Secure Low Cost AMR System Based on GPRS Technology

Alauddin Al-Omary, Wael El-Medany, and Sufyan Al-Irhayim

***Abstract*—This paper presents the design and implementation of a secure low cost automatic meter reading (AMR) system that measures and transmits the total electrical energy consumption to main server using general packet radio service (GPRS) technology provided by GSM networks. The proposed AMR system consists of three main parts: Accurate digital meter, a transmission facility and the billing server. To make affordable AMR system a low cost off-the-shelf materials are used. Successful demonstration of the system prototype has made it possible to be implemented in the kingdom of Bahrain and other Middle East countries on a larger scale for meter reading applications.**

***Index Terms*—AMR, GSM, GPRS, M2M**

I. Introduction

Automatic meter reading, or AMR, is one of the latest machine to machine (M2M) applications that have a huge contribution to the vision of M2M. AMR [1], [2], [3], [4], [5], [6], [7], [8], [9] is the technology of automatically collecting consumption, diagnostic, and status data from metering devices (water, gas, and electric) and transferring that data to a central database for billing, troubleshooting, and analyzing. This remote reading technique has many advantages. It saves utility providers the expense of periodic trips to physical locations for a meter reading. Billing can be based on near real time consumption rather than on estimates based on previous or predicted consumption value. It has also less contact with adverse elements (dogs, inclement weather, etc.). This timely information coupled with appropriate forecast analysis, can help both utility providers and customers to control the use and production of electric energy, gas usage, or water consumption value. AMR systems and devices covered in this paper are primarily used for measurement of electrical energy consumption.

II. Literature Survey

In order to overcome the problems of the traditional meter reading system, efforts are underway around the world to automate meter reading and to provide comprehensive information to the consumer for efficient use of the utilities [1], [2], [7], [8], [9], [10]. Researchers proposed different implementation techniques. In [1] SMS-based Reconfigurable Automatic Meter Reading System is introduced. The work uses the GSM network to send ARM data. In [11] a secure and scalable automated meter reading is introduced. The work uses existing local ISPs instead of requiring its own set of proprietary communication infrastructure. The gateway node basically consists of an embedded microprocessor system, based on embedded Linux, and a modem. In [12] remote real time automatic meter reading system that employs distributed structure based on wireless sensor networks, which consists of measure meters, sensor nodes, data collectors, server and wireless communication network. Similar work is introduced in [13] and [14]. These systems consist of measure meters, sensor nodes, data collector (gateway), management centre (server) and wireless communication networks based on ZigBee communication technology.

Manuscript received June 20, 2011; revised October 14, 2011. This work was supported in part by the Scientific Research Deanship of the University of Bahrain under Grant 43/2008.

Authors are with the College of Information Technology, University of Bahrain (e-mail: ala.alomary@gmail.com).

III. Limitations of Existing AMR Systems

Existing and traditional AMR systems are typically based on centralized point-to-point modem or radio connections which have two essential disadvantages: no scalability and weak security. The central system that collects and processes all meter values needs a pool of modems (or comparable means of communication) for parallel access to as many meters as possible. This approach does not scale very well if hundreds of thousands of meters have to be read every 24 hours, a number that is reasonable when it comes to private customer meter reading. The radio based system, or even Internet-based systems have weak security since the radio system can be intercepted and the normal Internet protocol (i.e http) is not secure unless an alternative secured protocol such as https is used.

The price of AMR system is still at a level where it usually cannot be applied widely to all customers. The price of AMR is mainly determined by the costs of the hardware, the installation and the communication infrastructure and the running cost. The cost issue plays a key factor in replacing traditional metering system with AMR system.

IV. The Proposed Method

During the last few years, a few venture companies explored the potential of introducing AMR in the kingdom of Bahrain. Their effort was driven by the fact that number of households in Bahrain is manageable. However, the cost of replacing all electricity meters and the introduction of an overall management system was too high.

To introduce the concept of AMR in the Kingdom of

Bahrain, a model of low cost wireless AMR using GPRS Technology has been developed. GPRS is quite often used for meters that need to transmit a lot of data or for meters that needs to communicate as a point to point link. In cases were a roll out is scattered over the region PLC cannot be used which results in a solution where the GPRS meter communicates directly with the central access server. Often this is called point to point so it is more secure than broadcast technique. It is also faster and is not sensitive for influences. The desired AMR system has the following requirements:

a. Scalability: It should be able to be used for ten meters as well as for hundreds of thousands of meters without altering the architectural principles.
b. Security: It should be based on state-of-the-art security methods that offer confidentiality and integrity of the measurement data.
c. Low-Cost: The cost of the system implementation should be reasonably low in order to be used for a large number of customers.

V. System Architecture

The proposed AMR system design consists of three main parts: Digital meter, a transmission facility and the billing server as shown in Fig. 1.

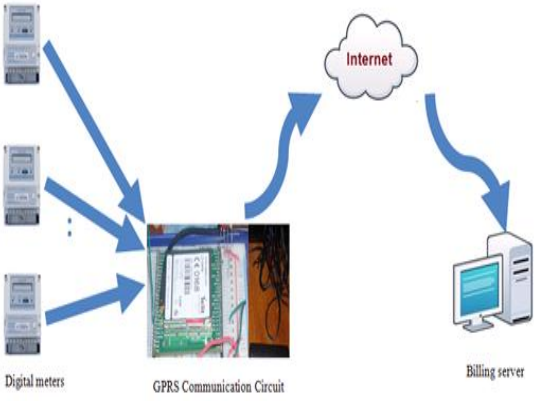

Fig. 1. AMR system architecture

A. The Digital Meter Design

1) Design assumption

Following assumptions are made in the meter design:

i. The meter should satisfy Bahraini power systems requirements. It runs with 230V/50Hz supply.
ii. The designed meter had a single-phase system mainly due to the budget allocation. Nevertheless, the theory of implementing a three-phase is identical to a single-phase wireless automatic meter-reading system.
iii. The meter can handle maximum current of 40 A.

