ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

# Different Architectures of Power Grid

[1] Priyanka Kanade, [2] Sujata Mendgudle
[1][2] Electronics Deparment
[1][2] Ramrao Adik Institute of Technology, Nerul

***Abstract* - There are many challenges that electrical grid face today such as mission critical power demands, diversion of energy sources and integration of renewable energy sources. Also, the different domains have their own requirements. To beat these challenges, it required the intelligent management of the electrical grid. So in this survey we represents the four different types of architecture which is suitable for the different domains.**

**Index Terms— Power grid, Cyber Structure, Micro Grid, IoT, Network Topology**

## I.INTRODUCTION

AN electrical grid is used for the source of the power from the generating stations to the consumers through transmission lines. The conventional grid has been in operation since the discovery of electricity and the idea of power distribution rst came into place. Its old organization and lack of possibilities for consumer-integration are making the meeting of growing demand for power a reserved vision. The increasing cases of shut down and power problems calls forth the requirement of a smarter grid which has strong and new structure, the capacity to meet the growing demand, supports the combination of renewable sources and consumer, with a view for supportable development. The intelligent grid improvises the conventional grid enabling a unique level of consumer participation. In this survey, we represent the four different architectures of power grid. First architecture is based on the agent, in that agent performs the important role in power grid to increase the efficiency, improve stability and reduce the complexity. Second architecture uses the IoT as central part of the architecture which present a Collaborative Service Oriented Power Grid using Internet of Things (CSOPGI). It allows on time and in full delivery of services for power generation, distribution and utilization with collaborative data processing in an intelligent way using Internet of Things. Third architecture is the microgrid architectures. Microgrid is nothing but the provision of autonomous energy sources of each smaller area as well as the connection of main grid. Fourth architecture concern about the cyber sequrity.

## II. AGENT BASED POWER GRID ARCHITECTURE

Design of the intelligent grid architecture aims to nd new ways of connecting appliances, whereas the software design tests the compatibility, exibility and auto-conguration capabilities of advanced software ideas. Architecture arrange in that chapter shown that the architectures standard and agent primarily based design will oer a good advantage for the combination of appliances into an intelligent grid and the creation of agents controlling them[1].

### *A. Control Architecture of Agent Based Power Grid*

Agent based Intelligent grid Architecture contains six layer and that is explain bellow[1]:


***Fig. 1. Control Architecture of Power Grid***

- Load level agents in charge of the checking of measurement and control equipment also switching of load.
- Prosumer agents synchronize with the upper and lower level agents and evaluation the amount of energy expected to be generated soon and expected demand based on information provided by load agent[1]. On the premise of this estimate and investigation prosumer agent settle on choice

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

either to buy or oer energy from the supply network.

- DER Agents interface with other DER specialists in the same distribution network to set the energy rating and redesign its status about the expected generation in the immediate future.
- Distribution level agent makes a platform between the micro grid and the main grid through TSO agent[1].
- TSO level agent makes major market decisions based on the in order about the energy demand received from the low-level agents and send its requirements to generation units.
- Main Grid agents are keeping the overall look on the whole system status and in case of issues which were not resolved by the low-level agents locally, they perform major decision to achieve the overall goal. The normal grid didnt contain the data about their parts, creations, productions, consumptions and needs in the real time. There is no faculty for storing of energy for longer period; accordingly, the energy produced ought to be used in the meantime. Without communication in electrical grid, there is irregular in productions and consumptions cycle and this makes wrong management in electrical system coming about misuse of power in one spot where as deciency of power on the other side[4].

### *B. Aadvantage*

- It provides the exible architecture. So we can extend the architecture as demand is increase.
- Agent System conguration is projected for self-ruling power systems management and recovery.
- Due to the DER agent continous power we get. there is no problem in irregular in productions and consumptions cycle.

## III. POWER GRID ARCHITECTURE USING IOT

In every organization power generation, their distribution and ideal utilization is challenges. To face that challenges, we required smart structure or system. Here we represent a Collaborative Service Oriented Power Grid using Internet of Things (CSOPGI). It allows on time and in full delivery of services for power generation, distribution and utilization with collaborative data processing in an intelligent way using Internet of Things which will also leads to green environment as well as optimal resource utilization.

