Asian Journal of Electrical Sciences
ISSN: 2249-6297 (P); 2583-7923 (E)
Vol.12 No.1, 2023, pp.31-38

DOI: https://doi.org/10.51983/ajes-2023.12.1.3676

Power System Security Protection in Microgrids Based on Advanced Metering Infrastructure

Benjamin Amough Kwembe and Yekini Suberu Mohammed
Lecturer, Department of Electrical/Electronic Engineering,
School of Engineering Technology, Federal Polytechnic Nsarawa, Nigeria
E-mail: benkwembe@gmail.com, engryek88@yahoo.com
(Received 11 March 2023; Accepted 26 March 2023; Available online 4 April 2023)

Abstract **- Modern electric power networks are progressively in demand for advanced protection systems due to the changing structures of the systems. In distribution power systems, emerging scenarios need some compelling protection efforts. In the last few decades, a lot of innovations such as Advanced Metering Infrastructure (AMI) have made incursions into the electric power sector. The development of AMI has fostered the integration of smart meter systems in microgrids and distribution networks with the capability to permit communication between electricity customers and utility service companies. Control and monitoring of information with regard to energy consumption is a phenomenal task that requires advanced information and communication technologies including some other essential parameters in real-time. Smart meters integrated into microgrids enable the utility to develop an electric power business efficiently. Therefore, this paper presents a study on the experimental on overview and investigation of the energy consumption pattern and data validation of smart meters installed in a smart grid project deployed by PowerGen in Nigeria. In addition, a comprehensive review of the security threats and control measures in microgrids was also presented. The results obtained show that utilities can increase their situational responses in a timely manner to the occurrence of abnormalities in the power grid to provide better monitoring and control services to energy customers.**
Keywords: **Smart Grid, Power System Security, Microgrid, Energy, Advanced Metering Infrastructure**

I. INTRODUCTION

The concept of network protection against security threats in modern electric power industry is as important as the protection of the entire power system investment. From the perspective of improving technological development, the system of protection in the power sector is a very dynamic endeavour. In the last few decades, there have been some tremendous changes in the physical structures and technical responses of power system protection devices. The evolution of new electric power structures and future distribution networks will require novel protective systems. Due to the dynamic characteristics of modern power systems, the emerging protection system is fast embracing new technologies that utilize smart communication and cyber security protection systems. There has been an increasing degree of automation of protective devices for improvement in reliability and sensitivity against attacks in power systems. Protection of power systems against any unwarranted technical attacks in any form is absolutely necessary to ensure a stable operation of the electricity business, especially in microgrids. Electric power microgrids are small-scale networks for providing electricity to an independent community. A smart microgrid has different kinds of components interfacing with one another for efficient energy delivery.

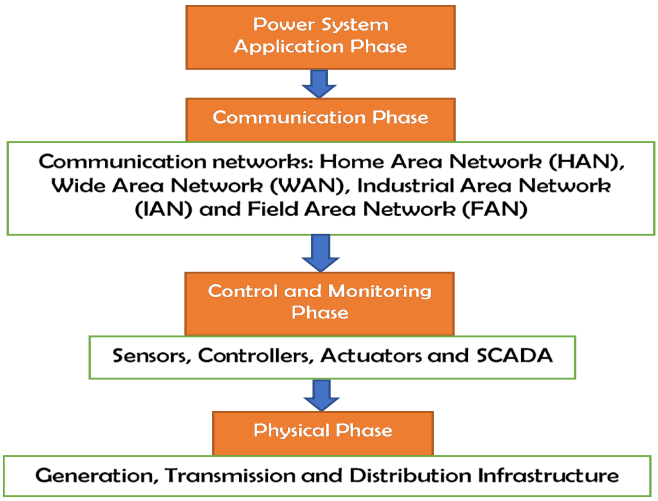

Fig. 1 Model of power system with communication and control interface

Figure 1 shows a model of a power system with a communication and control interface. The application of microgrids has solved a lot of energy crisis problems across different parts of the world [2]. Microgrid power components are less complex than the traditional large-scale power system but they are also in need of an effective protection structure for efficient power delivery [3].

Due to the increasing prominence of microgrids in the global power sector, the utilization of modern technologies in microgrids for the optimization of power generation and distribution services has also increased. Integration of intelligent and autonomous protective devices through the use of Information and Communication Systems (ICT) [3] has increased the capability of protection in microgrids. The capability of a power system equipped with intelligent devices to process information timely and accurately can be exploited to solve security problems to efficiently balance the demand and supply of energy. The recent transformation of microgrid power systems into smarter networks has further eased the task of power system protection [4] due to increasing abilities for collection, processing, computation, and subsequent exchange of important data [5].