2) Digital meter implementation

The meter is constructed using off the shelf components such as evaluation board (MCP3905A), a Microcontroller (PIC16F84A), and LCD (16*2).

The evaluation board is used to calculate the power by sensing the load that is connected to it. The PIC microcontroller is used to accumulate the consumed energy by saving the readings in the microcontroller memory. The LCD will display the reading in two lines.

3) The MCP390 evaluation board

The MCP3905 evaluation board was used to build Microcontroller-based digital energy meter. The MCP3905EV includes only the MCP3905 IC with jumpers to configure its inputs. The MCP3905A energy meter reference design (using the new MCP3905A/06A device) is a stand-alone low cost energy meter. It can act as either a stand alone energy meter, or as the analog front end design for LCD microcontroller based meters. According to data mentioned in the MCP3905 datasheet, the MCP3905 design is specified with an energy measurement error of 0.1% typical across 1:500 dynamic ranges for high accurate energy meter designs. This reference design is compliant with EMC requirements per energy metering standards IEC62053 and legacy IEC61036, IEC1046 and IEC687.The two prototype areas, input and output, are left to the user to be designed according to the user requirements. Regarding the input prototype area, a current-sensing element, such as shunt resister, has to be installed with the proper AC line and load connection to it. The shunt resistor is used to monitor the current in a circuit and translate the amount of current in that circuit into a voltage that can be easily measured and monitored. The simplified block diagram of the MCP3905 chip is shown in Fig. 2.

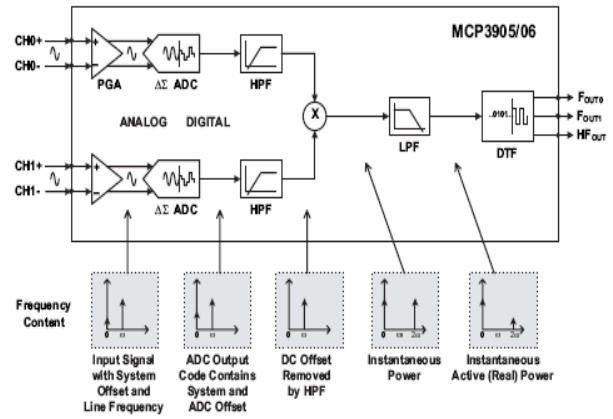

Fig. 2. Simplified MCP395 block diagram with frequency contents

4) The PIC microcontroller

The PIC16F84A microcontroller is used in building the meter. PIC16F84A has 18-pin enhanced flash/EEPROM (8-BIT) and belongs to the mid-range family of the PICmicro® microcontroller devices. The microcontroller is used to store the ID number of the subscriber and also is used to continuously monitor the instantaneous watt-hour (WH) reading and calculate the accumulated KWH and store it in its EPROM. Therefore, a controlling program is needed to perform these tasks.

5) The LCD screen

A 16x2 LCD (2 lines with 16 characters per line) is used to display the meter reading. It contains two registers, data and command. Data register is used to send any type of data to the

LCD. A command register is used to send addresses that initialize the LCD.

B. Transmission Facility

There are many different forms of communication links that can be utilized as the communication medium in an AMR system [4]. GSM network, with its vast coverage in most countries, and also its competitive ever-growing market, is becoming the main medium for the machine-to-machine applications, and AMR is not an exception. In this research the meter ID and its reading (KWH) are sent to a central server using general packet radio service (GPRS) technology. GRPS is the technology used the GSM network to connect mobile to the Internet. The communication is done using GM862 cellular Quad band module and Quad-band wired Cellular Antenna SMA.

1) GM862 cellular quad band module

The GM862-QUAD modules are a product family that are easy-to-integrate GSM/GPRS modules for all industrial M2M applications. The GSM modem has quad band cellular capabilities (850 / 900 / 1800 / 1900MHz frequencies). GSM modules can be controlled via AT commands according to GSM 07.05, 07.07 and Telit Enhanced. It has an on board SIM holder to place the SIM card and also it has GSM antenna.

2) Quad-band wired cellular antenna

A Quad-band antenna for embedded cellular devices is used to allow customer to connect his cellular module to the outside world. Operates on four frequencies and Comes with a 3M adhesive backing for mounting.

C. The Billing Server

The collected power consumption reading is sent to the central billing server where it is stored. Many commercial servers as well as management software are available in the market. However the cost of such server and software management system are very expensive. To decrease the cost of the proposed AMR system, in-house software is developed using ASP.

VI. Implementation and Testing

The AMR system prototype has been successfully implemented and tested in the Department of computer engineering at university of Bahrain. Each system part is developed and tested separately and then the different parts are joined to make the complete system.

A. The Meter Circuit

In order for the meter to sense the current two methods can be used, the current-sensing shunt and the current transformer (CT). The current-sensing shunt is a small piece of metal (typically made of manganese and copper) that is manufactured with a variety of mounting holes and wired connections. It acts as a simple resistor, with the voltage drop across it proportional to the current flowing through it. Parasitic inductances create frequency dependant voltage drops and mismatch in the phase response between channels. Shunt resistances are typically between 100 μΩ and 500 mΩ, with inductances specified between 1 and 5 nH. The advantage of this current sensing method is that the shunt is very low in cost. The disadvantage is that it is ultimately limited by its own self-heating and can typically not be used in meter designs with large maximum current requirements (IMAX >> 100A).

