Tanzania Journal of Science 48(1): 34-46, 2022
ISSN 0856-1761, e-ISSN 2507-7961


# Design and Implementation of Distributed Identity and Access Management Framework for Internet of Things (IoT) Enabled Distribution Automation

**Ally T Bitebo*, Hellen Maziku, Ndyetabura Hamisi, Charles N Tarimo, Kwame S Ibwe and Abdi T. Abdalla**

*College of Information and Communication Technologies, University of Dar es Salaam*
*P. O. Box 33335, Dar es Salaam, Tanzania*
**Corresponding author, e-mail: allybitebo@udsm.ac.tz*

Received 30 Aug 2021, Revised 4 Jan 2022, Accepted 25 Jan, Published Mar 2022
**DOI**: https://dx.doi.org/10.4314/tjs.v48i1.4

**Abstract**

The smart grid and Internet of Things (IoT) technologies play vital roles in improving the quality of services offered in traditional electrical grid. They open a room for the introduction of new services like distribution automation (DA) that has a significant advantage to both utility companies and final consumers. DA integrates sensors, actuators, intelligent electrical devices (IED) and information and communication technologies to monitor and control electrical grid. However, the integration of these technologies poses security threats to the electrical grid like Denial of Service (DoS) attacks, false data injection attacks, and masquerading attacks like system node impersonation that can transmit wrong readings, resulting in false alarm reports and hence leading to incorrect node actuation. To overcome these challenges, researchers have proposed a centralized public key infrastructure (PKI) with bridged certificate authority (CA) which is prone to DoS attacks. Moreover, the proposed blockchain based distributed identity and access management (DIAM) in IoT domain at the global scale is adding communicational and computational overheads. Also, it is imposing new security threats to the DA system by integrating it with online services like IoTEX and IoTA. For those reasons, this study proposes a DIAM security scheme to secure IoT-enabled distribution automation. The scheme divides areas into clusters and each cluster has a device registry and a registry controller. The registry controller is a command line tool to access and manage a device registry. The results show that the scheme can prevent impersonated and non-legitimate system nodes and users from accessing the system by imposing role-based access control (RBAC) at the cluster level.

**Keywords**: Distributed Identity and Access Management; Electrical Secondary Distribution Network; Internet of Things; IoT Enabled Distribution Automation; Smart Grid Security.

## Introduction

Tanzania Electrical Supply Company Limited (TANESCO) is the electrical utility company responsible for generating, transmitting, distributing and selling electricity in Tanzania. The utility company has started several initiatives to improve the quality of services offered to the final customers. To improve service availability, the utility company has an emergency desk unit to quickly respond to customer enquiries in case of power disruption which is mainly caused by electrical faults. Faults are mainly reported by customers, which makes the process of fault management to be manual and inefficient (Andegelile et al. 2019). To

improve the process of fault management, utility companies are integrating legacy electrical grids with advanced Information and Communication Technologies (ICT) which are known as smart grids.

A smart grid is an advanced electrical system that integrates a legacy electrical grid with Information and Communication Technologies (ICT). This enhancement opens up new opportunities to utility companies to offer modern and advanced services like demand response, bi-directional flow of power, automatic fault management and real-time monitoring and control. Moreover, this grid system enhancement at the electrical distribution network is known as Distribution Automation (DA) (Sorebo and Echols 2011). To deploy DA in Tanzania, TANESCO is using Supervisory Control and Data Acquisition (SCADA) and Distributed Management System (DMS) to monitor and control the transmission and primary electrical distribution network (PEDN). On the contrary, the secondary electrical distribution network (SEDN) has no automation system deployed, so this part of the network is not automatically monitored (Mnyanghwalo et al. 2019). Additionally, the DA technologies deployed at the PEDN are not directly fit to the SEDN because of its ubiquitous and distribution nature. To overcome this challenge, the Internet of Things (IoT) technologies have been applied to support the deployment of the DA technologies at the SEDN.

Internet of Things Enabled Distribution Automation (IoT-DA) is the usage of IoT technology for the deployment of distributed sensors, actuators, and advanced Intelligent Electronic Devices (IEDs) in the electrical distribution network to provide real-time monitoring and control of the electrical distribution grid (Mnyanghwalo et al. 2019). Sensors are installed in electrical equipment to read electrical grid data which is sent to the utility company Control Center (CC) through intermediate fog computing devices. On the other hand, actuators are installed in electrical equipment to accept control commands from field IEDs and CC and control electrical grid behaviour (Zidan et al. 2016, Mwifunyi et al. 2019). The IEDs which are mini-computers, sometimes termed as edge or fog computers are installed to support distributed computing (Aghenta and Iqbal 2019, Gilbert et al. 2019). These IEDs devices act as gateways to connect a number of distributed IoT devices to the utility server for further processing and storage, and this distribution nature is increasing cyber attacking surface and thus making the whole system to be vulnerable to cyber-attacks (Sorebo and Echols 2011, Kimani et al. 2019).