The quest for ease in control of power systems is responsible for the penetration of the Internet of Things (IoT), thereby increasing the likelihood of cyber security attacks in the networks [6]. Protection of electric power networks against cyber-attacks prevents lots of negative security consequences. Thus, this study presents a standard approach that enhances protection issues based on IoT authorization and confidentiality in simulation-based against security threats in microgrids. In addition, the planetary of this present study is regarding the analysis of the review of security issues in smart grids with mitigations and countermeasures. It also presents data validation and evaluation of energy consumption patterns of customers through the application of smart meters in an AMI smart grid project.

II. APPLICATIONS OF SMART SYSTEMS IN MICROGRIDS

Generally, security problems in electric power networks involve some serious techno-economic penalties. However, security issues in microgrids are even more challenging due to the flexibility of the networks. The cyber-physical nature of modern power systems enables command and control to be executed in better and more reliable ways. In microgrid power systems, the distributed nature of the system is fast becoming highly intelligent and users interact with increasing tendencies for demand-side and utility control of required information [7-8]. Traditional microgrids used less complex digital technologies compared to the modern days smart grids utilizing a series of smarter control technologies for the purpose of optimization of power systems for efficient protection. In modern power systems, demand response is a critical factor because it affects the dynamics of grid operations, stability, efficiency and integration of energy resources [9]. Smart systems used in electric power systems are based on the features of smart sensors, controllers and intelligent communication technologies using ICT tools. The construction as well operational systems of smart grid technologies use ICT networks. The interactions of the operational systems of smart microgrid components have created a lot of technical challenges with regard to the security and reliability of operations due to communication imperfections.

III. COMMUNICATION SYSTEMS IN MICROGRID PROTECTIONS

Communication networks are essential for the operation and protection of power grids. Violation of communication principles in electric power networks leads to problems and consequential protection failures thereby affecting the capability of the power system. The normal operations of the electric power system can be disrupted through erroneous measurements of control or dispatch signals. In the last few decades, communication has played some vital roles in the protection of microgrids. At present, there are large numbers of services expected to be accomplished in centralized and decentralized power systems. The modernization of the power system is based on the requirements for upgraded power quality, energy security and reliability. The application of modern communication technologies in power grids is to provide suitable control platforms for the realization of emerging EM strategy especially in networks using Distributed Energy resources (DERs). Application of modern smart communication technologies such as IoT, integrated smart sensors, cloud computing platforms, smart metering systems and smart control systems have aided a lot of paradigm shifts in EM.

The traditional power grid is characteristically unidirectional where power and information flow is just from the point of generation to the end users of electricity. This system has been in existence for an extended period of time before the emergence of an intelligent grid system based on smart technologies. Figure 2 shows a smart MG with demand-side energy storage. The concept of a smart grid is an electrical power grid with numerous operations for EM based on advanced communication technologies. A smart grid is a representation of an intelligent electrical grid with reliable, scalable, secure, interoperable and cost-effective electrical systems [10]. In reference [11], a smart grid has also been described as an electrically automated and distributed network characterized by the flow of electricity and information in a bi-directional mode to respond and monitor changes in the network. A smart grid can be applied to a smaller-scale power system like in a standalone MG [2]. Smart grid technologies embedded in an MG can help higher RES penetration with efficient monitoring and control [12]. In the operation of an MG, the communication layer is most importantly required for dealing with the bi-directional communication needed for power management. The communication layer interfaces with the security and application layers to deliver some

functions to customers and utility companies. The functions include network integrity and privacy control, system authentication in addition supply and distribution of power. A range of network capabilities such as Area Networks (HAN), Neighborhood Area Networks (NAN), and Wide Area Networks (WAN) are required for the operations of smart communication in MGs. The application of any of the area networks depends on the geographical coverage in the operations of the MGs. Until this day, there is some serious constraints in the privacy of data exchange between the operators of MGs and the customers due to cyber security attacks.