### *A. Internet of Things*

Fig4.1 shows the conceptual diagram of Internet of Things. Figure covers the convergence of dierent visions, service management also the enabling technologies. By combination of connectivity and content with collaboration, computing, cognition and context, there is a requirement of eective communication approach for transmitting information with dierent devices of the grid. The current technology of the IoT will provide network of intelligent devices and manage them like it provides eective delivery of power in the grid. IoT uses

***Fig. 2. Internet of Things: convergence of vision and services***

universal computing as well as ambient intelligence for task management with going beyond the traditional communication and IT infrastructure.

### *B. Power Grid Architecture Using IoT*

In current situations, there are number factors are aects the ecient working of a power grid. For example, damage to physical set-up during severe weather and other disasters, the increase in power demand, deregulation and fragmentation of industry, and regulatory environment compliances are some major factors. Such factors pose challenge to monitor,

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

control and govern the continuous service of the power grid. There is a requirement of an intelligent grid technology with self-healing system that can anticipate, respond to and insulate damage, moderate the impact and work towards speed recovery of the grid with improved reliability. With such an explicit power demands and implicit green energy requirements a CSOPGI is projected. Figure 3 presents the outline of CSOPGI[2].

***1) Data Gathering Process***

In data gathering process for gathering the information they use the IP based smart meters, Geographical Information System(GIS), sensors, e-services as well as internet. Smart meter will allow the bidirectional communication between meter and utility. Also, as it is IP based smart meter it is easy to communication among devices across the huge network. GIS is help to pass robust information for dierent operational decisions. Such a system prospers for accuracy (phase, connectivity and positioning accuracy). So, it helps to achieve a real time dynamic localization scheme[7]. Sensors is used to manage the to manage the mobility in task dynamic for the intelligent grid network. E-services in the form of web-based development helps to create an environment where collaborative problem solving can be adopted challenge.

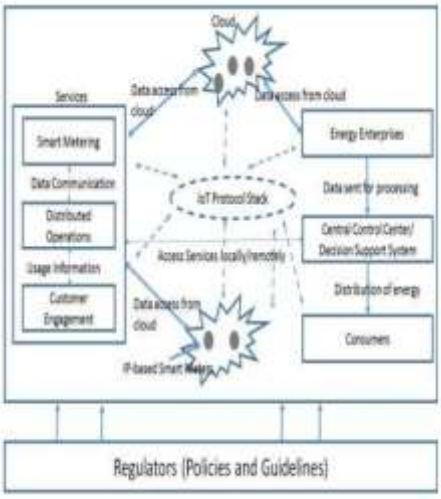


*Fig. 3. Architecture of CSOPGI*

***2) Distributed Network***

Distribution Network in the intelligent grid is such that it provides secure transmission of data as well as energy, able to provide continuous supply, propagation and time synchronization. By using IoT in intelligent grid system, it can cover wide range of network[10]. It facilitates the installation of sensors, which are key to the development of intelligent solutions for grid activities. Such solutions may include, enduser programming and development, performance evaluation, mobility support for universal data access, IoT oriented cloud architectures, context aware processing, energy and resource optimization. Internet of Things follows a typical protocol stack[2].

***3) Network Topology***

In IoT based architecture cloud based system is used for the connecting grids. Cloud based service will help to providing on time and full delivery of services due to that communication gap is reduced as well as provide robust decision making capabilities which helps to increase eciency of network. As the data, can accessed local as well as global so, it increases the productivity. It also provides exible infrastructure, IPbased devices so it can be utilized eective data processing. The fundamental convergence of such process is to distribute processing capability in a cooperative way to preserve energy and lessen cost[5].

***C. Power Grid Architecture Using IoT as Central Interface***

Fig. 4 presents a conceptual architecture for several tasks and components linked with the working environment of an intelligent grid.

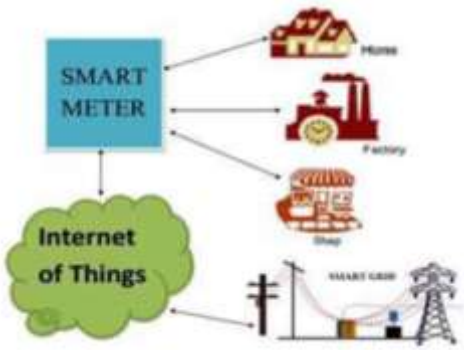


*Fig. 4. Power grid Architecture using IoT*

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

The diversity in technology pose limits on energy processing, storage and communication resources. Depending on the data rate, coverage constraints, bandwidth requirement and type of application, one or a combination of the given technologies can be used for communication between devices connected in IoT. Among all, Zigbee is used in wide variety of applications due to its support in various devices, oaring spectral bandwidth of 2.4GHz and frequently used in devices on ISM band. A combination of these technologies, depending on their features, may be applied in dierent regions. With the development of fourth and fth generation in mobile technology, a hybrid network should be preserved for best possible utilization of services[8].