These security issues can be classified as device security, communication network and protocol security, system process control security, smart grid security, and power estimation security (Baumeister 2010, Wang and Lu 2013). Power estimation security deals with systems' real-time state data that can be compromised leading to wrong decisions. Moreover, the security of IoT and electrical grid system devices play a vital role in securing the entire electrical grid system. This is because they are the entry point of the distribution automation system, and most of the systems' data are generated and fed to the system through sensor devices. Secondly, they are large in number and are installed in the widely distributed area where they can be easily manipulated (Shapsough et al. 2015). Lastly, a compromised device cannot only breach the communication network and protocol security but compromise device processes and hence, directly affect system process control operations and security.

To overcome the above-mentioned challenges, this paper proposes a Distributed Identity and Access Management (DIAM) scheme for IoT Enable Distribution Automation (IoT-DA) for secondary distribution networks. The proposed scheme has the following advantages: guarantees the identity of all system users and IoT devices; offers role-based access to system users and IoT devices; prevents non-legitimate users from accessing system information as well as non-legitimate IoT devices to communicate with other system legitimate IoT devices; ensures distributed and lightweight features, hence can be implemented in IoT devices to support Identity and Access Management

(IAM) mechanism at edge and fog computing level; supports the European Telecommunications Standards Institute (ETSI) technical specification for cyber security requirements for IoT consumers shown in Table 1 as detailed in Partida et al. (2021).

**Table 1**: ETSI technical specification

| Number | Key topic |
|---|---|
| 1 | No universal password |
| 4 | Securely store credentials and security-sensitive data |
| 8 | Protect personal data |
| 11 | Make deletion of personal data easy |
| 12 | Facilitate installation and maintenance |
| 13 | Validate input data |

**Related works**

The security of these new vast distributed interconnected IoT devices on the internet has drawn significant attention from industry and academia. This is because of the ubiquitous nature of these IoT devices and their integrity to the stability of the entire system (Baumeister and Dong 2016). Several researchers have proposed security architectures, frameworks and schemes to improve the security and integrity of the distributed IoT devices deployed in various domains like smart health, smart city, and smart grid systems. However, one of the known challenges is the lack of proper IAM mechanisms for IoT devices (Fan et al. 2020). To address this challenge, several researchers proposed a variety of approaches and mechanisms to improve IAM mechanisms in the IoT domain. Initially, centralized architectures by using Public Key Infrastructure (PKI) have been adopted for easy accessibility and security control (Saxena and Choi 2015, Baumeister and Dong 2016). However, the centralized architectures are prone to various security threats like Denial of Service (DoS) attacks (Moosavi et al. 2015, Tiloca et al. 2017). For this reason, decentralized architectures have emerged to support security in the IoT domain.

Some researchers have proposed decentralized architectures that include PKI in hierarchical and mesh bridged trust models (Baumeister and Dong 2016). However, the formation of these bridged trust models with a single bridged CA has created another challenge by creating a single point of failure and adding computational burden to end devices. Moreover, a study by Abreu et al. (2020) proposed an IAM for IoT devices in smart grid systems by proposing a two-step lightweight access control mechanism for IoT devices that are resource-constrained in terms of processing capabilities, power consumption, and low memory and storage. They used approaches like a disposable password which are Time based on One Time Password (TOTP) for securing unicast and multicast communication between the smart meters, and central systems through an intermediate data concentrator. However, the proposed mechanism requires a local master key to be deployed to the manufacturer hardware modules like smart cards which can be compromised if an attacker accesses the smart meters physically. Moreover, the two authentication steps will add delays to the IoT-DA.