There are two basic communication technologies commonly employed in smart MG: wired and wireless technologies. Wired technologies have multiple advantages compared to wireless technologies, especially in the cost of investment, system security, maintenance constraint, data transmission reliability and bandwidth flexibility. Over the years, wired communication technologies have been used successfully but in recent times, wireless communication has emerged with proven performances regarding the flexibility and scalability of the communication network. There is also greater ease in the implementation of wireless technologies in the context of efficient data transmission speed and intelligent communication [14], thereby granting the system access to communication capabilities like wired technologies [15]. However, both wired and wireless communication technologies in a power grid have different technological architectures, flexibility, investment cost and degree of scalability.

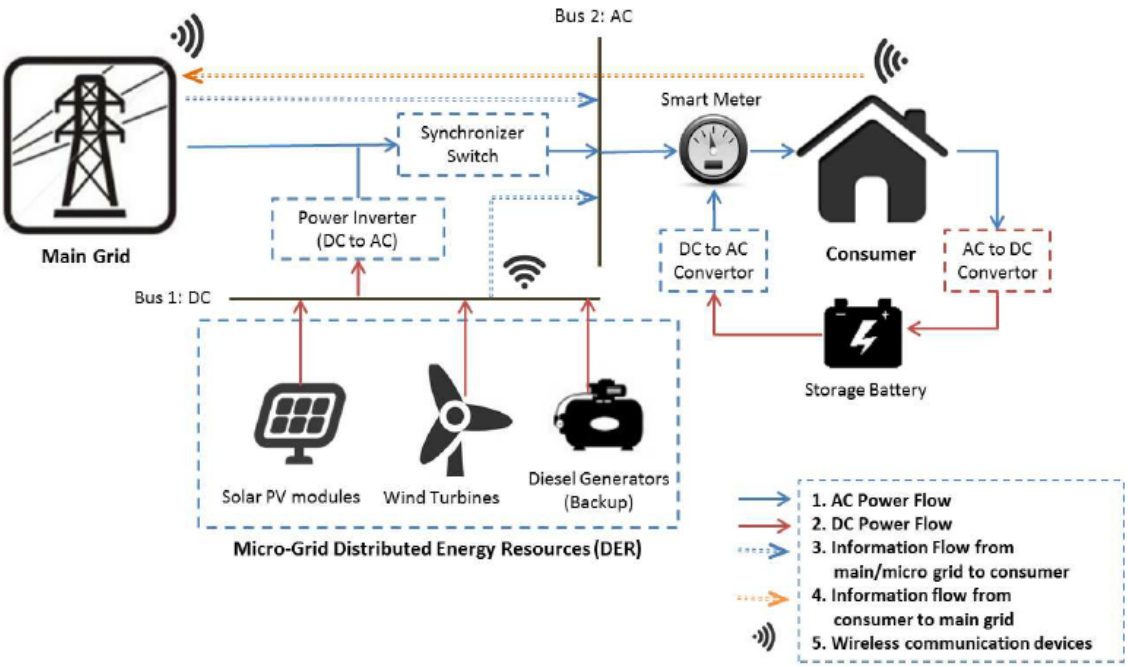

Fig. 2 Depiction of a smart MG with demand-side energy storage [13]

A. Wireless Communication Technologies

With the advent of internet-based communication technologies, the development of a smart grid has become interestingly an integral part of the evolution of modern society. Internet communications are based on wireless communication technologies. Wireless communication is a class of modern communication that can be achieved without the use of wires in network connectivity. The first generation of wireless communication was accomplished with radio waves. In MG communication, many different wireless communication networks such as Bluetooth, WiMAX, Wi-Fi, cellular network (3G/4G/5G) and ZigBee have successfully been used [3, 15]. Wireless communication technologies are available in different devices especially those that require low power consumption such as mobile phones and laptops. Wireless communication technologies are being developed by wireless computing companies using different concepts of wireless sensor networks to achieve the same objective with different data transmission capabilities. The span of area coverage of different wireless communication technologies varies significantly.

For example, WiMAX has long area coverage and higher speed compared to Wi-Fi. In terms of cost, Wi-Fi is more cost-effective than WiMAX while ZigBee and cellular networks are relatively cheap communication networks. The emergence of wireless communication technologies and subsequent implementation in hardware devices brought about the phenomenal application of Internet-of-Thing (IoT) in the smart grid. ZigBee is a good network for energy metering and management applications with low power consumption and affordable deployment cost [16]. The desire to maintain long-range communication in power systems based on low energy consumption and affordable cost is currently an area of keen interest to researchers in wireless communication technologies.

