manage and clear the fault occurred securely. In this case, these communicating devices must publish and subscribe to the different topics to support the fault management process. To achieve this, sensors must publish faults occurring to the respective topics' actuators must subscribe to specific topics and finally the gateway node and control centre computers must cooperate and coordinate

the fault management process. However, every communicated node must be authenticated and authorized before publishing or subscribing to the given topics.

For example, for sensing node can forward fault messages after detecting abnormalities in the sensed data. These messages and device information like node identifier, node username and password, security token and topic are forwarded to the gateway node for further processing. At the gateway node, the gateway controller forwards received information to the device registry to authenticate and authorize the sensor node and once is successful, can connect the node to the MQTT broker to publish the sensed fault to its respective topic as shown in Figure 6. On the other hand, actuators can receive command messages from gateway nodes or control centre, but before reaching the respective actuator, a gateway control must communicate with the device registry to authenticate and authorize both communicating nodes and once successfully, can forward the command message to the actuator as shown in Figure 7.

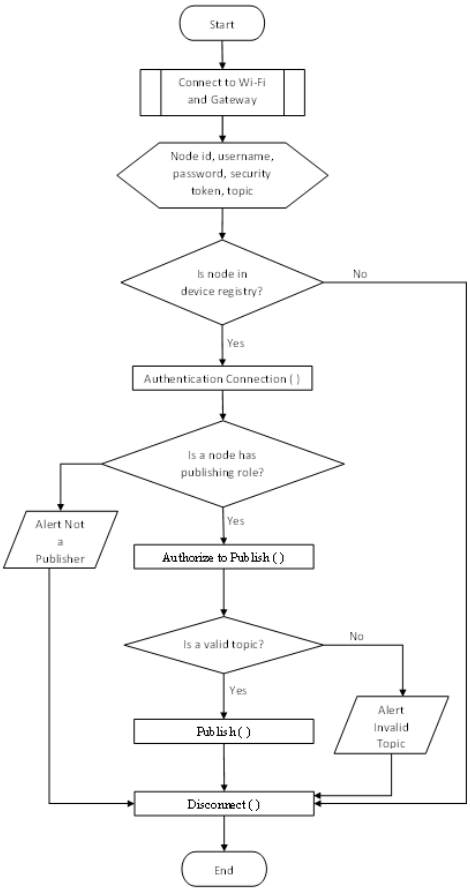

Figure 6: Flow chart to authenticate and authorize a system node before connected to the MQTT broker to publish to a given topic.

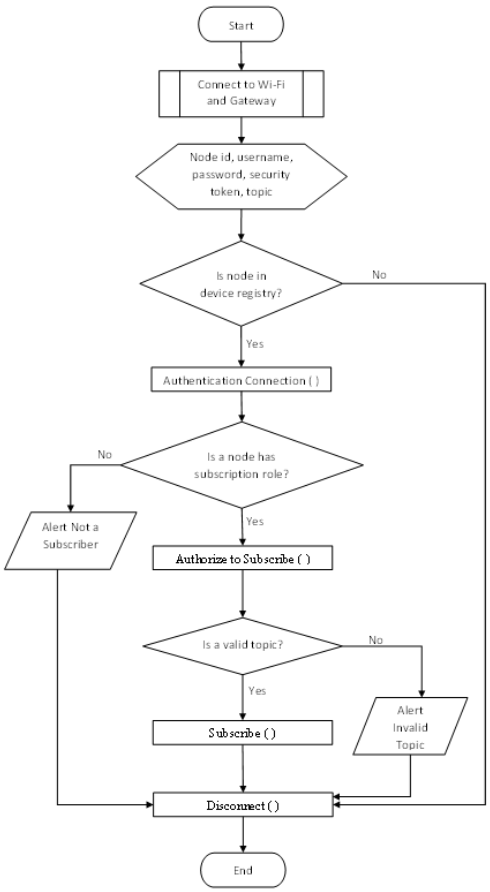

Figure 7: Flow chart to authenticate and authorize a system node before connected to the MQTT broker to subscribe to a given topic.

EXPERIMENTAL SETUP

The experiment was carried out by first considering the following parameters which are node type either a sensor with label "S" or actuator with label "A", the type of service or application are represented as follows; data streaming service as "str", publish to a given topic as

"pub" and subscribe to a given topic as "sub". So, a node with a given node ID n requesting the data streaming application or service is labelled as "NodeType-Node id" including subscript word with "Type of Application or Service" requested. For example, S-1_{str} means that a "sensor node" with node id "1" is requesting a streaming service. All six nodes and their label and description have been provided in Table 2. We have created six node points where five of them with node_id 1, 2, 3, 4, and 5 have been registered to the device register as system nodes and the sixth node with node id 6 is not registered to the device register. The main reason for doing this is to test the authentication functionality of the gateway node. The hypothesis of the experiment is "The gateway node must block all unregistered devices to communicate with system nodes". The results of this authentication experiment are presented in **Error! Reference source not found.**.