Additionally, a Decentralized Identity and Access Management (DIAM) for IoT devices has been proposed to support interoperability and device registry management of IoT devices by using Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) (Fan et al. 2020). It has been pointed out that a smart combination of different technologies is needed to avoid intentional attacks for resilient IAM in IoT enabled systems. Another proposed mechanism is cloud computing and blockchain to offer powerful computations and colossal storage and edge

computing to move computations close to the users and IoT devices (Partida et al. 2021). This approach uses existing IoT blockchain online platforms like IoTEX and IOTA, which are not suitable for an electrical utility company which needs to own its data privately. However, the proposed DIAM schemes above are targeting identity of system users and devices at the global scale by using blockchain technology, on which add computational complexity and delays for IoT DA systems. Moreover, the deployment of blockchain technology needs other security measures to mitigate security breaches in IoT based DA. Therefore, this study proposes a distributed IAM scheme for securing IoT devices in IoT-DA to support automatic fault management in the electrical secondary distribution network.

## Materials and Methods

### System architecture

Initially, an overview of the system architecture is presented; an IoT cloud architecture, as shown in Figure 1. At the start, sensors collect electrical state data from electrical lines and equipment, and then the data is sent to the CC for further processing through edge or fog computers. On the other hand, control commands are sent from the edge or fog or CC to the actuator to control states of electrical lines and equipment (Raza et al. 2017, Gilbert et al. 2019).

The proposed system architecture is delineated in Figure 1 which comprises five units: sensing node, actuating node, edge computer, fog computer and control center. All these are described hereunder:

a) Sensing node: is a combination of sensors and microcontroller with a Wi-Fi communication module. Its main role is to collect electrical current and voltage readings and forward them to edge or fog computing devices.

b) Actuating node: is a combination of the actuating module and microcontroller with a Wi-Fi communication module. Its main task is to accept control commands from edge or fog computing devices.

c) Edge computer: is a microcomputer with a Wi-Fi communication module. Its main task is to accept readings from sensors and forward them to fog computing devices and accept control commands from fog devices and forward them to actuating nodes.

d) Fog computer: is a minicomputer with a Wi-Fi communication module. Its main role is to accept readings from sensing nodes through edge devices and forward them to the control center and accept control commands from the control center and forward them to actuating nodes through the edge devices.

e) Control center: is a high-performance cloud computing device with high computational power and a large storage medium to store historical data for further analysis and management.

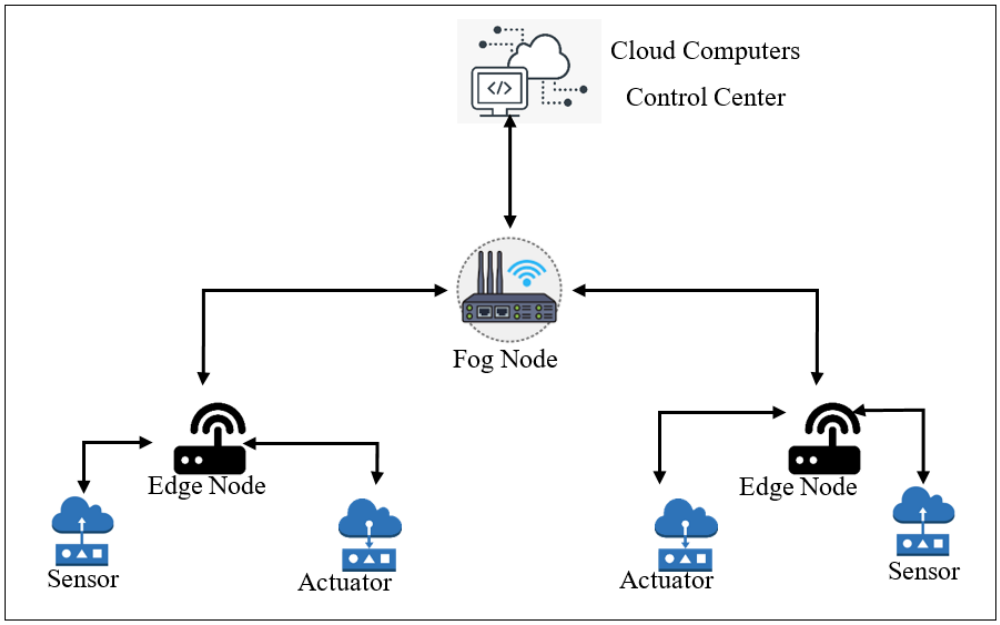


**Figure 1**: Overall system architecture.

**Security design goals**

The proposed DIAM scheme has the following security design goals to permit only authenticated system users or devices to operate in the system as well as to impose role-based access management to authorize system users and devices to specific services. The proposed system comprises of the following units:

a) Distributed security: The proposed DIAM scheme was designed in such a way that an area is divided in clusters where each cluster is controlled by a single fog node which acts as a master to cluster nodes. A fog node is responsible for controlling the device register of a given cluster as well as controlling communication traffic and access roles of all devices and users within the cluster.