The current transformer is another choice for sensing current when designing an energy meter. The device offers isolation through transfer of current from the primary to the secondary winding. The CT can handle higher currents than the shunt, while consuming less power. The trade-off is cost and, in some situations, accuracy. The CT is also susceptible to saturation through either a large DC component or a large over current situation. When the core saturates, the device becomes very non-linear. Table (1) summarizes some of the trade-offs between the shunt and the CT.

TABLE I: Shunt versus CT

Advantage	Shunt	CT
Low Cost	√	
High Current		√
Lower Power Consumption		√
Less Accuracy Issue	√	

In our system the current sensing method is used since the designed meter current is less than 100 A and since CT is susceptible to saturation. In order to reduce the power consumption a low value (200 μΩ) is used in the meter.

Figure (3) shows the complete meter circuit. As was stated in section five, the MCP3905 evaluation board was used to build a (Microcontroller-based) digital energy meter. The MCP3905EV includes only the MCP3905 IC with jumpers to configure its inputs. The two prototype area, input and output, have to be designed by user with his selection. Regarding the input prototype area, a current-sensing element (shunt resister) has been installed with the proper AC line and load connection to it. The shunt resistor is used to monitor the current in a circuit and translate the amount of current in that circuit into a voltage that can be easily measured and monitored.

A microcontroller (PIC16F84A) was connected in the output to accumulate the power consumption. The microcontroller sends the data to the LCD and to the GPRS communication circuit. The flow chart of the controlling program is shown in Fig. 4.The meter is tested by connecting different loads with known power consumptions to the meter and the reading of the meter was calculated and found to be accurate.

B. Implementation of the GPRS Communication Circuit

The GPRS communication circuit Figure is shown (5). This circuit consist of PIC 16F877a, GM862, LT317 adjustable voltage regulator, LM7085 voltage regulator, max3232, and LT1528 adjustable voltage regulator. The LM7085 was used to provide 5 volt for PIC. A logic converter, max3232, was needed in order to have communication between the microcontroller and the GM862. Since the data inputs on GM862 operate at 2.8-3.6 volt, 3 volt

was chosen to power up max3232.

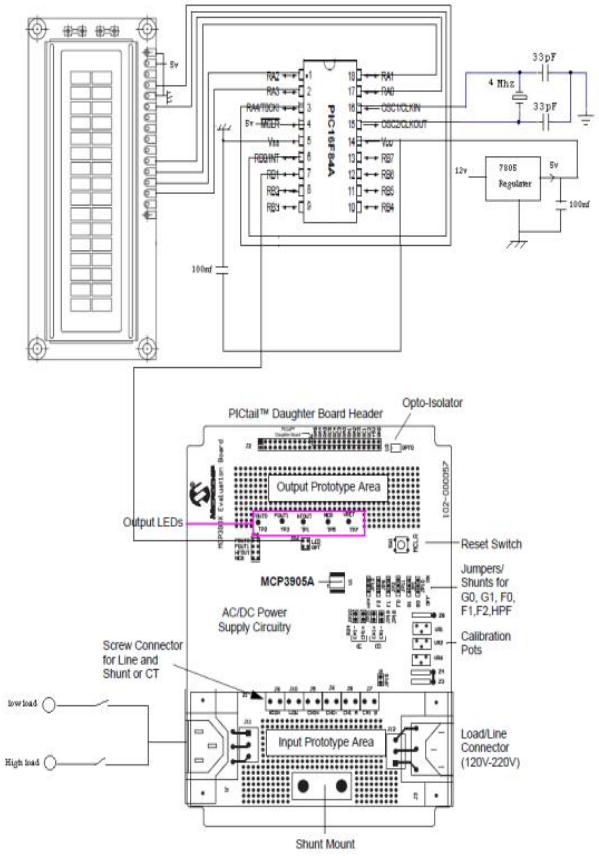

Fig. 3. The meter circuit

The data is sent from the meter PIC (PIC16F84A) to the GPRS circuit PIC (16F877A) according to the timing set in the PIC16F84A program. The GPRS circuit PIC analyzes the data, before sending AT commands to gm862. These commands send a signal to gm862 by triggering the transistor to establish a wireless connection to the billing server database and they provide updated power consumption readings.

The gm862 has a sim card slot and an interface for the antenna that made it easier for us to connect the GSM modem. The GPRS communication circuit is connected to the meter circuit and tested by sending a message to the billing server.