### *D. Adavantages*

- Collaborative processing for IoT based intelligent grid makes it an intelligent utility network due to that reliability is increase.
- It reduce paper consumption due to online metering.
- The Internet based management will reduce the frequency as well as time required to remote monitoring and conguration.

***TABLE I***
***VARIOUS PROTOCOL FEATURES FOR INTELLIGENT GRID UTILIZATION***

| Technology | Data Rate | Spectrum | Coverage | Utility |
|---|---|---|---|---|
| GSM | Upto 14.4 Kbps | 900-1800 Kbps | 1-10km | Global Wireless connectivity of the devices |
| GPRS | Upto 170 Kbps | 900-1800 Kbps | 1-10km | Internet service for the device |
| 3G | 384Kbps-2Mbps | 1.92-1.98 Ghz | 1-10km | Mobile Comm-unication and Internet services |
| PLC | 2-3Mbps | 1-30Mhz | 1-3km | Dynamic Resource allocation over long range areas |
| Wimax | Upto 75 Mbps | 5-8Ghz | 10-50km | Long range network ing and controlling of the devices |
| Zigbee | 250Kbps | 1-30Mhz | 30-50m | Smart meter and smart grid devices |
| Wavenis | 100 kbps | 433MHz | 14km | M2M, smart meter, Telemetry and Home automation |
| Dash7 | 200kbs | 433MHz | 2km | Mobile payments and Smart meter |

- It will decrease of system integration cost, minimization of operating cost, and system maintenance cost.
- It will help to client to manage consumption and cost.

With such a collaboration based approach, the vision of green environment may be realized using global digital platform and streamlined by the reducing energy and time costs for all contributors and increasing quality of life within the community

## IV. MICRO GRID ARCHITECTURE

In order to stimulate economically efficient provision of energy and distribution network support services, energy and ancillary service markets, the whole of intelligint grid is segregated into miniature areas having provision for independent energy sources as well as connection to the grid, known as micro-grids[3].It is envisaged that market operation together with system operation will be controlled automatically using the micro-grid central controller (MGCC)[10]. This automation is essential to keep the overhead cost of operating the micro-grids low.

***Fig. 5. Micro-grid system***

### *A. Control Hierarchy In an Intelligent Grid*

Regarding to architecture of microgrid control or any control problem there are two different approaches can be identified: centralized and decentralized. A fully centralized control relies on a big amount of information trasmittence between involving units and then the decision is made at a single point. Hence, it will present big problem in implementation since interconnected power systems usually cover extended

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

geographic and involves enormous number of units. The fully centralized control is currently considered as infeasible solution. On another hand, in a fully decentralized control each unit is controlled by its local controller without knowing the situation of others[3]. The fully decentralized control is also irrelevant in this context due to strong coupling between the operations of various units in the system. A compromise between those two extreme control schemes can be achieved by means of a hierarchical control scheme consisting of three control levels: primary, secondary, and tertiary.

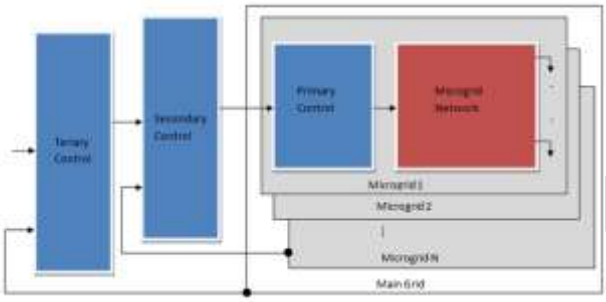


*Fig. 6. Hierarchical Control*

***1) Primary control***

The primary control is designed to satisfy the following requirements:

- To stabilize the voltage and frequency.
- To offer plug and play capability for DERs and properly share the active and reactive power among them, preferably, without any communication links.
- To mitigate circulating currents that can cause overcurrent phenomenon in the power electronic devices

The primary control provides the setpoints for a lower controller which are the voltage and current control loops of DERs. These inner control loops are commonly referred to as zero-level control[8].