b) Device register: The proposed DIAM scheme has a device register to store information of all users, user groups, system devices and assign their types based on the roles they perform.

c) Authentication: The proposed DIAM scheme uses user emails and passwords to identify legitimate system users and the passwords are hashed before being stored in a database and combined with salted text to preserve the password security and integrity. Besides, the scheme uses devices' physical addresses like MAC addresses and temporary JSON Web Token (JWT) based tokens to authenticate devices.

d) Authorization: The proposed scheme employs user groups to authorize system users. Likewise, it uses node types to authorize system nodes to respective services. The scheme first uses user groups which are categorized in two main groups: administrators and cluster administrators. Administrators are the super system users who can add, read, update and delete system users, nodes, user groups, and region information. Cluster administrators can manage devices within their clusters. For system nodes, the scheme uses device type to authorize devices to specific services in a system. The scheme has three main device roles which are controller node, actuator and sensor node. Controller nodes are the nodes which are edge or fog nodes running

as cluster master nodes. Actuator nodes are the ones which represent system actuators and sensor nodes represent system sensors.

e) Unique identification: The proposed DIAM uses a Universal Unique Identifier (UUID) to uniquely identify system users and nodes. The UUID will reduce the risks of assigning a single identifier to two different entities.

**Proposed distributed identity and access management scheme**

The proposed scheme was intended to protect the process of automatic fault management in electrical secondary distribution networks by offering role-based access control services to system users and devices. The scheme is authenticating only registered system users to manage and control system devices. System users are authenticated to access the system once they provide a correct combination of a username and password before accessing the system. Likewise, a scheme is authenticating only registered system devices like sensors, actuators and fog nodes to communicate with each other. System devices are authenticated to communicate with other system nodes once they provide the correct combination of MAC address and temporary JWT based token. For that reason, only registered system users are authenticated to access the services. Similarly, only registered system devices are authenticated to communicate in the process of automatic fault management in the secondary distribution network.

Moreover, the scheme is authorizing the registered system users and devices by grouping them into specific groups. These groups have specific roles which guide them to perform only intended functionalities. For example, a sensor node will always perform functionalities of sensing and not be able to perform the functionalities of the actuator node. For this reason, we will protect the automatic fault management by preventing impersonation attacks and preventing both non-legitimate users and devices from accessing and communicating in the process of automatic fault management in the secondary distribution network.

The proposed DIAM scheme is dividing the system into clusters and each cluster is controlled by cluster administrator. It offers identity and access management to all communicating devices within a system. It is granting access to only registered users and devices within a system and denying access to all unregistered users and devices. It consists of a device registry, registry service, and registry controller. Device registry is a relational database management system which stores information about system users and devices. Registry service is an application programming interface (API) to connect a registry controller with a device registry. It is allowing an administrator to manage and control device registry. Moreover, a registry controller is a command line tool used by administrators to manage device registry. From the system architecture, all of these three tools run in fog devices and each fog device controls its sub-devices within a given cluster as shown in Figure 2.