B. Wired Communication Technologies

Wired communication technologies encompass the transmission of communication data to the receiver via a transmitter and wired communication medium. The power system's most commonly used physical wired communication structure is the Power Line Communication Carrier (PLCC). In conventional power systems, High Voltage Lines (HVL), Medium Voltage Lines (MVL) and Low Voltage Lines (LVL) have been used for broadband communication [17-19] by the use of electricity distribution systems. There are varieties of competing wired line systems that can be used in smart grids [20] among which are PLCC, Ethernet, Digital Subscriber Lines (DSL) and Fiber-Optic (FO).

In PLCC, the existing power lines can be used for data communication networks and therefore making it less cumbersome to be implemented. The challenge of noise constraint is usually associated with wired communication at the early stage of its development until recently when advanced power electronics for the suppression of noise came into existence. Different wired technologies have their benefits and shortcomings. For example, the implementation of PLCC is cost-effective but it is associated with high signal interference. Also, for FO, the cost of implementation is quite high and upgrading the system may be difficult to achieve.

C. Integrated Smart Technologies in Microgrids

Many countries across the world now have MG development plans via some policies and legal flexibilities. In addition, few among these countries are also vigorously working towards the achievement of smart MGs due to their unprecedented effective control and EM opportunities. A smart MG is a classical power delivery system embedded with intelligent modernized networks that responsively can communicate in a bi-directional computerization approach. The operational domain of a Smart Micro-Grid (SMG) is basically on intelligent management of energy and other constraints such as demand response and automated generation control.

The implementation of modern communication technologies in power systems is responsible for the development of SMG systems. SMG is a kind of automated and information-based small-scale electric power grid with communication capabilities. The supply and delivery of secure and economically reliable electricity to customers can easily be achieved by using smart electric power concepts. Integrated communication sensors and automated computer systems formed the basic architectures of SMGs and they offer increased control opportunities with secure, reliable, and flexible energy delivery. Implementation of smart technologies in MGs improves the overall system operational procedure for the benefit of the investors, consumers, and the environment [21, 22].

IV. UTILIZATION OF IoTs IN MICROGRIDS

IoT integrated into power systems can offer better access control and protection than traditional digital technologies. Emerging technical devices used in IoT have good processing and storage capabilities with limited power consumption, due to the use of portable communication technologies for data transfer and network utilization in the applications. There are a series of technological evolution with regard to the application, data-link management, network layer, and transportation of information based on security protocols in the domains of IoT Communication.

Data-link management procedures are based on the physical linkages of the communication devices in the IoT environments using a wired or wireless communication protocol. Due to the ease of application and operational efficiency, wireless data transmission is usually preferred due to its communicational flexibility and operational activeness. The data link technologies developed by the Institute of Electrical and Electronics Engineers (IEEE) such as 802.15.4 has gained soaring popularity in the last few years. However, other IoT data link wireless technologies including Bluetooth Low Energy (BLE), IEEE 802.11ah, IEEE 802.11 (Wi-Fi), Z-Wave and ZigBee with different distance ranges and power consumption based on sleeping cycles have been developed.

Furthermore, the network layer of an IoT constitutes the routing layer involved in sending the information packages from the source to the destination. The commonly used network layers are Caching Array Routing Protocol (CARP) and 6LoWPAN. Developed by Microsoft, it exploited the Microsoft Proxy server for its implementation through the application of a single logical cache using the algorithms of Hyper-Text Transfer Protocol (HTTP). CARP network layer permits a web browser to control accurately where in the proxy array membership information can be stored based on the activeness of the proxy server.

On the other hand, 6LoWPAN has great popularity in IoT due to its cloud computing benefits and low power consumption. It has the presence of small link-layer frames that allows every node of the IPv6 address to connect easily and directly to the internet. It derived its name from Internet Protocol version 6 (IPv6) of Low Power Wireless Personal Area Network (LoWPAN) which is a standard of the Internet Engineering Task Force (IETF). Designed in a meshed form as shown in Figure 3, a 6LoWPAN permits free exchange of data with the assistance of an edge router acting as a gateway for the internet facility. It is consequently not difficult for the applications going through the nodes to access the IP packets to the server of the internet without any effect by the edge router.