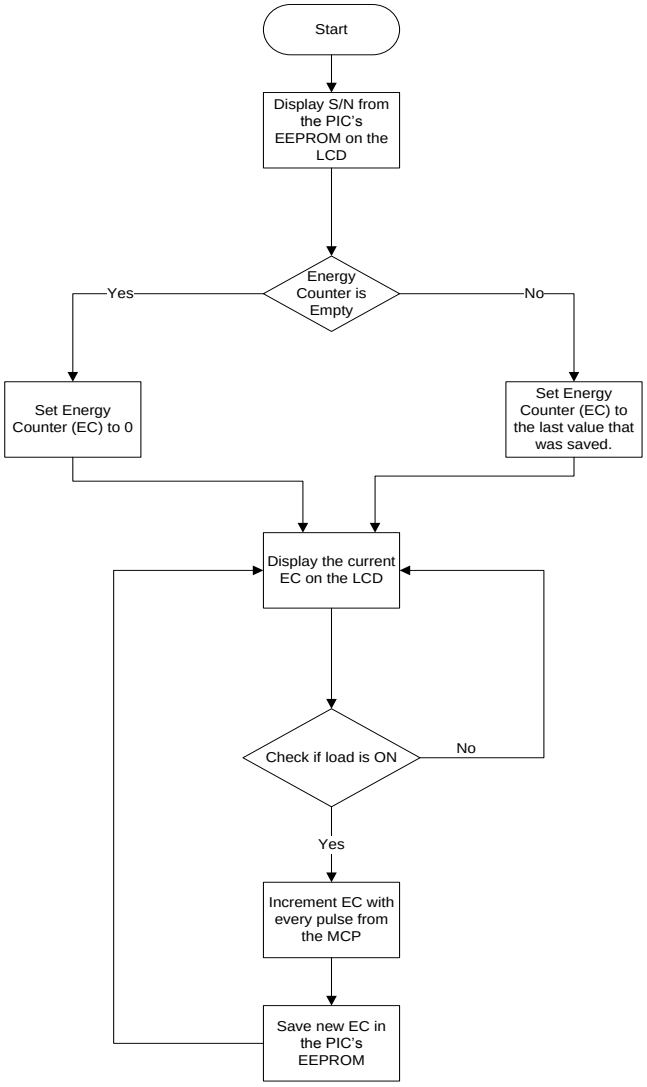

Fig. 4. The Flowchart of the controlling program

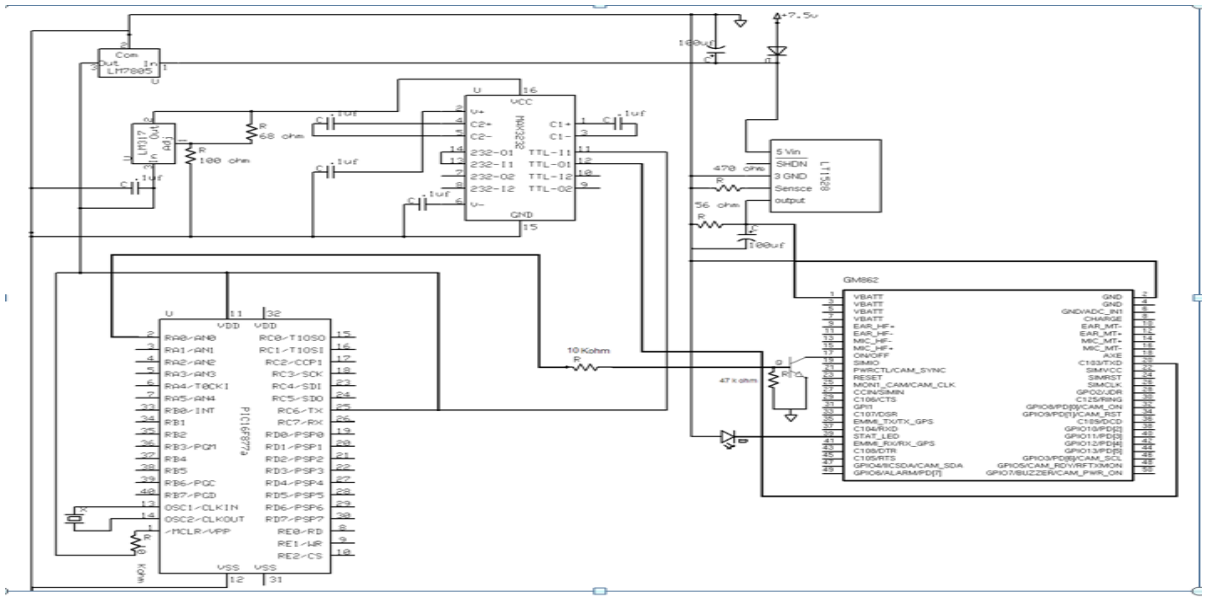

Fig. 5. The GPRS communication circuit

C. Billing Server Implementation

The server have many benefit for both providers and customers [15]. To decrease the cost of the proposed AMR system, in-house software is developed using PHP and SQL server and is used to control the central server. The implemented meter data management system has the following functions:

a) Remote metering: The server automatically receives the meter reading sent to the server from the meter using GPRS, place the reading in the AMR database and customers can remotely get their consumption by logging to the server.

b) Authentication: Customer is asked to enter his subscription ID and password as shown in Fig. 6.

c) Customer Profile: The system shows the customer profile and its property location as shown in Fig. 7.

d) Bill issuing: The billing system provides monthly bill for the customer as shown in Fig. 8.

e) Consumption statistic: The system provides a consumption statistic for any month chosen by customer as shown in Fig. 9.

f) Billing history: The billing history for all paid and unpaid bills can be shown. The user can enter the number of the month in the find field to show the consumption of that month. The billing history screen is shown in Fig. 10.

g) Payment: The user can pay his bill electronically.