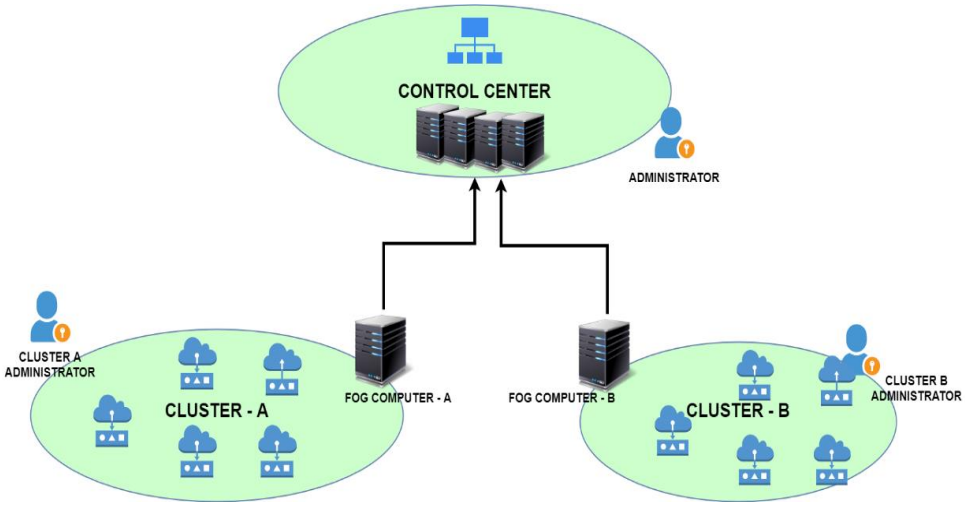


**Figure 2**: Proposed DIAM system cluster.

**Device registry**

The device registry database holds information about operational clusters, system users, and system devices, as shown in the Entity Relational Diagram (ERD) in Figure 3. The clusters represent the operational regions like Msasani area in Dar es Salaam and the region table holds information of the region by defining, unique identification number of a region (RegionID), region name (RegionName), and regional descriptions (RegionDescription). System user table holds information about all users allowed to access the system by defining; unique identification of a user (UserID), user name, user email, user password, his or her operating region, user groups which define their roles within a system, and date where the account is created. In the system, the nodes table has a system node identification number (NodeID), device address field which is a unique value, for example, MAC addresses of the devices, node type which can be a sensor, actuator, edge or fog device. Moreover, the node regional information where it operates, latitude and longitude positioning data, date created and master flag to identify the fog controller node it is attached to. Furthermore, the user group table has a user group ID number, group name, and group roles descriptions. The system administrator manages system users, user groups, regions and system nodes. On the other hand, cluster administrators manage only devices within their clusters and operating regions.

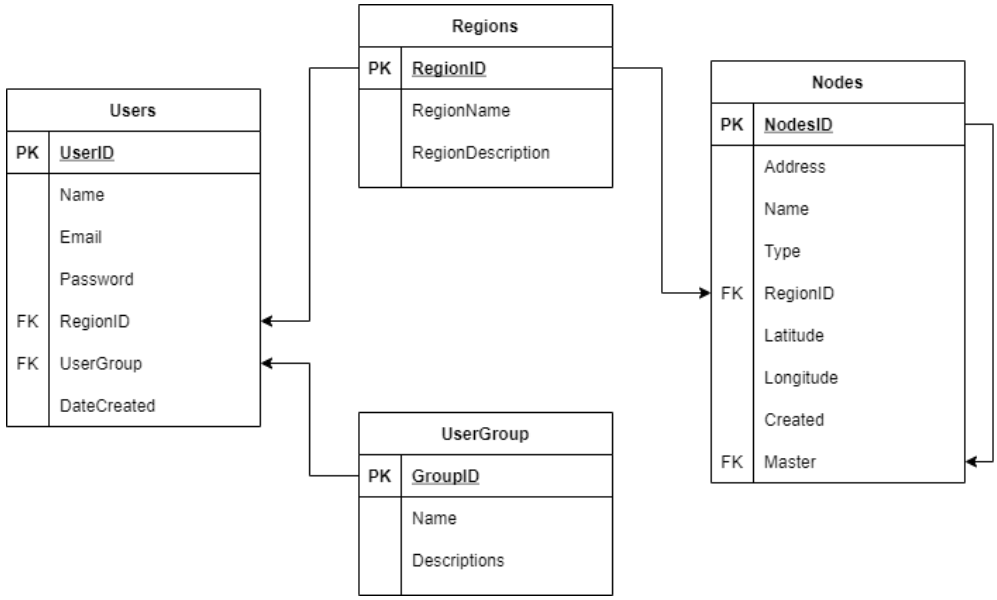


**Figure 3**: Entity relational diagram.

**Registry service**

Registry service is a command-line tool to manage all device registry operations. It logs all device registry operations performed by devices or system users.

**Registry controller**

Registry controller is the command-line tool to control registry operations like to initialize database connections, add, read, update and delete registry information like regions, users, systems devices and roles. The tool has its own built-in menu to assist system users in performing their intended functions, as shown in Figure 4. Moreover, a cluster administrator can manage users, devices, regions and user groups by using the following commands that are summarized in Table 2.

```
MINGW64:/d/EXPERIMENT/NEW REGISTRY/cmd/regctl
User@DESKTOP-7MFG6II MINGW64 /d/EXPERIMENT/NEW REGISTRY/cmd/regctl (master)
$ regctl add user -h
add a new entity to the network (users |nodes |regions )

Usage:
  regctl add [flags]
  regctl add [command]

Available Commands:
  nodes       add new node
  regions     regions --id <id> --name <name> --desc <description>
  users       users -n <name> -e <email> -p <password> -r <region-id>

Flags:
  -h, --help   help for add

Global Flags:
      --address string    the address of regsvc (default "http://localhost")
      --config string     config file (default is $HOME/.regctl.yaml)
      --password string   user password
      --port string       regsvc port (default ":8080")
      --uuid string       user unique identifier

Use "regctl add [command] --help" for more information about a command.
```