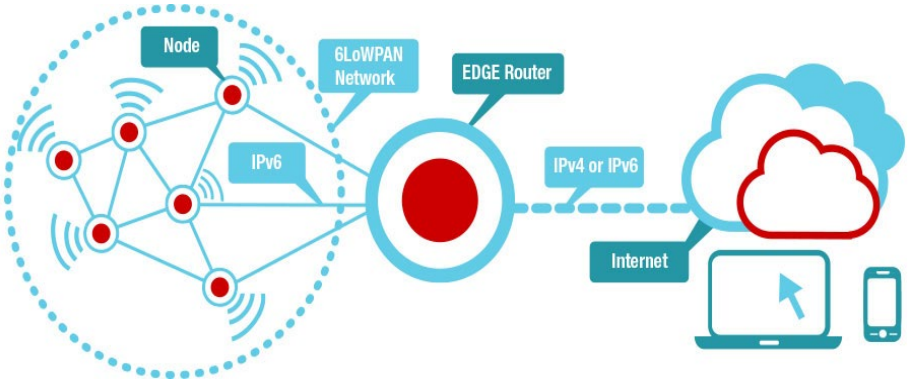

Fig. 3 Structural representation of 6LoWPAN

V. SECURITY VIOLATIONS IN MICROGRIDS

Microgrids can be attacked in several ways by attackers who intend to violate the system for unjustifiable benefits. Attacks are usually carried out through disruption of the cyber security protocols through unhealthy exploration of smarter contents of microgrids. In this case, the prevention or subsequent solution to attacks on microgrids can be found through simulations of the security scenarios since it is usually not economically feasible to build a physical microgrid prototype for test-running. Reconfiguration of physical microgrids for experimentation of security problems is another major challenge because of the flexibility condition of the of systems [23]. Microgrid security attacks may be done for different reasons such as energy theft, infringement on customers' or utility privacy for the stealing of sensitive information, and denial of access to electric power. Exploiting alternative simulation mechanisms for analysing security attacks in microgrids is a much easier and more economical approach. When microgrid security analysis is conducted in a computer simulation environment, there is the probability of achieving greater flexibility for the analysis of all the necessary data in the communication network. Security attacks on power grids can modify the data in a communication network of the power system, thereby disrupting the normal power flow. The essence of protection in power systems utilizing IoT is to prevent disruption of the security-conscious component of the systems such as the Advanced Metering Infrastructure (AMI).

AMI integrated into microgrids has several advantages, including intelligent management of the distribution network, provision of useful data and information, and provision of a two-way communication system from the control centre to the meter, among others. AMI offers sophisticated functions for data management and solutions through the use of IoT meters. AMI can be attacked in several ways individually or in clusters depending on the potential capability of the threats launched by the attackers through interruption of power consumption information on the metering devices. The system can be attacked by compromising the back-end utility servers harboring important power network processing information.

Power network attacks can occur in the form of the introduction of malicious data or alternation of the normal communication between consumers of electricity and utility companies. Successful malicious attacks have many consequential effects such as breach of network privacy, loss of electric power due to theft, constrictions in data concentrations, alternation of communication channels and disturbance of normal operations of the electric power flow.

The architecture of the hardware components of AMI is shown in Figure 4. AMI is an IoT system acting as an intermediate system to bridge the communication gap between the users and the utility domain through the utilization of available networks of HANs, NANs, WAN, and the system of intelligent end devices (IEDs).

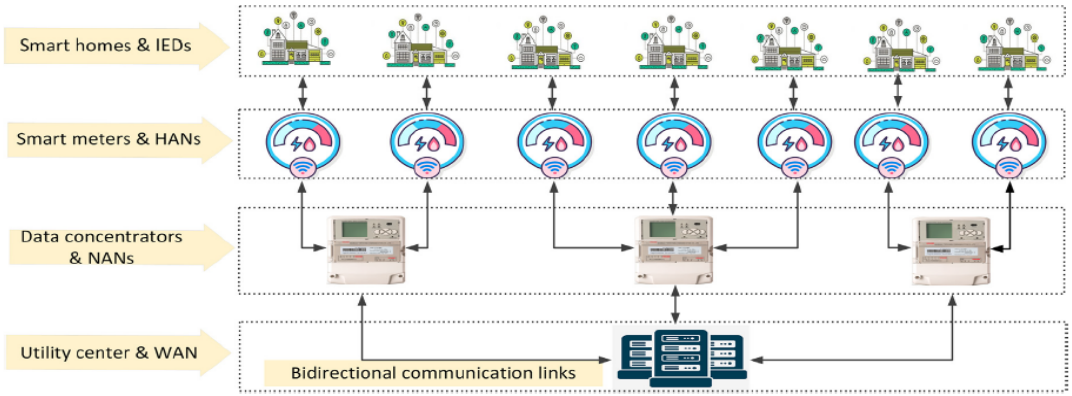

Fig. 4 Architecture of the hardware components of AMI [24]

In smart communication for the control and monitoring of electric power systems, the concepts of confidentiality, integrity, and availability are very relevant. However, security vulnerabilities in power systems may occur in any of the three different layers of physical, data and cyber communication layer. A secure AMI system prevents system failures, enhances efficient management of collected data, increased customer satisfaction due to timely access to reliable information and promotes overall efficiency.

