ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# SECURED AND RELIABLE ENCRYPTION FOR DATA COMMUNICATION AND SMART GRID USING WIRELESS MODULE

**D. Umamaheswara reddy*, Dr. Ch. Bala Swamy**

* M-tech Student, Dept Of ECE, QIS college of Engineering & Technology, Ongole.
Head of the Department of ECE, QIS college of Engineering & Technology, Ongole, Andhra Pradesh, India. -523272

**DOI**: 10.5281/zenodo.233403

## ABSTRACT

The main aim of smart grid was to maintain a secured and reliable electricity infrastructure to transfer data from smart meters to destinations. Now a day's data security plays a major role in communication i.e; data must be secured from the destructive forces and unauthorised users. The basic idea of this paper is to transfer data which is generated from smart meters or any other source securely from transmitting station to receiving station according to a standard algorithm with the help of zigbee modules and a specific controller. The information which is generated with the help of PS2 keyboard or from the smart meter is encrypted and sends to the destination. At the receiver end a junk message or garbage value is displayed and in order to view the original message the authorised user should press the encryption key which is present in the receiver section.

**KEYWORDS:** zigbee, encryption, smartmeter, PS2 keyboard, LPC2148 processor

## INTRODUCTION

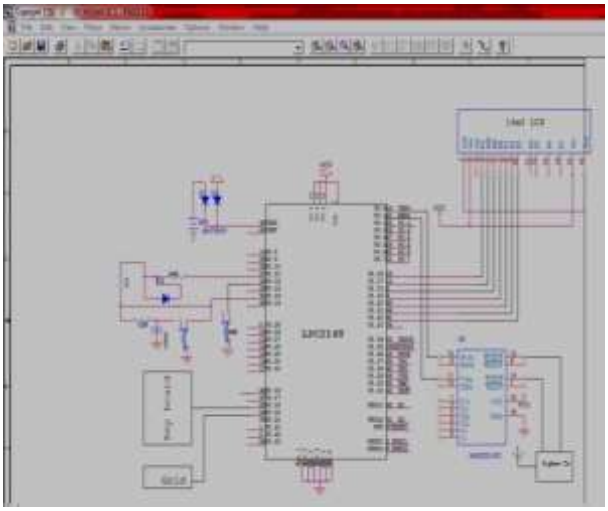
In the wake of globalization, the modern man is at cross roads pertaining to safety, security and privacy. Computer –enabled robbery, computer enabled invasion of privacy is undoubtedly a menace to his vision. To avoid this safety measure is largely essential. For any sector safety and security is the primary thing and becomes complicated so encryption has to be done for protecting the data and it is one of the popular methods. The original message can be retrieved by decrypting the data. The data is converted into an unreadable form and transmitted. The original message can be retrieved at the receiving end by performing the reverse process of encryption so the protection of data can be done by the standard formats encryption and 124decryption. This project is made more flexible by the use of wireless communication i.e. the project is free from cabling and complex hardware connections.

Coming to smart grid, it was a network of power infrastructure and wireless module which is used to manage and analyse the energy usage by continuous monitoring. Here the collector devices receive the information in an energy producer area. The operational centre of the producers manages the usage information. The wireless communication module shares the usage information or readings. Based on the readings taken by smart meter the billing is performed automatically.

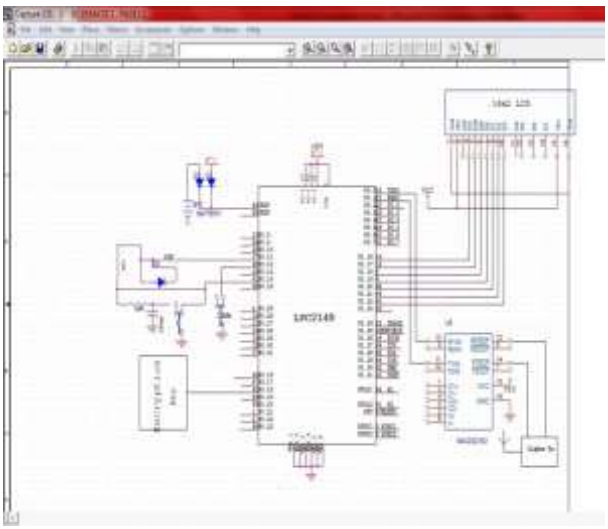
The technique proposed is built around controller, smart meter in the transmitting section and the receiving section .The functionality of the display and wireless control is provided by the controller and for given text it creates different display effects. There is a provision for connecting PS2 alphanumerical keyboard which can be used for typing the data and transmitting. This typed text can be transmitted to multipoint receivers. The keyboard can be disconnected by the user after entering the text .The addition or deletion or alteration of text. Here we can also have the knowledge on units of power consumed by the loads connected in the network. Suppose if two loads such as fan and light are connected and for example if they consumed five units then that information is displayed in the receiver LCD. So along with data security, we can also have the knowledge on no of units consumed by the loads in the network.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

## RELATED WORK



***Transmitter section***



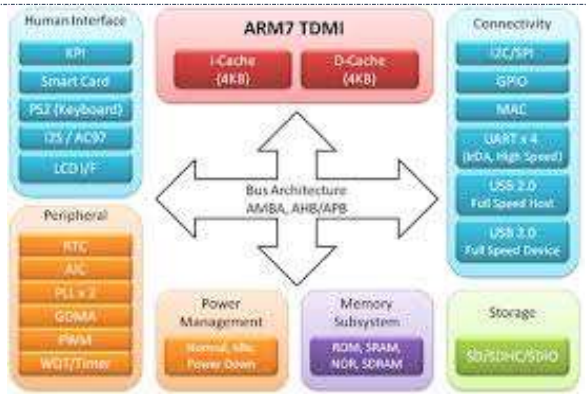
***Receiver section***

The project is built on LPC2148 processor based on a 16/32 bit ARM7TDMI-S™ CPU with real-time emulation and embedded trace support. The main features of LPC2148 processor are as follows:

[1] 64-pin ARM Microcontroller
[2] Flash Memory: 512 Kbytes
[3] SRAM Memory: 32 Kbytes
[4] I/O Pins: 45
[5] Timers: Two each 32-bit
[6] A/D Converter: 10-bit with Fourteen Channels
[7] DAC: 10-bit
[8] Real-Time Clock (RTC): Independent Power and Dedicated 32 kHz Input
[9] I²C: Two Modules with Master or Slave Operation
[10] SPI: Full Duplex Serial Operation
[11] UART: Two Modules
[12] USB: 2.0B Fully Compliant Controller with RAM
[13] External Oscillator: up to 25MHz with integrated PLL for 60MHz Operation

With serial communication interfaces they are well suited for gateways, embedded modems, protocol converters and many other applications.

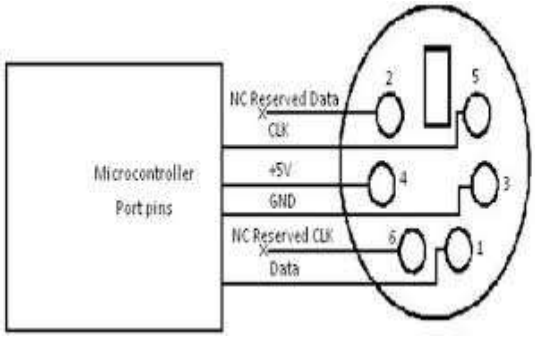
ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7




***ARM7 architecture***

**Power supply:** coming to power supply the project works on 3.3v, 500mA regulated power supply and 12v DC for relay. The 7805 voltage regulator is used for regulation. The bridge rectifier is used to rectify the AC output of step-down transformer (230/12v).

**Ps/2 port:**




The PS/2 port is a 6-pin connector which is used for keyboard interfacing. The text to be transmitted is entered through this port.

**Zigbee:**

ZigBee module can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. ZigBeeis used in low data rate applications that require long battery life and secure networking. ZigBee has a defined rate of 250 Kbit/s, best suited for intermittent data transmissions from a sensor or input device.

**Working procedure:**The data to be sent is given using keyboard and transmitted using zigbee module to remote location. In the same way the no of units consumed by the load is also transmitted to the receiver. At the remote location the garbage value is received. In order to view the original data the authorized person should press the encryption key present in the receiver section.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

**RESULTS**

***Transmitter section***

***Receiver section***


***Transmitting no of units 008.5***

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

***Garbage value received at receiver end***

***Original value retrieved when encryption Key is pressed***

***Transmitted data "smart grid" with ps2 keyboard***

***Garbage value received at receiving end***

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7


***Original text retrieved when encryption key is pressed.***

## CONCLUSION

In this project, secret-based wireless communication for smart grid environment is implemented and it works digitally with electric grid. Along with this there is provision to send user entered text to the destination .so this technology is used in two ways one for smart grid technology and also for user text communication, securely protecting from destructive forces.

## REFERENCES

[1] "The smart grid: An introduction" in DOE's Office of Electricity De- livery and Energy Reliability 2008.
[2] TingLiu, YangLiu,YashanMao, YaoSun, Xiaohong Guan, Weibo Gong and ShengXiao "A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication" IEEE-2013, IEEE Transactions on Smart Grid.
[3] JunbeomHur, "Attribute Based Secure Data Sharing with Hidden Policies in Smart Grid", IEEE Transaction on Parallel and Distributed Systems, Vol.24, No.11, pp. 2171-2180, November 2013.
[4] VinodNamboodiri, VisvakumarAravinthan, Surya Narayan Mohapatra and Ward Jewel, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids", IEEE Systems Journal, Vol. 8, No.2, pp. 509-520, June 2014.
[5] Anthony R. Metke and Randy L. Ekl "Security Technology for Smart Grid Networks", IEEE Transactions on Smart Grid, IEEE- June 2010.
[6] Depeng Li, ZeyarAung, SrinivasSampalli, John Williams and Abel Sanchez, "Privacy Preservation for Smart Grid Multicast via Hybrid Group Key Scheme", 2011.
[7] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid", IEEE Security Privacy, vol. 7, pp.75 -77, 2009
[8] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A lightweight message authentication scheme for smart grid commu-nications" IEEE Trans. Smart Grid, vol. 2, pp. 675–685, 2011.
[9] S. Nguyen and C. Rong, "ZigBee security using identity-based cryp-tography autonomic and trusted computing" in Proc. 4th Int. Conf. Autonomic Trusted Comput (ATC'07), vol. 4610, Lecture Notes in Computer Science, pp. 3–12, 2007.
[10] H. Li, S. Gong, L. Lai, Z. Han, R. Q. Qiu, and D. Yang, "Efficient andsecure wireless communications for advanced metering infrastructurein smart grids" IEEE Trans. Smart Grid, vol. 3, pp. 1540–1551, 2012.
[11] Husheng Li, Member, IEEE, Shuping Gong, Lifeng Lai, Member IEEE, ZhuHan, Senior Member, IEEE, Robert C. Qiu, Senior Member, IEEE, and Depeng Yang "Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids" IEEE Transactions On Smart Grid, Vol. 3, No. 3, September 2012.
[12] P.McDaniel and S.McLaughlin, "Security and privacy challenges in the smart grid" IEEE Security Privacy, vol. 7, pp. 75–77, 2009.