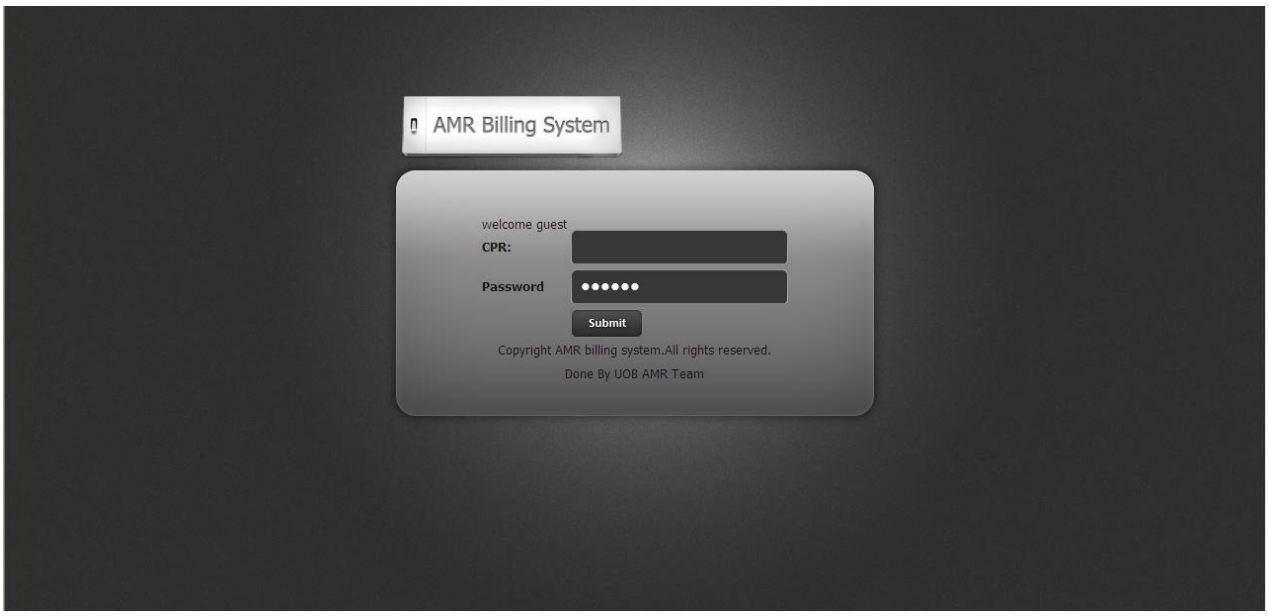

Fig. 6. The server authentication screen

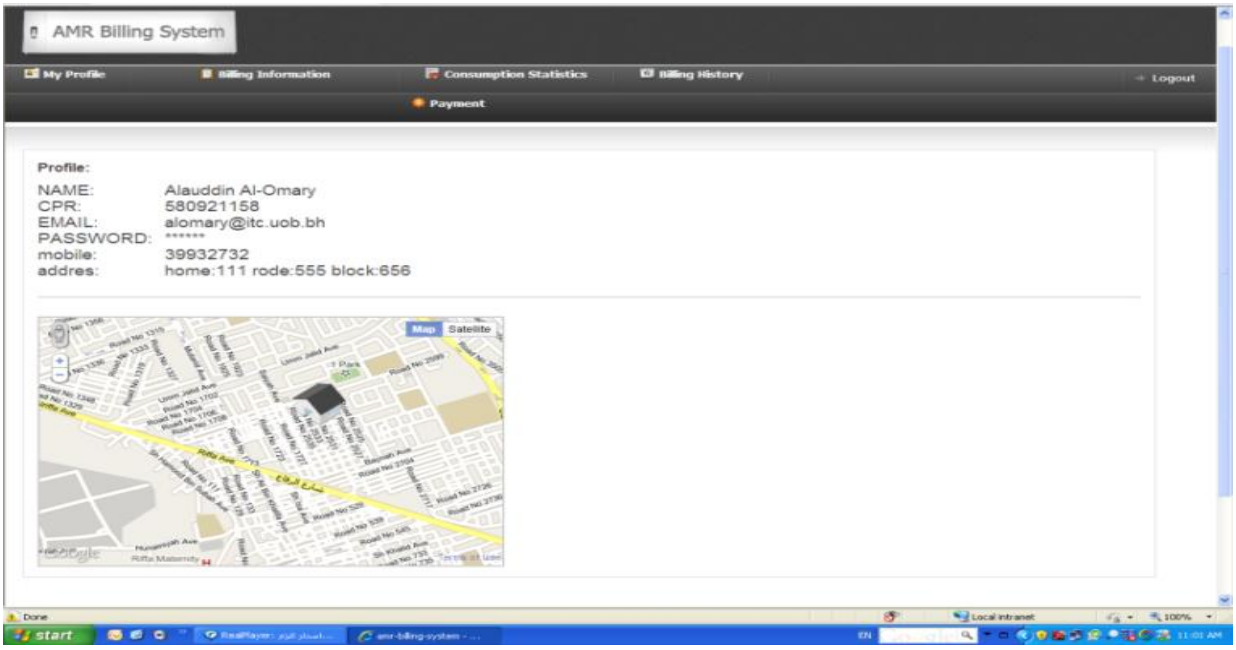

Fig. 7. Customer profile screen

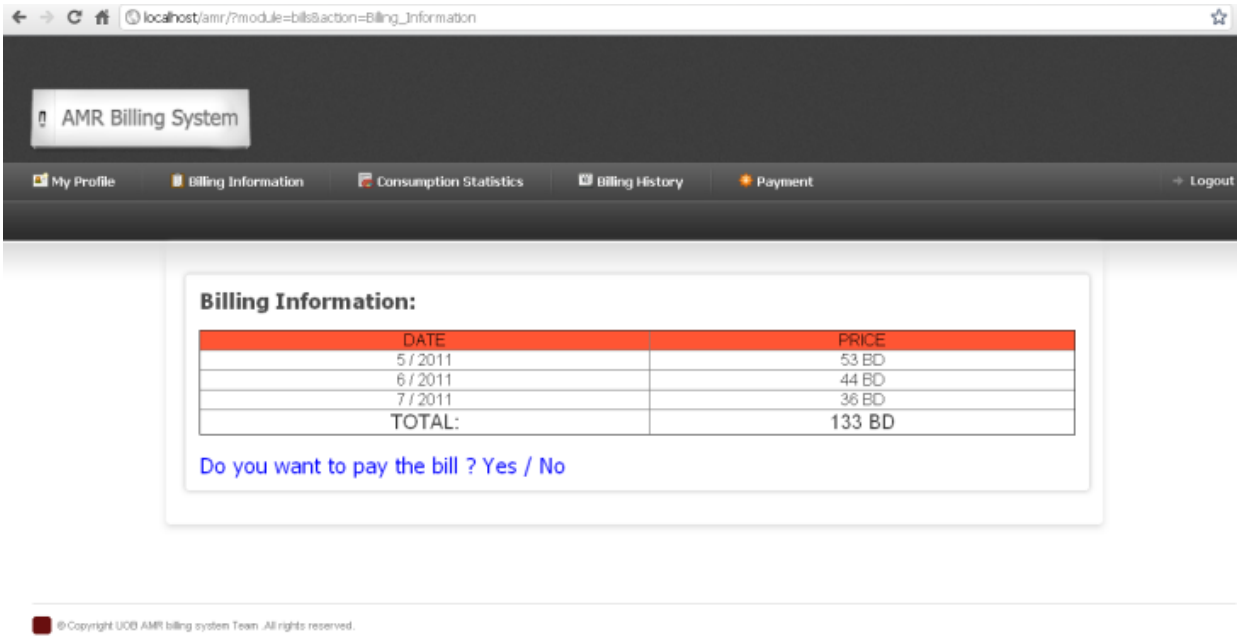

Fig. 8. Issued bill screen

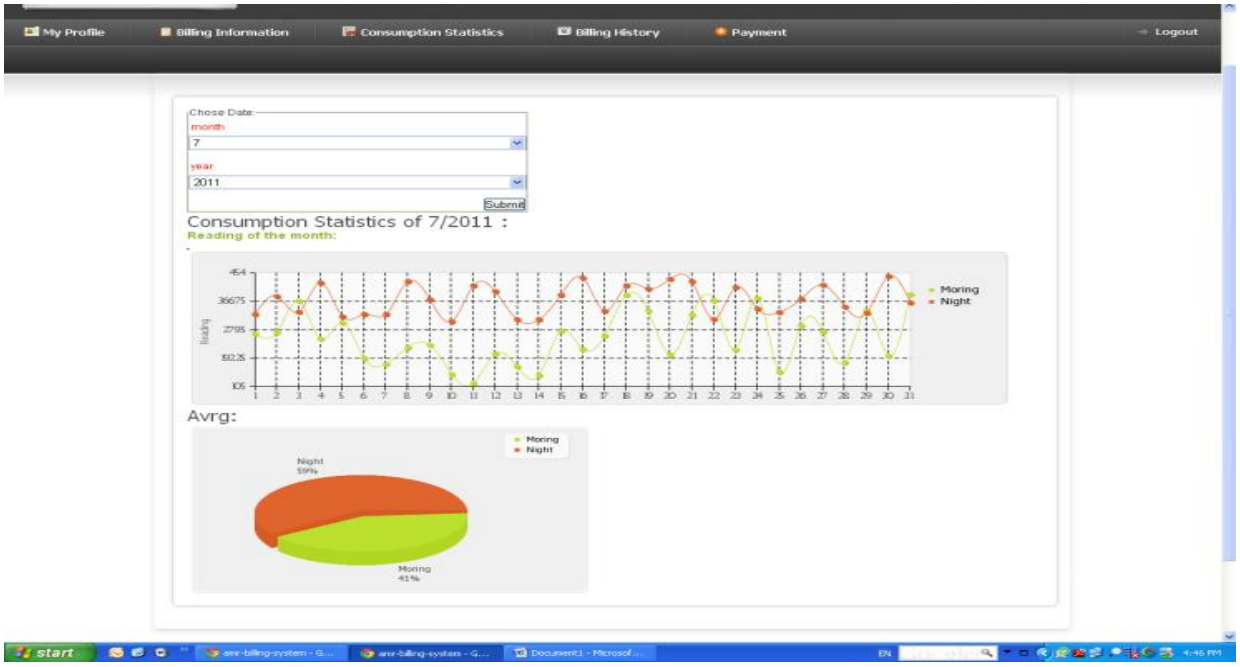

Fig. 9. Consumption statistics screen

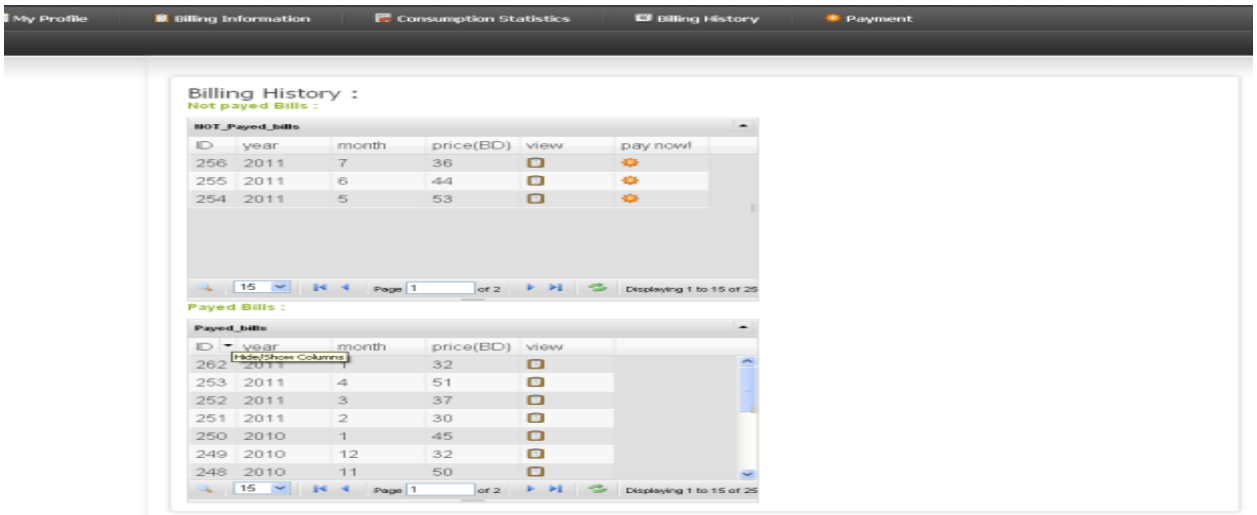

Fig. 10. Billing history screen

VII. System Security

A. GPRS Security

Security is an important part of the data transmission process [16], [11], [17]. GSM has a built in transport layer encryption, which is supported by most network providers. However, this encryption is commonly not used all the way, but only for radio transmission. As soon as the cable-bound GSM backbone is used, data is transmitted unencrypted. GPRS offers a number of security enhancements over existing GSM security. The standards themselves also offer technical features, which a network operator may choose to use.

Aside of that, a different form of security might be desired that in addition to the provided transport layer security. The key issue here is the distribution of keys between clients and data acquisition systems. It shall also be possible that different users such as utility companies and service providers use data originating from one cellular phone. The users shall not be able to read data that are not intended for them. This results in a sophisticated user structure that has to be reflected, for example, by having different keys available to communicate with different users.

The most intuitive way to implement security would be to use the smart card that is present in the mobile phone (the SIM, subscriber identification module). This will be done in any case, however currently the standardization of the Java 2 Micro Edition does not yet support full access to the Smart Card resources. For example it is not possible to conveniently