**Figure 4**: Registry Controller Menu.

**Table 2**: List of Registry Controller Commands

| Functionality | Command and Parameters |
|---|---|
| Add new entry | $ regctl add users [param lists] |
| | $ regctl add regions [param lists] |
| | $ regctl add nodes [param lists] |
| List registry entries | $ regctl get users [param lists] |
| | $ regctl get regions [param lists] |
| | $ regctl get nodes [param lists] |
| Update registry entries | $ regctl update users [param lists] |
| | $ regctl update regions [param lists] |
| | $ regctl update nodes [param lists] |
| Delete registry entries | $ regctl delete users [param lists] |
| | $ regctl delete regions [param lists] |
| | $ regctl delete nodes [param lists] |

**Demonstration prototype**

The proposed DIAM scheme is developed and demonstrated under the controlled environment. The DIAM scheme is deployed on a laptop computer to represent a fog device. Then, three Raspberry Pi mini-computers were used to represent sensors and actuators installed at the electrical secondary distribution network. The laptop has Intel (R) Core (TM) i7-4600U @ 2.10 GHz 2.70 GHz processor, RAM 8 GB, and 256 GB SSD Hard Drive. The laptop computer runs registry service, registry controller and device registry. The registry service is implemented by using Golang programming language and can be deployed in any platform based on demand. Since this study uses Windows 10, an executable file (.exe) was built to support the Windows platform. Similarly, the same executable file was built for a Registry Controller and both command-line tools were accessed by using Windows Command Line Tool for Registry Service and GitBash software for Registry Controller.

The device registry is implemented by using PostgreSQL relational database management system. The overall system prototype is connected wirelessly by a Huawei Wi-Fi Router with model number B315s-22 as illustrated in Figure 5. These three Raspberry Pi 4 model B+ mini computers run the Raspberry Pi operating system which was previously known as Raspbian. They send data periodically to the fog node running the DIAM scheme. Firstly, the implemented DIAM scheme is identifying the device initiating a communication by checking its availability to the device registry. Secondly, it authenticates the device by checking its unique ID and token or password. Lastly, the successfully authenticated devices are authorized to access only services assigned to their roles within a given group. Furthermore, the implemented DIAM scheme is logging all operational responses based on the requests and data it receives from Raspberry Pi mini computers.

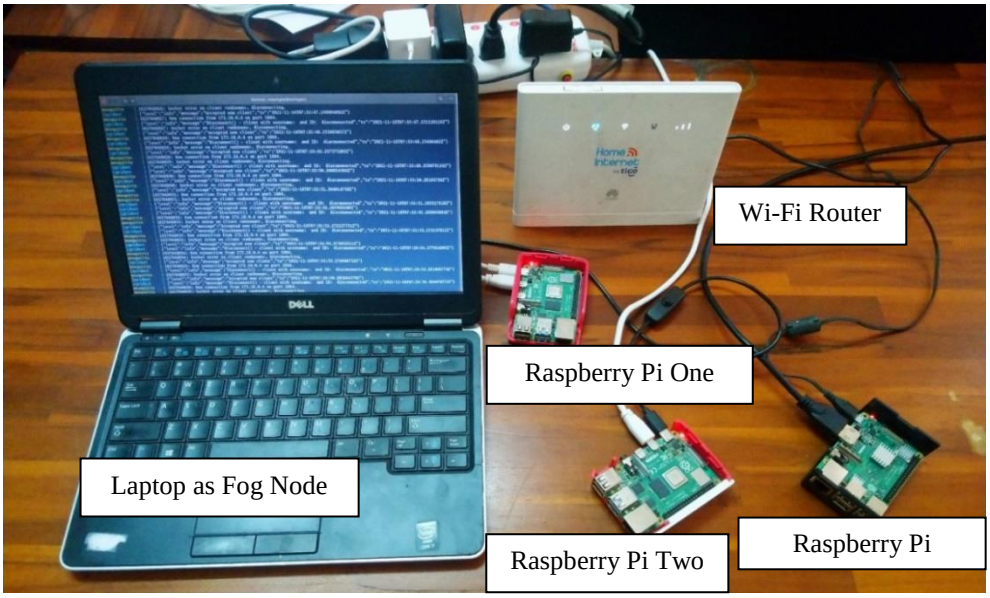


**Figure 5**: Prototype of the DIAM system.

**Evaluation**

**Experiment**

To evaluate the proposed DIAM scheme, the prototype was implemented as shown in Figure 5. The Raspberry Pi mini computers are used to initiate communication with laptop computer and send data periodically. The setup represents the process of interactions between sensors and actuators with fog nodes in the secondary electrical distribution network. These Raspberry Pi minicomputers must be authenticated and authorized each time they are communicating with a laptop computer. Furthermore, these Raspberry Pi are loaded with a computer program to initiate and send data to the laptop computer. We then simulated the two main scenarios to test the performance of the developed DIAM scheme; one for authentication and another for authorization functionalities.