A. Physical (Hardware) Layer

This consists of the smart meters and the system of data concentrators. Smart meters are usually located at the premises of energy consumers away from the utility control centre. This connotes that it can be attacked by hackers despite the fact that controls domicile with the utility command centre. Command information can be sent to the smart meters installed at various customer domains but attackers pretending to be utility personnel may send false messages to the customers.

B. Data Layer

Data layers deal with the integration of ICT systems into the grid for the transmission of information in the power networks. Data are important for analytical purposes such as load forecasting, energy management and other power distribution services. The collection, processing and storage of heterogenous datasets is accomplished by the data layer. As the system expands due to increasing customers' demand and power generation, the utility company looks towards a corresponding increase in the data system capacity to match up with the desired level of accuracy due to the increasing volume of data. An efficient data layer provides security-related information for real-time analysis with the help of other supporting system architectures in smart microgrids. An unauthorized modification of data can affect data confidentiality and integrity of the original data. In the case of very large data (big data), the use of cloud-computing space can mitigate the problem of large storage space needed for storing the data [25]. The data layer may use the Data Concentrator Unit (DCU) to synchronize data from a cluster of smart meters and the collective data is then sent to the data control unit.

C. Cyber Communication Layer

This layer plays the role of interfacing the smart meter and the IEDs through the communication channels for data transfer. Data transfer through communication channels could be vulnerable to attacks and threats from man-in-the-middle (MITM) attackers in the form of alteration and theft of consumer data. In addition, faulty conditions such as loss of bandwidth, breaks to the cables and path deterioration of the communication line can also be responsible for the vulnerability of the communication layer. In consequence, technical and communication disruption in the communication layer of AMI leads to the unavailability of electrical power services to the customers.

VI. EXPERIMENT IN MICROGRIDS

The case analysis presented in this study was based on experiments to determine the stability of the microgrid with respect to security threats based on real-time monitoring. The system uses the smart meter in AMI pilot project provided by PowerGen. The interactive situations between the feeders, distribution transformers and the smart meters installed at the consumer premises form the basis for this current study. The meters utilize a communication network for the realization of any communication to the DCU and the meter data management system which is the Meter Data Acquisition System (MDAS) in the microgrid. The pilot project integrates all the required interactive components for the measurement for the experimental investigation.

A. Wireless Communication Technologies

Validation of data is necessary for the purpose of determining any abnormal data input into the system. The presence of wrong data recorded by the meter signifies a threat to the normal working procedures of the microgrid. Deviation of recorded data from the normal or actual standard parameters can result in system security constraints considering the fact that the real usage may be difficult to be accomplished. Data usage must reflect the predefined standards based on standard validation mechanisms. The most commonly measured data are voltage, current, power factor, kilowatt-hour and power. The essence of data validation is basically to identify technical errors and breaches based on meter readings. The results of the readings recorded from the conduct of the experiment on a typical day for a period of 10 hours are shown in Table I. It was observed from the validation data obtained that at some random point in time, the data presented by the meters under observations were false, thereby indicating tampering conditions. There may be the possibility of abnormal behaviors of the consumers such as energy theft and system attacks resulting in missing gaps or errors in the readings of the meters.

Tampering with meters results in misinformation, especially regarding energy consumption or technical problems with power equipment. Tampering has consequential impacts on service stages. However, the consumption pattern of the customers based on DCU was also investigated for a period of 24 hours on four different days (Saturdays) in four different weeks in a month. This was accomplished in a different experiment. The results shown in Figure 5 revealed a deviated pattern with suspected irregular behaviors in the consumption pattern of the customers. Studying the normal pattern of daily energy consumption is a significant requirement in the monitoring and control of undesirable consumer actions. In the Figure 5, the daily consumption pattern is shown with the necessary information concerning the minimum and maximum energy consumption. The