Table 2: Node Label and Description

Node Label	Descriptions
S-1_{str}	***A Sensor Node with ID "1" and is requesting streaming application or service***
S-2_{pub}	***A Sensor Node with ID "2" and is requesting publishing application or service***
S-3_{sub}	***A Sensor Node with ID "3" and is requesting subscription application or service***
A-4_{pub}	***An Actuator Node with ID "4" and is requesting publishing application or service***
A-5_{sub}	***An Actuator Node with ID "5" and is requesting subscription application or service***
N-6_{non}	***A Sensor or Actuator Node with ID "6" is not a system node i.e. a node is not in the device registry***

The secured hybrid gateway node was implemented by deploying the MQTT broker and CoAP server to the gateway node. The MQTT broker and MQTT clients were implemented by installing Eclipse Mosquitto MQTT v5/v3.1.1, and the CoAP was implemented using a FreeCoAP library. These services were deployed to the computer laptop, as shown in Figure 8, and Raspberry Pi mini-computers were used to represent IoT devices. These Raspberry Pi and computer laptops were connected to the Wi-Fi LAN network offered by Huawei wireless router model B315s-22. The security of the transmitted data over a hybrid gateway node was implemented using secured communication protocols based on the nature of the traffic. The streaming of historical data operation using CoAP was protected using the DTLS protocol, and the TLS protocol protected the message switching operation.

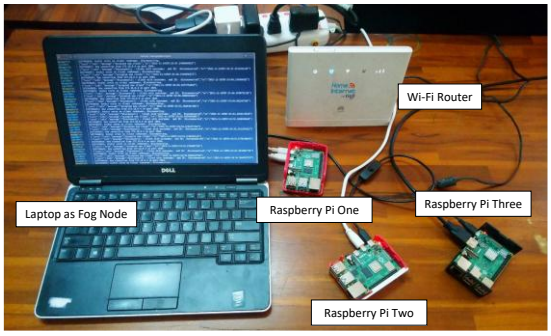

Figure 8: Experimental setup.

The implemented hybrid gateway node was evaluated using a set of three experimental tests with eight individual tests for each applied secured communication protocols. These tests incorporated the use COAP with DTLS and MQTT with TLS. Then, the traffics flows between communicating entities were captured by using Wireshark network analysis software, as shown in **Figure 9**9.

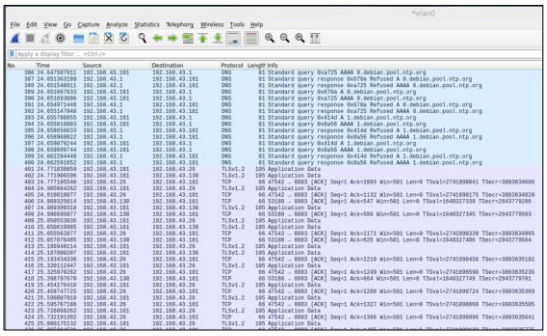

Figure 9: Wireshark analytic software.

RESULTS AND DISCUSSIONS

To secure communication network between communication system components, a security cipher suite was implemented and tested. This cipher suite security was implemented by adopting the TLS_AES_256_GCM_SHA_384 cipher suite as presented in Figure 9 and Figure 10 for client hello message and in server hello messages respectively. As a result, the communicating system components were secured by offering data confidentiality and data integrity.

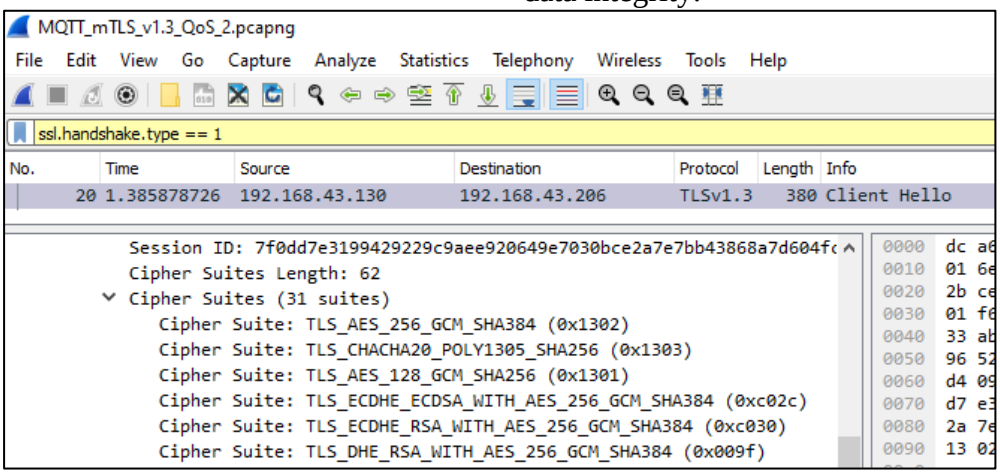

Figure 9: Client hello message with the list of supported cipher suites.