store encryption keys or use the crypto-co-processor of the SIM card. Some mobile phones have two SIM slots where the second one could be used for an ordinary smart card that hosts the security relevant parts of the AMR application. The preferable way of course would be to have one single SIM card that can execute multiple small applications on a mobile information device ("MIDlets") in a sandbox just like java cards can already do ("Cardlets") [11]. Until then, the processor of the mobile phone will host all parts of the AMR application.

Security, however, is not fully achieved by simply securing the data transmission channel with cryptographic methods even if they are done with a secure hardware like Smart Cards. A large part of security relevant aspects are of administrative nature.

B. Billing Server Security

It is clear that the AMR system is n-tier enterprise architecture. Hence, general security requirements and planning applies for this system. Researchers in [18] present similar projects that can be used to design and implement such secure systems. The server in the billing office implements highly secure tools which enabled only authorized staff members of the electricity supply company to work with collected data. These security tools will be used to attain confidentiality, integrity, availability and accountability (logging) of the AMR readings collection process.

VIII. Conclusion

The design and Implementation of secure and low cost wireless AMR using GPRS technology had been presented. The AMR system consists of a meter; a GPRS based transmitter and a billing server. The low cost was achieved using off-the-shelf available components. The system security was achieved using the smart card that store encryption keys or use the crypto-co-processor of the SIM card. A billing server with meter data management system implemented using ASP.net technology. The