figure presented energy consumption results for four different Saturdays in a month in the month of October 2022. It was observed that the consumption of Day 1 (8-10-22), Day 2 (15-10-22), and Day 4 (29-10-22) follow the same pattern while a deviation was observed on Day 3 (22-10-22). The information presented on the diagram is useful for the utility meanwhile the deviation observed on Day 3 is not in consonance with the planned energy management due to its unusual consumption nature. The unusual consumption scenario shows a nonconformity in the consumers' consumption situation. This occurrence can be attributed to the suspected activities of the abnormal behaviour identification of energy theft or irregular consumption pattern of the customers. Consequently, an abnormal daily consumption pattern has been observed compared to the normal pattern on the same day of the month. The utility may subsequently decide to investigate to identify the problems orchestrated by the unexpected deviation for technical actions.

TABLE I METER VALIDATION RESULTS BASED ON EXPERIMENTS

Meter ID	01-02 hr	02-03 hr	03-04 hr	04-05 hr	05-06 hr	06-07 hr	07-08 hr	09-10 hr	10-11 hr	11-12 hr
516457	N	N	N	N	N	N	N	N	N	N
145740	N	N	N	N	N	F	F	N	N	F
147464	N	F	N	F	N	N	N	N	F	N
432106	N	N	N	N	N	N	N	N	N	N
563219	F	N	F	N	F	N	N	N	F	N
342990	N	N	N	N	N	N	N	N	N	N
324146	N	N	N	N	N	N	N	N	N	F
238724	N	N	N	N	N	N	F	F	N	N
345685	F	N	F	N	F	F	N	N	N	N
561573	N	N	F	N	N	F	N	N	F	F

F: False consumption data obtained
N: Normal consumption data obtained

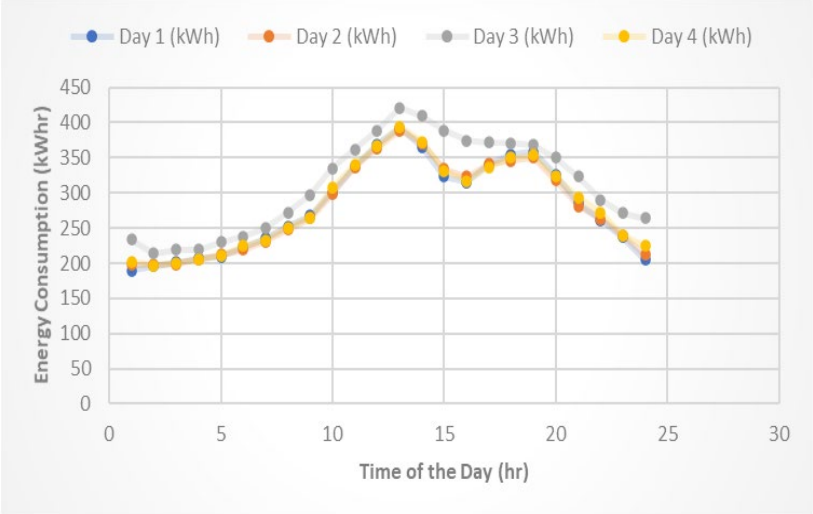

Fig. 5 Normal and deviated energy consumption profile

VII. CONCLUSION

Integration of smart concepts in a power system offer multidimensional solutions to some new challenges. While smart technologies permit electricity consumers to participate actively in the business of the electricity market and control strategies, they have also unleashed some potentially serious technical problems such as cyber security threats and disruption of energy services. Information obtained from smart meters can help both utility and customers to detect some potentially challenging issues and defend against them accordingly. Timely preventive actions by the utility against attacks on electric power networks can prevent quick changes in the overall system's abnormal situations. An experimental investigation of a pilot smart grid power project was conducted for the analytical conditions of smart meter information with respect to data validation and abnormal energy pattern examination. It is therefore observed that monitoring situations are critically important and offer promising responses to prevent abnormalities of misinformation and security threats in power systems.

ACKNOWLEDGMENT

The authors are thankful to Tertiary Education Trust Fund (TETFUND) for granting financial support for the conduct of this research through the Institution Based Research (IBR) research grant disbursed to the Federal Polytechnic Nasarawa, Nigeria.

REFERENCES

[1] L. Mariam, M. Basu, and M. F. Conlon, "Microgrid: Architecture, policy and future trends," *Renewable and Sustainable Energy Reviews,* Vol. 64, pp. 477-489, 2016.