Firstly, we register two system devices; Raspberry one and Raspberry two into the device registry, and Raspberry three is not registered. Raspberry Pi one was assigned in sensor group and Raspberry Pi two was assigned in actuator group. Thereafter, we allow all three devices to initiate communication with laptop computer. Then, we examined the system logs published to the registry controller. These published system logs were able to provide us with the answers regarding the process of authentication of all these three devices as shown in Figure 7.

Secondly, the laptop runs Mosquito version 1.6.15 software as a MQTT broker to evaluate the authorization functionality of the proposed DIAM scheme. We created two topics within a MQTT broker, one for sensors and another for actuators. We conducted four authorization sub scenarios and examined their logs published in the registry controller. Initially, we made an actuators' subscription request from a Raspberry Pi three which is unregistered. Then, the same devices made a publishing request to the sensors' publishing topic. We examined the system logs published to the registry controller.

Moreover, we initiated two requests from Raspberry Pi one to the MQTT broker. The first request is sensors' publishing request followed by an actuators' subscription request. Likewise, the sensors' publishing and actuator subscription requests were sent from Raspberry Pi two to the MQTT broker. Then, we studied the system logs published to the registry controller as shown in Figure 6.


**Figure 6**: Screen shot showing the system logs responses published to the registry controller when actuator node sends a publishing request to the fog node running proposed DIAM scheme.

**Results and Discussion**

This section presents the performance results of the proposed DIAM scheme for securing IoT-DA to support automatic fault management in the electrical secondary distribution network. We studied the output of the system logs published to the registry controller in each tested scenario. We monitored the behavior of the fog node in each scenario and compare it with our design goals. The results show that, the proposed DIAM scheme was able to support the management of DIAM by deploying distributed device registry to the fog node computers. The system was divided into clusters by creating and managing operating regions. Hence, the proposed DIAM scheme was able to reduce the effect of DoS attack compared to centralized IAM.

Moreover, the deployment of the device registry at the fog node computers was able to support the authentication and authorization of the communicating devices. Hence, was able to detect non legitimate node and block any attempt to communicate with legitimate devices. Figure 7 is the screenshot of the system logs printed at the registry controller when a non-legitimated device tries to communicate with the fog node computer running proposed DIAM scheme. Similarly, the proposed DIAM scheme was able to authorize legitimate system node to their respective services and block all attempts made to unauthorized services. Figure 8 is the screen capture showing the system logs printed at the device registry when legitimate system node tries to access unauthorized services. As a result, the proposed DIAM scheme is operating as distributed security mechanism and was able to offer authentication and authorization services at the given region.

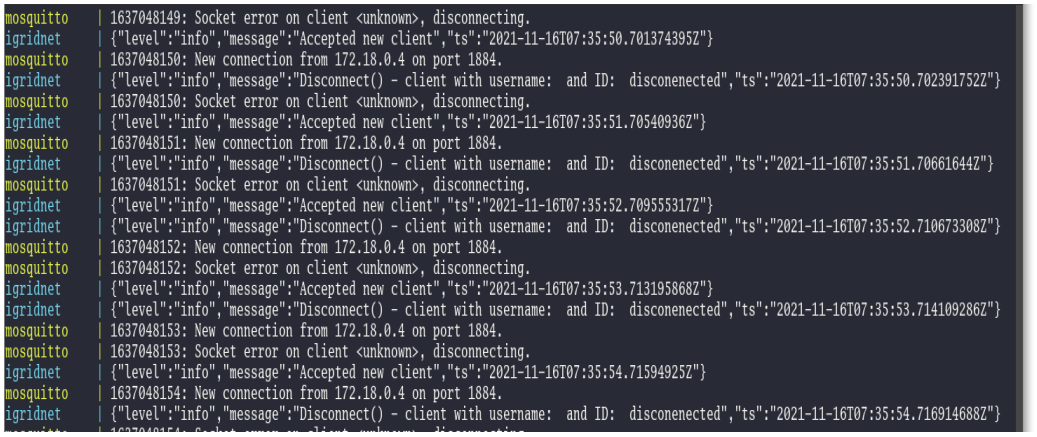


**Figure 7**: Screen shot showing the system logs responses published to the registry controller when unregistered node sends any communication request to the fog node running proposed DIAM scheme.