***2) Secondary control***

Secondary control has typically seconds to minutes sampling time (i.e. slower than the previous one) which justifies the decoupled dynamics of the primary and the secondary control loops and facilitates their individual designs. Setpoint of primary control is given by secondary controll in which as a centralized controller, it restores the microgrid voltage and frequency and compensate for the deviations caused by the primary control. The secondary control can also be designed to satisfy the power quality requirements, e.g., voltage balancing at critical buses[8].

***3) Tertiary control***

Tertiary control is the last (and the slowest) control level which consider economical concerns in the optimal operation of the microgrid (sampling time is from minutes to hours), and manages the power flow between microgrid and main grid.

***B. Advantages***

- It provides good solution to supply power in case of an emergency and power shortage during power interruption in the main grid.
- In the grid-connected mode, ancillary services can be provided by trading activity of microgrid and the main grid. In the islanded mode of operation instead, the real and reactive power generated within the microgrid, including the help of energy storage system should be in balance with the demand of local loads.
- Microgrid allows and facilitates integration of renewable energy generation such as photovoltaic, wind and fuel cell generations without requiring re design of the distribution system.

## V. CYBER ARCHITECTURE FOR POWER GRID

Current technology for power grid uses the analog as well as digital information from providers as well as client, to understand the behaviours of energy production and requirements. In the analysis of that data reliability, eciency and many other factors are depending on that. Due to the bilateral communication, more and more clients are connected in power generation, and that may increase the security issues. The interception and forgery of data packages owing in the communication links is becoming more and more convenient to realize. The

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

network attack in intelligent grid not only inuence users privacy, but also threaten the grid safety, event peoples life. Currently, many standards which have been proposed share a great concern on cyber network security. So in that chapter cyber architecture is represent that provides a cyber security[4].

### *A. The Architecture of Security Monitoring System*

#### *1) Cyber Structure*

The cyber structure of security monitoring is shown in Fig 7 It employs DMZ as a guard for the intranet. All the access to the internet and the visit of the resources in the intranet will be monitored by the gateways and servers inside the DMZ. Dierent resources will be granted with dierent level of authority according to the specications and guidelines like ENISA, OpenADR. Any intended access to the resources will be recorded and veried by the monitoring software deployed on DMZ gateways. Thus, the advantages of the DMZ are fully used and the security level of the cyber is improved further.Inside the intranet, servers which provide key services such as SCADA, EMS are distributed. The correspond DSO are responsible for the maintenances of these hosts and any access to these facilities can be easily recorded and monitored through the methods in mentioned guidelines or by video cameras. The monitoring software deployed within the intranet focuses on data ow analysis. Abnormal data ows can be used to diagnose the communication problems, invalid port access, and potential network violations. This function is signicant to keep the Power Grid communication network operating in a secure, load-balanced and high performance state. The SMN can be independent or coupled with the cyber according to the communication loads of the paths. In the links with

***Fig. 7.***

less requirement of delays and bandwidth, the SMN can use the cyber directly to transfer data. However, to monitor the links with higher requirement of the bandwidth and delays, the monitor node of it should use independent communication path to analyze the monitored data and transfer it[?]. With this conguration, the access paths to the core resources are limited. In some degree, the SCADA system and EMS system can focus on their kernel functions without caring the security monitoring of the network. The communications which require high performance of the network are kept away from the inuences of security monitoring system. Although the security monitoring pressure increased in the DMZ, we can use several Demilitarized Zones (DMZ) to share the pressure and provide higher reliability. Meanwhile, the visits from the outside internet are not inuenced, the resources are exposed transparently to the users who are authorized and veried[4].

#### *2) Standards Exploration and Deployment of Security Monitoring System*

With proposed cyber structure, related standards should be deployed on dierent dimensions. The standards can be classied into two categories, namely information standards and communication standards, according to the problems they intend to address. The Intelligent Grids DR communications are assumed to be modelled and operated in OpenADR framework. OpenADR is a research and standards development eort for energy management led by North American research labs and companies. It employs the leveraging of the market to balance power generation and consumption. Usually, the Implementation of OpenADR specication uses XML as a tool to dene DR signals and data models. Because no specic or proprietary technologies is restricted to OpenADR itself, practical and well-designed security monitoring system becomes a critical part of Intelligent Grid. For example, one of the security monitoring systems functions is to protect DR data and signals from forgery and interception, making sure that the grid operates in a safe and reliable environment, this can be guaranteed by only monitoring the XML data ows without the consideration of DR level[8]. While users privacy should be preserved, attacks should be detected by monitoring the data ow and cyber loads, these targets can be achieved by using current security