[2] Y. Yoldaş, A. Önen, S. Muyeen, A. V. Vasilakos, and I. Alan, "Enhancing smart grid with microgrids: Challenges and opportunities," *Renewable and Sustainable Energy Reviews,* Vol. 72, pp. 205-214, 2017.

[3] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Computer Communications,* Vol. 36, No. 17-18, pp. 1665-1697, 2013.

[4] H. Kopetz and W. Steiner, *Real-time systems: design principles for distributed embedded applications*. Springer Nature, 2022.

[5] Y. Zhu, X. Huang, J. Zhang, J. Luo, and J. He, "Fault Diagnosis for Power Equipment Based on IoT," in *Internet of Things: International Workshop, IOT 2012, Changsha, China, August 17-19, 2012. Proceedings*, Springer,, pp. 298-304, 2012.

[6] E. Bertino, "Data Security and Privacy in the IoT," in *EDBT*, Vol. 2016, pp. 1-3, 2016.

[7] K. Mets, J. A. Ojea, and C. Develder, "Combining power and communication network simulation for cost-effective smart grid analysis," *IEEE Communications Surveys & Tutorials,* Vol. 16, No. 3, pp. 1771-1796, 2014.

[8] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Transactions on industrial informatics,* Vol. 9, No. 1, pp. 28-42, 2012.

[9] K. C. Budka, J. G. Deshpande, and M. Thottan, *Communication networks for smart grids, Springer,* 2016.

[10] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. P. Chen, "A survey of communication/networking in smart grids," *Future generation computer systems,* Vol. 28, No. 2, pp. 391-404, 2012.

[11] T. Basso, J. Hambrick, and D. DeBlasio, "Update and review of IEEE P2030 Smart Grid Interoperability and IEEE 1547 interconnection standards," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT), IEEE,* pp. 1-7, 2012.

[12] R. E. Pérez-Guzmán, Y. Salgueiro-Sicilia, and M. Rivera, "Communication systems and security issues in smart microgrids," in *2017 IEEE Southern Power Electronics Conference (SPEC), IEEE,* pp. 1-6, 2017.

[13] A. Bhattacharya and J. P. Kharoufeh, "Optimal microgrid energy storage strategies in the presence of renewables," in *IIE Annual Conference. Proceedings*: *Institute of Industrial and Systems Engineers (IISE),* pp. 1348, 2014.

[14] M. Erol-Kantarci and H. T. Mouftah, "Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues," *IEEE Communications Surveys & Tutorials,* Vol. 17, No. 1, pp. 179-197, 2014.

[15] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *IEEE PES general meeting, IEEE,* pp. 1-7, 2010.

[16] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE transactions on Industrial informatics,* Vol. 7, No. 4, pp. 529-539, 2011.

[17] R. Pighi and R. Raheli, "On multicarrier signal transmission for high-voltage power lines," in *International Symposium on Power Line Communications and Its Applications, IEEE,* pp. 32-36, 2005.

[18] D. Hyun and Y. Lee, "A study on the compound communication network over the high voltage power line for distribution automation system," in *2008 International Conference on Information Security and Assurance (isa 2008)*, *IEEE,* pp. 410-414, 2008.

[19] R. Aquilue, I. Gutierrez, J. L. Pijoan, and G. Sanchez, "High-voltage multicarrier spread-spectrum system field test," *IEEE Transactions on Power Delivery,* Vol. 24, No. 3, pp. 1112-1121, 2009.

[20] M. Burns, "NIST SGIP catalog of standards," *October, nist. gov/twiki-sggrid/bin/view/SmartGridSGIPCatalogOfStandards,* 2010.

[21] F. H. Malik and M. Lehtonen, "A review: Agents in smart grids," *Electric Power Systems Research,* Vol. 131, pp. 71-79, 2016.

[22] E. Y. Song, G. J. FitzPatrick, and K. B. Lee, "Smart sensors and standard-based interoperability in smart grids," *IEEE Sensors Journal,* Vol. 17, No. 23, pp. 7723-7730, 2017.

[23] C. Dufour and J. Bélanger, "On the use of real-time simulation technology in smart grid research and development," *IEEE Transactions on Industry Applications,* Vol. 50, No. 6, pp. 3963-3970, 2014.

[24] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," *Future Generation Computer Systems,* 2022.

[25] C. Castelino, D. Gandhi, H. G. Narula, and N. H. Chokshi, "Integration of big data and cloud computing," *International Journal of Engineering Trends and Technology (IJETT),* Vol. 16, No. 2, pp. 100-102, 2014.