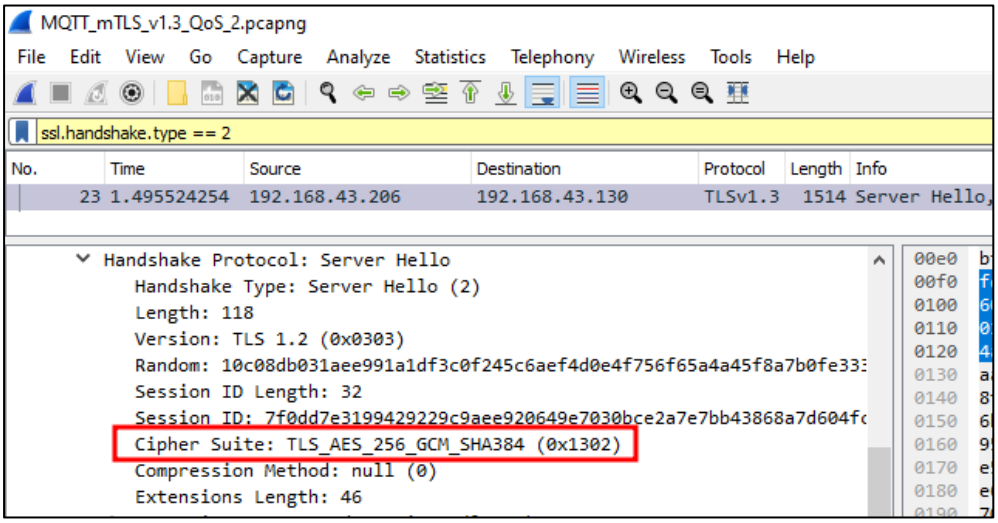

Figure 10: Server hello message with selected cipher suite.

Data Confidentiality

Since the communication messages were encrypted, this is successful test results for the provided data confidentiality mechanism by adopting Advanced Encryption Standard with 256 bits key Galois/Counter mode (AES 256 GCM).

Data Integrity

Since the resulting generated message was coded, it is an indication that data integrity was provided by generating Message Authentication Code (MAC) by using Secure Hash Algorithm 384 (SHA 384). The generated MAC is used to ensure that the transmitted data us received in the exact same way as it is sent.

Denial of Service Attack

This study has implemented a distributed security scheme by adopting a distributed architecture to minimize the effects of the DoS or DDoS attacks. The design of dividing operational area into clusters with

secured hybrid gateway nodes running as cluster heads, allows only compromised cluster to be affected by DoS or DDoS attacks and left other clusters to be operational.

Finally, the study designed and implemented a secured hybrid gateway node to protect the communication network in IoT-enabled Distribution Automation (IoT-DA) within the Smart Power Distribution Network (SPDN). The findings indicate that the developed secured hybrid gateway node effectively secures the network by utilizing two secure communication protocols: Datagram Transport Layer Security (DTLS) for UDP traffic and Transport Layer Security (TLS) for TCP traffic. The node supports multiple protocols, including CoAP and MQTT, following the design approach proposed by Akasiadis *et al*. (2019), Thantharate et al. (2019), and Zainudin *et al*. (2019). However, these previous studies implemented hybrid gateway nodes with minimal security measures, as shown in Table 2. Therefore, their designs need to be strengthened to reduce security vulnerabilities before being deployed in critical systems like IoT-DA.

Table 3: Study Authentication Availability Integrity Confidentiality

Study	Authentication	Availability	Integrity	Confidentiality
(Akasiadis *et al*., 2019)	NO	NO	NO	NO
(Zainudin *et al*., 2019)	YES	NO	NO	NO
(Thantharate *et al*., 2019)	NO	YES	NO	NO
Our Secured Hybrid Gateway	YES	YES	YES	YES

CONCLUSION

The findings of this study reveal that the implemented secured-hybrid-gateway node provides data confidentiality through the use of Advanced Encryption Standard (AES) with a 256-bit key in Galois/Counter Mode (AES-256 GCM). Additionally, it ensures data integrity by generating a Message Authentication Code (MAC) using the Secure Hash Algorithm 384 (SHA-384). Finally, the system's distributed architecture makes it resilient to Denial of Service (DoS) attacks. As a result, the proposed secured-hybrid-gateway node effectively secures the communication network in IoT-enabled Distribution Automation (IoT-DA) within the Smart Power Distribution Network (SPDN).