**Figure 8**: A screen shot showing the system logs responses published to the registry controller when authorized sensor refused to publish.

## Conclusion

In this work, we developed a distributed identity and access management scheme to support the process of identification, authentication and authorization of distributed IoT devices in IoT-Enabled distribution automation in secondary electrical distribution networks. The design of the proposed DIAM scheme was based on the distributed security, where the distributed device registry was deployed to fog node computers operating in given regions or cluster. The proposed approach is suitable for securing the distributed based IoT-DA compared to the blockchain global scaled based DIAM schemes proposed which are adding computational and communication overheads to the proposed system. These distributed fog node computers create multiple identification and access management servers compared to the one implemented in the centralized IAM which creates a single point of failure. Thereafter, the proposed design was able to authenticate communicating devices. Likewise, the scheme was able to authorize all communicating devices within the system.

In the future, we are going to integrate the proposed DIAM scheme with a hybrid proxy server to control and secure communication between system nodes. The integration will consider the introduction of secured channels by deploying security protocols to improve the security of the communication network in IoT Enabled Distribution Automation in the secondary electrical distribution network.

## Acknowledgment

This research is part of the capacity building iGrid-Project at the College of Information and Communication Technologies (CoICT) at the University of Dar es Salaam (UDSM) under the sponsorship of Swedish International Development Agency (SIDA).

## References

Abreu V, Santin AO, Viegas EK, and Cogo VV 2020 Identity and access management for IoT in smart grid. In *International Conference on Advanced Information Networking and Applications* 1215–1226.

Aghenta LO and Iqbal MT 2019 Development of an IoT based open source SCADA system for PV system monitoring. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* 1–4.

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

Baumeister T 2010 Literature review on smart grid cyber security. *Collaborative Software Development Laboratory at the University of Hawaii*. 650.

Baumeister T and Dong Y 2016 Towards secure identity management for the smart grid. *Security Commun. Networks* 9(9): 808–822.

Fan X, Chai Q, Xu L, and Guo D 2020 DIAM-IoT: A decentralized identity and access management framework for Internet of Things. In *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure* 186–191.

Gilbert GM, Naiman S, Kimaro H, and

Mvungi N 2019 A cloud-fog based system architecture for enhancing fault detection in electrical secondary distribution network. In *International conference on Computer Networks, Big data and IoT* 845–855.

Kimani K, Oduol V, and Langat K 2019 Cyber security challenges for IoT-based smart grid networks. *Int. J. Critic. Infrastr. Protect.* 25: 36–49.

Mnyanghwalo D, Kawambwa S, Mwifunyi R, Gilbert GM, Makota D, and 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.

Moosavi SR, Gia TN, Rahmani AM, Nigussie E, Virtanen S, Isoaho J, and Tenhunen H 2015 SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* 52(1): 452–459.

Mwifunyi RJ, Mvungi NH, and Kissaka MM 2019 Agents based service restoration in electrical secondary distribution network. In *2019 6th International Conference on Systems and Informatics (ICSAI)* 292–296.

Partida A, Criado R, and Romance M 2021 Identity and access management resilience against intentional risk for blockchain-based IOT platforms. *Electronics* 10(4): 378.

Raza S, Helgason T, Papadimitratos P, and Voigt T 2017 SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things. *Future Gener. Comput. Syst.* 77: 40–51.

Saxena N and Choi BJ 2015 State of the art authentication, access control, and secure integration in smart grid. *Energies* 8(10): 11883–11915.

Shapsough S, Qatan F, Aburukba R, Aloul F, and Al Ali AR 2015 Smart grid cyber security: Challenges and solutions. In *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)* 170–175.

Sorebo GN and Echols MC 2011 Distribution automation moving from legacy to secure. In *Smart Grid Security* 99–128.

Tiloca M, Gehrmann C and Seitz L 2017 On improving resistance to Denial of Service and key provisioning scalability of the DTLS handshake. *Int. J. Inf. Security* 16(2): 173–193.

Wang W and Lu Z 2013 Cyber security in the smart grid: Survey and challenges. *Comput. Networks* 57(5): 1344–1371.

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