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

mechanisms such as described in IEC 62443. Besides, the security mechanisms employed by OpenADR 2.0 are common ones without any modication. Due to the security monitoring standards and mechanisms mentioned by OpenADR are mostly deployed in DMZ physically, the inuences of the changes in OpenADR are reduced, and it will rarely block the operation of SCADA, DR, and

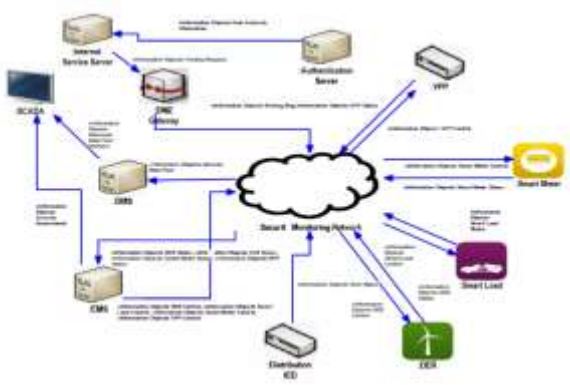

***Fig. 8. Information ow of Demand Response Activities with security monitoring system s***

EMS systems. While in the distributed solutions, normally the SCADA and DR are highly coupled with the security momtonng system. Thus, the changes in the mechanisms may cause the core functions of the intelligent grid to pause. Besides, the mechanisms should be inclined to the legality, integrity and validity of the information providers and receivers, while the correctness of the data inside the information should be guaranteed by the other applications[4]. The security monitoring must rely on the relatively matured standards and technologies like TSL, HTTPS rst, whilst be adaptive for the application of novel methods. Both Information standards and communication standards in SmarterEMC2 can be divided into two categories from the view of security, namely the security technology and security mechanisms. For the communication standards, security technologIes should be guaranteed by themselves, i.e. no matter PLC or Wi-Fi, they should consider their own techniques. against eavrsdrop, cracking, etc. when any extension is made. For information standards, the design of security mechanism is the main concern. It should be complete and leak less. However, OpenADR, one of the most applied standards amongs all use cases, didnt specity the concrete standards to use for addressing security issues. Mixing of dierent security standards due to no universal recommendation may cause safety problem[10].

***3) Deployment of Information Standards***

The term Information Standards mainly refers to the standards which format the exchanged data and give models of communicated entities. In construction of Intelligent Grid network, information standards such as IEC61850, IEC 61968, IEC 61970, etc. are consulted commonly. Most of these standards are oriented to high level applications and implemented by the combination of several communication technologies like COM, XML, and SOAP. The security monitoring system is responsible for preventing these XML signals or TSL packages from intercept and forging. After designing the deployment, the information objects generated by all the related actors can be derived as per the guidelines. For instance, in this use case, the information objects to be monitored are illustrated in Fig 8.

***4) Acess Sequence of the Proposed Cyber***

After the standard deployment, the several primary use cases to depict the functions of this structure when the user wants to have access with the resources inside the nework.The Internet access is the most common requirement for the islanded cyber. Because of the employment of DMZ, the number of the access points is limited, so it is easier to monitor the internet activities than the networks whose internet access points are distributed. Thus, in this kind of network, the sequence of the internet activity is shown in the gure 9. If the cyber is constructed without DMZ, the internet access servers or gateways may distributed in the network and become harder to cooperate with other services.Besides the internet access control, the authentication control is another important part of security monitoring, all the visitors outside and inside the cyber will be authenticated by the authentication server. The progress of the authentication are shown in figure 10. The last case is

