ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Energy Meters using Internet of Things Platform

Shraddha Vijay Kadu[1], Prof. D.S.Bhosale[2]
Student[1], Professor[2]
Department of E &TC
JSPM BSIOTR, Pune, India

Abstract:
In smart grid, typical applications are distributor-centric rather than customer-centric. These applications typically have issues of scalability and user acceptance. To address this we propose architecture and implementation of energy meter with internet-of-things platform. Energy meter is the closest interface to end users as part of smart grid where energy is consumed. Our approach has four facets of novelty: 1) Integration of smart grid and home application using common infrastructure. 2) Data collection from heterogeneous sensor communication protocols 3) Secure and tailored data access and 4) Sensor and actuator mapping to common abstraction layer which can be leveraged to build concurrent applications. For demonstration kit has been built and validated with specific ZigBee meters and gateways, IoT server and custom user interface.

Keywords: Energy meters, IoT (Internet- of-Things), smart meter.

I. INTRODUCTION

Energy meter is closest to end user at distribution level in a smart grid. It is a two-way communication between customers and electric power distribution companies or agencies, converting passive end-users into active partners [1] in the power distribution network. Residential customers need a simple way to control energy consumption and production, and to exchange power usage data with energy providers or distributors. From the point of view of market acceptance and penetration, it is just one aspect of the broader concept of smart home and smart buildings. It enfolds new possibilities for end users in residential and commercial segments to optimize power consumption and partner in demand-response management. Based on demand response policies, end users may explore local generation and actively participate in a smart grid power distribution network. Most customers need a simple way to control energy consumption and exchange usage data at proper level of granularity with power utility companies. However, smart-grid architectures in the literature focus on complete power grid management. They connect to customers premises with network of meters enabled by General Packet Radio Service (GPRS) or in certain cases dedicated programmable logic controller (PLC) technology [2]. They do not consider possibility that customers already have other smart home infrastructures [3]. Some solutions proposed in the literature based on a smart home infrastructure are not scalable [4].

II. METHODOLOGY

The proposed platform consists of three main parts-sensor and actuator networks, IoT server and user interface. Sensor and actuator nodes communicate in bidirectional way with the IoT server [5]. Communication between the nodes and the IoT server follows the TCP/IP client-server model. We developed a platform for remote monitoring and control using IoT as a scalable distributed system that can seamlessly support an in-home smart grid and different concurrent applications. The platform architecture consists of three main components, sensor and actuator networks, the IoT server and the user interfaces for visualization and management. A reliable bidirectional communication is enabled with sensor and actuator nodes leveraging the IoT server. The communication between the nodes and the IoT server follows the TCP/IP client-server model. Sensors communicate via messages in their native format to the IoT server over an encrypted link. The IoT server then converts the raw payload, containing information from heterogeneous nodes, into a standard format, containing identifier, type, measurement unit, data field, geographical position, and timestamp. Thus data can be easily represented, manipulated and aggregated without considering the communication protocol of the originating source. A web-based graphical interface allows users to access real time and historical sensor data including administration privileges to manage networks and single nodes. Access to Third-party software can be provided using a representational state transfer application programming interface (API)[6]. The platform ensures an adequate security level both to end-to-end communications and to data access considering the possibility of using the system to collect sensitive and confidential data. For security reason, users need to be authenticated before they can access the platform and can only access specific sets of sensor data through HTTPS. At a finer level of detail, the IoT platform consists of several hardware and software components, each described by its functions and by its interfaces with other components.

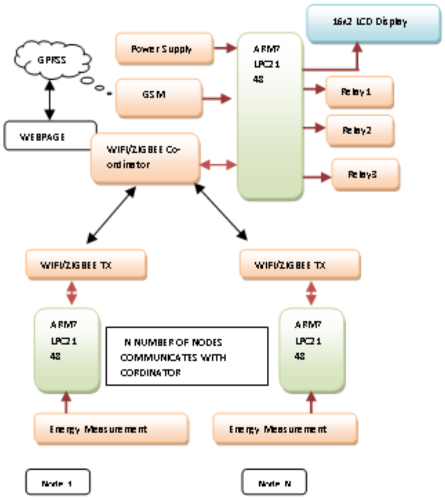


Figure.1. System Block Diagram

In this aspect, the architecture is easily scalable and robust. Each component can be modified, redesigned, and extended with minimum impact on the rest of the system. The components are described in more detail in the consequent subsections.

A. Sensor and Actuator Networks

The sensor and actuator nodes are part of networks implemented with wired or wireless network protocols. For this demonstration we have used ZigBee protocol. The data management translates information to the format required by the sensor database. On the other hand, bidirectional communication channels to/from the nodes enable the IoT server to configure and program them. Configuration messages mainly carry node-specific information such measurement thresholds, alarm settings or firmware updates. We use gateway concept to integrate heterogeneous networks with an external network [7]. The system uses a gateway-based methodology [8], where the gateway converts data into a universal format.