REFERENCES

Aghenta, L. O., & Iqbal, M. T. (2019). Development of an IoT Based Open Source SCADA System for PV System Monitoring. *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*: 1–4.

Akasiadis, C., Pitsilis, V., & Spyropoulos, C. D. (2019). A multi-protocol IoT platform based on open-source frameworks. *Sensors*, **19**(19): 4217.

Andegelile, Y., Chugulu, G., Bitebo, A., Mbembati, H., & Kundaeli, H. (2019). Enhancing faults monitoring in secondary electrical distribution network. *International Conference on Social Implications of Computers in Developing Countries*: 712–723.

Bekara, C. (2014). Security issues and challenges for the IoT-based smart grid. *Procedia Computer Science*, **34**: 532–537. doi:10.1016/j.procs.2014.07.064

Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020). Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication. *IEEE Access*, **8**: 60539–60551.

Elkadeem, M. R., Alaam, M. A., & Azmy, A. M. (2018). Improving performance of underground MV distribution networks using distribution automation system: A case study. *Ain*

Shams Engineering Journal, **9**(4): 469–481.

Hossain, M. S., Rahman, M., Sarker, M. T., Haque, M. E., & Jahid, A. (2019). A smart IoT based system for monitoring and controlling the sub-station equipment. *Internet of Things*, **7**: 100085.

Iglesias-Urkia, M., Casado-Mansilla, D., Mayer, S., Bilbao, J., & Urbieta, A. (2019). Integrating electrical substations within the IoT using IEC 61850, CoAP, and CBOR. *IEEE Internet of Things Journal*, **6**(5): 7437–7449. doi:10.1109/JIOT.2019.2903344

Iglesias-Urkia, M., Urbieta, A., Parra, J., & Casado-Mansilla, D. (2017). IEC 61850 meets CoAP: towards the integration of smart grids and IoT standards. *Proceedings of the Seventh International Conference on the Internet of Things*: 1–9.

Imran, B., Ahsan, M., Akbar, A. H., & Shah, G. A. (2024). D4GW: DTLS for gateway multiplexed application to secure MQTT (SN)-based pub/sub architecture. *Internet of Things*, **26**: 101172. doi: 10.1016/j.iot.2024.101172

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, **25**: 36–49. doi: 10.1016/j.ijcip.2019.01.001

Mnyanghwalo, D., Kawambwa, S., Mwifunyi, R., Gilbert, G. M., Makota, D., & Mvungi, N. (2019). Fault Detection and Monitoring in Secondary Electric Distribution Network Based on Distributed Processing. *2018 20th International Middle East Power Systems Conference, MEPCON 2018 - Proceedings*: 84–89. doi.:10.1109/MEPCON.2018.8635141

Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, **52**(1): 452–459. doi.: 10.1016/j.procs.2015.05.013

Rani, S., Shabaz, M., Dutta, A. K., & Ahmed, E. A. (2024). Enhancing privacy and security in IoT-based smart grid system using encryption-based fog computing. *Alexandria Engineering Journal*, **102**: 66-74. doi : 10.1016/j.aej.2024.05.085

Sorebo, G. N., & Echols, M. C. (2011). Distribution Automation Moving from Legacy to Secure. In *Smart Grid Security* (pp. 99–128).

Thantharate, A., Beard, C., & Kankariya, P. (2019). Coap and mqtt based models to deliver software and security updates to iot devices over the air. *2019 International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*: 1065–1070.

Tom, R. J., & Sankaranarayanan, S. (2017). IoT based SCADA integrated with fog for power distribution automation. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*: 1–4.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, **14**(4): 998–1010.

Zainudin, A., Syaifudin, M. F., & Syahroni, N. (2019). Design and Implementation of Node Gateway with MQTT and CoAP Protocol for IoT Applications. *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*: 155–159.

Zidan, A., Khairalla, M., Abdrabou, A. M., Khalifa, T., Shaban, K., Abdrabou, A., El Shatshat, R., & Gaouda, A. M. (2016). Fault detection, isolation, and service restoration in distribution systems: State-of-the-art and future trends. *IEEE Transactions on Smart Grid*, **8**(5): 2170–2185. doi: 10.1109/TSG.2016.2517620