implemented system is developed based on the Bahraini power systems requirements. A prototype of the system was developed and tested and proved to be reliable and secure. Successful demonstration of the system prototype has made it possible to be implemented in Bahrain on a larger scale for meter reading applications. The developed AMR system generate considerable interest by the ministry of electricity, and water (MEW) for possible implementation in Bahrain where home privacy is important by the local people and entry of the meter-readers (mostly men) into their homes for recording utilities' consumption during day time, when men of the family are at work and only the women are at home, is not always welcomed. According to CTIA [19], the available scientific evidence does not show that any health problems are associated with using wireless devices. Therefore, use of wireless automatic meter reading is not expected to yield any negative health effects on the consumers [19].

The overall cost of AMR system (cost of the Meter and the GM862 CELLULAR QUAD BAND MODULE and not including the server cost) has been calculated to be about US $250, which was within our budget range of US$500.

Acknowledgement

The authors like to thank the Deanship of scientific Research, University of Bahrain who supported this research under grant no. 43/2008. Many thanks to Maryam Al-Mutaw'a, A.Fattah matter and Mohammad Deeb for their help in implementing different parts of the AMR system.

References

[1] A. Abdollahi, M. Dehghani, and N. Zamanzadeh , "SMS-based reconfigurable automatic meter reading system," *IEEE International Conference on Control Applications* (CCA 2007), Oct, 2007, pp. 1103 – 1107.

[2] C. Brasek, "Urban utilities warm up to the idea of wireless meter reading," *The IEE Computing and Control Engineering*, Vol. 15, No. 6, pp. 10-14, December/January 2004/05.