B. IoT Server

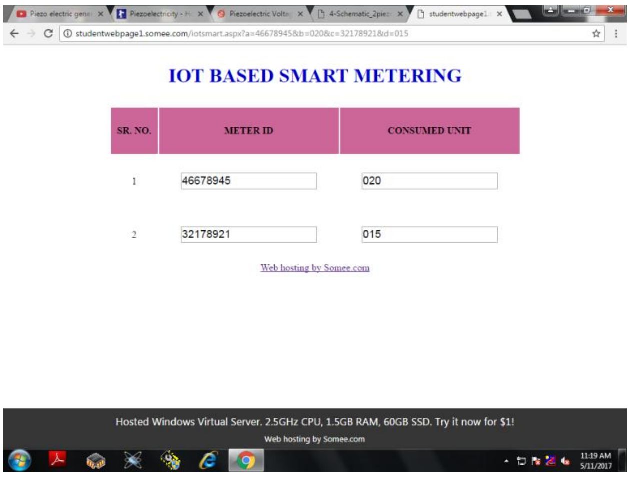
- Message coordinator manages bidirectional communication between each gateway and the rest of the system. It deals with low-level communications from nodes to the data management unit and from the configuration unit to the nodes. It has the main task of getting inputs to new connections from IP nodes that want to join the system. For every connection, it decrypts incoming packets and forwards them to the data management unit, for interpretation and storage.
- Data Management Unit and Database Storage: This unit is a collection of software modules that enable management of messages of a specific sensor network type. These components receive node packets in their native format and extract their payload. If the payload contains measurement data from a sensor or an event notification by an actuator, data are stored in a unique format in a streaming sensor database. If the payload contains specific network messages (configuration, management information, communication channel, node address, etc.), messages are stored in the original format into the configuration database.
- Configuration Unit and Database: This unit configures networks and nodes based on inputs from users, authorized applications and according to the system status stored in the configuration database. It is a collection of software components, each dedicated to a specific type of sensor/actuator network. For any new added sensor network protocol, dedicated modules must be added to the configuration unit.
- Security system: It ensures privacy and data protection. It coordinates all communication between end-users and the IoT server. It provides access to information and configuration only to authorized users or third-party applications, based on a database of users and their permission to each networks, node.

C. User Interface

A web based API provides interface to service providers, users and application developers. It offers two main functionalities based on client profiles: standard users and administrators. Standard users can access sensor data and control actuators. Administrator can also see the configuration and the status of the nodes and dynamically configure them.

The web interface is categorized into visualization Interface that displays current and historical information from sensors and actuators is a series of pages. Users can create custom data views and visualization pages; send commands, set rules and alarm notifications. The other web interface is administration that allows users with the possibility to remotely manage and configure their networks. It is elaborated in detail in following sections,

- Visualization Interface: Current and historical information from sensors and actuators can be accessed via the visualization interface in a series of pages. Additionally, the visualization interface allows authorized users to send commands to actuators. It offers users to customize data views and visualization pages execute commands, set rules and alarm notifications.
- Administration Interface: Remote management and configuration of network can be done using administration interface. Additionally users can set the data visibility of their own sensors and manage third party access and privileges to their nodes. Depending on the type of networks and on the corresponding protocols, the layout and the fields included in the administration interface pages may vary. Remote registration of new gateways and configuration of new network connections can be easily done in administrator interface.



IOT BASED SMART METERING

SR. NO.	METER ID	CONSUMED UNIT
1	46678945	020
2	32178921	015

Web hosting by Somee.com

Hosted Windows Virtual Server. 2.5GHz CPU, 1.5GB RAM, 60GB SSD. Try it now for $1!

Web hosting by Somee.com

Figure.2. Sensor Data Visualization Using Webpage

The network name, IP address of the message dispatcher, the port number on which it accepts connections and the network AES security key is utilised to determine and establish the connection. For this reason, gateway has to be registered and configured. Leveraging the web interface the administrators can add a new network on their admin page, by inserting the gateway address, selecting the type of network and assigning a name, a description and a network location. By generating a network security key ,the server will save it in the user database along with the network information. Once this configuration with security key is complete, the gateway connects to the server sending a request connection. The server processes the request, analyses the new process and lets it communicate directly with the gateway. The network information for this task is acquired from the configuration database and informed to the gateway that it can begin the encrypted communication. The network appears on the configuration page of the user after the communication is setup.

- Web Service API: Web service APIs is the platform to service providers and new client applications. APIs are an easy and unified way to retrieve information collected from heterogeneous sources. Service providers, utilities and third parties use the API to obtain single, multiple or aggregated measurement data, and to provide information to the customers concerning for example, dynamic changes to the tariffs, alarms, weather-related data, that can be used by customer-defined rules set (or accepted) by the users. Considering this, the implementation of demand-response policies can be enabled. The sensor owner can define thirdparty access to protect sensitive information and accessibility of collected data. Only registered endusers and authorized third-party applications can retrieve sensor data from the sensor database through the API.