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

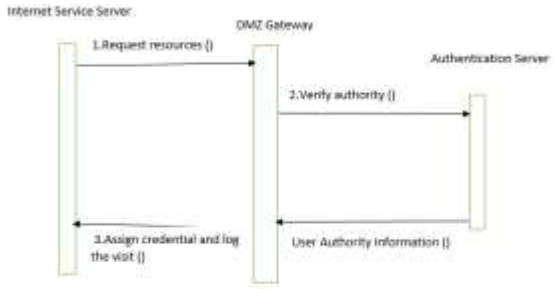


*Fig. 9. Time sequence diagram of Internet access control*

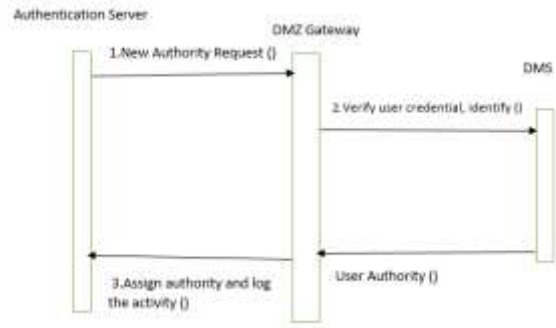


*Fig. 10. Time sequence diagram of Authentication control*

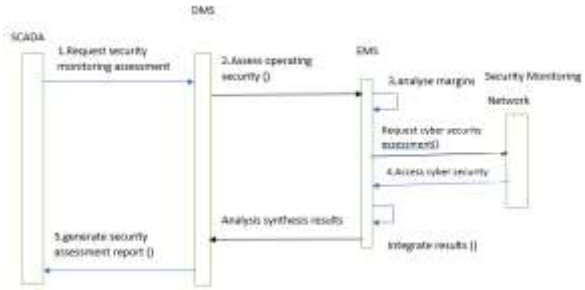


*Fig. 11. Time sequence diagram of Security monitoring and communication ow control*

the security monitoring and communicatoin ow. In this case, the data of communication ows is collected by the SMN, then it will be analysied by the DMS to determine whether there are abnormal data ows and whether the cyber is suer from port scaning or other attacks. Then the SCADA will generate the reports to the administrators[6]. The procedures are shown gure 11.

### *B. Advantages*

- Adaptability for the changes in both security related standards and the communication standards[10].
- Due to the guard of the DMZ, construction of special network for security monitoring is minimized because the monitoring system can share the same network when particular requirements are satised.
- Isolates the communicating load, which mitigates the inuences caused by users visits outside the DMZ.

## VI. CONCLUSION

Thus in this survey dierent types of architectures are present which are suitable for the dierent domains. For example Agent based Intelligent grid is projected for self-ruling power structures management and recovery, that is useful in complex system ,where huge number of devices are connected. Intelligent grid architecture using IOT is propesed where large amount of data is exachnged. Micro grid Architecture is used where great number of integrated functions is required also the need of extensive communication network is requred. Cyber Architecture are used where security is main concern.

## REFERENCES

[1] Siddappa, M., GC Bhanu Prakash, and H. S. Sridhar. ”Agent based communication architecture for smart grid.” In Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on, pp. 1920-1925. IEEE, 2016.

[2] Zaveri, Mukesh A., Saurabh K. Pandey, and J. Sathish Kumar. ”Collaborative service oriented smart grid using the Internet of Things.” In Communication and Signal Processing (ICCSP), 2016 International Conference on, pp. 1716-1722. IEEE, 2016.

[3] Seema, P. N., V. Deepa, and Manjula G. Nair. ”Consumer level intelligence in a Smart micro-grid.”

In Energy Efficient Technologies for Sustainability (ICEETS), 2016 International Conference on, pp. 320-324. IEEE, 2016.

[4] Hu, Rui, Weihao Hu, and Zhe Chen. "Research of smart grid cyber architecture and standards deployment with high adaptability for Security Monitoring." In Sustainable Mobility Applications, Renewables and Technology (SMART), 2015 International Conference on, pp. 1-6. IEEE, 2015.

[5] Ansari, H. Thameemul, S. PremKumar, and V. Saminadan. "Heterogeneous network modeling for smart grid technology." In Communication and Signal Processing (ICCSP), 2016 International Conference on, pp. 2336-2339. IEEE, 2016.

[6] Yan, Ye, Yi Qian, Hamid Sharif, and David Tipper. "A survey on smart grid communication infrastructures: Motivations, requirements and challenges." IEEE communications surveys tutorials 15, no. 1 (2013): 5-20.

[7] Pipattanasomporn, Manisa, Hassan Feroze, and Saifur Rahman. "Multiagent systems in a distributed smart grid: Design and implementation." In Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES, pp. 1-8. IEEE, 2009.

[8] Bidram, Ali, and Ali Davoudi. "Hierarchical structure of microgrids control system." IEEE Transactions on Smart Grid 3, no. 4 (2012): 1963-1976.

[9] Galli, Stefano, Anna Scaglione, and Zhifang Wang. "Power line communications and the smart grid." In Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 303-308. IEEE, 2010.

[10] Kim, Kwangsoo, Hyochan Bang, and Seong-il Jin. "Efficient data collection for smart grid using wireless sensor networks." In Consumer Electronics (GCCE), 2013 IEEE 2nd Global Conference on, pp. 231-232. IEEE, 2013.