[3] C. Jägerlind, "Improvements for the automatic meter reading process in electricity distribution companies," Master Thesis, Dep. *Industrial Info and Control Systems, Royal Institute of Technology, Stockholm*, Sweden 2006.

[4] C. Nunn, P. Moore, & P. Williams "Remote meter reading and control using high- performance plc communication over the low voltage and medium voltage distribution networks," in 7th *International Conference on Metering Apparatus and Tariffs for Electricity Supply*, 1992, pp. 304-308.

[5] J. Tsoi, "Device management of largescale amr systems," MSc thesis, *Dep. of Industrial Information and Control Systems, Royal Institute of Technology in Stockholm* (KTH), Stockholm, Sweden 2006.

[6] L. Cao, J. Tian, and Y. Liu , "Remote wireless automatic meter reading system based on wireless mesh networks and embedded technology," *Fifth IEEE International Symposium on Embedded Computing*, 2008. SEC '08, Oct, 2008, pp. 192 – 197.

[7] M. Baker, "Added value services through the use of amr in commercial and industrial accounts", *Conference on Metering and Tariffs for Energy Supply*, 25-28 May 1999, pp. 210-212.
[8] M. Venables, "Smart meters make smart consumers," *IET Engineering and Technology*, Vol. 2, No. 4, p.23, April 2007.
[9] Wikipedia Page (22/9/2010) [Online] available: http://en.wikipedia.org/wiki/Automatic_meter_reading
[10] T. Whittaker, "Final word," *IET Control and Automation*, Vol. 18, No. 3, p. 48, June/July 2007.
[11] P. Palensky and Ge. Pratl, "Secure and scalable automated meter reading," *Domestic Use of Energy Conference* 2003, pp. 233-236.
[12] L. Cao, J. Tian, and Y. Liu "Remote real time automatic meter reading system based on wireless sensor networks," 3rd International Conference on Innovative Computing Information and Control, 2008 (ICICIC '08), Dalian, Liaoning, August 2008, pp. 591 – 591.
[13] G. Álvarez, H. Cepeda, I. Laniella, N. Ben fez, and C. Amuch ástegui, "Embedded system for a wireless automatic meter reading management," *IADIS International Conference of Applied Computing* 2007, 2007, pp. 777-780.
[14] T. Jamil, "Design and implementation of a wireless automatic meter reading system," *Proceedings of the World Congress on Engineering*, Vol. I, WCE 2008, July 2 - 4, 2008, London, U.K.
[15] R. Ghajar* and J. Khalife, "Cost/benefit analysis of an AMR system to reduce electricity theft and maximize revenues for E´ lectricite´ du Liban," *Applied Energy Magazine*, Vol. (76), pp. 25–37, 2003.
[16] R. Tahboub, D. Lazarescu, and V. Lazarescu , "Modeling and simulation of secure automatic energy meter reading and management systems using mobile agents," *International Journal of Computer Science and Network Security (IJCSNS)*, VOL.7 No.1, January 2007.
[17] T. Sauter and P. Palensky: "Security considerations for fan-internet connections;" 3nd *IEEE Workshop on Factory Communication Systems, Barcelona*, pp. 309-315, 2000.
[18] R. Tahboub and M. Alsaheb, "Security in database web access", *Sixth Scientific Conference on IT*, Baghdad, Iraq, November 2000.
[19] CTIA page (22/8/2010) [Online]. Available: http://www.ctia.org/consumer_info/safety/index.cfm/AID/10371

Alauddin Al-Omary Holds PhD degree in system and information engineering from Toyohashi University, Japan, 1994. Since 2005, he is an associate professor at the Department of Computer Engineering, College of Information Technology, University of Bahrain. His research interests include Hardware/Software co-design. Machine-to-Machine Communication, ASIC and embedded system design using VHDL and FPGA. Since 2008, Dr. Al-Omary is a technical committee member of The International Arab Journal of Information Technology (IAJIT), the official journal of the Colleges of Computing and Information Society (CCIS), stemming from the Association of Arab Universities. He is also a reviewer in many international conferences and acts as chairperson in many conferences. He has been actively involved in many research projects and published two books and more than 28 papers. He was a member of the Institute of Electrical and Electronic Engineers (IEEE) and the Japanese Information Processing Society

Wael Mohamed El-Medany from University Of Bahrain, College of IT. He holds a PhD degree from Manchester University, UK, July 1999, with a major in Electrical Engineering and a minor in Chip Design and its application in error control coding. He got his MSc degree in computer communications from Faculty of Electronic Engineering, Menoufia University, October 1991, and his BSc degree in Electronic Eng from the same University May 1987. He has been Awarded the prize of excellence in Designing and Developing E-courses at the Universities of Gulf Cooperation Council, 2010, and he nominated and his biography was included in the 27th Edition of Who's Who in the World, 2010. El-Medany is also IEEE and IEEE Communications Society member, as well as a member of IASTED Technical Committee on Telecommunications, Canada, 2009-2012. He is also a reviewer in many international conferences and journals, and acts as chairperson in many conferences. El-Medany has over thirty publications, and he attended several national and international conferences, and workshops. His research interest in programmable ASIC design using VHDL, and embedded systems.

Sufyan Al Irhayim, holds a Ph.D. degree in electrical and electronics engineering, University of Bradford, UK, 1985. He is an Associate Professor at the department of Computer Engineering, University of Bahrain, and has co-authored many research papers. During the past couple of years, he worked as the Director of Standards and Metrology at the GCC Standards Organization. His main area of interest is in Computer Engineering (Networking and Security).