III. EXPERIMENTAL DEMONSTRATION

We have performed several extensive tests of implementation to verify operation and reliability. We have used several different energy measurement systems units and data of consumption has been wirelessly transmitted and accessed through web page and meter display. In figure 3, a sample kit with live energy data measurement system is shown. Data is wirelessly transferred using ZigBee and also locally displayed on LCD screen. Data transferred from several meters is hosted on a web page and access to webpage can be configured based on specific needs.

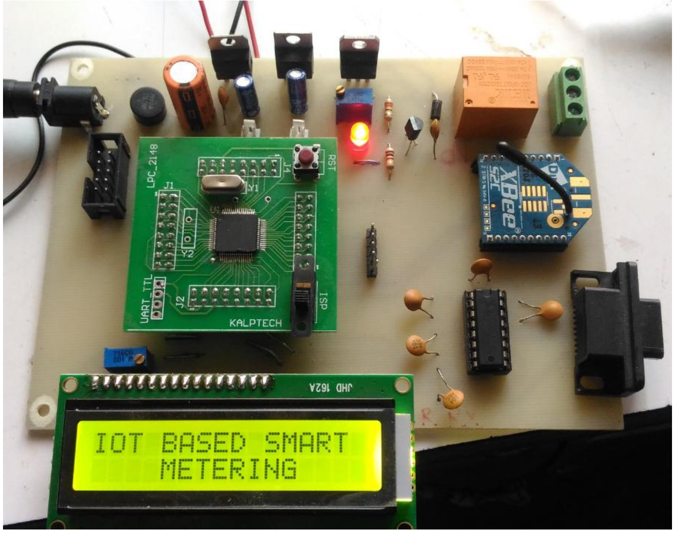


Figure.3. Experimental kit

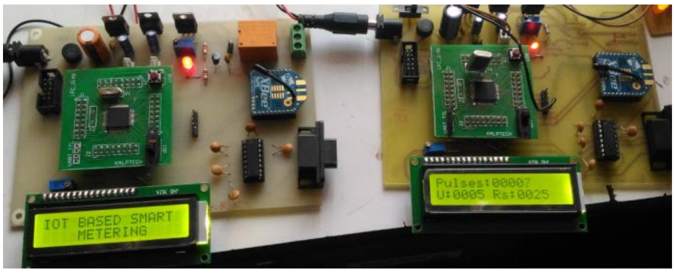


Figure.4. output of meter 1 is being sensed and transmitted. Data is locally displayed on the lcd panel

IV. CONCLUSION

We have presented the introduction, Literature review, Methodology, Project Overview and Layout and design of the set up based on the platform for the IOT that can host broad range of smart home appliances. Considering novelty in this domain, our proposal has unique features and elements as compared to the state of the art: it is customer focused; it reduces deployment of particular smart grid infrastructure, and unfolds possibilities in smart home applications, sensors and networks. This is key for a widespread acceptance of smart grid applications and equipment to be deployed at home.

V. ACKNOWLEDGEMENT

I take it a deemed privilege to express my sincere thanks to JSPM's Bhivarabai Sawant Institute of Technology and Research, Wagholi to complete this research.

VI. REFERENCES

[1]. V. Giordano, F. Gangale, and G. Fulli, "Smart grid projects in Europe: Lessons learned and current developments, 2012 update" Eur. Commission, Joint Res. Centre, Inst. Energy Transp., Sci. Policy Rep., 2013

[2]. Energy Community. (2010). Energy Community Regulatory Board, A Review of Smart Meters Rollout for Electricity in the Energy Community [Online]. Available: http://www.energycommunity.org/pls/portal/docs/744178.PDF

[3]. A. A. Khan and H. T. Mouftah, "Web services for indoor energy management in a smart grid environment," in Proc. 2011 IEEE 22nd Int.Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), pp. 1036–1040.

[4]. Y. Yang, Z. Wei, D. Jia, Y. Cong, and R. Shan, "A cloud architecture based on smart home," in Proc. 2010 2nd Int. Workshop Educ. Technol. Comput. Sci. (ETCS), vol. 2. Wuhan, China, pp. 440–443.

[5]. E. Spanò, S. Di Pascoli, and G. Iannaccone, "An intragrid implementation embedded in an internet of things platform," in Proc. 2013 IEEE 18th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD), Berlin, Germany, pp. 134–138.

[6]. R. T. Fielding, "Architectural styles and the design of network-based software architectures," Ph.D. thesis, Dept. Inf. Comput. Sci., Univ.California, Irvine, Irvine, CA, USA, 2000.

[7]. N. Meratnia et al., "Decentralized enterprise systems: A multiplatform wireless sensor network approach," IEEE Wireless Commun., vol. 14,no. 6, pp. 57–66, Dec. 2007.

[8]. S. Lei et al., "Connecting heterogeneous sensor networks with IP-based wire/wireless networks," in Proc. 2006 4th Softw. Technol. Future Embedded Ubiquitous Syst., 2nd Int. Workshop Collab. Comput., Integr.Assur. (SEUS-WCCIA), pp. 127–132.